



mrs 5.1
message.routing.system

Server Administration



cycos

The range of functions described in this documentation were accurate at the time of this manual's printing. The manufacturer reserves the right to make technical and functional changes as well as extensions and reductions without prior notification. No liability is assumed for any discrepancies contained within this manual.

Protocols pertaining to devices connected to the system are based on norms or extensions as required by marketing demands. Individual manufacturer protocols have been tested, but no liability is assumed for error free performance in the various possible system configurations. Furthermore, manufacturers protocols are subject to change without notice. Likewise, possible subsequent licensing conflicts could occur in regards to support of these protocols. For this reason, even if depicted in this documentation, manufacturer specific protocols can only be offered after agreement with the individual customer.

The information contained within this documentation is continuously being further developed and improved, and is subject to change without prior notice. No part of this documentation may be reproduced in any form, by any means without the prior written permission of CYCOS AG, Alsdorf, Germany.

mrs, CY-FAX, CY-CALL and CY-COS are registered trademarks of Cycos AG.

All other company names, brand names and product names are the property and/or trademarks of their respective companies.

Access-Security:

A Cycos software product or system, e.g. Cycos.Office or mrs, also products under different names, can be supplied with remote access maintenance software or accesses to enable remote maintenance. This can be done by modem-lines, internet or phonecalls. Remote maintenance software are such as PC-Anywhere or NetOp or other. The customer or operator is responsible for the access security and must ensure that access is only granted to authorized persons or organizations. Cycos AG cannot be held liable for damages or loss of warranty claims against Cycos AG or their daughter companies resulting from misuse. The customer or operator is liable for any security breaches.

Copyright © 1992-2003 CYCOS AG

Joseph-von-Fraunhofer-Str. 7, D-52477 Alsdorf

Tel.: +49 2404 901 0

Fax: +49 2404 901 100

Table of Contents

1 Introduction	11
2 Concepts	13
2.1 MRS Structure	13
2.1.1 Message Transfer Agent	13
2.1.2 Database	13
2.1.3 Extended Message Reporter Service	14
2.1.4 Name Locator	14
2.2 MRS Addressing	14
3 Administrative Procedures	17
3.1 Starting and Stopping the Server	17
3.2 Installation and Start of Individual Components	18
3.3 Stop and Deinstallation of Individual Components	19
3.4 Complete Deinstallation of the MRS Servers by Hand	19
3.5 Event Viewer	21
3.6 User Data Administration	22
3.6.1 Field Significance	23
3.6.2 Privileges	35
3.6.2.1 Customer Specific Privileges	42
3.7 MRS Service Provider (MSP)	43
3.7.1 Configuration	43
3.8 Client Login via the Windows User Account	48
3.9 Client Updates	49
3.9.1 Installing a new Version on the MRS Server	49
3.10 Backup	50
3.10.1 Backup Values Data	51
3.10.2 Implementation Suggestion	52
4 Services on the MRS Server	57
4.1 Telematic Gateways	57
4.1.1 Analog Connections	57
4.1.1.1 Fax G3 and Fax G3 Polling	57
4.1.1.2 SMI Transport (Remote System Links)	58
4.1.1.3 GSM Script (CIT, SMS)	60
4.1.2 Integrated Services Digital Network (ISDN)	61
4.1.2.1 Fax G3, Fax G3 Polling	61
4.1.2.2 Fax G4	63

Server Administration

Table of Contents

4.1.2.3 Euro File Transfer	64
4.1.2.4 ISDN SMI Transport (Remote System Links)	66
4.1.2.5 ISDN Voice (Playback)	66
4.1.2.6 Short Message Service (SMS)	66
4.1.2.7 Fax-on-Demand Server	66
4.1.2.8 Standard Voice/Fax Mailbox	72
4.1.2.9 CIT over ISDN Voice	72
4.1.2.10 The Pager Protocol	73
4.2 Email Gateways	77
4.2.1 Microsoft Exchange	78
4.2.2 Lotus Notes	78
4.2.3 Internet Mail	78
4.2.3.1 POP3 and IMAP4 Servers	78
4.2.3.2 POP3 Mail Import	80
4.2.4 SAP R/3 Gateways	80
4.2.4.1 SAP R/2, R/3 File Interface Protocol	81
4.2.4.2 SAP R/3 APL	81
4.2.5 Novell Groupwise	82
4.2.5.1 Addressing	83
4.3 MSPTSP	83
4.3.1 Setup	84
4.3.2 Configuration	84
4.3.2.1 Error Logging	90
4.3.3 Update	91
4.3.4 Deinstallation	91
4.3.5 MSPTSP via Microsoft Outlook	91
4.3.5.1 MSPTSP Configuration in Microsoft Outlook	92
4.4 Lightweight Directory Access Protocol (LDAP)	92
4.5 Mailing Lists	93
4.6 Broadcasts	93
4.7 The NIL Protocol	95
4.8 HP Digital Sender	96
4.8.1 Hardware Installation	96
4.8.2 HP Digital Sender Software Installation	96
4.8.3 Configuring a User Pool	97
4.8.4 Installing the HP Digital Sender Protocol	97
4.8.4.1 Host to File Interface (FIAPL)	97
4.8.4.2 File Interface (FiAPL) to Host	98
4.8.5 MRS User Configuration	98
4.8.6 Reports	98
4.9 WAP Services	98

4.9.1 Wireless Application Protocol (WAP)	98
4.9.2 WAP Architecture	99
4.9.2.1 WAP Server	99
4.9.2.2 WAP Gateway	99
4.9.2.3 WAP Client	100
5 MRS Monitor	105
5.1 Security	105
5.2 Operation	105
5.3 Creating a new Monitor Layout	106
5.3.1 Configuring a Logging Monitor	107
5.3.2 Configuring Line Monitors	108
5.3.3 Saving Monitor Layouts	108
5.4 Standard Monitor Options	109
5.4.1 Modules	109
5.4.2 Line Monitor	110
5.4.3 Logging Monitor	110
5.4.4 Main Log file	111
5.4.5 Active Alert	111
5.5 Monitor Usage Examples	111
5.5.1 Line Monitor	111
5.5.2 Special Analysis Session	112
5.6 Local Installation	112
6 MRS Modules Configuration	115
6.1 Integrated Services Digital Network (ISDNAPL)	115
6.1.1 Protocols	115
6.1.1.1 Euro-File Transfer Server	116
6.1.1.2 Euro File Transfer Client	118
6.1.1.3 Fax Group 3	118
6.1.1.4 Fax Group 3 Polling	121
6.1.1.5 Fax-Fax-Converter (Transparent/Server)	121
6.1.1.6 Fax Group 4	121
6.1.1.7 MRS SMI-Protocol	122
6.1.1.8 SMS (TAP or UCP Protocol)	122
6.1.1.9 Scripts	124
6.1.1.10 Voice Play-back via Telephone	135
6.1.2 Extensions	136
6.1.3 Voice mail	137
6.1.3.1 General Settings	138
6.1.3.2 Messaging Settings	139

Server Administration

Table of Contents

6.1.3.3 Recording Settings	140
6.1.3.4 Security Settings	141
6.1.3.5 Call Transfer Settings	142
6.1.4 Telematic Protocols	143
6.1.5 Originator Addresses	144
6.1.6 Extensions	146
6.1.7 Devices	147
6.1.8 Trunk Groups	149
6.1.9 Bindings	150
6.1.10 Resources	151
6.1.11 Charges	152
6.1.12 Restart	153
6.1.13 General Voice Mail Settings	154
6.2 Ergo Configuration	154
6.2.1 Generals	154
6.2.2 Settings	155
6.2.3 Ergo Configuration Tabs	155
6.2.3.1 General	155
6.2.3.2 Options	156
6.2.3.3 Menu	157
6.2.3.4 System	158
6.2.3.5 Special	159
6.2.3.6 Customer	161
6.2.3.7 Test	163
6.3 Dialogic (DlgAPL)	164
6.3.1 Telematic Protocols	164
6.3.1.1 Hicom Message Waiting Indicator	165
6.3.2 Extensions	166
6.3.3 General Voice Mail Settings	167
6.3.4 Telematic Protocols	167
6.3.5 Originator Addresses	168
6.3.6 Extensions	169
6.3.7 Devices	170
6.3.8 Line Bundles	173
6.3.9 Bindings	175
6.3.10 Resources	175
6.3.11 Charges	176
6.3.12 Restart	177
6.3.13 General Voice Mail Settings	178
6.4 Message Transfer Agent (MTA)	178
6.4.1 Automatic Maintenance	179

6.4.2 Remote System Links	184
6.4.3 Routing Rules	187
6.4.4 Advanced	189
6.4.5 Global Journal	193
6.4.6 Logical Lines	195
6.4.7 Text-to-Speech	196
6.4.8 Fax Conversions	197
6.4.9 Licences	198
6.5 Mail APL	199
6.5.1 Printer Embedded Codes	199
6.5.2 True Unified Messaging	201
6.5.3 Vanity Numbers	202
6.6 Microsoft Exchange Gateway (ExchAPL)	204
6.7 SMI Transporter	204
6.7.1 Named Pipes (PipeAPL)	204
6.7.2 SPX (SPXAPL)	205
6.7.3 TCP/IP (TCPAPL)	205
6.7.3.1 Firewall	206
6.7.3.2 Name Resolver	208
6.7.4 Remote System Links	208
6.8 Internet Email, POP3/IMAP4 Server and POP3 Mail Import (SMTPAPL)	209
6.8.1 SMTP (Simple Mail Transfer Protocol) Server	209
6.8.2 Outgoing Emails	213
6.8.3 POP3 Server	214
6.8.4 IMAP4 Server	215
6.8.5 Secure Sockets	216
6.8.6 Formats	219
6.8.7 POP3 Mail-Import	220
6.8.7.1 New Database Fields	220
6.8.7.2 Active Schedules	221
6.9 Web Server (WEBAPL)	223
6.9.1 HTTP	224
6.9.2 CGI	225
6.9.2.1 WAP Protocol	226
6.9.3 HTML	228
6.9.4 SSL	230
6.9.5 Web Client	233
6.9.6 Firewall	234
6.10 Modem (V24APL)	234
6.10.1 Identification	235
6.10.2 Telematic Protocols	236

Server Administration

Table of Contents

6.10.3 Devices	237
6.10.4 Bindings	238
6.11 GammaFax (GammaAPL)	238
6.11.1 Telematic Protocols	239
6.11.1.1 Fax Group 3	240
6.11.1.2 Fax Group 3 Polling	241
6.11.2 Originator Addresses	242
6.11.3 Extension Number Ranges	242
6.11.4 Communication Devices	244
6.11.5 Bindings	245
6.11.6 Resources	246
6.11.7 Configuration Examples	246
6.11.7.1 Channel Reservation for In or Outbound Fax Traffic	246
6.12 Gateways over General File Interface (FIAPL)	247
6.13 Department Printer Settings (PrintAPL)	249
6.14 Hicom Applications Connectivity Link Settings	253
6.15 Computer Telephony Integration (CTIAPL)	255
6.15.1 Configuration	255
6.15.1.1 Link via TAPI	257
6.15.1.2 Link via TSAPI	258
6.15.1.3 Link via CSTA	259
6.15.1.4 Expert Parameters	260
6.15.1.5 Monitoring	262
6.16 SAP R/3 Gateway (SAPR3APL)	263
6.17 Creating Reports (RepAPL)	268
6.17.1 Generating Report Jobs	269
6.17.2 Global Settings	275
6.17.3 Parameters	277
6.17.4 Version	278
6.18 Short Message Service (SMSAPL)	278
6.18.1 Configuration Steps	278
6.18.2 Supported Hardware	279
6.18.3 Configuration	280
6.18.4 Sending SMS Messages	281
6.18.5 Receiving SMS Messages	281
6.19 MWI to Alcatel 4400 (ABCAPL)	282
6.19.1 Telephone Display Support	282
6.19.1.1 Waiting Message Retrieval	282
Index	285

1 Introduction

This manual is written for the administrator of a MRS Server. First a short overview of the server will be presented, following with a description of the individual components as well as start and stop procedures of the server.

Next the administration of the database will be discussed along with all associated tasks. These tasks comprise the installation and configuration of new users, security, and other various administrative duties that occur within the daily operation.

Subsequently, an overview of the various MRS Services and their addressing will be presented.

In the following the individual MRS components will be explained. Since it is used for the central surveillance and configuration of the MRS Server, careful attention should be given to those portions concerning the MRS Monitor.

Note: Please read the current release notes (in the root directory of the MRS installation CD). There you find program and process modifications as well as the latest information on the compatibility of hard and software components that could not be considered in the manual. In addition you can obtain further information from the corresponding readme files. These are found in the directories of the single components.

2 Concepts

2.1 MRS Structure

The MRS Kernel is built upon four components: *Message Transfer Agent* (MTA), *Database* (Infostore), *Extended Message Reporter Service* (XMRSvc), and *Name Locator* (NameLoc). Access to the kernel is through the various Access Protocol Layers (APLs) which implement the external protocols e.g. ISDN, SMTP, Exchange Gateway, and TCP/IP. The Access Protocol Layers thus allow access to the server over various communication mediums. Access Protocol Layers are principally optional components whose application and configuration will be discussed later.

With the exception of the Name Locator (organizes the communication in a distributed system), all other components can be seen in the MRS Monitor.

2.1.1 Message Transfer Agent

The Message Transfer Agent processes all jobs that can be independently executed from one another simultaneously. Only jobs whose chronological order is critical are processed sequentially in separate threads.

Simultaneously processed tasks are:

- Routing of documents and dialogs
- Conversions
- Distribution list resolution

Sequentially processed are:

- Report assignments
- Line states
- Database access

2.1.2 Database

The Infostore is based on the database cTree. Journals, user, and charge information are managed by the database. The database is so constructed, that address book synchronization with other databases is possible e.g. MS Exchange.

Dialing numbers in the MRS Server are given a normalized representation. If a fax is to be sent to the number +49-2404-12345, this address would have the MRS Address form of NVS:FAXG3/49240412345. Since addresses are managed by the appropriate APL, no outside dialing information is contained within.

2.1.3 Extended Message Reporter Service

This centralized service gathers all Log information from the various MRS components. Monitor processes distributed over the network, can be logged-in with XMR-Service giving various and dissimilar system reports.

In this way, special surveillance MRS Monitors can also be configured. On one MRS-Monitor security information could be displayed while on another Monitor fax information is shown etc.

2.1.4 Name Locator

The Name Locator frees the Intertask-Communication from having to know which task is being performed on what computer. The Name Locator runs in the background on every computer which contains a working component of the MRS Server, and disseminates the names of these computers to other computers which contain components of the MRS Server within the network.

2.2 MRS Addressing

The MRS Server uses the following addressing form which is independent of the protocol and target system structure.

NVS: NODE . CLASS/USER

or

NVS: NODE/USER

The first portion of the address (NVS:) is never modified since it characterizes the syntax of the address type. In this way it is later possible to insert new address types.

The target network is described through the use of **NODE**. Typical nodes are FAXG3, SMS, TCPIP, SMTP, LN etc.

Example:

NVS: FAXG3/491234567890

FAX G3 Subscriber +49-1234-567890.

NVS: EXCH/MAYER

Microsoft Exchange User MAYER.

NVS: SMTP/info@cycos.com

TCP/IP E-Mail from SMTP Protocol to TCP/IP user **info** in the Domain **cycos.com**.

Through the optional entry **CLASS**, various accesses of a similar type within a network node can be given. If a server is connected with seven logical fax lines to the network, and the network to the public exchange, these seven logical fax lines could be individually selected through the use of **CLASS**. If no entry for **CLASS** is given, the router would decide through the use of internal evaluation tables, which access to the network node is to be used. The entry **USER** corresponds to the local syntax of the network. In the case of a fax this is the fax number in a normed form.

Example:

NVS:FAXG3.1/491234567890

FAX G3 member +49-1234-567890 over logical line (CLASS) 1.

NVS:FAXG3.2/491234567890

FAX G3 member +49-1234-567890 over logical line (CLASS) 2.

MRS Addresses always define a logical access to and from the MRS System. Access Protocol Layers define the individual structure of a physical point of access to the network.

Server Administration

MRS Addressing

3 Administrative Procedures

3.1 Starting and Stopping the Server

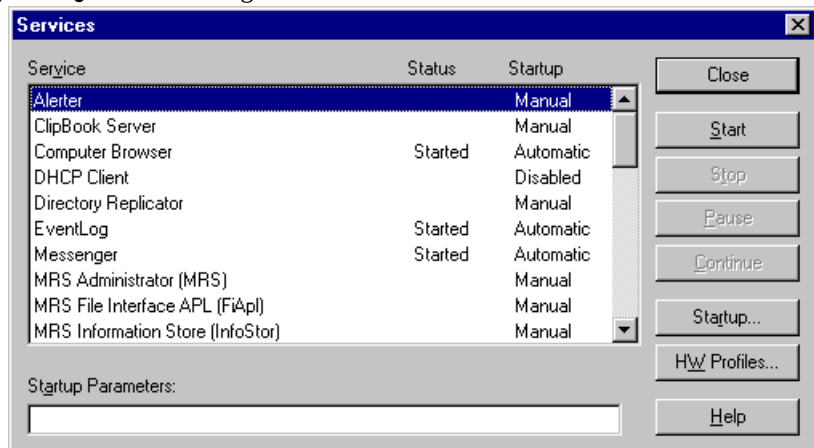
There are various methods for starting and stopping the MRS Server. In most cases the user sees none of this, since the server runs without any logged-in users and therefore requires no display output.

The status of the server start can be continuously followed through the use of a previously started MRS Monitor. The following methods are also available and will be described in more detail below:

- Start/Stop through the Start resp. Shutdown of the NT Server
- Start/Stop through installed Program icons resp. selection of these programs from the Start menu
- Start/Stop through the *Service Control Manager* of Windows NT
- Start/Stop locally from the Commandline
- Start/Stop locally and remotely from the Commandline Interpreter with the utility `sc` (part of the Windows NT Resource Kit).

During the installation, the program icons “Start MRS Server” and “Stop MRS Server” were installed. These can be found in the Start Menu of Windows NT 4.0.

The second method is through the *Service Control Manager*. This is found under the entry **Settings**. After starting **Services** all services and their status can be seen.



The service **MRS Administrator (MRS)** starts the complete MRS Server. Stopping a service is accomplished by selecting the service from the list and subsequently selecting

Server Administration

Installation and Start of Individual Components

the **Stop** button. Through this action the server is shutdown. This method can also be used for shutting down and restarting individual components.

In most cases the service **MRS Administrator (MRS)** has the Startup type **Automatic**. With this setting the MRS Server is automatically started when the computer is started. If this is desired, the **Startup** type can be changed to **Manual** and the MRS Server started “from hand” after the computer is started.

Every MRS Server component can be started or stopped from the Commandline Interpreter. The component name (found in parenthesis in the *Service Control Manager*) is entered along with the command **Start** resp. **Stop**. To start or stop the MRS Server the commands “MRS Start” or “MRS Stop” would be used. Locally, it is also possible with the NET commands. In this case, “net start <Service>” or “net stop <Service>” would be entered.

All the methods mentioned thus far function only on the local computer (computer where the MRS Server is installed). Starting and stopping the MRS Server is also possible from other computers within the network. This service is provided by the utility **sc**. This utility is not included with the standard distribution of Windows NT, but contained in the Windows NT Resource Kit. The acquisition of the Resource Kit is suggested not only for this utility, but also for the useful knowledge contained within for the execution of the system administrator’s duties.

This utility allows the management and querying of services from the Commandline Interpreter for the local computer as well as other computers within the network. The call for starting and stopping the MRS Server is as follows:

```
sc \\Servername start mrs
sc \\Servername stop mrs
```

The server name is the name of the computer in the Windows network, and is not required when this utility is executed for services on the local computer.

3.2 Installation and Start of Individual Components

Almost all MRS components can be installed at a later time using the Setup program. This is not possible for certain MRS SDK¹ test modules or newly developed modules that were not included in the delivered Setup program. Installation instructions for these modules through use of the Commandline Interpreter is as follows:

Every APL or kernel component can be installed with the call

```
Name install
```

1. MRS Software Development Kit. Various individual components can be developed for the MRS server with this kit.

from the Commandline. An attempt is made to incorporate meaningful default values, but a complete configuration of the component should be subsequently performed from the MRS Monitor. Several components e.g. the Exchange Gateway APL require a greater expenditure and therefore should only be installed through the Setup program.

Example: tcpapl install

So that these components are also started, the following command must be given in the Commandline Interpreter

Name start

or in the *Service Control Manager* through the selection of the service and subsequent selection of the **Start** button. Usually, the **Startup** type “Manual” is entered during the component installation.

Since components installed in this way are not started automatically by the MRS Administrator, they have to be individually started by hand. If the automatic start of these components is desired, the component must be inserted in the registry under the *Key*

HKEY_LOCAL_MACHINE\Software\PP-COM\MRS\Services

in the REG_MULTI_SZ-Value *Access Protocol Layer*.

3.3 Stop and Deinstallation of Individual Components

In a likewise manner to that of the installation, individual components can also be deinstalled from the Commandline Interpreter through the use of

Name remove

Prior to its removal, the component should be shut down through the *Service Control Manager* by selecting the component and subsequently the **Stop** button or from the Commandline Interpreter with the command

Name stop

3.4 Complete Deinstallation of the MRS Servers by Hand

Normally the deinstallation of the MRS Server occurs through the delivered *MRS Deinstallation Wizard*. If the deinstallation is to be done by hand, the necessary steps are as follows:

1. All MRS Server shared directories (Shares) must be given the status “Not Shared” on the MRS Server where the kernel components are installed. These are normally in the MRS installation directory unless they were changed during or after the

Server Administration

Complete Deinstallation of the MRS Servers by Hand

installation. This refers to the following directories (Sharename) for a complete installation.

- Backup (MrsBackup\$)
- Client (MrsClnt\$)
- Folders (MrsFolders\$)
- Monitor (MrsConfig\$)
- PipeBuff (MrsXfer\$)
- Userdata (MrsUserdata\$)

2. All components, as written above, could be deinstalled with

Name remove

The name of each component is found in the *Service Control Manager* in parentheses behind the full name of the component. All server components beginning with the abbreviation MRS also have a full name describing the service.

3. The MRS installation directory and all sub-directories must be deleted. If during the installation or at a later time directories in other locations of the file system were installed, these should also be deleted.
4. Using the Registry Editor regedt32 the Key

HKEY_LOCAL_MACHINE\SOFTWARE\PP-COM\MRS

must be deleted. If an Administrative Client was installed then the Key

HKEY_LOCAL_MACHINE\SOFTWARE\PP-COM\Aachen32

must also be deleted.

5. In the *Value* NullSessionPipes under the *Key*

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
LanmanServer\Parameters

all entries that begin with MRS and end with IPC must also be removed, as well as those entries that end with APL. This normally transpires with the deinstallation of the individual components, but a little control never hurts.

6. In the *Value* NullSessionShares under the *Key*

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
LanmanServer\Parameters

all entries that begin with MRS must be removed. All Shares mentioned above should have an entry here.

3.5 Event Viewer

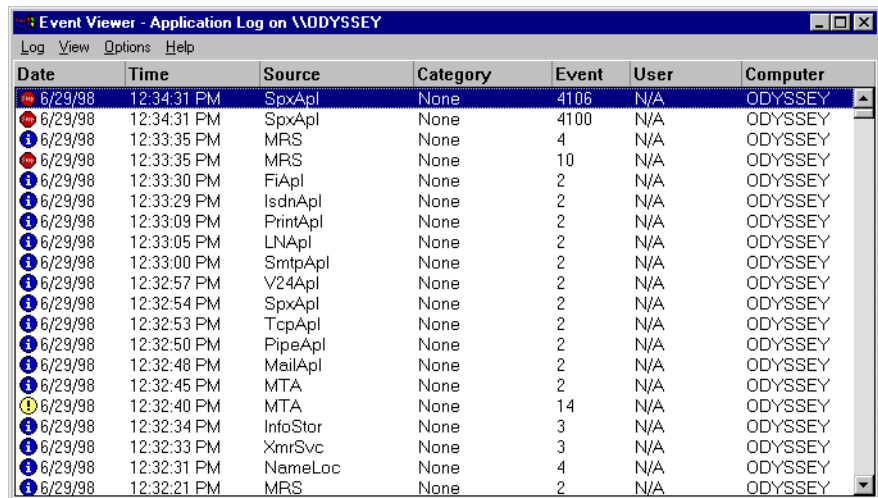
In the Windows NT operating system, an event is any significant occurrence in the system or in an application that requires users to be notified. For critical events such as a full server or an interrupted power supply, a warning message may be seen on the screen. For many other events that do not require immediate attention, the Windows NT operating system adds information to an event-log file to provide information without disturbing the workload of the user. This event logging service starts automatically each time the computer is started under Windows NT.

The Event Viewer can be used for System management, Security, and Application event logs. Event logs can also be stored as an archive.

The System log records events logged by the Windows NT system components. For example, the failure of a driver or loading of a system component during startup is recorded in the System log.

The Security log records security events. This helps track changes to the security system and identify any possible breaches to security. For example, attempts to log on the system may be recorded in the Security log, depending on the Audit settings in User Manager. The Security log may only be viewed by the administrator of the computer.

The Application log records events logged by applications. For example, a database application might record a file error in the Application log. Reports sent by the MRS Server can be found here.



Date	Time	Source	Category	Event	User	Computer
6/29/98	12:34:31 PM	SpxApl	None	4106	N/A	ODYSSEY
6/29/98	12:34:31 PM	SpxApl	None	4100	N/A	ODYSSEY
6/29/98	12:33:35 PM	MRS	None	4	N/A	ODYSSEY
6/29/98	12:33:35 PM	MRS	None	10	N/A	ODYSSEY
6/29/98	12:33:30 PM	FiApl	None	2	N/A	ODYSSEY
6/29/98	12:33:29 PM	IsdnApl	None	2	N/A	ODYSSEY
6/29/98	12:33:09 PM	PrintApl	None	2	N/A	ODYSSEY
6/29/98	12:33:05 PM	LNAPL	None	2	N/A	ODYSSEY
6/29/98	12:33:00 PM	SmtApl	None	2	N/A	ODYSSEY
6/29/98	12:32:57 PM	V24Apl	None	2	N/A	ODYSSEY
6/29/98	12:32:54 PM	SpxApl	None	2	N/A	ODYSSEY
6/29/98	12:32:53 PM	TcpApl	None	2	N/A	ODYSSEY
6/29/98	12:32:50 PM	PipeApl	None	2	N/A	ODYSSEY
6/29/98	12:32:48 PM	MailApl	None	2	N/A	ODYSSEY
6/29/98	12:32:45 PM	MTA	None	2	N/A	ODYSSEY
6/29/98	12:32:40 PM	MTA	None	14	N/A	ODYSSEY
6/29/98	12:32:34 PM	InfoStor	None	3	N/A	ODYSSEY
6/29/98	12:32:33 PM	XmrSvc	None	3	N/A	ODYSSEY
6/29/98	12:32:31 PM	NameLoc	None	4	N/A	ODYSSEY
6/29/98	12:32:21 PM	MRS	None	2	N/A	ODYSSEY

The following data is displayed in the Event Viewer:

- **Source**
The software that logged the event, which can be either an application or a component of the system, such as a driver.
- **User**
Specific text that exactly matches the text in the User name field. This field is not case sensitive.
- **Category**
A classification of the event, as defined by the source.
For example, the categories for Security event logs are Logon and Logoff, Policy Change, Privilege Use, System Event, Object Access, Detailed Tracking, and Account Management.
- **Computer**
The exact name of the computer where the logged event occurred. This field is not case sensitive.
- **Event**
Shows an event number to identify the specific event.
The Event helps product-support representatives track events in the system.
- **Type**
A classification of the event by the Windows NT operating system, such as Error, Warning, Information, Success, or Failure.

The Event Viewer is found under the program group **Administrative Tools (Common)**.

3.6 User Data Administration

The user database contains important administration data required to coordinate and validate the access of individual users to the services of the MRS Server. The database contains files which allow the MRS Server to route incoming documents and reports to a user. The database also includes the passwords used to check privileges.

The user data is managed through use of the administrative client Communications. Log-in with the administrator account created during the setup. For detailed instructions on using Communications please refer to the Communications manual.

As an alternative, user data can be updated via the Web Administrator. The corresponding procedure is also described in the associating manual.

Three groups are included as default; **Supervisor** (to include all administrators, since this group has all privileges), **Service** and **User** (to include all normal users).

Service has some additional privileges, enabling it to handle some administration tasks. Please note that any one user can only be included in one group.

3.6.1 Field Significance

The following tables describe the significance of all standard database fields. Since access authority to the server could be modified, *SUPERVISOR* privileges are required for the fields Group, Password, and PIN.

Access Authority

Field	Significance
USER	The log-in name, also used as alias (E-Mail). This name must be unique and should be restricted to the characters A–Z and 0–9 (otherwise problems may occur when addressing via gateways). Please note that although the maximum entry length is 63 characters, this allocation must never be fully used since the maximum length of an MRS address is also 63 characters and some non-addressable users would be generated in the event that e.g. the NVS:MAILBOX/, required to form the address, could not be prefixed owing to the lack of space then. We recommend to restrict a user ID to fewer than 26 characters if possible.
Name	Full name of the user. Although this entry does not affect privileges, but is included in this part of the database mask for easier identification of an actual person with a log-in name which are frequently relatively short.
Password	The user password. Passwords are <i>not</i> displayed in plaintext, but represented by asterisks. Passwords are additionally protected in the database by one-way encoding, so that they cannot be read there. There is no default password. Thus, a password must be entered, since the MRS Server allows <i>no</i> access via blank passwords. If when installing, all NT domain users were automatically imported, these are automatically installed with the user name as log-in name and password. Users should be reminded to choose passwords which are not identifiable by simple methods, such as trying all the words in a dictionary.

Access Authority

Field	Significance
PIN	Personal Identification Number. This number is required for remote inquiries of the Voice Mailbox. PINs are <i>not</i> displayed in plaintext, but represented by asterisks. PINs are additionally protected in the database by one-way encoding, so that they cannot be read there. There is <i>no</i> default PIN. However, it is a good idea to use 111111, because the Standard Voice/Fax Mailbox Script uses this PIN as default.
Privileges	The privileges box is modified via a menu-based privileges editor. All privileges displayed in gray are permanently assigned via the user's group and cannot be removed. Additionally assigned privileges are color-highlighted (selected).
Group	The group in which the user is included. Groups are defined by entries in the database boxes USER, Name and Privileges. The box USER contains the group name, Name contains a description of the group and Privileges contains the privileges assigned to the group. By inclusion in a group, a user thus receives all group-related privileges, in addition to those explicitly defined in this privileges box. Please note that any one user can only be included in one group.
LMAccount	If the domain\account of a Windows user has been entered here, the Windows account can be used for logging in at the MRS Server per option to be set in the MSP profile for this user. Under Windows NT/2000/XP a validation is automatically performed via the logged in user. Under Windows 9x/ME the user must validate him or herself again via entry of their Windows password for each client application used since here, for security reasons, no password is saved within the Windows system.

Message Routing

Field	Significance
Preferred	The preferred mode of routing for incoming messages. Another database box, containing the actual address, must be referenced as entry. If there is no <i>active routing</i>, Mailbox is the referenced database box. In this case, the system waits until the user calls up incoming messages himself, which is normally when he logs in for the first time. Thus, there is no automatic routing of new incoming messages. The user himself must ask the Server whether new documents have arrived since he last logged in. All other addresses are actively routed to, if the user is currently logged in at the Server, i.e. if he has entered an SMI Transport, such as PIPE, TCPIP or SPX. The database box of the SMI Transport then contains the address to which the MRS Server should route the message. Since the user's current log-in status is known, each new incoming message is routed on if the user is logged in. If not, messages are routed to his mailbox until he logs in again. This field is also used with alias entries for e.g. the selection of telematic services. Care should be taken that telematic services are only entered in those fields that are not suffixed with a #. These fields use an internationally normed number for the telematic services. Example: FAXG3 instead of FAXG3#.
Mailbox	A unique mailbox name. Normally, the user's log-in name is used since it is also unique. Incoming messages are collected in this mailbox until the user collects them.
Stand-in	A user to whom all incoming documents should be routed, e.g. in case of absence through illness or holiday. Stand-in must be entered in the field Preferred as soon as the delegation is to become active. Note that with this type of delegation the stand-in only receives original messages and no copies. In old database layouts the stand-in field name may occur as well.

Message Routing

Field	Significance
CIT	A <i>Message Waiting Indicator</i> (MWI) is sent to the address entered here. The applicable protocol must be made available by an APL. More information to CIT can be found in section 4.1.1.3 and section 4.1.2.9.

Telematic Services

Field	Significance
FaxG3#	User extension number for inbound fax G3 documents. This number is used by the server for the routing of inbound fax G3 documents to the user's mailbox.
FaxG3	

This number, as with all telematic numbers of the MRS Server, is internally transcribed in international notation, whereby characters other than digits are disregarded. The number sign is also excluded, and the internationally normed number subsequently found in the field FAXG3. The MRS Server requires these extensions in the distinctive form provided through this process.

The administrator requires a user entry that is easy to read and to maintain. In the field with the suffixed number sign (#), extensions may be entered in plain text so that a readable entry is available to the administrator.

Example:

(FAXG3#) +49-2404-98765-432
(FAXG3) 49240498765432

The 49 corresponds to the international prefix for Germany, 2404 the local area code for Alsdorf. The rest of the number is the number of the PBX plus that of the user's extension.

This example displays the transcription of an extension number by the server to an internationally normed number:

(FAXG3#) 432
(FAXG3) 49240498765432

Telematic Services

Field	Significance
	All fields within the database that are suffixed with a number sign (#), are readable entries and have a corresponding field (without number sign), which is used by the server for routing purposes. This field is also found in the user database template for checking the number transcribed by the server.
FaxG3-ID FaxG3-Kenn	Fax G3 user ID. This ID is found in the header of all outbound fax documents. If this field is missing, the default ID of the APL would be inserted. In older database templates the field name FAXG3-KENN may appear. Example: +49 2404 98765432
FaxG3-Headline FaxG3-Kopf	Default Fax G3 user headline. This entry appears in the header of all outbound fax G3 documents. If this field is missing, the default ID of the APL would be inserted. In older database templates the field name FAXG3-KOPF may appear. Example: Mister AG/Germany
Voice# Voice	User voice mail number. Since a distinction between services can be made through the ISDN service indicator, the same extension number may be used for the services Fax G3, Fax G4, voice, ISDN Telex and Euro file transfer. The correlation between the two database fields is explained above in the discription of Fax G3#/FaxG3. Example: 49-2404/98765(432)
FaxG4# FaxG4	Fax G4 user number for inbound fax documents. This number is used by the server for inbound routing to the user's workplace. Since a distinction between services can be made through the ISDN service indicator, the same extension number may be used for the services Fax G3, Fax G4, voice, ISDN Telex and Euro file transfer. The correlation between the two database fields is explained above in the discription of Fax G3#/FaxG3. Example: 49240498765432

Server Administration

User Data Administration

Telematic Services

Field	Significance
FaxG4-ID FaxG4-Kenn	Fax G4 user ID in accordance with F.200 standards. This ID is found in the header of all outbound fax documents. If this field is missing, the default ID of the APL would be inserted. In older database templates the field name FAXG4-KENN may appear. Example: +49 - 240498765432=MISTER
ISDNNTX# ISDNNTX	ISDN Telex user number. This number is used by the server for the inbound routing of ISDN Telex messages to the user's workplace. Since a distinction between services can be made through the ISDN service indicator, the same extension number may be used for the services Fax G3, Fax G4, voice, ISDN Telex and Euro file transfer. The correlation between the two database fields is explained above in the discription of Fax G3#/FaxG3. Example: 49240498765432
ISDNNTX-ID ISDNNTX-Kenn	ISDNNTX user ID in accorcence with F.200 standards. This ID is found in the header of all outbound Telex messages. If this field is missing, the default ID of the APL would be inserted. In older database templates the field name ISDNNTX-KENN may appear. Example: +49 - 240498765432=MISTER
EFT# EFT	User Euro file transfer number. This number is used by the server for inbound routing of EFT files to the users workplace. Since a distinction between services can be made through the ISDN service indicator, the same extension number may be used for the services Fax G3, Fax G4, voice, ISDN Telex and Euro file transfer. The correlation between the two database fields is explained above in the discription of Fax G3#/FaxG3. Example: 49240498765432

Telematic Services

Field	Significance
SMS# SMS	GSM mobile telephone of the user to which SMS messages may be sent. Additionally, this number is used with optional CIT Client applications. The correlation between the two database fields is explained above in the discription of Fax G3#/FaxG3. Example: 49172567890 Furthermore the entry of a mobile phone number in this field is used to put out a voice mail at the mobile phone with implemented WAP functionality.
CostInfo	User information used for billing purposes by the PBX. This information is combined in the extension number through special sequences so that billing can be assigned by the PBX to a user or cost center.
Phone# Phone	Users' telephone extension number, usally found at their workplace. The correlation between the two database fields is explained above in the discription of Fax G3#/FaxG3. This field is required by CTI applications for establishing connections between the user's telephone and other subscribers or connections. This number is also used for internal telephone books, so that the user can be called via a mouseclick. Since a unique number is required by all users on the MRS Server, an extension number may not be assigned to more than one user. This number is still used by the MRS Server for the CTI journal when logging user information.

Gateway Addresses

Field	Significance
SMTP	User SMTP address (Internet email standard). This entry must be present if the user is to receive messages through the Internet. A reference to this entry in the field PREFERRED routes all incoming messages to the email address. Example: ju@sample.com

Server Administration

User Data Administration

Gateway Addresses

Field	Significance
Exch	User Microsoft Exchange address. A reference to this entry in the field PREFERRED routes all incoming messages to the Exchange Gateway. Example: Joe User
LN	User Lotus Notes address. A reference to this entry in the field PREFERRED routes all incoming messages to the Lotus Notes Gateway. Example: Joe User/SAMPLE
MS	User MS mail address. Referencing this field in PREFERRED forwards all incoming messages to the MS mail gateway. This database field is usually only found in older MRS Server installations. Example: NOVELL/POSTOFF/HMUSTER
CC	User Lotus cc:mail address. Referencing this field in PREFERRED forwards all incoming messages to the cc:mail gateway. This database field is usually only found in older MRS Server installations.

General User Data

Field	Significance
ZIP	Zipcode. Can be used in fax cover pages or templates.
City	City. Can be used in fax cover pages or templates.
Country	Country. Can be used in fax cover pages or templates.
Company	Company. Can be used in fax cover pages or templates.
Division	Division/Department. Can be used in fax cover pages or templates.
Addr1	Line one of the address. Can be used in fax cover pages or templates.
Addr2	Line two of the address. Can be used in fax cover pages or templates.

General User Data

Field	Significance
Remark	Freely usable field in which remarks or comments may be entered.
Privtel# Privtel	Private telephone number of the user. This field is optional and can be used in CTI Client applications e.g. MRS TrayPhone. The correlation between the two database fields is explained above in the discription of Fax G3#/FaxG3.
Privfax# Privfax	Private fax number of the user. The correlation between the two database fields is explained above in the discription of Fax G3#/FaxG3.
GSM# GSM	Private mobile telephone number of the user. This field is optional and can be used in CTI Client applications e.g. MRS TrayPhone. The correlation between the two database fields is explained above in the discription of Fax G3#/FaxG3.
Keyword	This field can be used for individual sorting procedures. Appropriate keywords can be entered in these fields and then the keyword selected from a keyword list.
Printer	Printers listed in the Print APL can be entered in this field. This field can then be subsequently used in conjunction with the Routing Rules for the automatic printing of inbound user fax documents.

Client Connections

Field	Significance
TCP/IP	TCP/IP address of the user's computer. Either a name that can be resolved by the DNS server or a direct entry such as 222.222.222.106 can be given. This entry occurs automatically via the Client when the TCP/IP transport is used and active delivery (default) is activated.

Client Connections

Field	Significance
Pipe	The computer name within a Windows network used for connecting the Client 2.50 over a Named Pipe. Named Pipes are the only type of transport that allow the connection of client to the server when both are found on the same computer. This entry occurs automatically via the Client 2.50 when the Named Pipe transport is used and active delivery (default) is activated. More recent Client applications do not use this protocol any more.
SPX	SPX address of the user's computer. This address is formed from the worldwide unique network card ID. This occurs automatically when the client is connected to the server through SPX and the automatic mail delivery (standard connection) is set SPX. Example: 1.400526D51D

POP3 Mail-Import

Field	Significance
PMI-SCHEDULE	See POP3 Mail-Import on page 220.
PMI-HOSTNAME	See POP3 Mail-Import on page 220.
PMI-USERNAME	See POP3 Mail-Import on page 220.
PMI-PASSWORD	See POP3 Mail-Import on page 220.

Examples of User Entries

Field	Contents	Significance
USER	JU	User's initials, used as E-Mail address and log-in name.
Name	Joe User	User's name, can be used in fax cover-pages and fax templates.
Addr1	Any Street11	Postal address – line 1. Free entry.
Addr2	12345 Town	Postal address – line 2. Free entry.

Examples of User Entries

Field	Contents	Significance
Remark	Arbitrary User	Box for free entry, in which explanatory remarks may be entered.
PrivTel#	01234-567890	User's private telephone number. Entry format freely-selectable.
PrivFax#	01234-567891	User's private fax number. Entry format freely-selectable.
GSM#	0171-567890	User's private mobile telephone number. Entry format freely selectable.
Keyword	Hotline	Arbitrary keyword used to expedite search procedures for specific criteria.
Password	*****	User's password. Password is not displayed in plain text. Attention: The MRS Server does not distinguish between small/capital letters with passwords.
PIN	*****	User's Personal Identification Number for the Voice Mailbox, not displayed in plain text.
Privileges		This entry is handled via a special editor. In the example, the user has no special privileges.
Group	USER	Standard group for normal users. The user has the privileges of this group.
Preferred	PIPE	The user normally logs in via Named Pipes and receives new incoming documents immediately routed to the PC referenced in the field Pipes.
Mailbox	JU	Incoming messages are stored within this mailbox when the user is not logged-in.

Server Administration

User Data Administration

Examples of User Entries

Field	Contents	Significance
Stand-in	MK	If Stand-in were entered in Preferred, messages intended for HM would be routed to user MK. Thus when the original recipient is absent, the stand-in is target for incoming messages and can immediately react to important ones.
CIT	SMS	New message arrival is displayed to the user on the mobile telephone entered in the box SMS, via an SMS short message.
FaxG3#	491234567890	Incoming Fax G3 documents are routed to this extension.
FaxG3-ID	+49 1234 567890	User Fax G3 ID.
FaxG3-Headline	Sample Co.	User Fax G3 header attached to outgoing fax documents.
Voice#	491234567890	Incoming voice mail messages would be routed to this extension.
FaxG4#	491234567890	Incoming Fax G4 documents are routed to this extension.
FaxG4-ID	491234567890=JU	User Fax G4 ID.
ISDN TTX	491234567890	Incoming ISDN Teletex documents are routed to this extension.
ISDN TTX-ID	491234567890=JU	User ISDN Teletex ID.
EFT#	491234567890	Incoming files sent via EFT are routed to this extension.
SMS#	49171567890	User GSM cellular telephone number.
CostInfo	12	The cost center, to which outgoing messages of the user JU are booked. This entry depends on the PBX system in use and is built into the call number, enabling the PBX system to read it.

Examples of User Entries

Field	Contents	Significance
SMTP	ju@sample.com	User's email address used for messages to and from the Internet.
Exch	Joe User	The user's "real" name can be used for addressing with Microsoft Exchange.
LN	Joe User/SAMPLE	The user's "real" name followed by the certifier is used for addresses in Lotus Notes.

3.6.2 Privileges

The user's authority is dependent upon the assigned privileges. The user's authority is commensurate to that of the group in which they belong plus any additional privileges assigned by the administrator.

A privilege is required for almost every transaction. The standard privileges and their significance are listed in the following table. Individual privileges can also be defined if additional restrictions are required. The necessary steps for defining privileges will be discussed at the end of this section.

Privilege	Significance
SUPERVISOR Privilege	Database fields can be so created that this privilege is required to make alterations. Furthermore it authorizes the use of the user data editor and the MRS Monitor via which the MRS Server is configured. Attention: With this privilege all rights are implicitly assigned even if some of the following privileges have not been assigned to the corresponding user.
SERVICE Privilege	Database fields can be so created that this privilege or that of a supervisor is required to make modifications. Furthermore it authorizes the use of the user data editor and the MRS Monitor via which the MRS Server is configured.

Server Administration

User Data Administration

Privilege	Significance
USER Privilege	Database fields can be so created that this privilege or that of a supervisor is required to make modifications. This privilege is mandatory for logging in at the server.
ISDN Service Remote Access	This privilege has no significance for MRS and is only included for compatibility reasons with a NVS server on a QNX basis where it handles remote access to the NVS server via the ISDN APL.
Fax Logo- and Coverage Editor	Fax logos and cover sheets can be created or modified with the client's editor.
Client Beta-Tester	A beta test version of the client in the server file system is offered as update.
Advanced USER	This privilege is intended for client applications that can link certain functions to this privilege, for example the configuration options in the ACD Agent client.
ACD Monitor Privilege	The user is permitted to use the ACD Supervisor client for viewing current call center data. He or she cannot perform any configuration modifications.
ACD Supervisor Privilege	The user is permitted to use the ACD Supervisor client for viewing current call center data and can modify the configuration.
VMS Administrator Privilege	Administrator privilege for the TUI VMS by Siemens.
Special Delivery Options Privilege	Privilege for the TUI VMS and PhoneMail by Siemens.
TTS Capabilities Privilege	The user is permitted to play back messages via a TUI per Text-to-Speech.
Internal Call Privilege	With the Siemens TUI PhoneMail the user is permitted to recouple.
Global Distribution List Editor	Global distribution lists can be created or modified with the client's editor.

Privilege	Significance
Global Distribution List Send Messages	Global Distribution List Send Messages can be sent to a global distribution list.
Global Alias Editor	The alias (short) database can be created or modified with the client's editor. Local or private contacts are always permitted. With a remote system link this privilege is required for the user account via which the remote MRS Server is validated if user data synchronization is to occur. In this case the remote MRS Server users are defined on the local MRS Server as contacts so that they are addressable.
Server Query	Research operations in the server's global journal may be executed.
Document Chain Query	Document routing and response tracking may be viewed.
Local Call Privilege	Telematic services can be used within the area code.
National Call Privilege	Telematic services can be used within the country.
International Call Privilege	Telematic services can be used worldwide.
Server File Access	Access to the MRS Server virtual file system through the server file manager on the client.
Local File Access	Access to the local file system through an appropriate file manager on the client. Revoking this privilege is only meaningful when the client PC is to be used as a terminal and booted over the network. In this case local files are non-existent.
Query Result Document View	Documents given by a research of routing or reply tracking on the server may be viewed. Without this privilege only the header information can be read.

Server Administration

User Data Administration

Privilege	Significance
Trusted Domain Privilege	This privilege can be used for services and gateways. Through the configuration of a pseudo user FAXG3 or MS, privileges assigned to the pseudo user are also assigned to all incoming FAXG3 documents or incoming documents over the MS-Mail gateway. This is used for example when further costs are accumulated by a routing where the originator does not have the necessary authority. This privilege is required for validation by Remote System Links.
Private Query	This privilege allows the users to research their individual documents. If this privilege or the SYS_RECH is not assigned, no research may be executed.
External Archive Query	This privilege allows the research of external archives. Currently not implemented.
Telex Privilege	Telex messages may be sent. Telex services are not within the performance spectrum of the server and require a remote system link to a QNX based NVS server.
FAX G3 Privilege	Fax G3 may be transmitted
FAX G4 Privilege	Fax G4 may be transmitted.
e-Mail Privilege	E-mail may be transmitted.
Voice Privilege	Voice mail may be transmitted.
Short Message Privilege	Short messages to cellular phones may be transmitted.
Fax G3 Poll Privilege	Documents may be polled from a fax on demand server.
AMIS Privilege	External voice mail servers may be addressed per AMIS protocol.

Privilege	Significance
Send dictates privilege	The TUI VMS by Siemens allows the user to record dictates. These may become relatively long and require space accordingly.
Send broadcast privilege	This user may use the broadcast service. If send jobs were generated for which the user has no privilege, they would be executed just the same. This feature is used, for example, by the Siemens TUI VMS.
Euro-Filetransfer Client Privilege	User files may be sent/received from a EFT server.
Paging Privilege	The pager service may be used.
Euro-Filetransfer Receive	EFT server privilege. The MRS Server may act as an EFT server. If an EFT client queries a MRS Server, files may also be downloaded from the EFT server.
Euro-Filetransfer Send	Same as “Receive” with the exception that files may be uploaded to the EFT server.
Euro-Filetransfer Rename	Same as “Receive” with the exception that files may be renamed on the EFT server.
Euro-Filetransfer Remove	Same as “Receive” with the exception that files may be deleted on the EFT server.
Euro-Filetransfer Overwrite	Same as “Receive” with the exception that files may be overwritten on the EFT server.
Internal Fax Privilege	Internal fax message forwarding is allowed in the Siemens TUI PhoneMail.
Local Fax Privilege	Local fax message forwarding is allowed in the Siemens TUI PhoneMail.
National Fax Privilege	Nationwide forwarding of fax messages is allowed in the Siemens TUI PhoneMail.
International Fax Privilege	World-wide forwarding of fax messages is allowed in the Siemens TUI PhoneMail.

Server Administration

User Data Administration

Privilege	Significance
Telex dialog	Authorization to use telex dialog services. Telex services are not within the performance spectrum of the server and require a remote system link to a NVS server on a QNX basis.
e-Mail dialog	Authorization to use email dialog services (chat). This is only possible from one MRS Client 2.5 to another. A remote system link is required for clients on dissimilar servers.
Voice dialog	Authorization to use voice dialog services.
Login via Phone possible with PIN from all devices	With the Siemens TUI VMS and PhoneMail you need this privilege to log in at your mailbox from any telephone device.
File Owner Access	This privilege can be assigned to a file in the virtual MRS Server file system. Therewith a file can be assigned to a user. Direct assignment to a user is not considered useful.
File Group Access	This privilege can be assigned to a file in the virtual MRS Server file system. Therewith a file can be assigned to a user group. Direct assignment to a user is not considered useful.
Message Save Privilege	The user receives this menu in the Siemens TUI PhoneMail.
Recording Menu Privilege	The user receives this menu in the Siemens TUI PhoneMail.
Mailbox Options Menu Privilege	The user receives this menu in the Siemens TUI PhoneMail.
Change Referral Extension Menu Privilege	The user receives this menu in the Siemens TUI PhoneMail.
Answering Options Menu Privilege	The user receives this menu in the Siemens TUI PhoneMail.
Receive Dictates Privilege	The user may receive dictates in the Siemens TUI VMS.

Privilege	Significance
Set CIT for FAX G3	Only when set a message waiting signal is sent over CIT for incoming Fax G3 messages . This privilege is not used with Notification APL usage.
Set CIT for FAX G4	Only when set a message waiting signal is sent over CIT for incoming Fax G4 messages. This privilege is not used with Notification APL usage.
Set CIT for e-Mail	Only when set a message waiting signal is sent over CIT for incoming email messages. This privilege is not used with Notification APL usage.
Set CIT for Voice	Only when set a message waiting signal is sent over CIT for incoming voice mail messages. This privilege is not used with Notification APL usage.
Set CIT for EFT	Only when set a message waiting signal is sent over CIT for incoming Euro file transfers. This privilege is not used with Notification APL usage.
No obligation to change password after first login	The user need not perform the mandatory modification of his or her PIN in the Siemens TUI VMS and PhoneMail after the initial login.
No obligation to record name after first login	The user need not perform the mandatory recording of his or her name in the Siemens TUI VMS and Phone-Mail after the initial login.
Company announcement file enabled	Special privilege for Siemens TUI VMS. The special company announcement is played for the user.
VoiceMailSystem is prompted	Special privilege for Siemens TUI VMS. The announcement “This is the Voice Mail System“ is played for the user.
ConnectToInfoboxOfUser is prompted	Special privilege for Siemens TUI VMS. The announcement “You are connected with the infobox for user ...“ is played for the user.
Long prompts available	Special privilege for Siemens TUI PhoneMail. The user can choose among long and short voice prompts.

Privilege	Significance
Additional Recording Info Privilege	Special privilege for Siemens TUI VMS. During recordings, additional information announcements are given.
Short Recording Start Info Privilege	Special privilege for Siemens TUI VMS. Only the announcement “Please speak after the tone” is played without an indication of the maximum recording time.

3.6.2.1 Customer Specific Privileges

Privileges are defined through database entries. Customer specific privileges can be defined and inserted at anytime. These new privileges could then be inserted as conditions in the Registry *Value* Privileges under the *Key*

`HKEY_LOCAL_MACHINE\SOFTWARE\PP-COM\MRS\MTA\RULES`

This occurs through the entry of the privilege and it’s address separated by a comma. Further entries would be individually entered as lines in `REG_MULTI_SZ`. Addresses that conform to the listed wildcards require the corresponding privilege. For this purpose pattern matching for the given service and number is used. Some manufacturers use expensive telephone numbers for software updates and support. These updates can now be assigned download privileges for service personnel with EFT access.

Example: `EFT_0190,NVS:EFT/0190*`

In order to insert this privilege into the database, a privilege number must first be obtained from Cycos AG. Now a text file e.g. `x.txt` can be created with the following contents:

CLASSNAME	CLASS	KEYNAME	KEY
PRIVILEGES	EFT_0190	0x74	Euro file transfer 0190

Exactly one TAB must be inserted as a separator between the individual parts! The privilege number in the example is 0x74. Using the commandline interpreter with the command

`infotool CLASSIMPORT FILE=x.txt CLASS=PRIVILEGES`

this definition is imported into the database. The MRS Server must be re-started before this new privilege comes into effect. Afterwards, a privilege would be required for all file polling via Euro Filetransfer with a 0190 number.

3.7 MRS Service Provider (MSP)

The MRS Service Provider is used as a global sub-structure for all Client applications using MRS Server services, e.g. Communications, TrayPhone, Lotus Notes LSX, Outlook CTI Extensions, ACD Agent, ACD Supervisor or Application Generator. While several Client applications can run on a computer simultaneously, only one instance of the MRS Service Provider is available.

The following services are provided:

- Local database (cache)

It is not necessary for every Client application to keep an individual database up to date. If required, the MRS Service Provider synchronizes its local database with the database of the MRS Server. Thereby the contents of the local database is made available to all Client applications so that fast access is enabled anytime.

- Store & forward interface

Client applications can send documents to or receive them from an MRS Server. This refers to classic communication per fax, e-mail etc. The CTI journal of the Message Routing System operates via this interface as well.

- Transaction interface

Client applications can communicate with APLs of the MRS Server which support transactions. This enables in particular the CTI functionality for Client applications as TrayPhone or the Outlook CTI Extensions.

According to requirements the MSP is automatically implemented upon the installation of an MRS Client component. When the installation is completed, you find the file `MSP.INSTALL.LOG` in your Temp Directory, helping to detect errors if problems should occur.

The MRS Service Provider is started by the first Client application requiring it. Such an application is the MRS Service Provider configuration module in the control panel.



Service Provider

3.7.1 Configuration

Configuration of the MRS Service Provider is accessed with a doubleclick on **Start → Settings → Control Panel → MRS Service Provider**. Here MRS Servers can be added and a new profile be created for new users resp. an existing one be modified.

User Profiles

To connect a Client application with an MRS Server, a **User Profile** is required. Two options are available:

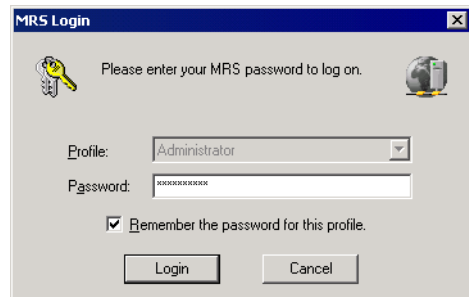
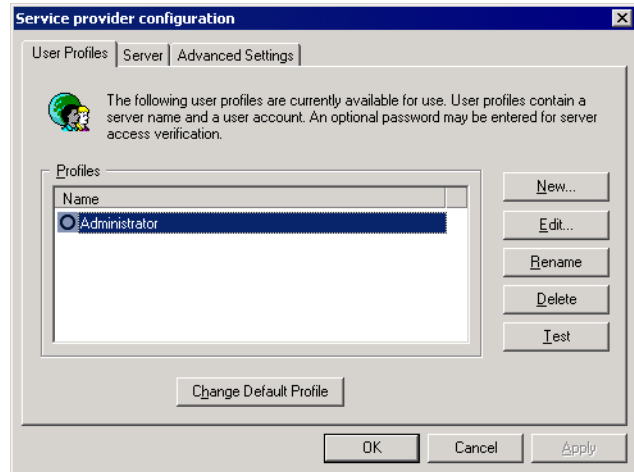
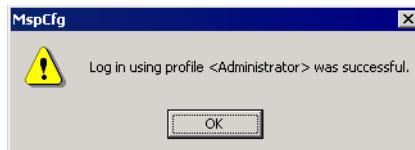
1. A profile containing the name of an MRS Server, a user account on this server and optionally the account's password.
2. A profile with the MRS Server name. For logging in the logged in Windows user account is used. See also section "Client Login via the Windows User Account" on page 48. During the installation a default user profile "My Windows Account" is automatically defined which is linked to the first MRS Server found in the network.

Click on **New** to generate a new profile. The name of the currently logged in user is suggested as **User Name** which should be altered to the MRS User Name.

Edit displays the selected user profile for you to perform modifications (see "Editing a Profile" on page 45); **Rename** allows altering the selected profile name; **Delete** removes the marked user profile.

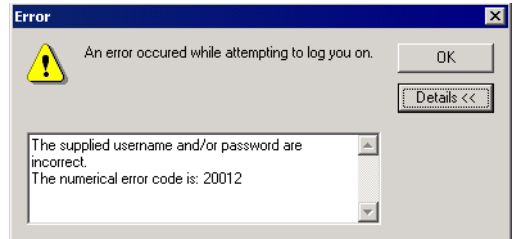
Next validate the configurations made with an attempt to log in to the MRS Server via **Test**.

This process either results in a message of success



or, in case of failure, a possible reason for the error is given

In the event that several profiles are available, one of the existing user profiles can be selected via **Toggle Default** for permanent use. The default profile is indicated by a dot which appears in the circle preceding the user name. If you click on the **Toggle Default** button when a user entry with default profile has been selected, the default profile setting for this user is cancelled. In this case the applications using the MSP always provide a Log-in form in which the desired profile has to be selected from the existing ones. Otherwise log-in would be performed directly without query. However, this again requires entering the password associating the user account.

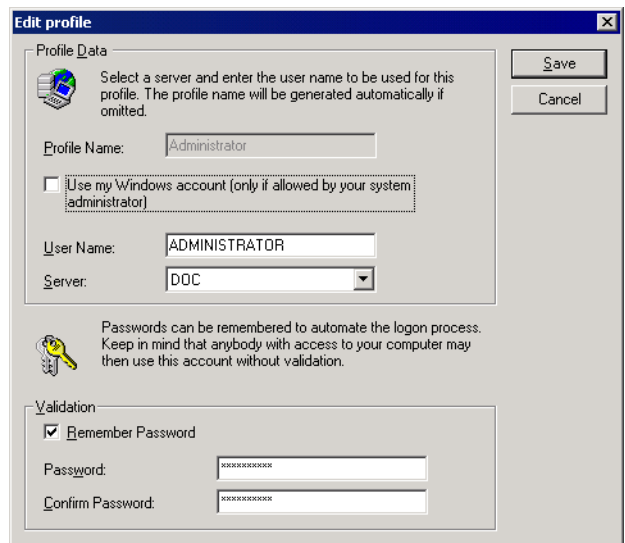


Editing a Profile

The **Profile Name** is a descriptive entry displayed for selecting different profiles later on.

If no profile name is entered with the creation of a new user profile, an entry consisting of the specified **User Name** and the **Server** is automatically generated.

In the event that only one server is available it is pre-set and cannot be modified. For information on the configuration of MRS Servers and how to look them up see the description further below.



The log-in process is performed automatically when the **Remember Password** option is activated and a **Password** is subsequently entered. Since the password is not displayed while you enter it, a repetition of the entry in a second field is required for verification.

Attention: Please remember that with activating this option every person to whom the respective PC is accessible can use this profile without further validation and thus also this MRS user account. Therefore click on **Lock Workstation**² under Windows NT, 2000

Server Administration

MRS Service Provider (MSP)

or XP and with Windows 9x or ME at least a screensaver with password option should be used when you leave your workstation.

With editing an existing profile the same options can be set, however, the name of the profile cannot be altered any more.

A click on **Save** stores the user profile just generated or modified.

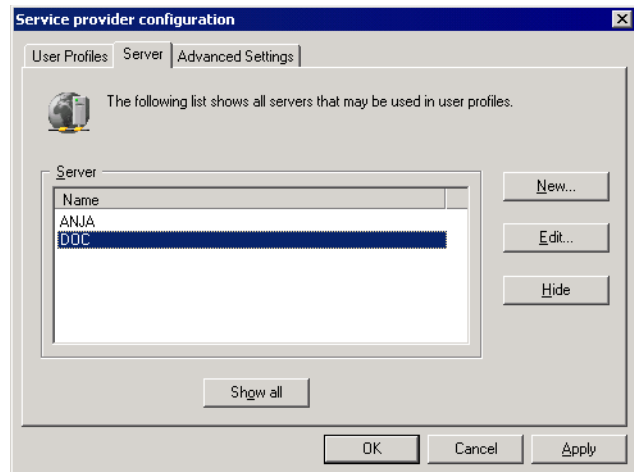
The **Use my Windows account** option carries out a validation of the logged in Windows user via the MRS Server. The user's Windows domain and his or her user account must be entered in the LMACCOUNT database field so that the MRS Server can perform the corresponding assignment. See also section "Client Login via the Windows User Account" on page 48.

Server

Here all MRS Servers found in the network environment are displayed and can thus be selected for user profiles.

Depending on the network environment it may happen that the MRS Service Provider does not automatically find all existing MRS Servers.

In this case these MRS Servers can manually be added via **New**. First select the desired network protocol³ (TCP/IP or SPX) and enter the network address of the missing MRS Server. The network address is protocol specific, so with TCP/IP it is the hostname (e.g. mail.cycos.com) or the IP address (e.g. 10.1.14.128).



-
2. Under Windows NT/2000 press the keys [Ctrl], [Alt] and [Del] simultaneously to open a menu for selecting the option "Lock Workstation" (Windows NT) resp. "Lock Computer" (Windows 2000).
 3. For this purpose the corresponding APL, thus TCP/IP resp. the SPX APL, must run on the MRS Server. Both can be used parallel and are based on the corresponding network protocol which must be installed on the Server as well as on the Client computers.

Then click on **Lookup**. The MRS Service Provider now searches for an MRS Server according to the network address specified and when a server has been found, its name is entered in the **Server Name** field. In the event that the MSP could not address an MRS Server a corresponding message is issued.

A click on **Save** appends the MRS Server to the

server list. In user profiles only servers included in this list can be used.

Through use of the **Hide** button the MRS Server can be faded out of the display. Since the MRS Server is, with reference to the network environment, a globally available resource (similar to a Windows NT Server in the Server Manager), it cannot be “deleted” or “removed” because the MSP stores the information about this server for a longer period.

So if a displayed server is not to be used in your user profiles, it can be “hidden”, that is marked, so that it does no longer appear in the server list. However, this selection only applies to the user currently logged in whereas another one would see the complete server list again.

In case a hidden server is to be displayed again later, click on **Show all** so that all MRS Servers known to the MSP are listed again.

An MRS Server used in an individual profile cannot be hidden.

Alternatively you can enter a * as **Address** and subsequently click on **Lookup**. Now the MRS Service Provider starts a new attempt to find an MRS Server among all addresses reported by the network router and displays the first one found. In the **Server** configuration tab also all newly found MRS Servers are displayed now; the button **Show all** probably needs to be clicked here again. With SPX it is also possible to enter the subnet number and to initiate the search for all MRS Servers existing in this subnet via **Lookup**.

Edit server

On this page, you can manually add a server to the service provider configuration.

Network Parameters

Please specify a network protocol and a network address in order to automatically look up the server name.

Protocol: TCP/IP Protocol

Address: 10.1.14.128:8944

Server Name

You can enter the server name here manually or use the 'Look up' button to avoid typing errors.

DOC

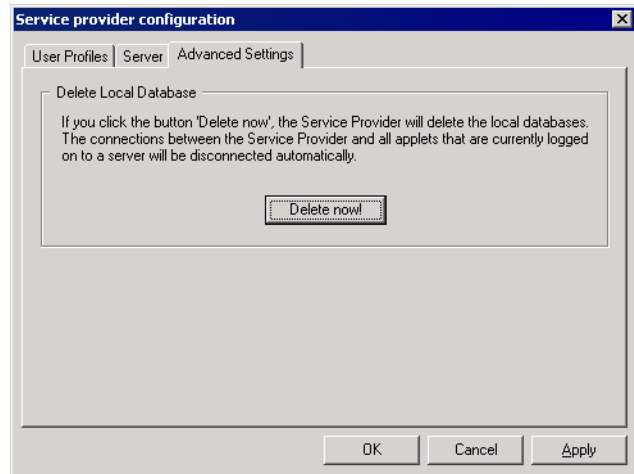
Save Cancel

Server Administration

Client Login via the Windows User Account

Extended Settings

If you notice discrepancies between the MRS Server database and local databases administered by the Service Provider, you can delete the databases so that the MRS Server polls all data anew. This is normally only required when the server was reinstalled with the same name and thus the server database was reinitialized as well. In practice this scenario only occurs in test labs.



3.8 Client Login via the Windows User Account

Instead of a user profile with MRS user account and password you can also assign the Windows user account to an MRS user account. In this way, in a scenario with an Exchange connection, the administrator need not maintain individual MRS user profiles for the respective client computer but uses the logged in Windows user account for the required login of e.g. the Outlook Forms or the Outlook CTI extension.

In the LMACCOUNT database field a user's Windows domain and account must be entered. Example: the entry for user MK in the TEST domain would be TEST\MK. Subsequently activate the corresponding option for the MSP profile and login under Windows NT/2000/XP is performed automatically via validation at the domain server.

Validation at the domain server under Windows 9x/ME requires a password being entered for each client application to be logged in. This requirement is a result of the security restrictions of these Windows operating system versions.

To perform this type of login, an MRS user must not have a \ in his or her USER field. Thus you can, for example, also log in at the WebClient, WebAdmin or via POP3/IMAP4. As login name enter the Windows domain and the Windows user account as stated above. There is, however, the security gap that for access via HTML, POP3 or IMAP4 the Windows password would be transmitted in plain text. This restriction exists as well when the Exchange Server is addressed via POP3/IMAP and can be evaded by using the SSL connection for these types of access.

The LMACCOUNT field is automatically correctly filled in with usage of the LDAP APL and an Exchange 2000 Server connection and maintaining the user data in the Active Directory. Furthermore, with the installation of a client in the MSP, a default profile is always defined for the logged in Windows account so that no further MSP profile needs to be defined on the client computers. If logging in with the Windows account via this standard profile fails, you are prompted to install a corresponding MSP profile. For this reason the LMACCOUNT field should always be updated before the automatic distribution of client applications to the respective client computer. With maintaining the Exchange 5.5 user data the field must be added to the MRS database fields displayed in Exchange.

The MSPTSP application cannot be logged in via the Windows user account since this application runs in the system context and thus does not know the logged-in Windows user.

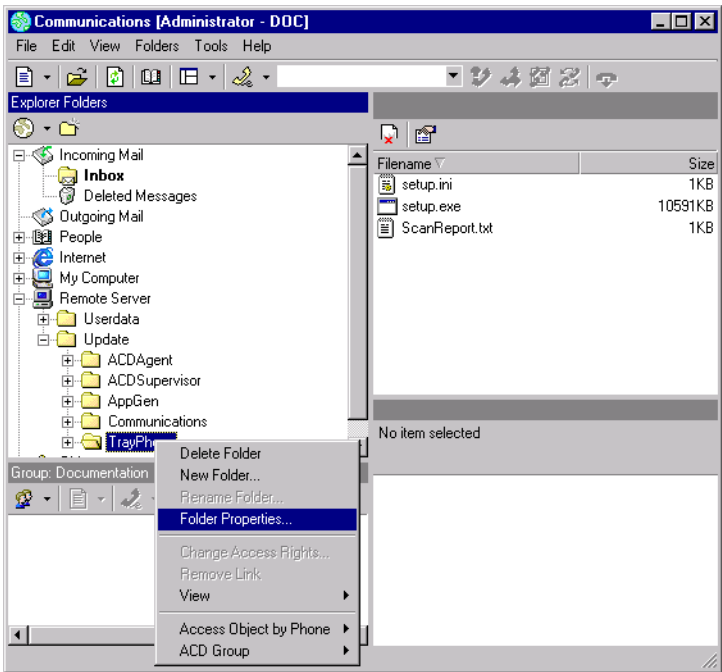
3.9 Client Updates

The latest versions of client applications installed in the customer environment can be stored as update on the MRS Server during the server installation. Certain entries are then automatically made in the MRS database so that the clients are offered these updates while logging in. After a corresponding note you can have this update automatically copied by the MRS Server to the client PC and subsequently have the update installation called.

3.9.1 Installing a new Version on the MRS Server

If you want to do this yourself, copy the client installation files to the <MRS Root>\client\update\<Application> directory. The name of the <Application> directory must correspond to the name of the application as is found in the SETUP.INI as section name. Next you need to adapt the keys in the MRS database.

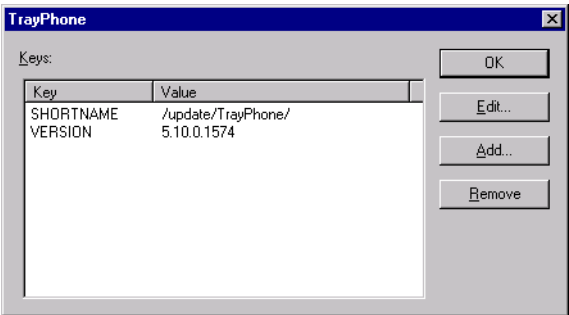
Communications is used for this purpose. In there open a window by means of **View → Explorer Folders** and access the context menu in this window with a click of the right mousebutton. The **Remote Server** option in the context menu must be checkmarked.



In the Explorer Folders window expand **Remote Server** → **Update** → to rightclick **<Application>**. In the context menu now open select **Folder Properties...** to have the available keys displayed.

Enable **Edit** to adapt the **VERSION** key to the correct value of the new client installation files copied to the directory by hand. The value can be taken from e.g. the **SETUP.INI** file.

In the **SHORTNAME** key the directory is specified in the **/update/<Application>/form**. **<Application>** is the application name as found in the **SETUP.INI** as section name.



3.10 Backup

To avoid losing data in case of a system crash or hardware defect it is mandatory to save MRS Server data in regular intervals. This section only refers to data that are cat-

egorically saved and to the data recovery procedure with an MRS Server standard configuration. More complex systems, distributed systems or similar require an adaptation of the security concept which can also be done with the information provided here.

As precondition we assume that a server is set up with identical hard and software in case data recovery becomes necessary. In particular the MRS Server is newly installed on this server as well so that server components realized as services correctly register with the system. To fulfill this precondition a corresponding imaging software could be used with which an image is created after the initial installation. If then a hardware failure, for example a damaged harddisk, occurs, this image can later be installed again.

The backup software is executed under a Windows user account which has read and write privileges on the files and directories to be saved. The write privilege is required for resetting the archive bit that is normally used by the backup software to display a file successfully read and saved to a backup medium.

Furthermore the backup software must be assigned read privilege on the Windows registry elements to be saved.

Owing to the MRS database size and in particular to the document directory and the resulting time required for a backup it is impossible to receive an exact image at a fixed time. Possible deviations, however, only refer to data processed during backup generation and do not influence the principal data recovery. The only way to avoid this would be to stop the MRS Server except for the kernel components, which is normally unacceptable.

3.10.1 Backup Values Data

A system backup does not have to include the entire data amount but can restrict itself to important data so that the entire system is not unnecessarily loaded by the backup process. Only the data amount just sufficient for recovering the system in case of a complete data loss must be saved.

Backup values data are:

- **System configuration (registry)**

The relevant server settings are found in the registry key HKEY_LOCAL_MACHINE\Software\PP-COM\MRS and in the corresponding subkeys.

Depending on the installed system, saving further registry parts is reasonable. Under HKEY_LOCAL_MACHINE\SOFTWARE\Siemens for example you find the corresponding settings for Cornet-N or Cornet-NQ, D-channel protocols used by Siemens.

Since these data cannot be directly saved, they need to be exported from the system registry to files. These files can be saved with the rest of the data.

- **User and system data (correlation database)**

- Message database (journal database)**

- Since these databases are exclusively open through the server, a backup of these files is not possible with a running server. For this reason data to be saved need to be exported. This export file can then be saved as usual with a backup program.

- The export is already regularly performed via the Maintenance Script. See also the MTA configuration.

- **Personal greetings and other user specific data**

- These are stored in the share \\<Server>\MrsUserData\$ and in the corresponding subdirectories. They are saved in this share by way of a backup of all files and directories.

- **Documents**

- All documents are stored in the share \\<Server>\MrsFolders\$ and in the corresponding subdirectories. They are saved in this share by way of a backup of all files and directories.

- **Program files**

- Program files are found in the directories \<Install>\MRS\Bin, \<Install>\MRS\Monitor and \<Install>\MRS\SDKTools. With a new installation they would be automatically recovered. In order not to lose corrections implemented in the meantime we recommend to save these directories as well.

3.10.2 Implementation Suggestion

This suggestion on the implementation of the above concept is restricted to the basic process with simple means that should be available on each system.

A maintenance script job is used for backup control. This may appear as follows:

FullBackup

```
{
  Periodicity = 24h@1:00
  Task
  {
    Execute cmd=$(ScriptDir)\regbackup.bat
    Export Record=FULL file=$(Backup)\fullexp.exp
    Execute cmd=$(ScriptDir)\fullbackup.bat
  }
}
```

This script is performed every 24 hours at 1 a.m. and consists of three tasks:

- Executing the file `regbackup.bat`
- Full export of the InfoStor databases
- Executing the file `fullbackup.bat`

The batch processing file `regbackup.bat` saves the settings stored in the registry to single files. The second call of `regedit` serves here as example of further registry parts to be saved. `logserv` generates an entry in the standard protocol of the MRS monitor.

`regbackup.bat`:

```
logserv script=FullBackup msg="regbackup.bat started."
regedit /e LW:\siemens\xpr\backup\regexp_serverconf.reg
        HKEY_LOCAL_MACHINE\SOFTWARE\PP-COM\MRS
regedit /e LW:\siemens\xpr\backup\regexp_<Other>.reg
        HKEY_LOCAL_MACHINE\SOFTWARE\<Other>
logserv script=FullBackup msg="regbackup.bat finished."
```

After exporting the registry the database export is started. Not until its accomplishment the batch processing file `fullexport.bat` is exported.

`fullexport.bat`:

```
logserv script=FullBackup msg="fullbackup.bat started."
SET FullBackup=\\BACKUPSERVER\SHARE
NET USE %FullBackup% <Password> /user:DOMAIN\BACKUPUSER
IF ERRORLEVEL 1 GOTO ERROR
IF EXIST %FullBackup%\fb6.bkf DEL %FullBackup%\fb6.bkf
IF EXIST %FullBackup%\fb5.bkf MOVE
    %FullBackup%\fb5.bkf %FullBackup%\fb6.bkf
IF EXIST %FullBackup%\fb4.bkf MOVE
    %FullBackup%\fb4.bkf %FullBackup%\fb5.bkf
IF EXIST %FullBackup%\fb3.bkf MOVE
    %FullBackup%\fb3.bkf %FullBackup%\fb4.bkf
IF EXIST %FullBackup%\fb2.bkf MOVE
    %FullBackup%\fb2.bkf %FullBackup%\fb3.bkf
IF EXIST %FullBackup%\fb1.bkf MOVE
    %FullBackup%\fb1.bkf %FullBackup%\fb2.bkf
```

Server Administration

Backup

```
IF EXIST %FullBackup%\fb.bkf MOVE
    %FullBackup%\fb.bkf %FullBackup%\fb1.bkf

LW:\WINNT\system32\NTBackup.exe backup
    "@LW:\<Install>\res\maint\fb.bks" /v:no /r:no /rs:no
    /hc:off /m copy /j "FullBackup" /l:s /f
    "%FullBackup%\fb.bkf"

NET USE %FullBackup% /DEL

GOTO FINISH

:ERROR

logserv script=FullBackup msg="Network share not found!
    fullbackup.bat aborted!"

:FINISH

logserv script=FullBackup msg="fullbackup.bat finished."
```

In this example data are saved to a server in the network. To save the files, NTBackup is used.

First comes a log-in at a share installed on a server for backup purposes. Since the maintenance script runs under a local system account per default, a user, having privileges on the server, and a password are to be specified here. Through generation of a backup user account and restrictive privilege setting of the fullbackup.bat file, the risk of misuse can be minimized.

Furthermore, available backup files are renamed. Consequently you receive a backup over a desired period. The oldest file is deleted.

Subsequently NTBackup.exe is executed. Please gather the parameters specified in the example from the NTBackup documentation (ntbackup /?). Changing the parameters enables an incremental or differential backup as well as a backup to another medium. Which files are saved by NTBackup is stated in the fb.bks file.

fb.bks:

```
LW:\<Install>\Bin\
LW:\<Install>\Monitor\
\\<Server>\MrsUserdata$\
\\<Server>\MrsFolders$\
LW:\<Install>\Backup\regexp_serverconf.reg
LW:\<Install>\Backup\regexp_<Other>.reg
LW:\<Install>\Backup\fullexp.exp
```

The `fullbackup.bks` file can be created with a normal editor but must be saved with the Unicode coding to be legible for NTBackup.

4 Services on the MRS Server

All available services provided by the MRS Server will be described in the following sections. Configuration of the various services is done using the APL settings dialogs found in the MRS Monitor. Specific configurations will be described in Chapter 6 of this manual.

4.1 Telematic Gateways

4.1.1 Analog Connections

These services are realized through the implementation of the V.24APL. A description of the configuration procedures is provided on page 229ff of this manual.

4.1.1.1 Fax G3 and Fax G3 Polling

This protocol enables the transmission of Fax Group 3 documents. The Fax G3 protocol must be installed and coupled to at least one modem in the V.24 APL. Configuration of the Fax G3 protocol starts in the **Identification** tab of the V.24 APL. In this dialog, a global identification and headline can be entered. If an individual user requires an identification or headline different to that of the global, these would be entered in the data fields **FaxG3-ID** or **FaxG3-HeadLine** of the user database.

An extension number (in an international format) must be entered in the field **FAXG3#** for every user in the user database. Incoming fax documents cannot be routed if this entry is not present. This number is internally normed and transcribed to the field **FAXG3** for use by the MRS Server. Example: The number +49-1234-5678-90 is internally transcribed to 491234567890.

In the MRS Client transmission is possible via entry of the destination number with simultaneous selection of the service Fax G3 in the send dialog. It is also possible to select the service Email, and enter the address as **FAXG3/ <Number>**.

Example:

```
491234567890
FAXG3/491234567890
NVS : FAXG3/491234567890
```

The last address in the example is the complete address in a MRS format. This kind of address is generated e.g. by a Mail Gateway when a Fax G3 document is transmitted.

Similarly, it is also possible to poll a fax from a Fax-on-Demand Server by entering the corresponding polling number. In the MRS Client, select the option **File→Poll** and enter

the dialing number of the desired document as address for the selected service **Fax G3 Poll**. The FAXG3REV protocol must also be enabled in the V.24 APL for this service.

Example: 071117864040

When a fax document is to be polled over an email gateway, the fax number of the document as well as the service and the mandatory address element **NVS:** must precede the number.

Example: NVS:FAXG3REV/491234567890

For fax reception a unique number must be assigned to each user in the field FaxG3 of the user database. As for all telematic numbers used by the MRS Server, this number must be entered in international notation.

Since the V.24 APL is purely analog, extension numbers cannot be assigned to individual users within the V.24 APL. Inbound fax documents are therefore routed to the recipient who was entered in the V.24 APL configuration (Postmaster, secretary, etc.), who later distributes these to the individual users.

4.1.1.2 SMI Transport (Remote System Links)

The SMI Transport protocol is used for communication between the MRS Server and MRS Clients. If a connection to the server is made either through a modem or over a serial cable, then the SMI transport protocol must also be coupled to one of these devices. The connection of several servers is possible through the use of the SMI protocol. This type of connection is referred to as a “Remote System Link”.

Remote System Links must be configured in the MTA configuration dialog (found in the Module window under Settings in the MRS Monitor) prior to its activation. The Remote System Link address is given as follows:

Example: NVS:MODEM/491234567890

The frequency (in seconds) at which connections to the MRS System are made must also be entered. This could for example be every 43,200 seconds. Therefore, twice daily (or every 43,200 seconds) a connection is established via modem to the MRS Server. Subsequently, an automatic coupling of all logical lines from the other system is initiated. For more detailed information see page 184ff.

It should be noted that lines imported over a remote system link from another MRS Server are unidirectional. A bidirectional link between two servers is only possible when a Remote System Link is executed by both servers to the other.

Two methods of validation are possible:

- Users are entered in the database of both systems. In the database of the remote system an additional data field is configured for the name of the remote MRS Server. A data field is also created for each user in the remote system with the

account name of the user. The user's account name is also inserted in the new data field. The server now recognizes the user, and will correspondingly route messages in accordance with assigned authorities.

Example:

Two MRS Servers (BRUSSELS and AACHEN) are connected to one another by a Remote System Link. The user database from BRUSSELS is expanded with the data field AACHEN, and in AACHEN with the data field BRUSSELS.

If user HUGO in AACHEN wants to send a message to a user in the BRUSSELS system, this message would be routed to the recipient on the system BRUSSELS, because of the database entries

Database field	Contents
USER	HUGO
Group	USER
Aachen	HUGO

the user HUGO is recognized on the BRUSSELS system, and through the group assignments has the authority to send messages.

The disadvantage to such a method is that user data in both systems must be maintained parallel to one another.

- The second method is through the use of pseudo user accounts on both systems. Both these accounts are assigned "Trusted Domain" group privileges, and each pseudo account is assigned the name of the other remote system. Example: The pseudo account on BRUSSELS is assigned the name AACHEN and vice versa. In addition to Trusted Domain group privileges, the pseudo account must also be granted the same privileges as those of a user on that system.

Example:

Two systems (BRUSSELS and AACHEN) are connected by Remote System Link. On the system BRUSSELS, a user is configured:

Database field	Contents
USER	AACHEN
Group	USER

Likewise, the system in AACHEN has the user:

Database field	Contents
USER	BRUSSELS

Database field	Contents
Group	USER

In addition to the authorities of the group USER, both users are assigned the “Trusted Domain” privilege, so that authority of these users is inherited by all incoming documents of the remote system.

The assignment of a password is not necessary and in this case not desired. MRS does not allow the log-in of users without a password. The pseudo-user cannot be used as a real account.

4.1.1.3 GSM Script (CIT, SMS)

Further protocols can be coupled to GSM (General State Machine) scripts. Delivered Scripts include MWI (Message Waiting Indication) for the Siemens Hicom PBX, email connection through Compuserve, and SMS (Short Message Service) transmissions.

CIT over the Siemens Hicom PBX

A Message Waiting Indication (MWI) is sent through the corresponding service of the Siemens HICOM PBX for new inbound messages. In the user database field CIT an entry for this service must be present and the extension number of the telephone to where the MWI is to be sent.

Example: CIT_BASIC/432

Short Message Service (SMS)

This service enables the sending of short text messages (up to 160 characters) to cellular phone users in GSM networks. These messages appear on the LCD display of the cellular telephone. Messages can also be transmitted during a telephone conversation. When the cellular phone is switched off, messages are stored for up to 48 hours by the cellular network providers. No additional costs are incurred by the receipt of SMS messages.

Notification of incoming messages can also be sent (CIT) by the MRS Server to cellular users through SMS messages. In the database field CIT a reference to the SMS field is entered. This field contains the cellular telephone number of the user.

Database field	Contents
CIT	SMS
SMS	49171567890

Alternatively, the cellular telephone number can be entered in the field CIT.

Example:

Database field	Contents
CIT	SMS/49171567890

In the case of an incoming message the user would receive a short message such as: “Sername: Message from Joe User received at 14:34.” If a fax message is received, the name of the sender would only be included if contained within the alias database, otherwise the fax ID would be transmitted in the SMS message.

In the case of CIT over SMS, the signal is not reset by message receipt.

4.1.2 Integrated Services Digital Network (ISDN)

This service is provided by the ISDN APL. A description of the configuration is found page 115ff.

4.1.2.1 Fax G3, Fax G3 Polling

This protocol enables the transmission and receipt of Fax G3 documents as well as the polling of documents from Fax-on-Demand servers. The operation and addressing from the client over a mail gateway is the same as described above. See page 57ff for the analog realization of this protocol.

If the fields FaxG3-ID or FaxG3-Headline are set in the user database, then this data will be used with fax transmissions. If not set, the global value from ISDN configuration would be used. For these services an ISDN card with an analog fax module (fax piggy) is required.

Fax Forward Protocol

If the MRS Server is to be employed as a fax concentrator, then the Fax Forward protocol would be used. Example: all outbound fax traffic from a fax device is to be managed by the MRS Server taking advantage of Least Cost Routing, or a distribution list triggered by a fax in the MRS Server.

This has several technical and organizational consequences:

- How is the sender to know that the fax has reached the recipient at two in the morning?
- Which fax ID should the recipient receive? That of the MRS Server or of the internal fax device?

Various possibilities provide a solution to these problems. Currently the MRS Server supports two different Fax Forward modes:

1. Fax Forward transparent mode (FFORWT). In this mode the MRS Server is invis-

ble to the fax recipient. The structure is as follows:

- The internal fax device sends a fax to the MRS Server, whereby the Server also receives the external recipient number.
 - MRS accepts the fax and assumes the fax ID of the sending device.
 - Through the fax ID of the server the internal device receives the MRS message ID as reference number.
 - Through the use of routing rules, the buffered fax is sent at a predetermined time to the external recipient. The fax contains the original ID of the internal fax device and no header is inserted. The fax document remains un-changed and has no second fax header.
 - After successful transmission of the fax document, the server sends a fax-receipt to the originating device (optional). The receipt contains various information: Transmission date, time, recipient ID, charges, etc.
 - If delivery of the document is not possible a fax-receipt is sent to the originating device (optional). Reason for non-delivery are contained within the fax-receipt.
2. Fax Forward server mode (FFORWS). In this mode external recipients see only the MRS Server and not the internal originating device. The procedure is the same as the FFORWT mode with the exception of:
- The header of the originating device is removed by the MRS Server. By the transmission of a fax document the ID and header of the MRS Server is inserted into the document. From the perspective of the external recipient, the document is from the MRS Server.

In order to activate a Fax Forward mode, add one of the Fax Forward protocols and create an extension range in the numbering plan for all possible external numbers. The option **Variable Length** should also be checked, so that external addresses of any length can be used. Additionally, a *Routing Rule* must be created that routes transmitted fax documents to the concentrator (see *MRS System Architecture*). Example:

```
NVS: FFORWS. */4924041234547* [FLAG!=FLAG1]=  
NVS: FAXG3/* [FLAG=FLAG1; DEFER=2:00]
```

In accordance with this rule, all incoming fax documents with the prefix 47 and whose FLAG1 is not set, would be rerouted at 2:00 and the prefix 47 removed. Simultaneously FLAG1 is set, so that normal extensions that begin with the prefix 47 would not be continually processed.

Since the ISDN APL uses internationally normed dialing numbers by default, the individual extension must precede the Fax Forward prefix in international format in the above routing rule. The required extension is the OAD assigned to this protocol in the ISDN configuration.

In the above example the connection number is 49-2404-12345. Without the international dialing mode the *Routing Rule* would have the following appearance:

```
NVS:FFORWS.* /47*[FLAG!=FLAG1]=  
NVS:FAXG3/*[FLAG=FLAG1;DEFER=2:00]
```

Essentially, through the use of the prefix as selection criteria, an almost unlimited range of conversions is possible. In the above example the fax is internally sent to the example number 4701234567890, which is then sent by the MRS Server at two-o'clock in the morning to the number 01234567890. If the portion of the *Routing Rule* DEFER=2:00 was excluded, the fax would then be immediately rerouted.

4.1.2.2 Fax G4

This is the digital fax version. With ISDN, fast transmission rates and high resolutions (200x200, 240x240, 300x300 and 400x400 dpi) are possible. If the field FaxG4-ID is set in the user database, then this data would be used with all fax transmissions. If not set, the global value from ISDN configuration would be used.

The extension number (in an international format) must be given in the field FAXG4# for every user in the user database. Incoming fax documents cannot be routed if this entry is not present. This number is internally normed and transcribed to the field FAXG4 for use by the MRS Server. Example: The number +49-1234-5678-90 would be internally transcribed to 491234567890.

Since the type of service can be differentiated through the ISDN Service Indicator, this extension may be the same as that of fax G3.

Since fax polling for fax G4 is not possible, there is no protocol provided for this service.

In the MRS Client, sending is possible by entering the destination number with simultaneous dialing of the service fax G4 in the send mask. Email can also be selected as service and the dialing data FAXG4/<Number> entered.

Examples:

```
491234567890  
FAXG4/491234567890  
NVS:FAXG4/491234567890
```

The final version of the address is the complete address in MRS format. This version is created e.g. by a Mail Gateway when a fax G4 document is to be sent.

4.1.2.3 Euro File Transfer

MRS can act as an EFT-Server and Client.

EFT Server

The EFT Server is a personal Euro file transfer mailbox (directory on the Server), which must be configured for the MRS user by the administrator, through the allocation of an EFT extension number. When files made available by the user are passively transmitted (polled by another user from the EFT mailbox) or received, an appropriate journal is made. The file sent to this number is then automatically delivered to the user.

With passive reception, the user subsequently sees the files received quite normally in the inbound journal. Technically, these are copies of the files received, which as with any other document, would be automatically deleted by the Server.

The original incoming files remain in the Euro file transfer mailbox, which is normally the guest directory, unless another directory has been explicitly created for the user.

Important:

If the EFT originator has the corresponding authority, they can overwrite or delete files in these directories!

With passive transmissions, available files are polled from the Euro file transfer mailbox. Files are made available by copying them to the directory in which the EFT partner will access. This is accomplished through the use of the Server file manager of the MRS Client. The MRS user must have the appropriate authority for use of the file manager.

It is also possible for the user to make these files available without this authority by transferring the files to their own extension with the EFT Client and so using the same directory (mailbox) as that of the EFT partner. The file is now in the corresponding directory in which the EFT partner has access.

The directory in which the EFT partner accesses depends on whether they have an EFT account (user name and password) or not.

If the EFT partner has no account, they would only have limited access to the guest directory (...\\Userdata\\EFT\\Guest). Normally a guest cannot modify files (rename, delete, etc.). If recipients are only to view files made available to them, they must have an account in the user database.

If an EFT account is used, it is read as an MRS user and the authority validated with the user database of MRS. In this case, the remote EFT user accesses a private directory specifically assigned to them. The name of the directory is automatically formed from the user's account name.

Authorities must be assigned through the user administration. There are five authorities: send, receive, overwrite, delete, and rename.

Important:

A remote EFT partner with extended authority and an account who wishes to dial-up the MRS Server must be entered in the user database.

The EFT Server supports all Navigation Services, i.e. it also makes sub-directories available. Only few EFT Client Programs are able to switch to sub-directories, e.g. not even the EFT Client Service in MRS. It is therefore only appropriate to make sub-directory files available if you are sure that the correspondent is using an appropriate EFT Client.

EFT Client

Using the MRS Client, files can be actively sent and received per Euro file transfer, provided that the MRS user has the necessary authority. This authority is recognizable when in the polling dialog, the services “EFT Request” or in the send dialog “EFT” is visible.

To actively send a file select the menu entry **File→Send**. The file is then selected and confirmed by selecting the **Open** button. The dialing number of the remote EFT Server is entered in the **Address** field of the dialog and the service “EFT” selected. In the out-bound journal the corresponding entry appears at the completion of the transaction. An EFT account (name and password) that is required for access to the remote server can be optionally entered in the subject field and separated by a slash (/). The slash is also required when an empty password is entered.

If the remote EFT Server is an MRS System, this would then be interpreted as an MRS Account.

The file must be sent via a Mail Gateway to `NVS:EFT/<Number>`.

For actively receiving files, the menu option **File→Poll** must be selected in the MRS Client as well as the Service “EFT Request”. The number of the remote EFT Server is entered in the poll dialog and the name of the desired file in the “Subject” field. The file is then polled from the remote server by the MRS Server. Optionally, the account initiating an active transmission can be appended behind the filename, with the same syntax as above for active transmissions and separated by a comma. If the filename is omitted, the directory of the remote server will be queried.

The result of polling procedures is found in the inbound journal via the answer references.

The address mode for an EFT file polling via a Mail Gateway is `NVS:EFTREV/<Number>` with the name of the file desired in Subject, as described above.

4.1.2.4 ISDN SMI Transport (Remote System Links)

The ISDN SMI protocol is used for the internal communication between MRS Servers and clients (16 Bit clients under Windows 3.11 only). This must also be installed if a server connection is to be made over ISDN. The connection of numerous servers over the ISDN SMI transport protocol is also possible (Remote System Link).

In order to activate a Remote System Link it must be configured in the MTA, and the MRS Address of the remote system given as follows:

NVS : ISDNSMI/491234567890

The frequency must now be entered in seconds, at which the connection is established. This could be for example 86400 seconds. So that once daily an ISDN connection is established to the MRS Server, and an automatic coupling of all logical lines of the other system is performed. Further options can be found on page 184ff.

Additionally, an appropriate ISDNSMI entry must be made in the call numbering plan of the ISDN APL. For this purpose an extension number should be entered for the ISDN SMI transport that is to be used for Remote System Links. At the remote system an entry should also be made to ensure the correct delivery of reports.

The validation steps listed on page 58ff for analog server coupling apply here also.

4.1.2.5 ISDN Voice (Playback)

The ISDN voice protocol is used for the playback of voice mail messages via the telephone. In most cases this protocol is called directly by the MRS Client.

4.1.2.6 Short Message Service (SMS)

Enables sending messages of up to 160 characters to mobile telephones in the mobile networks. The messages appear on the mobile phone display.

Addressing and operation is done through the client or a mail gateway. Otherwise the same applies as for the analog realisation of the protocol (See page 60).

4.1.2.7 Fax-on-Demand Server

The **Fax-on-Demand Server (FOD.e)** E-script offers three modes for fax polling and to store Fax-on-Demand documents:

Normal Mode:

- Direct fax document polling with the telephone without DTMF entries.
Dial the document's extension number via telephone and the fax to be polled is subsequently diverted to a fax device or a fax calling number.

- Direct fax polling from a fax device in fax reverse polling mode.

Dial the document's extension number at the fax device and subsequently press the start button to start fax polling.

DTMF Mode:

- Fax polling with the telephone via document selection per DTMF entry.

Dial a DTMF access number on the telephone. When the connection has been established you are prompted per voice menu to enter the extension number(s) of one or several fax documents. Thereafter you are asked to press the start button at your telephone/fax combination or to divert the fax document to another fax calling number.

Supervisor Mode:

- Filing, renaming and deleting Fax-on-Demand documents via DTMF entry.

A specific access calling number and a (PIN) take you to the administrator area where administrative functions can be executed per voice menu.

The Fax-on-Demand server requires the setting of the corresponding E-script in the Telematic APL (ISDN APL). The default settings (unconfigured script) only enable the user to use the normal mode.

Direct Fax Polling per Telephone (Normal Mode)

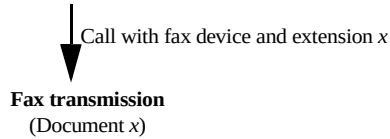
In this mode documents are selected on grounds of the dialed extension number. The number of pollable fax documents is restricted by the service provider's allocation of calling numbers that limits the extension's number of digits. For each possible extension number assigned to the Fax-on-Demand script in the number plan, a corresponding fax document must be deposited.

The caller does not need a DTMF compatible telephone. The extension number of the Fax-on-Demand document is dialed per telephone and when a fax tone becomes audible at the receiver, the document is manually diverted to the fax device's calling number or a fax calling number.

Direct Fax Polling from a Fax Device in Fax Reverse Polling Mode (Normal Mode)

Just with direct fax polling via telephone, document selection with direct fax polling per fax device in fax reverse polling mode occurs by the dialed extension number. Consequently the number of fax documents that can be deposited is also limited by the service provider's calling number allocation.

For each possible extension number assigned to the Fax-on-Demand script in the number plan, a corresponding fax document must be deposited.



The extension number of the Fax-on-Demand document is dialed at the fax device and when a connection has been established the start button needs to be pressed.

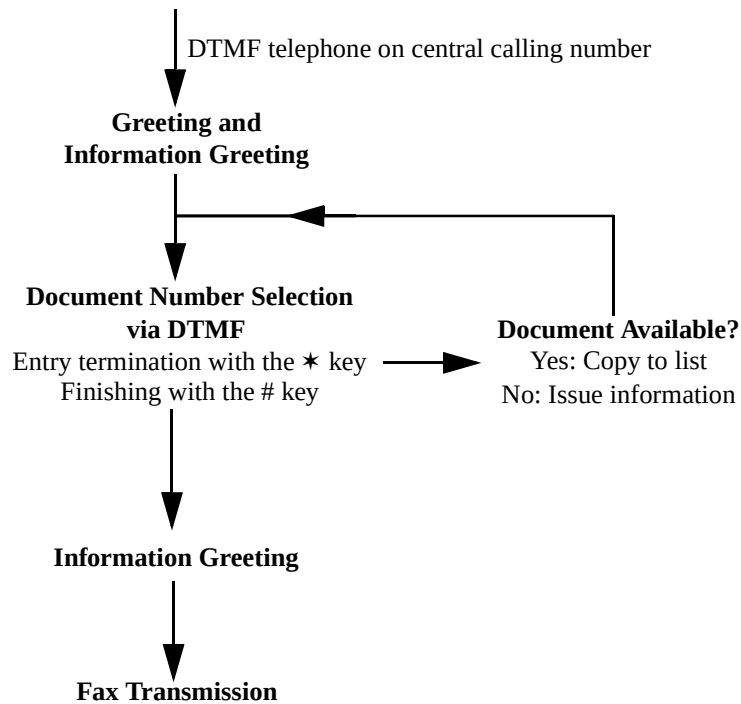
Fax Polling per Telephone via DTMF Entry (DTMF Mode)

In this configuration version you only need a central calling number for the Fax-on-Demand server to take you to a voice menu. The central calling number is entered in the Fax-on-Demand script's configuration dialog (see page 130).

The voice menu enables the caller, after a greeting, to select documents via DTMF entries.

The advantage of this version is that an arbitrary number of documents can be stored and the document number may have an arbitrary length. Besides that the caller can poll any number of fax documents during a call since they can be selected one after another in an entry loop. As soon as all desired documents have been selected, fax transmission can be started via the # icon. Finally only the start button needs to be pressed at the telephone/fax combination. If no fax device is available, the document can be diverted to a fax calling number.

Here as well the pollable documents are stored as `mr s<n_1> . fax` (default setting).



Depositing Fax-on-Demand Documents

The documents to be polled must be stored in the *<MRS System Path>\userdata\fod* directory. They must be available in the fax G3 format as generated e.g. by the fax printer driver of the MRS Server or MRS client. The file names always begin with the “mrs” prefix, then comes the document’s extension number followed by the suffix “fax” (e.g. mrs500.fax).

The Fax-on-Demand script also enables the specification of an alternative suffix if you want to store the documents e.g. as *.FG3. This requires the modification of the setting **Fax document names** in the **Documents** tab of the script’s configuration dialog.

There are two options to deposit Fax-on-Demand documents:

- Files can be directly sent to the virtual file system of the MRS Server. Those for a Fax-on-Demand system are automatically converted in the desired fax format.

The MRS Server knows the address *NVS:<Script Name>/<Extension>* (Fax-on-Demand file in the MRS fax G3 format). *<Script Name>* is the script denomination assigned to the Fax-on-Demand script in the configuration dialog (see page 132). *<Extension>* is the desired calling number under which the fax can be polled.

Example:

NVS:FOD/399

- Filing a Fax-on-Demand document via the supervisor mode.
This method is described on page 70.

Supervisor Mode for Administration

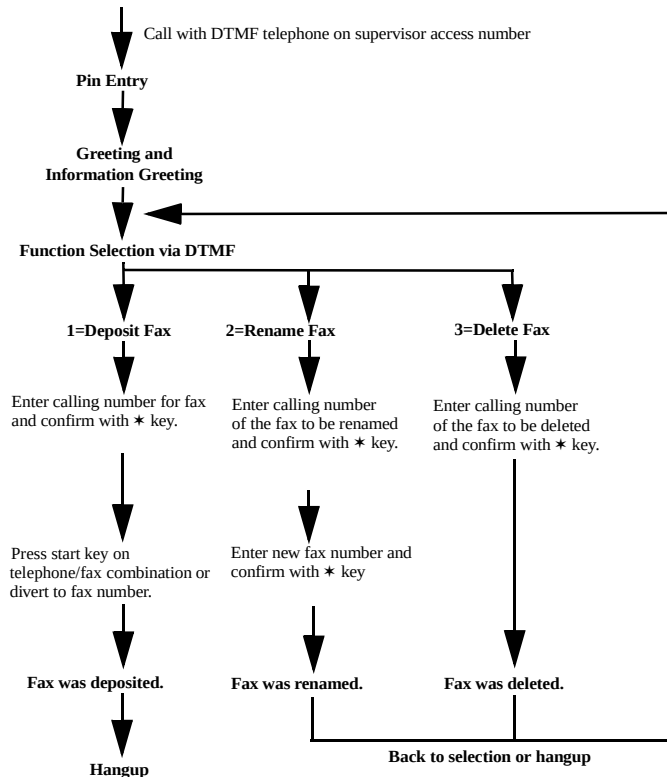
Via a calling number defined in the configuration of the Fax-on-Demand script (see page 133) you reach the supervisor mode. This calling number is taken from the number plan of the Fax-on-Demand script so that under this number no fax document can be polled.

To access the supervisor mode you need to identify yourself by entering a PIN after dialing the access number. The number of login attempts can also be specified in the configuration dialog. After a successful login you are taken to the supervisor menu where you can

- deposit (key 1),
- rename (key 2)
- and delete (key 3)

Fax-on-Demand documents.

The following diagram shows the use of a voice menu.



Depositing a Fax-on-Demand Document (Key 1):

With key 1 you can file Fax-on-Demand documents. The voice menu prompts you to enter the calling number under which the Fax-on-Demand document is to be stored. Entry of the calling number is accomplished with the * key. Subsequently you need to press the start key at the telephone/fax combination. The document is provided in the folder `<MRS System Path>\userdata\fod` in the syntax `mrs<Calling Number>. fax` for fax polling.

Renaming a Fax-on-Demand Document (Key 2):

With key 2 you can rename a Fax-on-Demand document. The voice menu prompts you to enter the calling number of the Fax-on-Demand documents that is to be renamed and to conclude this entry with the * key. Subsequently you need to enter the new calling number and finish this entry with the * key as well. The Fax-on-Demand document is now stored in the folder `<MRS System Path>\userdata\fod` under the new calling number. Now you can return to the selection menu.

Deleting a Fax-on-Demand Document (Key 3):

With key 3 you can delete a Fax-on-Demand document. The voice menu prompts you to enter the calling number of the Fax-on-Demand documents that is to be deleted and to conclude this entry with the * key. The selected Fax-on-Demand document is now deleted from the folder <MRS System Path>\user data\fod. Now you can return to the selection menu.

4.1.2.8 Standard Voice/Fax Mailbox

Standard Voice/Fax Mailbox

This Script acts as the personal telephone answering machine for users in which received voice mail messages can be played-back.

Depending upon the selected options (see page 126), and the available hardware, they could:

- process received fax documents and reroute e.g. to a fax device
- process email messages and reroute as a fax or apply text-to-speech for email reading
- administer distribution lists and send messages to them
- return calls directly using callback functions
- change the spoken language of the Script to e.g. French

The complete menu structure with all selectable options can be seen in the manual *Standard Voice/Fax Mailbox*.

4.1.2.9 CIT over ISDN Voice

Message Waiting Indicator (MWI) signals can be transmitted over the ISDN voice protocol with the Integral telephone system from Bosch Telekom. For this purpose two numbers must be configured in the PBX for setting and resetting MWI signals.

The entry VOICE/<telno> can now be entered in the field CIT of the user data base to set the signal. The entry <telno> is the internal number used for the switching sequence. This number is followed by the extension number to which the signal is to be sent.

In order to reset the signal an additional data base field XCIT, must be inserted into the data base. The entry VOICE/<telno2> is the internal number used for the resetting sequence and is followed by the extension number.

Example:

Database field	Contents
CIT	VOICE/9500543 The sequence 9500 is programmed as the switching sequence for the Integral PBX and the Message Waiting Indicator would be sent to the extension 543 by incoming messages.
XCIT	VOICE/9501543 The sequence 9501 is programmed as the reset sequence for the Integral PBX. The Message Waiting Indicator is reset for the extension 543.

These protocols send a voice message to the extension entered here. This message is ignored by the Integral PBX and only the number is evaluated.

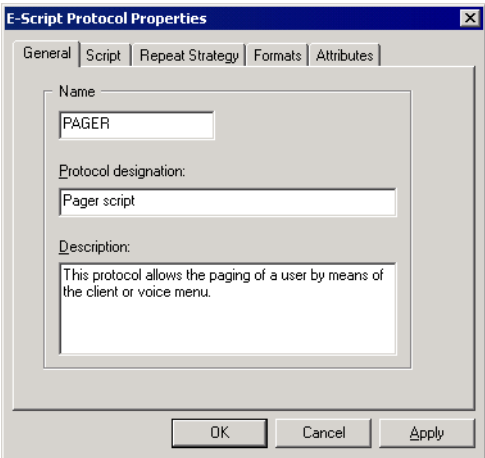
These voice messages can be used for general applications when the data base field CIT contains the entry VOICE/<telno>. The entry <telno> is the extension to where the voice message is sent.

The CIT must be switched on during the installation of the MTA so that it is active.

4.1.2.10 The Pager Protocol

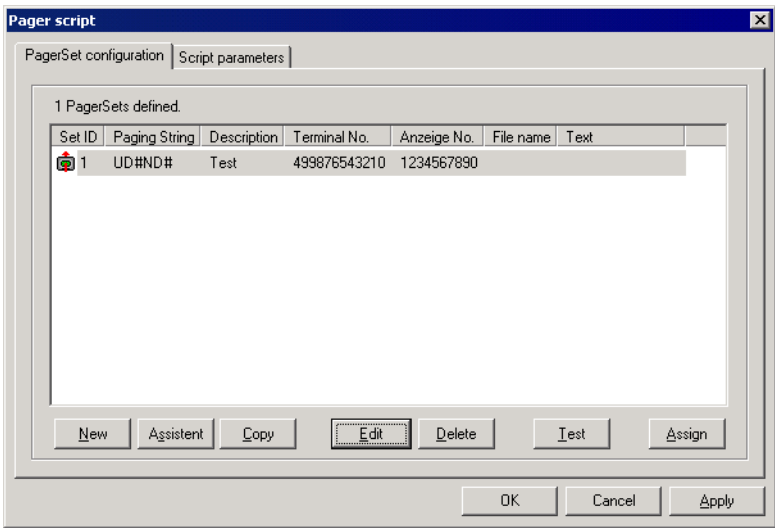
A pager is a notification receiving device. Simple models respond by emitting an acoustic signal only whereas more sophisticated ones display a number for a return call on a display or receive a voice message. For these pager services providers are available, offering the corresponding service. For the pagers registered with them, the providers enable access via a paging terminal that can be called to address the desired pager in a certain way. This type of addressing differs from paging terminal to paging terminal so that it needs to be configured each.

First add the pager protocol as E-script. Enter **PAGER** as name since this is the default protocol name that, with the corresponding configuration via the WebAdmin, is used by the Notification APL for notifying the pager.
 You can also bind the protocol to an extension number so that you can trigger a call to a configured pager via a Telephone User Interface (TUI).



Via the Script tab and the **Parameter** button contained therein you reach the actual protocol configuration tab.

Since there are many types of paging terminals and



the access mechanism is not standardized, you need to first configure the DTMF sequence for the desired service provider and its paging terminals. This pager configuration is called PagerSet. We recommend to use the assistant described in the following for the configuration.

Assistant

The following questions result in a paging string which determines the type of access and the type of data transmitted to the paging terminal.

First a **Description** or a name is required for the PagerSet.

The paging string determined by the assistant comprises the following elements:

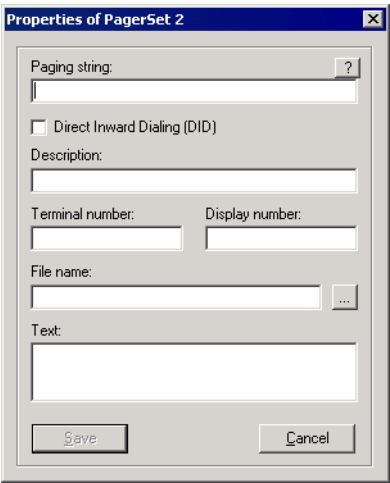
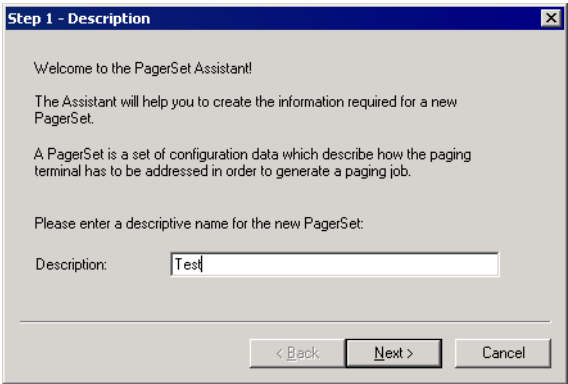
Element	Significance
M	Terminal number
U	User pager number
N	Display number
P	Sound file
D	Delay/short pause
0-9#*	DTFM tone

Without the assistant you can also create a new PagerSet via the **New** button or copy one from an existing PagerSet by means of **Copy**. **Edit** serves for modifying an already created PagerSet. Pressing any of these buttons takes you to the opposite dialog.

Here you can directly enter the **Paging string** using the elements described in the above table. The **File name** refers to a voice file that is to be transmitted to the pager. You can optionally enter a text as well. This text is then, via Text-to-Speech, converted into the voice message to be transmitted.

Display number is the return call number to appear on the pager display.

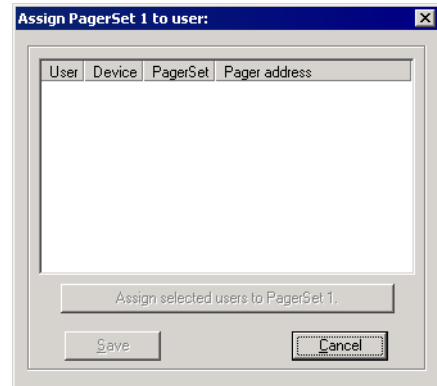
Activating the **Direct Inward Dialing** option dials the pager number along with the paging terminal access number so that it is not an element of the paging string.



Assigning PagerSets to Users

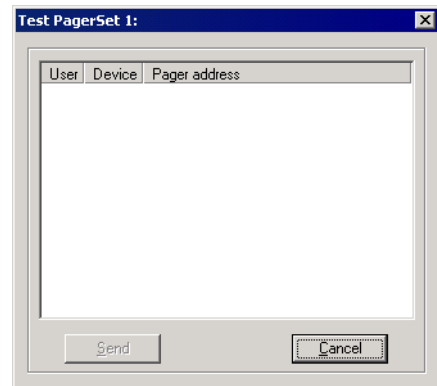
After defining the PagerSets you can click **Assign** to assign these to the individual pager users. Each user with a pager address is displayed here and you can select those reachable via this PagerSet to assign them to the PagerSet with a click on the **Assign** button.

Accomplish the process with **Save**.



Testing PagerSets

Click the **Test** button to display the users assigned to a PagerSet. Now you can select these and perform a notification test via the **Send** button.



Script Parameters

The screenshot shows a window titled 'Pager script' with two tabs: 'PagerSet configuration' and 'Script parameters'. The 'Script parameters' tab is active. It contains several sections: 'Paging options' with a checkbox 'Check originator for pager privilege'; 'Paging parameters' with input fields for 'Length of a delay (in 1/10 s):' (5), 'Length of a DTMF tone (in ms):' (100), 'Pause after one DTMF tone (in ms):' (100), and 'Enter the number of delays (see above) that are to be used as start delay:' (2); 'Voice menu options' with checkboxes 'Allow paging via voice menu' and 'Use telephone display', a numeric input 'Paging(s) per call' (1), and a dropdown 'Menu language:' (English (US)); and 'Customer specific parameters' with a text area and a note: 'Note: Non-recognized parameters will not be displayed when the configuration is called again.' At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Paging Options

By means of **Check originator for pager privilege** the originator of a pager notification is checked for having the *Paging Privilege*. When this option is inactive, everybody is permitted to notify a pager user with a beep.

Voice Menu Options

When you activate the **Allow paging via voice menu** option and an extension number has been assigned to the pager protocol, this number can be dialed and a notification sent via TUI. The **Use telephone display** option simplifies TUI usage for internal users. This requires telephones supporting this option.

With n **Paging(s) per call** you can restrict the number of pagings to occur with a call.

The last option in this section enables setting the TUI **Menu language**.

Paging Parameters

These are special parameters for setting the length of the delays used in the PagerSet and of DTMF tones. Modifying the default values should not be necessary.

4.2 Email Gateways

In most cases all document types can be transported through email gateways. Fax documents as well as voice messages can be sent as email.

4.2.1 Microsoft Exchange

Please refer to the manuals *MRS and Microsoft Exchange*, *MRS and Microsoft Exchange 2000* and *Outlook Extensions*.

4.2.2 Lotus Notes

Please refer to the manuals *MRS and Lotus Notes – Administrator Manual* and *User Manual*.

4.2.3 Internet Mail

SMTP (Simple Mail Transfer Protocol) defines an international standard for email transmissions within the Internet. Messages are exchanged worldwide in a 7 Bit ASCII code.

An extension of SMTP is MIME (Multipurpose Internet Mail Extensions) in which arbitrary data (images, voice mails, binary files, etc.) is transmitted through SMTP.

Since there are numerous extensions to the SMTP protocol, the term ESMTP (Extended Simple Mail Transfer Protocol) is generally used in association with Internet mail. Among these extended services, Delivery Status Notification (RFC 1891) is supported by the SMTP APL so that, depending on the server, delivery reports are sent to the message recipient.

Another ESMTP feature is the AUTH-Token which serves to authorize the SMTP originator by means of a password. Via this AUTH-Token the connected client is informed that the SMTP server has this feature and the client can thus use it.

For the CRAM-MD5 process the SMTP APL needs to know the password in the clear text. This, however, is not possible with the default database entry `PASSWORD`. Therefore the database `POP-PASSWORD` is used here which should be added to the user database with type `CIPH`, `CHAR` and a reasonable password length (approx. 40 characters) when the above feature is employed. With the `PLAIN` and `LOGIN` processes, the entry `PASSWORD` is used alternatively to a not existing or empty `POP-PASSWORD` database field.

Please note that a possibly desired authorization as regards the SMTP server in the Netscape Messenger cannot be explicitly configured. The Netscape Messenger uses the automatic `PLAIN` process if it is offered. In the event that no explicit authorization per password is desired, the `AUTH` function must be switched off via the registry.

4.2.3.1 POP3 and IMAP4 Servers

SMTP always attempts to deliver the messages directly to the recipient. Since the majority of computers are not in continuous operation, and few are directly connected to the Internet, the POP3 (Post Office Protocol Version 3) Server acts as an intermedi-

ate storage facility until POP3 clients pick-up their mail. Generally, when mail is queried by a POP3 mail client the mail is transferred to the client's computer.

The IMAP4 (Internet Message Access Protocol Version 4) serves the same purpose as POP3 but is more modern. Messages remain on the server and therefore, the deletion of messages are dependent on the servers configuration. IMAP4 offers several advantages since messages can be presorted to various mailboxes. This allows for a clear concise overview with large amounts of incoming mail. In most cases, the IMAP4 client retrieves only the header file when querying for new mail. The complete message is only retrieved when explicitly requested. As opposed to the POP3 client which retrieves all new messages, this method of retrieval allows users with lower transfer rates select only those messages immediately needed.

Computers where a WWW browser such as Netscape or Microsoft Internet Explorer is installed contain a POP3 or IMAP4 client which provides these features to the user.

In Microsoft's Internet Explorer (version 5) the functions are incorporated in the program Outlook Express, which can be used as a mail client for Microsoft Exchange applications.

The TCP/IP address for in and outbound mail is required for the configuration of the client. This should be the TCP/IP hostname of the MRS Server. In addition an unique name and email address must be assigned for the client. The account name (precedes the @ in the email address) corresponds to that of the users login name on the MRS Server. Assigned to the login name is a password which, along with the login name are required for login to the MRS Server. It should be observed that the password is sent in a non-encrypted form. Anyone with an IP package monitor installed on computer over which messages are routed will be able to read the password.

Configuration of the server is described on page 209ff of this manual.

It should be noted that the colon (:) in a MRS Address is not accepted in an Internet address. For this reason a dot (.) may also be used.

Another possibility is by disregarding the normally mandatory MRS Address portion NVS:. This portion will be reinserted by the SMTP gateway prior to sending the message to the MTA.

Example:

`NVS.FAXG3/1234567890@SAMPLE.DE`

This would send the email as a fax transmission. If the SMTP gateway was so configured, the switching authorities would be checked, and the originator must be assigned fax G3 transmission privileges. If this is not done, anyone from within the Internet could address the MRS Server in this way and send fax messages.

Besides that comments are supported by the email address. These comments are set in parenthesis and enable the definition of document properties.

Each document property can be generated via these comments. The \$ character is used as indication for such a property assignment and the syntax within the comment is:

`$<Property Name>=<Property Value>`

If several properties occur they are separated by semicolons⁴. The \$ character must prefix each of these assignments. Via the `$DBO(<Property Name>)` resp. `$DBR(<Property Name>)` operators, the document properties of the originator (`$DBO; Originator`) resp. of the recipient (`$DBR; Recipient`) can be set.

Example:

`FAXG3/57890($FAXCOVER=x.db1;$DBO(NAME)=Mayer)@any.where`

This would send the email as a fax transmission. Simultaneously the file `x.db1` is default set as fax coverpage and for the variable `DBO(NAME)` (name of the originator which is automatically inserted in the fax coverpage) the value Mayer is set

Attention: The maximum length of an MRS address is 63 characters which are quickly reached when document properties are used.

4.2.3.2 POP3 Mail Import

Internet mail from another POP3 server can be down loaded to the MRS Server using either a PPP or a RAS connection with the POP3 mail import. Either an Alias account is used under which all internet mail from the provider is pooled for the user, or each user is assigned a time frame in which a connection is to be made. If the account for which messages are being fetched has no entry in the user database, it will be treated as an Alias account for a complete User/Domain group.

At the time of the connection all new messages would be fetched and any outgoing messages sent.

This configuration can be seen on page 220ff of this manual.

4.2.4 SAP R/3 Gateways

Two different methods are available for configuring a gateway from SAP R/3 to the MRS Server. The first method is through the File Interface APL and the SAPcomm interface. The second method is through the newer SAPconnect interface and the associated SAP R/3 APL.

4. This separator can be configured since e.g. Microsoft Exchange always cuts the address after a semicolon though this is a legal character in a RFC 822 conform comment according to RFC 822.

4.2.4.1 SAP R/2, R/3 File Interface Protocol

The SAPcomm process must be running on either SAP R/3 or SAP R/2, and be installed in accordance with those guidelines for NVS servers as described in the SAPcomm documentation. In SAP, this is principally a post script printer configuration whose output is over the SAPcomm interface to the MRS Server. Since the post script option is supported by the MRS Server, a format loss does not occur during fax document transmissions.

A network share must be configured for the connection in which both the SAPcomm process as well as the File Interface APL have access. The **SAP R/2, R/3 FiAPL Protocol** must be installed in the File Interface APL. Refer to the page 247 in the Gateways over General File Interface (FIAPL) section on page 247ff.

During the configuration, a network share is assigned as **Poll-Directory** and **Body-Directory** for fax documents from the host (SAP) to the File Interface APL. A sub-directory **sap_in** must be created in the network share as the **Header-Directory** for reports transmitted to SAP.

4.2.4.2 SAP R/3 APL

The configuration of the SAP R/3 APL is described page 263ff. Basically, Internet Mail, fax and from SAP R/3 version 4.5 also Pager (SMS) services are available to the user.

Any MRS address can be used for transfer via an Internet address under SAP R/3, e.g. `NVS:SMS/01213456789@hostname`, so that all available MRS services may be employed. In the example `hostname` represents a subset of the address range configured under SAP R/3 for the address type INT (Internet Mail). At this the SAP R/3 APL also supports a simplified addressing mode if the entire Internet email is sent via the MRS Server. The SAP R/3 APL then filters out addresses of the type `<Address>@<Service>` and converts these into correct MRS addresses. The above example could thus also be addressed as `49123456789@SMS`. The missing dot in the domain portion of the address serves as indication of an MRS service.

To send a fax document only the corresponding fax number must be given and the MRS Server needs to be configured as recipient of the SAP address type FAX.

From SAP R/3 version 4.5 the SAP address type “Pager (SMS)” is available so that SMS messages can also be addressed from SAP in the following way: `D1: <Number>`, `E+: <Number>`, ... The abbreviations of the mobile phone suppliers are default given for this service by SAP.

4.2.5 Novell Groupwise

The gateway to Novell Groupwise is realized through a File Interface protocol (see page 247). The network protocol *NWLink IPX/SPX Compatible Transport* as well as the *Gateway Service for Netware (GSNW)* are both required for the installation under Windows NT.

The `API.NLM` must be installed under Novell Netware. A user must subsequently be configured as a member of the group `NTGATEWAY` and have all access privileges to the directories `API_IN`, `ATT_IN`, `API_OUT`, and `ATT_OUT` of the API process.

The configuration of the *Gateway Service for Netware* should now be done with the Control Panel of the Windows NT computer. The name and password of the user configured under Netware (`NTGATEWAYUSER`) must be entered here. The directories `API_IN`, `ATT_IN`, `APT_OUT`, and `ATT_OUT` must now be configured as shares.

The configuration of the protocol must have the following network directory entries in the APL Properties dialog:

Host to FI APL

Poll-Directory: \\ <MRS Server>\API_OUT

Text-Directory: \\ <MRS Server>\ATT_OUT

FI APL to Host

Header-Directory: \\ <MRS Server>\API_IN

Body-Directory: \\ <MRS Server>\ATT_IN

The field **Pattern**, should contain the entry `*.api` and **FaxFmt** the entry `Tiff-Fax`. Finally, an adaptation of the script must be made. The script is called-up through use of the **Edit Script** button in the section **Host to FI APL**. At the beginning of the script, the following **System Specific Settings** are found:

```
#define GWDOMAIN "nd_sample"
```

```
#define GWPOSTOFFICE "sample_fax"
```

The `GWDOMAIN` and `GWPOSTOFFICE` must be entered as configured in the API process.

```
char head_out[]="\\\\<MRS Server>\\api_out\\";
char text_out[]="\\\\<MRS Server>\\att_out\\";
char text_in[]="\\\\<MRS Server>\\att_in\\";
char head_in[]="\\\\<MRS Server>\\api_in\\";
```

The directories previously mentioned above are entered in UNC notation. It should be observed that a backslash (`\`) is interpreted by the script as an escape character. If a backslash is required, then a double backslash (`\\`) must be entered.

4.2.5.1 Addressing

When addressing users under Novell Groupwise from MRS the following address format is used: `NVS:GROUPWISE/*`. The `*` must be replaced with a valid Novell Groupwise user address.

Conversely, the canonic form `GWDOMAIN.GWPOSTOFFICE (Node/User)` is a valid To-Field entry for Groupwise users sending messages to MRS. The To-Field entry is under Groupwise still converted according to configurable rules. The Groupwise administrator can define simple addressing formats, so that through the use of these rules, addresses are transformed to the canonic form.

4.3 MSPTSP

The MSPTSP (MSP TAPI Service Provider) enables calling out of Microsoft Outlook e. g. For Outlook there is only the possibility to dial out. For certain other applications there are also the following possibilities (the TAPI functions occur in brackets):

- Answer a call (Answer)
- Transfer without consultation (BlindTransfer⁵)
- Call completion, z. B. Rückruf wenn besetzt (CompleteCall)
- Conference nach Rückfrage (CompleteTransfer)
- Forward after consultation (CompleteTransfer)
- Drop an incoming call (Drop)
- Hang up (Drop)
- Forward (Forward)
- Please do not disturb (Forward)
- Hold (Hold)
- Call (MakeCall)
- Pick up (Pickup)
- Redirect (Redirect)
- Three-party conference (SetupConference)
- Consultation (SetupTransfer⁶)
- Alternate (SwapHold)

5. *Blind Transfer*: an incoming call will be transmitted to another extension even if the line is busy or the corresponding subscriber cannot be reached. In this, the caller has to call again because he will not be switched to the other party if the line is free.

6. For the *Setup Transfer* you have the possibility to forward a call or to set up a conference.

- Unhold

The MSPTSP enables you to use several lines at a time, i. e. an application can be opened several times and in different ways. Several calls can be made on one line, one active call and one call on hold e. g. The MSPTSP enables access to MRS CTI functionalities also for foreign TAPI based applications via third party TAPI clients.

4.3.1 Setup

The setup copies the TSP files into the system directory and installs the TSP. In case the MSP has not been already installed the MSPTSP setup will install the MSP prior to the TSP setup.

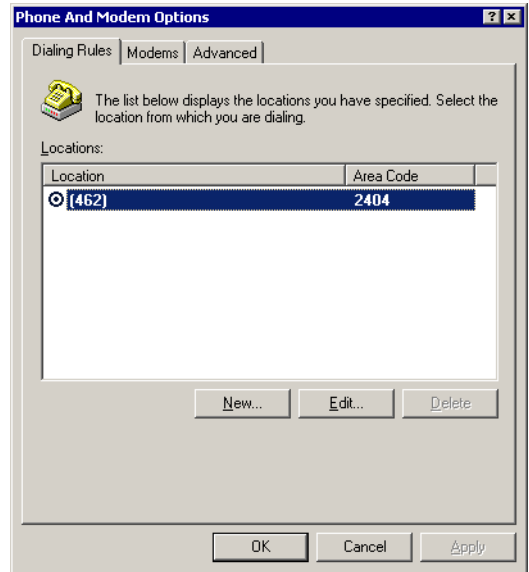
4.3.2 Configuration



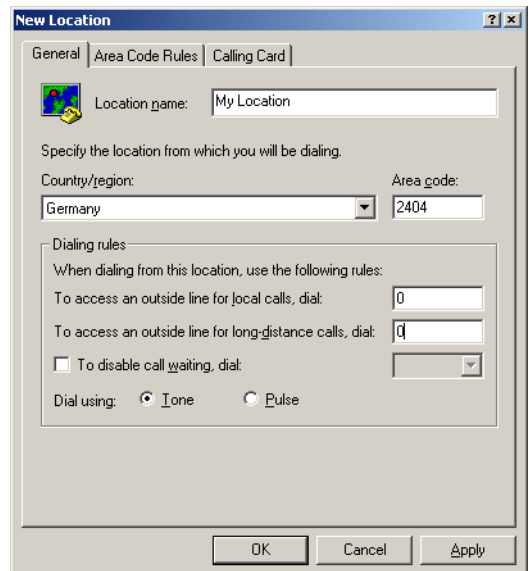
The configuration is described for the Windows 2000 operating system. The description may be different for other Windows operating systems.

After the setup has been finished, the MSPTSP prompts you to start the programme now. This is especially recommended for unexperienced users. Otherwise, you can configure the MSPTSP later in the start menu under **Settings > Control Panel > Phone and Modem Options** on the **Advanced** tab under **MSP TAPI Service Provider**. The configuration of the MSPTSP can also be done via the **MSPTSP** icon on the desktop (as far as it has been created). Alternatively, the configuration can be done in the corresponding application (e. g. MS-Outlook) (the different configuration possibilities will be described later on in the text).

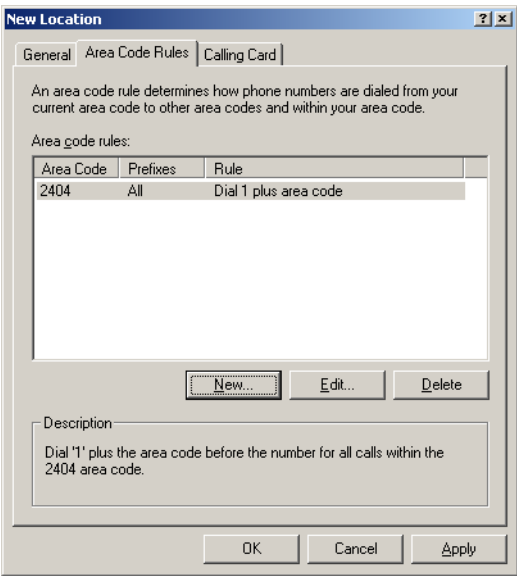
You will see the dialog at the right by selecting **Settings > Control Panel > Phone and Modem Options** in the start menu. There, you can configure the TSP via the **Dialing Rules** and **Advanced** tab.



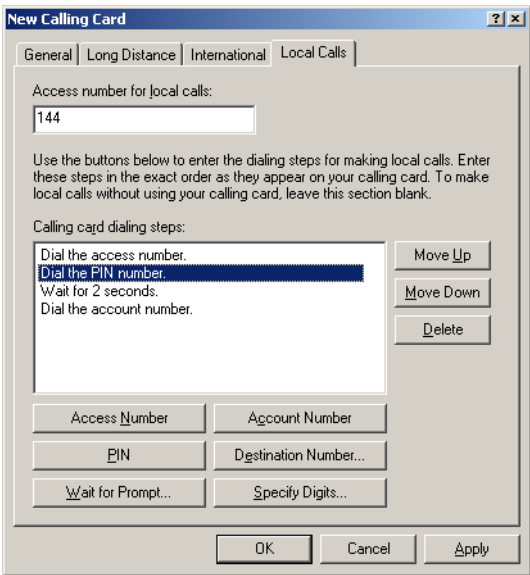
You can configure your location settings on the **Dialing Rules** tab. Click on the **New...** button (as far as no location exists) and configure the corresponding settings on the **General** tab in the **New Location** dialog. Enter the **Location name**, **Country/region**, the **Area code**, the number to **access an outside line for local calls** and the number to **access an outside line for long-distance calls**. Afterwards, click on **Apply** and **OK**.



You can define rules for phone numbers of your own and of other area codes on the **Area Code Rules** tab. You can determine how phone numbers are to be called within your area code and outside. Click on the **New...** button in order to create a **New Area Code Rule**.



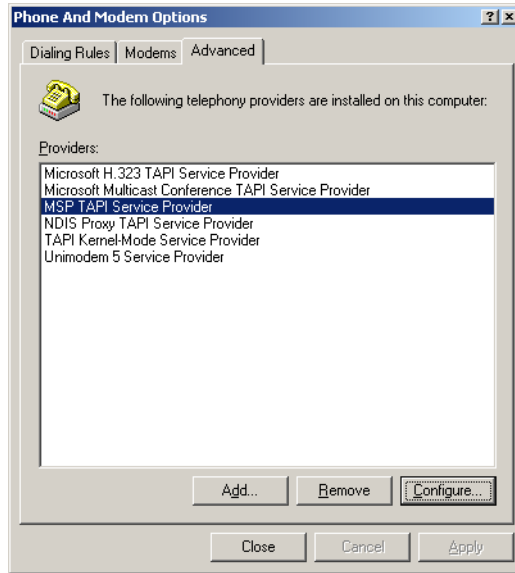
You can either select a calling card⁷ on the **Calling Card** tab or define a new one. Select a calling card from the list of card types or define a new one by clicking on the **New...** button. There, you can determine general settings like the **Account Number** and your **Personal Identification Number (PIN)**. Furthermore, you can define dialing steps like Access Number, PIN, Wait for 2 seconds etc. on the tabs **Long Distance**, **International** and **Local Calls**. The sequence of the dialing steps will be defined by clicking the buttons **Access Number**, **PIN** etc. in the desired order. The sequence of dialing steps can also be changed afterwards by clicking on the cor-



7. *Calling cards* offer a certain call credit. But, they do not possess a chip like phone cards. The customer dials a service number and will be asked to identify himself by his PIN number which he has to scratch free on his calling card.

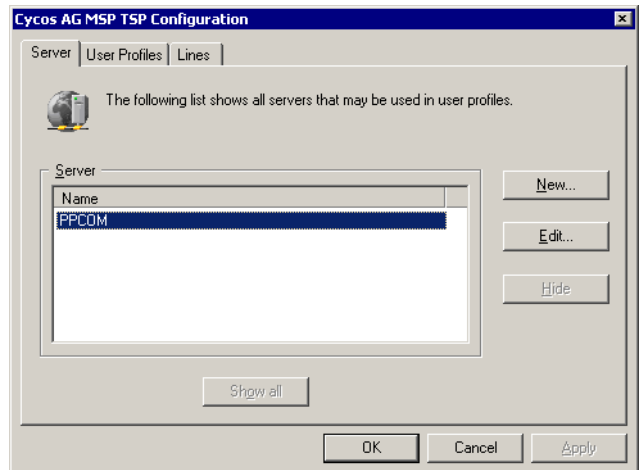
responding step you want to move. Click on the button **Move Up** or **Move Down**. Selected dialing steps can be removed by the **Delete** button.

Select the **Advanced** tab in the **Phone and Modem Options** dialog (**Start Menu > Settings > Control Panel**). Select the *MSP TAPI Service Provider* entry and click on the **Configure...** button in order to define the server settings, user profiles and lines.



The configuration of the MSPTSP can either be done via the MSPTSP entry in the start menu, by the **MSPTSP** icon on the desktop (as far as it has been created) or in the start menu via **Settings > Control Panel > Phone and Modem Options > MSP TAPI Service Provider**. Click on the **Configure...** button.

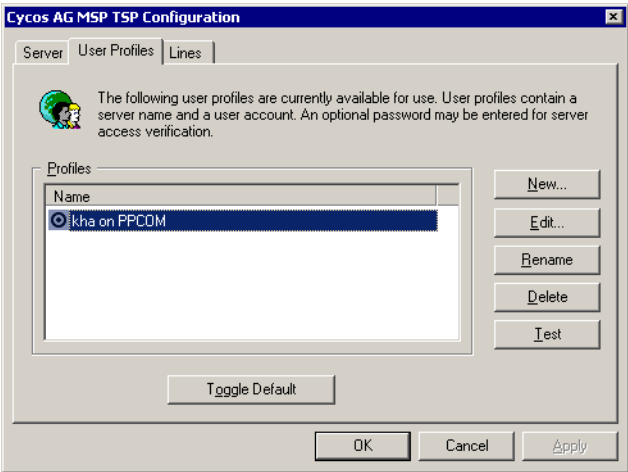
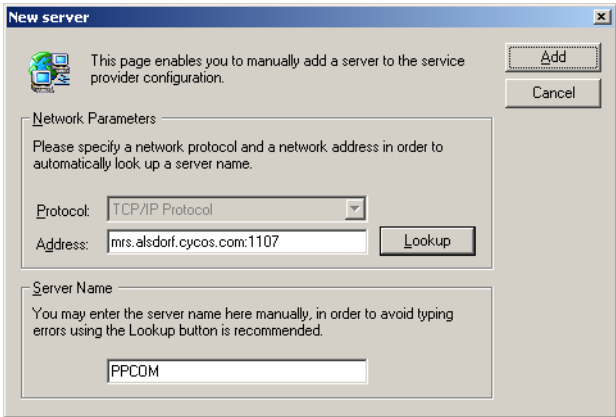
The dialog at the right appears when you select the **Advanced** tab. The **Server** tab occurs first when the setup program has been unable to find a communication server. The MSP already looks for existing servers during the installation and adds them to the list in the dialog at the right. If your communication server does not occur in the list add a communication server by clicking the **New...** button.



Enter the network address or the name of the computer on the **Server** tab > **New...** and search for the number of the port and the server via the **Lookup** button in order to avoid typing errors.

If a communication server already exists but no user profile is configured the **User Profiles** tab appears first.

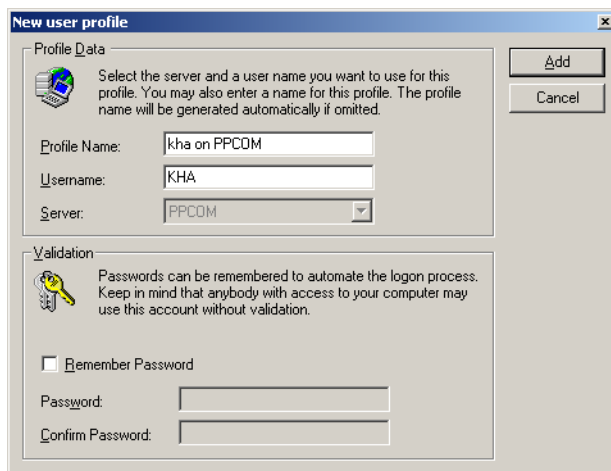
Select the **New...** button in order to create a new user profile. As the MSPTSP runs in the system context, it cannot read existing user settings from an already installed MSP. Thus, a new user profile has to be created anyway. The corresponding configuration settings can be seen and changed in the MSPTSP as well as in the TAPI application.



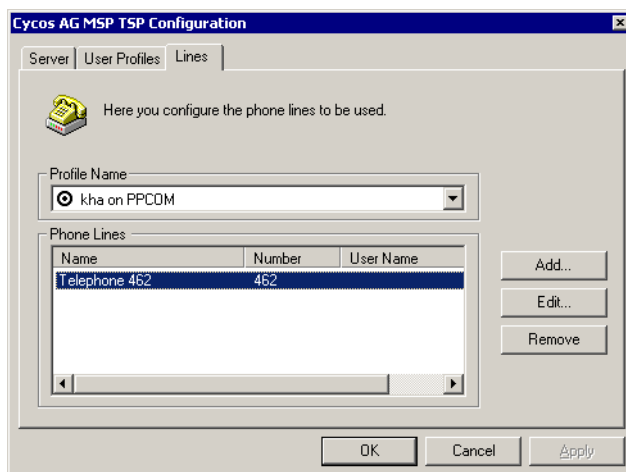
Create one or more user profiles on the **User Profiles** tab via **New...** The **Profile Name** does not have to be entered, as it is generated automatically. Enter the **Username**. This is necessary for the login on the server. Enter the server name under **Server**. Afterwards, you save your password by activating the **Remember Password** check box. Enter your password and confirm it by entering it once again. Afterwards, click on **Add**.

You can enter the lines resp. the telephones you want to use on the **Lines** tab. Therefore, click on the **Add...** button.

Telephone devices as well as lines can be added or deleted dynamically. Lines can be closed or opened as necessary. Therefore, existing user profiles cannot be used so that new user profiles have to be created anyway.



The 'New user profile' dialog box is divided into two sections: 'Profile Data' and 'Validation'. In the 'Profile Data' section, there is a text box for 'Profile Name' containing 'kha on PPCOM', a text box for 'Username' containing 'KHA', and a dropdown menu for 'Server' set to 'PPCOM'. In the 'Validation' section, there is a checkbox for 'Remember Password' which is unchecked, and two text boxes for 'Password' and 'Confirm Password'. A key icon is next to the 'Remember Password' checkbox. On the right side of the dialog, there are 'Add' and 'Cancel' buttons.

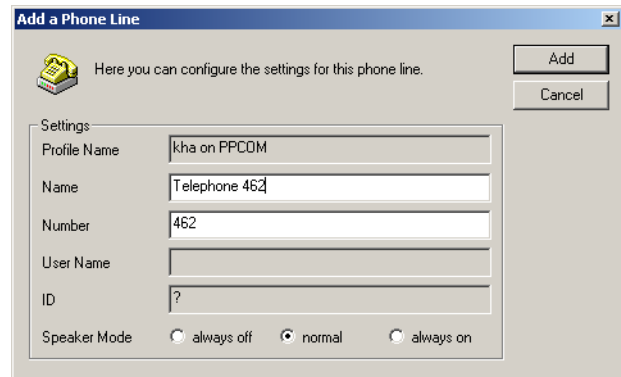


The 'Cycos AG MSP TSP Configuration' dialog box has three tabs: 'Server', 'User Profiles', and 'Lines'. The 'Lines' tab is selected. It contains a section for 'Profile Name' with a dropdown menu set to 'kha on PPCOM'. Below this is a 'Phone Lines' table with columns 'Name', 'Number', and 'User Name'. The table contains one row: 'Telephone 452', '452', and an empty 'User Name' field. To the right of the table are 'Add...', 'Edit...', and 'Remove' buttons. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

Name	Number	User Name
Telephone 452	452	

Click on the **Add** button on the **Lines** tab. The **Profile Name** already exists. Enter the name of your extension under **Name**, e. g. Telephone 462. Enter the number of your extension under **Number**. The **User Name** and the **ID** will be generated automatically. Select the desired **Speaker Mode**. The speaker mode option **always off** means

that the speaker is always off independent of the settings done in the TAPI application. **Normal** means that the speaker can be controlled by the TAPI application as far as the corresponding settings can be done there. **Always on** means that the speaker is always on independent of the settings done in an attached TAPI application. We recommend the option **always on** because most TAPI applications do not control the speaker mode. Afterwards, click on **Add**. The changes will become active at once.



All changes will become at once active after clicking the **Apply** or **OK** button. The computer resp. the TAPI application do not have to be restarted.

4.3.2.1 Error Logging

An error logging is activated by default. The error logging will be written into the system directory into the MSPTSP . log. But, the path to the error file as well as the size of the error logging can be modified by entries in the registry. You can enter a complete file path under the key HKLM\SOFTWARE\Cycos AG\MSPTSP\5.0 into the variable value of the **LogFile**. The error logging size can be defined with the DWord value **LogFileLevel**. The following values are specified:

Bit 1 (=1): Fatal errors

Bit 2 (=2): Errors

Bit 3 (=4): Warnings

Bit 4 (=8): Information

Bit 17 (= 0x10000): Function end

Bit 18 (= 0x20000): Function values that are no return values

Bit 19 (= 0x40000): Functional exception

Bit 20 (= 0x80000): Internal logs

In order to activate several of the error values, add up the values in the brackets; e. g. $1+2+4+8 = 0xF$ and enter this value into the **LogFileLevel**.

Fatal errors, errors, warnings and information will be indicated by default. Modified settings will become active at once, i. e. without restart.



The LogFile size cannot be limited automatically up to now. Therefore, we recommend to check the file size from time to time in order to prevent the file to become too large.

4.3.3 Update

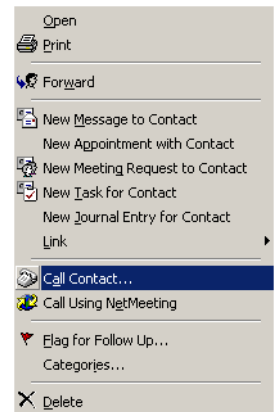
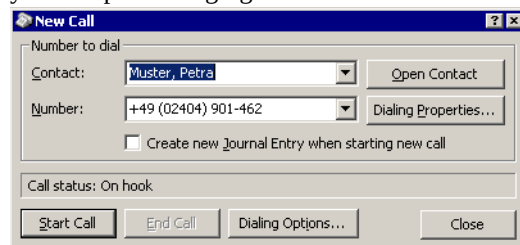
The automatical update of the MSPTSP via server is not supported up to now. Please make sure that the MSPTSP does not run anymore if you want to replace it by a newer version.

4.3.4 Deinstallation

All providers using the TSP will be removed during the deinstallation. Afterwards, the TSP files will be deleted in the system directory. Problems may occur, as the TSP cannot be deleted if it is used by one or several TAPI applications. Make sure that no TAPI applications are running anymore if you want to remove the TSP.

4.3.5 MSPTSP via Microsoft Outlook

In order to make a call out of Microsoft Outlook select an existing address entry under **Contacts**. You will get into a context menu by a rightclick. In this context menu select **Call Contact...** Afterwards, click on the **Start Call** button. Your telephone rings and the connection to the corresponding party will be established. If your speaker mode is set on **always on** the connection will be established directly without your telephone ringing.



Furthermore, you have the possibility to dial a phone number that does not exist in the contact folder. A telephone icon  will appear when you open the contact folder. Click on the arrow on the right of the telephone icon. There, you will find the menu

Server Administration

Lightweight Directory Access Protocol (LDAP)

items **Redial**, **Speed Dialing**⁸ and **New Call...** besides the entry of an existing contact. Click on **New Call...** In the menu **New Call...**, you can enter the desired phone number. Afterwards, click on **Start Call**. Alternatively, you may enter the shortcut key *Ctrl + Shift + D* in order to start a new phone call.

4.3.5.1 MSPTSP Configuration in Microsoft Outlook

The **MSPTSP Configuration** can also be done via Microsoft Outlook. Open a context menu by clicking with the right mouse button on an address entry, select **Call Contact...** Here, you can set the **Dialing Rules** under **Dialing Properties** as described for the **MSPTSP Configuration** (see page 84 in the Configuration section).

The **Dialing Options** are also available here. The **Line Parameters** can also be entered here as well as in the **MSPTSP Configuration**. Furthermore, you have the possibility to configure the **Dialing Properties**.

You can make the configuration settings under **Dialing Properties... > Dialing Rules > New...** in the **New Location** dialog as in the **MSPTSP Configuration** dialog (see also page 84 in the Configuration section).

4.4 Lightweight Directory Access Protocol (LDAP)

If a connection from the MRS server to the Internet exists, then the LDAP global directory is supported. Another possibility is the LDAP server within the Intranet. The format **LDAP/<Name>** is used to send messages.

Example: **LDAP/Joe User**

In the Internet the LDAP directory is queried and the resulting email address is that of Joe User. If this address is a valid email address then the message is sent, otherwise the initiator would receive a list of all directory entries containing this name. If no recipient is found an error report will be generated.

If the address is not a valid address, then other filter conditions may be set in RFC 1558 format to narrow the search area. This deals with a portion of the X.500 DAP whereby, a LDAP server does not have to be a part of the global X.500 directory.

Example: **LDAP/(& (cn=Joe User) (o=ACME Co.))**

One or more filter conditions (Qualifiers) may be given with a total length of up to 54 characters. Filter conditions can be combined through the use of **&** (logical AND), **|** (logical OR), and **!** (logical NOT).

8. Speed dialing numbers can be entered in the **Dialing Options...** dialog in Microsoft Outlook (**Contacts > Call Contacts... > Dialing Options...**).

4.5 Mailing Lists

The Mail APL administers mailing lists similar to those used in the Internet. For this purpose there are three commands that can be used in a text message to the user LISTPROC:

SUBSCRIBE Listname Name Surname

Subscribe to a mailing list. The mailing list is used for sending messages to the various subscribers (email address).

Example: SUBSCRIBE LP-DEVELOPMENT Joe User

UNSUBSCRIBE Listname

Removes individual names from the mailing list. Messages will no longer be sent to these email addresses by the mailing list processor.

Example: UNSUBSCRIBE LP-DEVELOPMENT

HELP

With this command a message is returned with operational help and a list of all mailing lists existing on the MRS Server.

Internally mailing lists are treated as distribution lists that begin with the abbreviation “LP”. The configuration and maintenance of mailing lists is done with the help of the Distribution List Editor in the MRS Client.

To include a message in a mailing list, the message is sent to

LST:LISTNAME.

Upper case letters are used exclusively by The MRS Server for mailing lists.

4.6 Broadcasts

Broadcasts are a special type of automated distribution lists with which recipients are determined from the user database according to certain criteria. Sending a broadcast requires the *Send Broadcast Privilege*. This privilege applies comprehensively to all recipients so that, for example, you can transmit messages to automatically determined fax recipients without the *Fax G3 Privilege*. Thus a broadcast reaches all potential recipients.

Syntax of possible target addresses:

NVS: <Server>/BCU: <Keyname> or

NVS: <Server>/BCU: <Expression>

<Server> is the MRS Server name, <Keyname> is a corresponding field from the user database and <Expression> an optional expression that must apply to a user so that he or she receives the message. BCU means *BroadCast User* since broadcasts can only be

Server Administration

Broadcasts

sent to users. For *<Keyname>* and *<Expression>* only capital letters may be used. If you want to refer to a database field in an *<Expression>*, provide this with the UPPER attribute so that the content can be reasonably processed via the *<Expression>*.

To send a message to all users of the MRS Server, address to NVS: <Server>/BCU:. The PREFERRED database field is default set and can be omitted.

Examples

Given are two users with the following database entries on the XPR server:

John Doe:

CLASSNAME	CLASS	KEYNAME	KEY
USER	JOHNDOE	PREFERRED	VOICE
USER	JOHNDOE	VOICE	4924041234567
USER	JOHNDOE	SMTP	johndoe@some.where
USER	JOHNDOE	BUILDING	RED

Jane Doe:

CLASSNAME	CLASS	KEYNAME	KEY
USER	JANEDOE	PREFERRED	EXCH
USER	JANEDOE	VOICE	4924047654321
USER	JANEDOE	EXCH	JaneDoe@XPR
USER	JANEDOE	BUILDING	BLUE

NVS:XPR/BCU:

Two messages are sent, one to NVS:VOICE/4924041234567 and the other to NVS:EXCH/JaneDoe@XPR.

NVS:XPR/BCU:EXCH

One message is sent to NVS:EXCH/JaneDoe@XPR because John Doe has no Exchange address.

NVS:XPR/BCU:VOICE

Both users receive a message because both have an entry in the VOICE database field. Target addresses: NVS:VOICE/4924041234567 and NVS:VOICE/4924047654321

NVS:XPR/BCU:BUILDING=RED

Example of an address with *<Expression>*. Only when the expression BUILDING=RED is true, the message is sent to the corresponding user's preferred address. In this case a send job thus occurs to NVS:VOICE/4924041234567.

4.7 The NIL Protocol

The Mail APL provides the logical line NVS:NIL for data transmissions. All documents sent over this line are immediately deleted by the MRS Server. Documents are replaced with a notice which contains information over the administrative deletion. Researching such a transaction in the global journal can only be done by an administrator.

The purpose of this protocol is to provide a means of automatically filtering out undesirable (Spam) messages, so that server resources are conserved.

This can be carried a step further by sending all messages to the address NVS:NIL/ATOMIZE. In this case the message is deleted completely, and no journal entries are made. Researching such a transaction is generally impossible since there is nothing to indicate that a message was sent to this address.

Example:

- If Spam mail continues to arrive from a single originator, these can be eliminated through use of a routing rule e.g.

NVS:*.*/*[org=NVS:SMTP.*/*@spam.org]=NVS:NIL/ATOMIZE

from a domain or a specific user.

- Another application of the NIL protocol could be for restricting the size of outgoing transmissions. A routing rule for this purpose would have the following appearance:

NVS:*.*/*[org=NVS:\$NODE/*;LEN>1000000]=

NVS:NIL/TRASH[SUBJ=Mail too long - denied]

Through the use of this rule, all email messages originating from the system that are larger than 1,000,000 bytes would not be sent. Subsequently, the document would be deleted and the subject line modified with a message to the originator.

If this rule is used in together with a database query, specific users can be excluded from this rule.

- A type of Robinson list via which transmission to specific users is prevented. For this purpose define a group (for example ROBINSON) and subsequently a rule such as:

NVS:FAXG3/*[GROUP(REC)=ROBINSON]=NVS:NIL/FAIL

All FAX G3 send jobs concerning recipients who are members of the ROBINSON group would be reported to originator as failed. Via the corresponding report forms this could be done in a more ingenious way to adapt the error report accordingly.

4.8 HP Digital Sender

Connecting the HP Digital Sender with the MRS Server has been realized via the File Interface APL. Thus each user entered for the HP Digital Sender can read in documents at this network integrated scanner and immediately send them via the MRS Server after entering the fax number at the scanner. Since distribution lists can be connected with a fax number at the MRS Server, they can be transmitted via the HP Digital Sender as well.

Beyond that users entered at the HP Digital Sender can be identified as MRS users so that charges incurred by the transmission of documents can be assigned to them.

4.8.1 Hardware Installation

The HP Digital Sender must be installed in the same network segment as the MRS Server. The user performing the installation must have administrative privileges within the segment. In particular an IP address must have been assigned to the HP Digital Sender. Please refer to the *HP Getting Started Guide* for further technical information.

4.8.2 HP Digital Sender Software Installation

The installation of the HP Digital Sender Daemon can be on any Windows NT server within the domain in which the HP Digital Sender and MRS Server are found. This could also be for example, the MRS Server itself. Administrator privileges must be granted to the user who is conducting the installation.

As preparation an NT user account, which must have the privilege to “LogonAsService”, should previously be generated. Subsequently, a new directory is created with the share name “HPSSCAN”. Within this directory a sub-directory must then be created with the share name “HPFSCAN”. This directory acts as a repository for documents read by the scanner. Now Setup can be started from the HP installation-CD for 9100C, Build 806 or higher (green CD).

First set the language (English) and subsequently select **Install HP Digital Sender**. After enabling the **Next** button twice, click on **Install Administrator**. On the page now displayed choose the options **Administrator Software** and **HP Digital Sender Service**. The third selectable component **Client Software Distribution** is optional and only required if fax transmission reports are to be received via the HP Client Software later on.

Now Setup starts the HP JetAdmin Software installation. HP JetAdmin Software allows network administrators to quickly configure scanners and their associated user

pools. After entry of the above generated user account for this service and the corresponding password you are asked whether additional fax service functions are to be installed. Confirm this and select the fax service **MRS Unified Messaging**. The share (HPFSCAN) that was manually created during the installation of scanner service, should be entered as the polling directory.

If **Client Software Distribution** has been selected further above you are now queried for the clients to be distributed. Select all, thus installing the installation versions of all operation systems supported by HP.

4.8.3 Configuring a User Pool

With the HP Address Book Manager now installed, users can be entered to allow them sending faxes after logging in to the Digital Sender. Further processing of documents delivered by the Digital Sender is performed by an E script of the File Interface APL on the MRS Server side.

4.8.4 Installing the HP Digital Sender Protocol

The HP Digital Sender Protocol is realized as File Interface APL Script. In order to install it the **Settings** options of the **FiAPL** should be selected in the Modules window of the MRS Monitor and subsequently under **Protocols** the *HP Digital Sender* protocol is **Added**. Operation of the File Interface APL Configuration Dialog is described on page 222 ff. In the following only the corresponding **Properties** of the HP Digital Sender Protocol are described:

4.8.4.1 Host to File Interface (FIAPL)

Poll-Directory

Here the directory is set where fax documents are stored, e.g.: \\<Server>\HPFS-CAN\

Body-Directory

Here the directory is set where send information is stored, e.g.: \\<Server>\HPFS-CAN\

Pollrate

Every *n* seconds the above directory is queried for new fax documents.

Header-Patterns

The scanner stores the transmission information for newly read documents with the extension hp_f. *.hp_f must be entered in this field.

4.8.4.2 File Interface (FiAPL) to Host

Reports

The **Reports Filter** should be set to **All**, and no entry is required in the field **Suffix**.

Header-Directory

Here the directory is set where transmission data is stored. Example:
\\<Server>\HPFSCAN\

Once the configuration settings have been completed the HP Digital Sender is operationally ready. Rebooting of the MRS Server is not necessary.

4.8.5 MRS User Configuration

In order to identify users entered at the HP Digital Sender as MRS users another database field must be added to the user database. This field has the same name as the E script, normally HPNSJ5. If a different name is preferred the script must be renamed before installation.

Enter the account name of the user defined at the HP Digital Sender in this field so that charges incurred can be assigned accordingly.

4.8.6 Reports

Users that wish to receive fax transmission data must poll them from the HP Digital Sender. Delivery is either performed via the above mentioned HP Client or per Internet mail. For the latter service an SMTP address must be assigned to users upon their configuration via the HP Address Book Manager.

This Internet address should correspond to the one entered in the user database and is delivered to the user via the MRS Server SMTP APL. Thus every client supported by the MRS Server can be used to receive reports, e.g. all POP3 or IMAP4 Clients. A prominent example of this type of programs is Microsoft Outlook with all its versions.

4.9 WAP Services

The desire to be able to access the Internet and thus also mailboxes of an MRS system via mobile phone led to the development of suitable protocols to combine these two technologies. Since mobile phones only have a small display and furthermore the data transfer capacity is relatively small, web pages cannot be represented in the traditional way. In addition, storage capacity, CPU performance and entry options are restricted.

4.9.1 Wireless Application Protocol (WAP)

Monitoring and standardizing the Wireless Application Protocol (WAP) occurs through the WAP forum, consisting of about 150 members mostly from the lines ter-

minal device manufacturers, network operators and IT technology companies. This forum aims at processing and transmitting Internet pages to mobile terminal devices and working out global protocol specifications that allow wireless communication between technically different mobile phone networks. Naturally this is all done from the point of view that existing standards are supported and future standard extensions must be possible.

WAP is an industrial standard based on the client/server model, currently supporting nearly all mobile phone standards worldwide. It includes the following features:

- based on the standardized file formats of the WWW
- standardized protocols for the radio interface
- standardized client (mobile phone) functionality
- Wireless Markup Language (WML)
- script language (WML script) that adapts to the client's potentialities in order to work with restricted devices (low display resolution, small storage capacity, low CPU performance and a small band transmission medium).

4.9.2 WAP Architecture

WAP architecture consists of three components:

- WAP Server
- WAP Gateway
- WAP Client

4.9.2.1 WAP Server

The WAP Server is the resource (data, memory and process handling) providing instance. It can be a standard WWW Server or a specially extended communication server (e.g. the MRS Server with WAPAPL).

4.9.2.2 WAP Gateway

Contrary to the Internet the WAP architecture includes another element placed between the WAP Server and the client : the WAP Gateway. It has two important functions:

1. it serves as protocol converter
2. it is used as proxy

As protocol converter it turns the application protocol HTTP (Hyper Text Transfer Protocol), employed between the WAP Server and the gateway, to the WSP Protocol (Wireless Session Protocol) used for the communication between WAP Gateway and

client. Additionally the amount of data is reduced in the gateway as this is necessary with reference to the small bandwidth available for transmission to the client.

The proxy function makes sure that the WAP terminal device can pose queries to the gateway which are then forwarded to the WAP Server. Beyond that the data sent by the server are filed on the proxy. When the client then queries for a page already sent, the data can quickly be forwarded. So pages already called can directly be answered by the proxy without accessing the server again.

4.9.2.3 WAP Client

A special WAP terminal device (mobile phone) mostly serves as client. It needs to be equipped with a micro browser which is generally the case with devices of the latest generation. Most of the preceding models (e.g. the Nokia 7110 or 6210) can be reconfigured. Please consult mobile phone manufacturers and network operators for the corresponding information. An excellent information source are their Internet pages.

A tip with reference to possible connection configurations in the various networks: if your mobile phone can be configured automatically then this option should be chosen. Normally you only need to call the corresponding network provider via a certain calling number and apart from a few confirmation entries the configuration process occurs automatically. A manual configuration is not recommended due to many, relatively complicated entries to be made on the mobile phone.

Connection between WAP Mobile Phone and WAP Server

By the example of the Nokia 7110 we shall describe in the following how to log in to a WAP Server. Other types of mobile phones are, apart from different key allocations, configured in a similar manner.

Singular Mobile Phone Configuration

- Switch on the mobile phone and enter the PIN
- Select “Services” via “Menu” and press the scroller (**do not** select “Start”!)
- A menu is displayed in which you need to scroll to “Bookmarks”. Press the scroller to select this entry.
- Next enable the “Options” key to open a menu where “Add bookmark” is found and called with the scroller.
- Enter the WAP Server address in the entry field available now (the format normally is “http://xxx.yyy.zzz.com/wap.wml”). Enabling “OK” saves the address. Another entry field opens where you define the name under which the previously entered address is to appear in the menu.

Connecting the MRS Server for Information Query

- Switch on the mobile phone and enter the PIN

- Select “Services” via “Menu” and press the scroller (**do not** select “Start”!)
- A menu is displayed in which you need to scroll to “Bookmarks”. Press the scroller to select this entry.
- Scroll to the name of the WAP Server address in the list displayed and press the scroller once again. The ensuing connection setup to the WAP Server has been accomplished when the Login window appears.



Server Administration

WAP Services

- Scroll downwards until you reach the entry field under “User” and press the scroller.



The user name entry field appears. Enter the user ID with the mobile phone keys and confirm the entry with “OK”.

- This takes you back to the Login window where you are prompted for the password. Scroll to the entry line under “Password” and press the scroller to open the corresponding entry dialog. Enter the password and confirm with “OK”.
- Under the password entry the menu option “Login” is faded in. Select this option and press the scroller to activate it.
- Provided the entries made so far are correct, the WAP Server can be accessed now.



For more details on the operation and the functions of the MRS-WAP Server please refer to the separately available “WAP User Manual”.

5 MRS Monitor

The MRS Monitor is used for displaying status, performance, diagnostic, etc. messages for the complete MRS System. The configuration of individual MRS components is also done through the use of the MRS Monitor.

The MRS Monitor can be started from any Windows NT/2000/XP computer within the network, so that the administration of the MRS Server can be comfortably performed. With the MRS Server installation a share is implemented from which you can start the monitor when you do not operate the MRS Server itself.

Remote maintenance can also be performed by trained personnel without having to be on-site using the Remote Access Service (RAS) from Windows NT.

5.1 Security

Working with the MRS Monitor requires logging in at the MRS Server. Via the log-in options you can specify whether this logging in is to be permanent for a session or is to become automatically invalid after a configurable period. The last option is considered useful for example to prevent unauthorized users from accessing the MRS Server via the started MRS Monitor after an authorized person has logged in at the server.

5.2 Operation

After its installation, the MRS Monitor displays per default data of the local computer where the MRS Server is running. This information is provided in the monitor windows **Modules of <Server>**, **Lines**, and **Default Logging**.

All components installed within the MRS Server are displayed in the **Modules of <Server>** window. A topic area is assigned to each component where log information can be displayed. If a log report is generated that has no topic area, this report would appear in the general *without topic* section. In the logging window all general information, error, and warning reports are displayed. If at a later time a component is to be added or special debugging information is required for error analysis, the desired topic can be seized with the left mousebutton kept pressed and dropped in a logging monitor. A dialog is then opened in which the filter for the selected topic can be configured.

All components that administer lines are displayed under **Lines**. As with the logging information, lines can also be moved to a line monitor per drag&drop and displayed there. The line monitor displays all lines. When a connection on one of the lines is established, this can be seen in the line monitor (fax number, telephone number., etc.).

The last entry found in the **Modules of <Server>** window is the *Settings* option. Configurable MRS components can be configured here.

Server Administration

Creating a new Monitor Layout

The **Toolbar** and **Status Bar** can be switched on or off under the menu entry **View**.

Fast access to many of the Monitor's functions can be found by clicking on the icons within the toolbar. A short description of the icon's function appears (QuickInfo), when the mouse pointer is positioned over the icon.

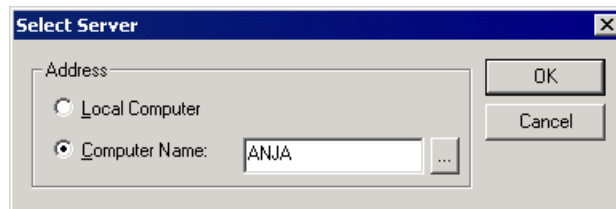
Current date and time are always displayed in the status bar.

Following this general introduction of the functions of the MRS Monitor, a review of all Monitor possibilities will be presented. This will be accomplished by creating a complete Monitor-layout. Any of the delivered Monitor layout examples may also be used.

5.3 Creating a new Monitor Layout

In the following a new Monitor layout for a MRS Server will be created. Throughout the Monitor set-up important concepts and various configuration possibilities of the MRS Monitor will be demonstrated.

First create a new monitor layout and select the computer where an MRS Server is running. In the example, the computer with the name *Anja* has been selected on which an MRS Server named *Anja* is running..



A window now opens in which all components of the server are contained. A component is made up of the following:

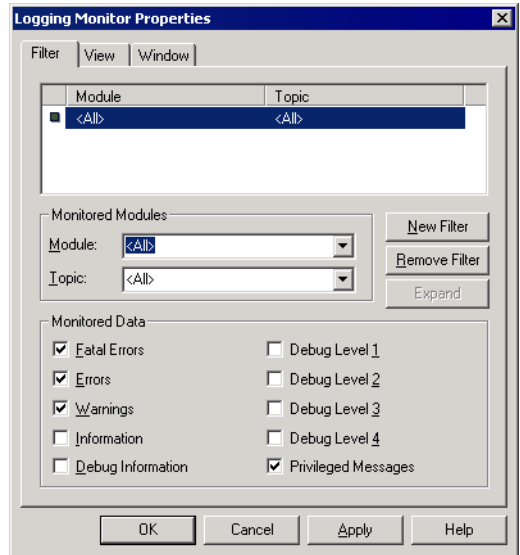
- Topic: Categorizes component output
- Lines: Displays the physical and logical connections.
- Settings: Components configurations can be viewed and modified.

At the top of the list is the name of the server and the connection status. Individual monitor windows can be created for lines and topics. The individual monitor windows can either be confined within the MRS Monitor, or placed independently within the user interface. The last-mentioned (floating monitors) are visible even when the MRS Monitor is minimized.

5.3.1 Configuring a Logging Monitor

Next a logging monitor is to be defined in which error reports, warning messages, and general information of all MRS Modules will be displayed.

Select the menu entry **View** and subsequently the entry **Logging Monitor**. After the appearance of the new monitor, click with the right mouse button to call the pop-up menu and select the **Properties** dialog. In the **Filter** tab, select the **New Filter** button for all components and topics. In the **Monitored Data** section check the entries **Fatal Errors**, **Errors**, **Warnings** and **Privileged Messages**. The last-named are selected messages additionally flagged. Developers can flag any type of message so that important information messages are displayed even when this type of message has otherwise been disabled.



If you want to install a Logging Monitor for specific APL topics, you can also select a module and click on **Expand**. For each topic of this APL an individual filter entry is generated then. Those not needed can be deleted. With several APL topics required this procedure is normally less time-consuming than defining each of these filters separately.

In the **View** tab of the Logging Monitor properties window a file name may be entered so that all protocol information is simultaneously logged for evaluation at a later date.

If several Logging Monitors are to be created, a unique name must be entered for each monitor for the log file! Fonts as well as various font colors may be used to separate the various types of monitored data. In this manner, error reports could appear in red to enhance their visibility.

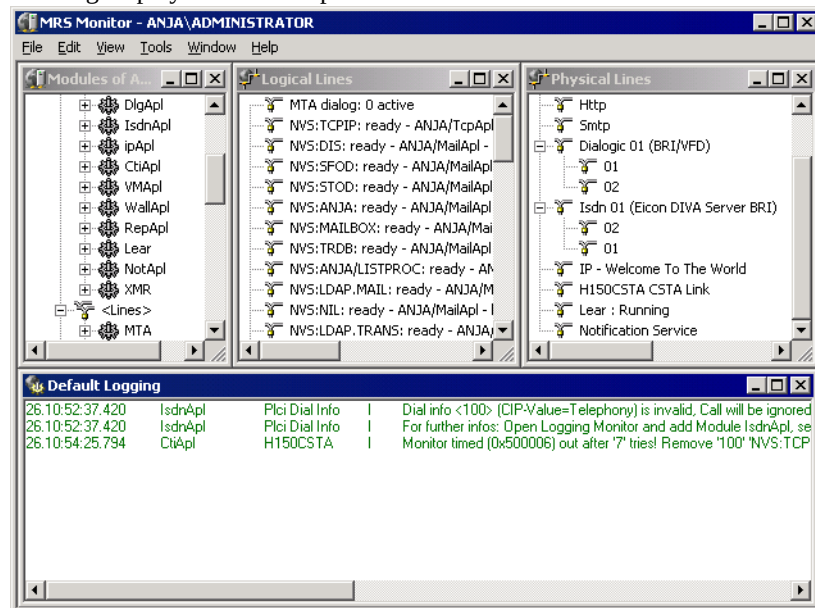
In the **Window** tab of the properties dialog a title can be assigned to the monitor describing its function. By checking the **Show Caption** entry, the monitor title is displayed in the title bar of the monitor thus reducing possible confusion when numerous monitors are in use.

5.3.2 Configuring Line Monitors

The Access Protocol Layer converts physical lines into logical lines. A physical line is defined and provided through an external network and represented by connection (network hardware). Logical lines are independent of the external networks and are determined by network type and protocol. Logical lines are represented through the **NODE** and **CLASS** of an MRS Address. With the exception of the Access Protocol Layers, the complete MRS Server works exclusively with logical lines. Physical lines can be made-up of numerous logical lines if the various protocols are available to the network.

Two monitors will now be configured for displaying physical and logical lines. The module MTA (Message Transfer Agent) administers all logical lines. By selecting the menu entries **View** and **Line Monitor** and then using the Drag and Drop method with the MTA module, a new line monitor is created, displaying the logical lines of the MRS Server. The other MRS Modules administer only physical lines, if any at all. The creation of a new line monitor for physical lines is the same as for logical lines with the exception that the MTA module is excluded from the filter settings.

The resulting display is here as depicted:



5.3.3 Saving Monitor Layouts

The monitor layout can be stored and later loaded for use on another computer through use of the menu entry **File→Save As Template**. The server name can be changed for fur-

ther applications with the layout. If the layout was created e.g. for use on a local computer, it can also be reused on any computer within the network.

If the option **File—Save As** is selected, the MRS Server settings are saved along with the layout and when re-opened, immediately display data for the configured server.

If you want to immediately start the MRS Monitor with a selected or generated layout on your computer with each log-in, create a shortcut with the `MrSMon.exe` file in the autostart directory and specify the layout that you have saved as parameter.

5.4 Standard Monitor Options

Every new monitor window is assigned the default settings as defined under the menu entry **Tools—Options**. These settings may be changed at a later time for an individual adaptation of the Monitor windows.

5.4.1 Modules

This portion of the MRS Monitor is used to configure the default appearance of the Module window. In the **Display automatically** section, sub-trees are selected, which are to be displayed in the expansion. Additionally, the menu option Sorting can be switched either between **By Module** or **By Type** (Topic, Lines, Settings), and a configuration assigned to both types.

The type of sorting used for the creation of a new Module window is dependent upon the entry in the menu option **Sort**.

When sorted by Type, all Topics, Lines, and Settings are respectively summarized and displayed. When sorted by Modules, Topics, Line, and Settings are displayed under their various Modules.

Various reports from the modules are found under **Topics**. General reports without specifically assigned topics are filed under **Without topic**. Further topics are provided by the modules for special topic areas, in which targeted report selection is possible. All lines administered by the modules are physical lines with the exception of the MTA (logical lines only). Module configuration, testing, and validation is accomplished under **Settings**.

Via activation of the **Pop-up Properties Automatically** option under **Drag & Drop**, properties dialogs are automatically displayed. Now when a new monitor is created and a topic inserted with the drag and drop method, the properties dialog automatically appears for immediate configuration and individual adaptation of the monitor window.

5.4.2 Line Monitor

For lines, two configuration tabs, **Window** and **Filter**, are available. The **Window** tab allows the assignment of a name or caption to a new line monitor as switching on or off the caption bar. These configurations can be individually adapted for other line monitors.

In the **Filter** configuration tab, the entry **Display sub-lines automatically** determines whether sub-lines are automatically shown for the displayed lines.

Connections are defined through the displayed data in the **Data to be displayed** section. Various parameters can be selected for defining the connection: **Line State Information**, **Remote/Local Address**, **Cost**, **Baud Rate**, **Error Rate**, **Incoming/Outgoing Bytes**, **Total Bytes to Send**, **Incoming/Outgoing Pages**, **Total Pages to Send**.

The parameters listed above are not provided by every line type. Baudrates, e.g. for connections within a local network are not available for report information, even though this information would be of interest with a modem connection.

5.4.3 Logging Monitor

For the configuration of logging monitors three configuration tabs, **Filter**, **View**, and **Window** are used. In the **Window** configuration tab you can default set the caption for a new logging monitor and switch on or off the caption bar. These settings can be individually modified for each window late on.

In the **Filter** configuration tab you can select information to be displayed in a new logging monitor per default:

- *Fatal Errors*: Errors that lead to abnormal module termination.
- *Errors*: Non-critical errors. In most cases the module remains in a functioning state.
- *Warnings*: That e.g. reports are generated for intermittent configuration discrepancies.
- *Information*: Normal operation reports.
- Various debug level reports used by developers and service personnel for diagnostic purposes. For the average user these reports are meaningless.

As default **Topic**, either **<All>** or **<Without Topic>** may be selected. In most cases the entry **<All>** should be selected since each module has special topics defined for its output and a categorical distribution is then possible.

The appearance of new logging monitors is set using the options in the **View** configuration tab.

Fonts can be selected as well as font color assignment for the various report types (F - fatal error, E - error, W - warning, I - informational, debug info, debug levels (1-4)). Through the use of the various colors the gravity of a report can be recognized at a glance.

Through the selection of the **Background Color...** button, the background color of the logging monitor can be changed.

Selection of the **Reset** button returns all values to the preset defaults. As with other settings in the **Properties** dialog, the **Reset** function applies only to the monitor being configured.

A speciality is the **RotoLogger** option which can be selected to limit the size of log files and simultaneously to specify the number of log files to be stored. If you looked for an error that occurs very rarely or only after hours of extreme server loading, the debug log file would become far too large considering that only the last detailed information on the error would be of importance. Therefore the log files are overwritten by the Roto-Logger using the Round-Robin method so that the maximum size entered for all log files will not be exceeded. To activate the Roto-Logger the option **Log into File** must be check marked and subsequently a file name entered in the corresponding field.

5.4.4 Main Log file

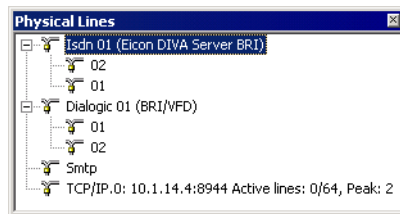
Filter settings for the main log file are configured in this dialog. This log information is always included with the main log file.

5.4.5 Active Alert

Filter settings for Active Alert reports generated by the MTA (see page 183). All of the log reports listed in this dialog can be used for Active Alerts. Active Alerts could be used e.g. as error notification to an administrator or the accountable service hotline.

5.5 Monitor Usage Examples

5.5.1 Line Monitor



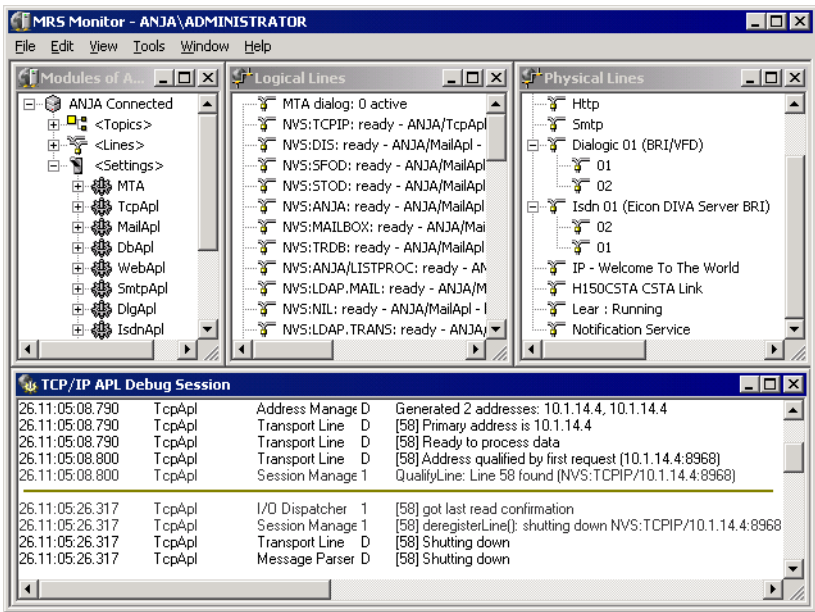
The MRS Monitor can be used in a number of varying situations. One possible application is as an activity monitor for all physical lines. For this purpose generate, as above, a new monitor layout with a server view. Subsequently create a floating line monitor (**View→Floating Line Monitor**) in which all physical connections are

displayed. Even when the MRS Monitor is minimized, the floating monitor remains open displaying the server's activity over the physical lines.

All floating line and logging monitors can have their own toolbars. These toolbars are activated by a right mouse button click within the window, and subsequent selection of this option.

5.5.2 Special Analysis Session

When specific modules require a more detailed examination, an individual logging monitor should be created in which the various reports are stored and all possible filters conditions are set.



As seen in the above illustration a monitor has also been created for the TCP/IP module. By pressing the spacebar a line can be inserted in the Logging Monitor that acts as an optical separation for the easy identification of test phases.

5.6 Local Installation

On the computer where MRS Server components are installed, a share MrsMonitor to the configuration DLL's of these components is automatically installed as well. On the kernel computer you then also find in this directory the actual MRS Monitor.

We recommend to install a link to the `MrsMon.exe` file in the MrsMonitor share on the kernel computer and thus always to start the monitor from the server. In this way you automatically receive the correct version with an MRS Server update.

The MRS Monitor always loads a required configuration DLL from the computer where the APL to be configured or the kernel component runs. For this purpose it is loaded from the corresponding share on this computer. Consequently, version conflicts are avoided when you have e.g. a local, deviating version of this configuration DLL. This case might occur when you administer several MRS Servers of different version status with one MRS Monitor.

If you want to install the MRS Monitor on a local computer, copy the files `MrsMon.exe`, `MrsRsrc.dll` from the monitor share of a kernel computer and for the online user assistance all files with suffix `chm`. In this case make sure to copy these files anew when performing an update.

6 MRS Modules Configuration

6.1 Integrated Services Digital Network (ISDNAPL)

The ISDN APL, as with all components of the MRS Server, is installed using the MRS Setup program. The configuration of the ISDN APL is done through use of the MRS Monitor. The ISDN configuration dialog is started by double clicking on the **Set Options** entry found under **Settings** in the module window of the MRS Monitor. Under the option **Set Advanced Options**, further settings for the APL configuration are available, but in most cases these options under normal configuration are sufficient.

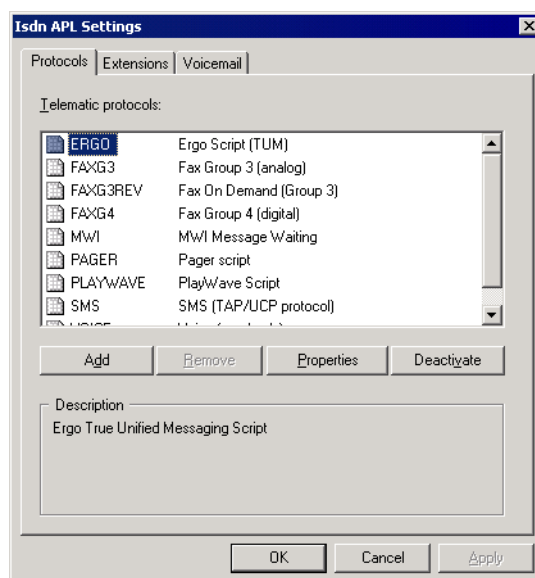
Since all modifications are dynamically effected, a restart of the ISDN APL is not necessary after changes have been made.

6.1.1 Protocols

All protocols supported by the ISDN APL are listed in this dialog.

Other protocols that are installed on the MRS Server can be inserted by selecting the **Add** button. Protocols that are already installed can be deleted by selecting the **Remove** button or disabled with the **Deactivate** button. The ISDN APL also supports Euro File Transfer servers resp. clients (see page 64), fax transmissions and reception, fax G3 polling from fax-on-demand servers (see page 57), fax G4 transmissions and reception (see page 63), MRS SMI protocol (see page 58), voice mail playback over the telephone (see page 66), and script based protocols such as the Fax-on-Demand Server (SFOD, see page 66), the standard Voice/Fax mailbox (MCK, see page 72), or the modern voice mail system Ergo (see individual manual).

Parameters of the various protocols can be displayed and modified through selection of the **Properties** button. A description of the protocol settings follows.



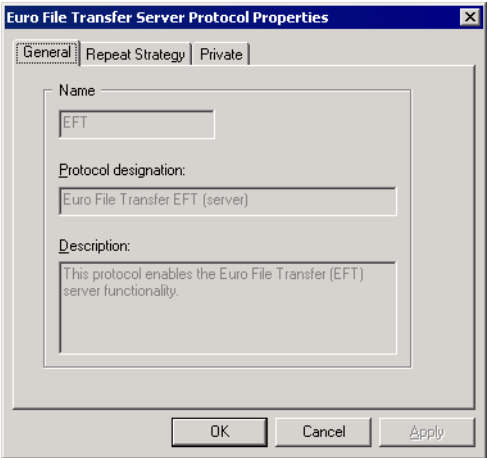
6.1.1.1 Euro-File Transfer Server

General

Since this is a standard protocol, the various elements are displayed, but cannot be modified.

Displayed elements are comprised of the protocol **Name** (over which the protocol is addressed), **Protocol designation:** (used for display in the MRS Monitor), and a detailed **Description:** of the protocol and its functions which appears in the configuration tab when selected.

Script based protocols may be arbitrarily named and standard protocols inserted under another name. When inserted under another name, the properties of the standard script may be modified.

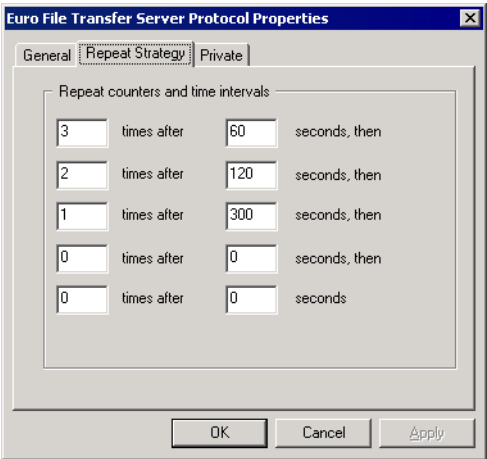


Repeat Strategy

The number of redial attempts and at which intervals they are initiated can be set under **Repeat counters and time intervals**. The number of redial attempts is entered in the left-hand portion of the dialog, and the corresponding interval between the various attempts in the right-hand portion of the dialog.

Up to 5 different counters with varying time intervals may be used. The counters are executed sequentially until a successful redial has been made or the last counter is expired.

If after all repeat attempts have expired and a successful transmission was not possible, the message originator will be informed through a status report.

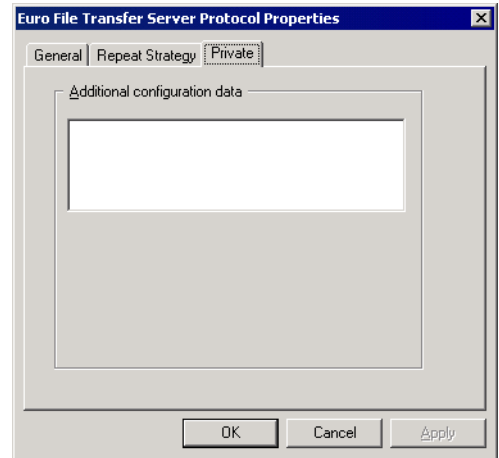


Private

Private Data. These settings correspond in their operation to those in the INI configuration files from the Windows 3.1. One protocol specific entry may be entered per line (Value=...).

Example: GuestUser=EFTGUEST

The following table contains a list of the possible entries for use with the Euro File Transfer Client:



Value	Significance
GuestGroup	MRS User group which is the owner of the guest account. This account is required for Euro File Transfer and is by default the guest user that was entered during the installation. The account can be re-assigned to another user account.
GuestName	MRS User Name (description) for the Euro File Transfer guest access. This account is by default the guest user entered during the installation. The account can be re-assigned to another user account.
GuestPrivileges	MRS Privileges for the Euro File Transfer guest access. These privileges are by default those of the guest user entered during the installation. This entry applies only to those EFT privileges that can be entered here and separated by a comma.
GuestUser	MRS Login name for the Euro File Transfer guest access. This name is by default the guest user entered during the installation. The account can be re-assigned to another user account.
UserDirCorrelField	Normally, an individual Euro File Transfer directory is installed for each user. If this database field entry exists, directories can be installed for numerous users.

Value	Significance
WelcomeText	General welcome text. This greeting is automatically copied to the users directory when it is installed.

6.1.1.2 Euro File Transfer Client

This protocol contains the following configuration tabs that have already been described in the *Euro-File Transfer Server Protocol*: **General**, **Repeat Strategy**, and **Private**.

6.1.1.3 Fax Group 3

This protocol contains the following configuration tabs that have already been described in the *Euro-File Transfer Server Protocol*: **General** and **Repeat Strategy**.

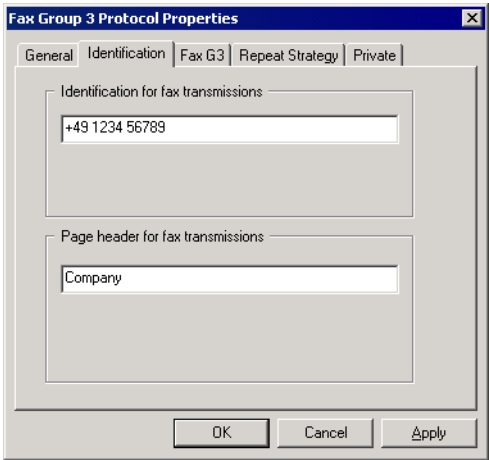
The following settings are also available in the configuration tabs.

Identification

If an entry is present in the fields **Identification for fax transmissions** and **Page header for fax transmissions**, these would be used instead of those global settings of the MRS Server for fax G3 identification and page header.

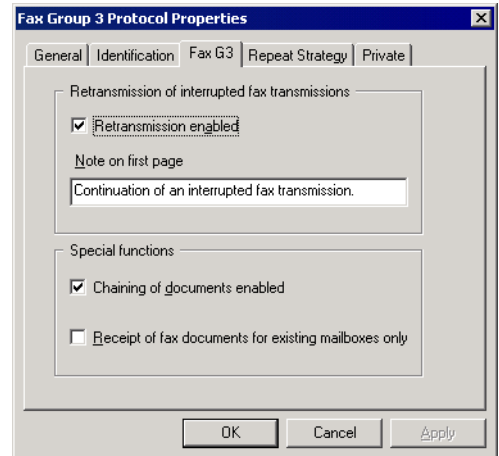
When individual identification and page header have been entered in the user database, these entries would be used instead of those of the MRS Server global settings.

The Identification should correspond with those of the T.30 standard which allows only digits, spaces, and plus signs (+).



Fax G3

When the option **Retransmission enabled** is enabled, fax documents which are interloped due to termination of the connection will be retransmitted from the point where the interruption occurred. To notify the recipient of this fact, the text contained in the field **Note on first page** is printed on the first page of the retransmitted fax document. If this method should fail the document will be retransmitted in its entirety until successfully received.



Activation of the option **Chaining of documents enabled** allows the transmission of several fax documents from various users to a single recipient. Originator, recipient and the fax resolution used must match.

The **receipt of fax documents** can also be restricted so that **only existing mailboxes** are allowed to receive incoming fax documents. This option has various advantages:

- If an incoming fax document is targeted for an unknown mailbox the server would not accept the call. This prevents unnecessary costs for the originator of the document.
- Since fax documents targeted for unknown addresses are not accepted, the Postmaster's account is not tasked with disseminating incorrectly addressed fax documents.
- Storage space on the harddisk is allocated only for deliverable fax documents.

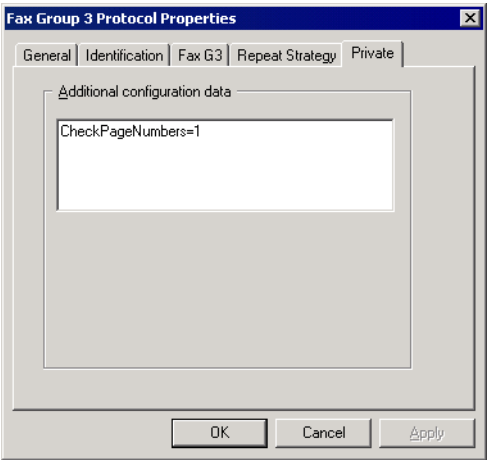
Fax documents are retransmitted until the document is correctly received or the conditions of the repeat strategy have expired.

Private

Private Data. These settings correspond in their operation to those in the INI configuration files from the Windows 3.1. One protocol specific entry may be entered per line (Value=...).

Example: InsertMidHl=1

The following table contains a list of the possible entries for use with the Fax G3 protocol:



Value	Significance
CheckPageNumbers	When set to 1 an OK report is only sent when the number of sent pages reported by the CAPI driver corresponds to the number of pages in the document. Otherwise it would be possible to receive an "OK (2 pages sent)" report for a four-page document.
DocChainIgnoreOrig	Only documents addressed to a single recipient and originating from a single sender may be chained when set to 0 in fax chaining for the fax G3 protocol. When set to 1 only the recipient address must be the same for the chained documents. In this case the originator address is not observed. If for example numerous fax documents are printer queued and two are addressed to the same recipient, both documents would be sent as a single transmission. In this case billing information is not processed.
InsertMidHl	When set to 1 the message ID will be inserted into the headline. The headline may be up to 22 characters in length.
UseFaxIdAsOAD	Calling Line Identification (CLI) would be used as the originator's OAD with inbound fax documents. If this field is empty while no CLI can be determined, the number in the fax ID will be used as CLI. When this value is set to 1 the fax ID will always be used as the CLI with inbound fax documents.

Value

Significance

Set this value to 1 if you always want to have the fax ID figures as originator instead of the transmitted CLI.

6.1.1.4 Fax Group 3 Polling

This protocol contains the following configuration tabs that have already been described in the *Euro-File Transfer Server Protocol* and with the *Fax G3 Protocol*: **General**, **Repeat Strategy**, and **Private**.

6.1.1.5 Fax-Fax-Converter (Transparent/Server)

Both Fax-Fax conversion protocols are described on page 61 of this manual. Possible settings correspond to those found in *Fax G3 Protocols*. The following table contains further configuration possibilities for the **Private** configurations tab:

Value

Significance

FfuAmt

Only when the *IntlDialMode* is set to 0 an exchange for Fax Forward Reports can be configured. Normally *LinePrefix* would be used.

FfuSendErrRep

When set to 1 an error report will be sent to the transmitting device by the MRS Server when an error occurs in Fax Forward mode.

FfuSendMidInId

When set to 1 internal fax devices receive the message ID number as fax ID by fax forward.

FfuSendOkRep

When set to 1 an receipt report will be sent to the transmitting device from the MRS Server by successful transmissions in Fax Forward mode.

FfuSendRundRep

When set to 1 an receipt report (with all recipients) will be sent to the transmitting device from the MRS Server by successful transmission of a distribution list in Fax Forward mode.

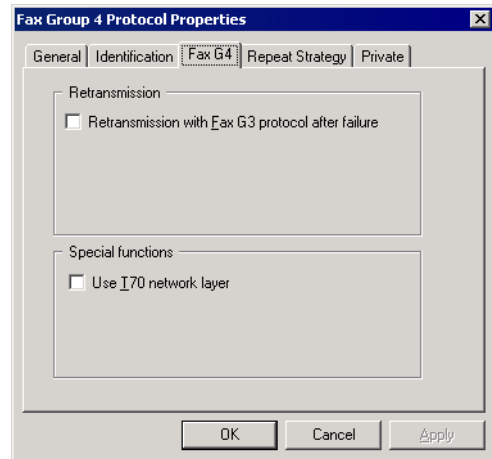
6.1.1.6 Fax Group 4

This protocol contains the same configuration tabs as those described in the *Euro-File Transfer Server Protocol*: **General**, **Repeat Strategy**. A **Private** configuration tab is also available but no options can be set in it yet.

Additionally, the **Identification** configuration tab is available for use. It should be noted that a page header may not be used with Fax G4 transmissions, but in accordance with F.200 standards, characters may be used in the fax identification.

In the **Fax G4** configurations tab the option **Retransmission with Fax G3 protocol after failure** enables the automatic retransmission of a document in a Fax G3 format. If the address entered for the Fax G4 is that of an analog and not that of a digital fax device, the resolution of the document would be reduced and sent as a Fax G3 transmission.

The switch **Use T70 network layer** uses either the older T70NL or ISO8208 as Layer 3. When in doubt the ISO8208 should be used since an incompatibility exists and Fax G4 documents cannot be transmitted from a T70NL connection to a ISO8208 connection.



6.1.1.7 MRS SMI-Protocol

This protocol contains the same configuration tabs as those described in the *Euro-File Transfer Server Protocol*: **General**, **Repeat Strategy** and **Private**. Currently no settings can be configured via the Private configuration tab.

6.1.1.8 SMS (TAP or UCP Protocol)

This protocol contains the same configuration tabs as those described in the *Euro-File Transfer Server Protocol*: **General** and **Repeat Strategy**.

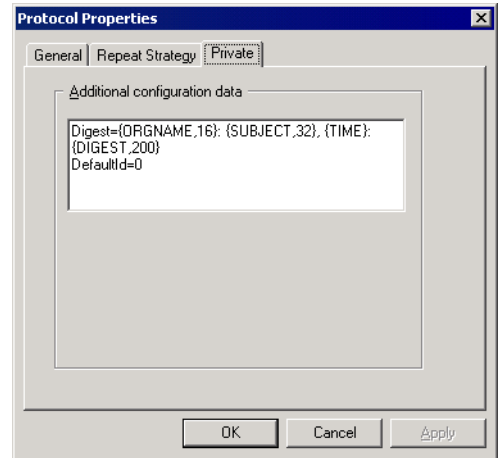
Private

Private Data. These settings correspond in their operation to those in the INI configuration files from the Windows 3.1. One protocol specific entry may be entered per line (Value=...).

Example:

Digest={{DATE}}, {DIGEST}}

The following table contains a list of the possible entries for use with the Fax G3 protocol:



Value	Significance
DefaultId	Default caller ID for SMS messages. Only with the UCP protocol a caller ID can be transmitted that is normally taken from a user's SMS database field. Otherwise the default ID specified here is delivered. Vodafone D2 uses UCP, whereas T-D1 uses TAP which does not allow originator ID transmission.
Digest	Transmitted text messages can be modified through the use of several variables: transmission time, etc. Possible variables corresponding to those used in CIT notifications are displayed in the following table.

Overview of variables used in the SMS Protocol value Digest

Variable	Significance
{DATE}	Date.
{DIGEST[, <Max>]}	A portion of the original message is embedded in the Report. The maxim length can be defined through the optional entry <Max>. The algorithm used for building the Digest attempts to retrieve the text without a loss of information. Example: Empty lines, greetings, ...
{FORMAT}	Original message format (e.g. Voice, Fax or E-Mail).

Server Administration

Integrated Services Digital Network (ISDNAPL)

Variable	Significance
{ORGRNAME[, <Max>]}	Readable form of the originator address. If information over the fax originator is contained in the Alias database, this could appear as a name instead of a fax number. The maxim length can be defined through the optional entry <Max>.
{ORGRNODE}	Incoming Service
{ORGRUSER}	Originator Address
{RECRNAME[, <Max>]}	A readable form of the recipient address. The maxim length can be defined through the optional entry <Max>.
{RECRNODE}	Target Service
{RECRUSER}	Recipient Address
{SUBJECT[, <Max>]}	Subject line of the original message. The maximum length can be defined through the optional entry <Max>. If the actual length is longer than <Max>, it will be truncated and “...” appended.
{TIME}	Time

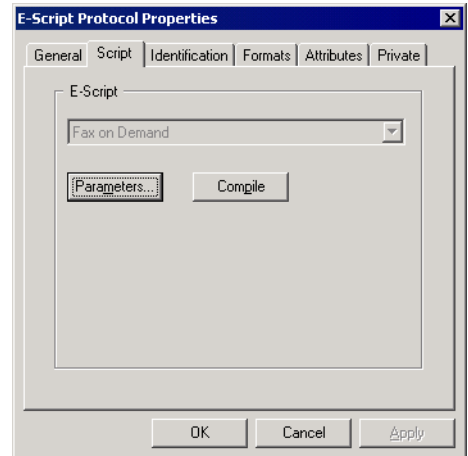
6.1.1.9 Scripts

The Cycos own ‘E’ script language enables implementing further **Protocols**. Just like with the precursor VFS, individual voice and fax mailboxes, Fax-on-Demand server etc. can be realized with E providing a significantly more efficient language and, in particular for programers, a more comprehensive API with nearly all MRS specific functions.

The standard scope of delivery already includes scripts for the first two applications the configuration of which is described in the following. These are here the VFS based standard voice/fax mailbox and Fax-on-Demand realized with E. As TUI the modern ERGO, aimed at convenient Unified Messaging, is available. It was written in E and its configuration and operation is described in an individual manual.

Via the **Script** configuration tab you can select one of the installed E- or VFS scripts. Selecting the **Parameters...** button enables the actual configuration of the script and **Compile** is used for script compilation. This is only required when you have developed new scripts yourself which are thus present in the source. In most cases an already compiled object file is available which can be executed by the server.

In the following, various standard MRS script configurations are described. These settings are found through selection of the **Parameter** button.



Standard Voice/Fax Mailbox

This script is the user's personal answering machine in which voice mail messages can be received and played-back anytime. Inbound fax messages can be rerouted to other fax devices and email messages can be read using the text to speech module.

The menu structure of this script can be seen in the *Standard Voice/Fax Mailbox* documentation.

Further configuration occurs by selecting the numbered button preceding the Script name *Standard Voice/Fax Mailbox*.

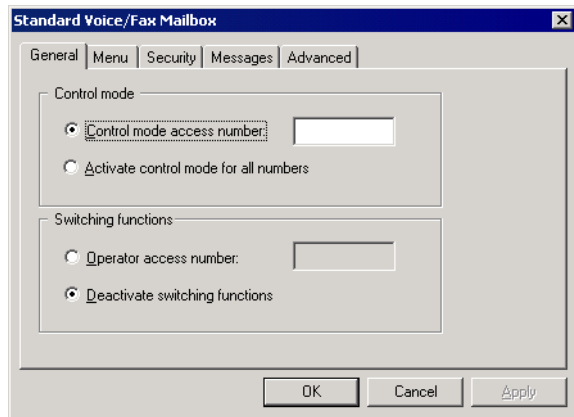
With a click on the numbered button before the installed script **Standard Voice/Fax Mailbox**, occurs the further configuration of this service.

The **Control mode access number** is the number allocated from the extension number range required by mailbox owners to access their mailboxes. Here users can retrieve their messages and e.g. route fax documents to fax devices. Example: The extension numbers 10 to 99 are allocated to the script. The extensions 10 to 98 are used as access numbers to the users mailbox for outside callers wishing to leave a

voice mail or fax messages. The extension 99 would be designated as the control access number in which the mailbox owner dials. After entering their mailbox number and PIN code through a DTMF (touchtone) telephone, the user may query any inbound messages in their mailbox.

The option **Activate control mode for all numbers** is normally used when the control mode number does not originate from the extension number range of the user. In this case, two extension number ranges would be assigned in the number plan. One range is the user mode to which inbound messages are sent. The other range consists in most cases of a single number which is used as the control mode number. Over this number the mailbox owner switches directly in the control mode and is then able to query any inbound messages.

If switching is possible with the implemented ISDN boards, thus they have, for example, an MVIP bus (e.g. ITK Ix Octo or ITK Ix Primary), the operator or the person chosen for this role can be directly dialed from mailbox operation via **Operator access**. A mailbox owner can just as well directly connect him or herself to a caller that left a



message. This function of the standard voice/fax mailbox can also be deactivated. Thus three modes are available for switching functions:

- **Operator access number:** selected, but no number specified.
External switching is permitted but there is no operator that could be dialed for help.
- **Operator access number:** selected and a number specified.
External switching is permitted and beyond that you can contact an operator if problems occur.
- **Deactivate switching functions** selected.

Options available to all mailbox owners are determined in the configuration tab **Menu**. The speech menu is expanded with each activated option item, and therefore becomes more complicated. The individual options are listed as follows:

- **Fax**

All fax functions. This menu tree must be deactivated if the script is bound to an ISDN card that does not have fax functions.

- **Distribution lists**

Distribution lists can be administered from the telephone and used for message transmissions to numerous recipients.

- **Outbound journal**

Outbound journal querying e.g. status of fax transmissions.

- **Automatic inbound query**

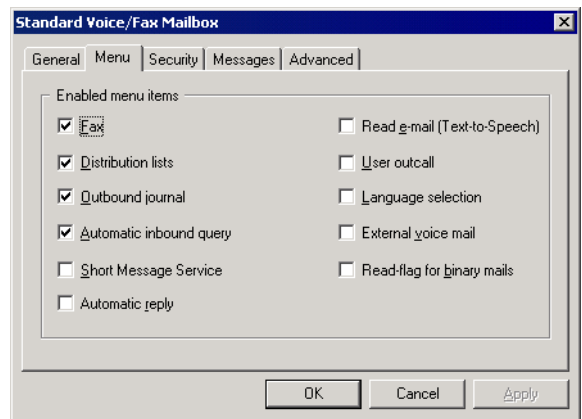
This function enables the sequential querying of all new messages by depressing one DTMF key.

- **Short Message Service**

Notification of new message delivery can optionally be over SMS Short Message Service to cellular telephone entered in the user database.

- **Automatic reply**

When a valid address is available, replies to messages can be made without manual input of the address.



Server Administration

Integrated Services Digital Network (ISDNAPL)

- **Read e-mail (Text-to-Speech)**

Inbound email messages can be read over the telephone through use of text to speech integration.

- **User outcall**

Mailbox owners can reply directly to callers who have left messages when the ISDN card is equipped with a MVIP bus.

New message notification can optionally occur per user outcall. In this case the MRS Server calls the specified number and plays the selected greeting. Subsequently you need to legitimate yourself by entering the individual password (PIN) before new messages can be accessed.

If a user selects this notification option per voice menu, then “<protocol>/<number>” is written in the CIT database field, thus for example MCK/123456789.

- **Language selection**

The script is available in various languages. The mailbox owner has the option of switching between the various languages.

- **External voice mail**

Voice mail messages can only be sent internally by default. When this option is activated, transmission of voice mail messages to external addresses is possible.

- **Read-flag for binary mails**

Sets all received emails and fax messages (only in voice operations) automatically to “read”. This delivers the status message “No new messages” after playing-back voice mail messages and resets the message waiting lamp on the telephone.

Thus the Standard Voice/Fax Mailbox provides three different types of new message notification which the user can select via the speech menu:

- **Notification via telephone LED.**

If a user has selected this notification option, the protocol and number for setting the LED is written in the CIT database field. “CIT_BASIC/<number>” (Hicom PBX via modem of the V.24 system) or “MWI/<number>” (MWI protocol via CTI APL or the E-script MWIIsdn.e in the ISDN or Dialogic APL), thus for example MWI/123. The protocol depends on the PBX.

- **Message waiting lamp.**

“CIT_BASIC/<Number>” is entered in the database field CIT, e.g. CIT_BASIC/123.

- **Notification over SMS Short Message Service.**

- **Notification over User Outcall.**

The **Default PIN** (Personal Identification Number) **at first login**: for mailbox owners is set in this dialog. This entry is valid unless the administrator has assigned PIN numbers in the appropriate field of the user database.

Notice: Since this is a default PIN number, it should be immediately changed by the new mailbox owner.

The switch **Pin expires after**: determines the validity length of the PIN number. Mailbox owners are automatically instructed to enter a new PIN number after expiration of the time period.

The **Maximum voice mail length**: for recorded messages is defined in the **Messages** configuration tab.

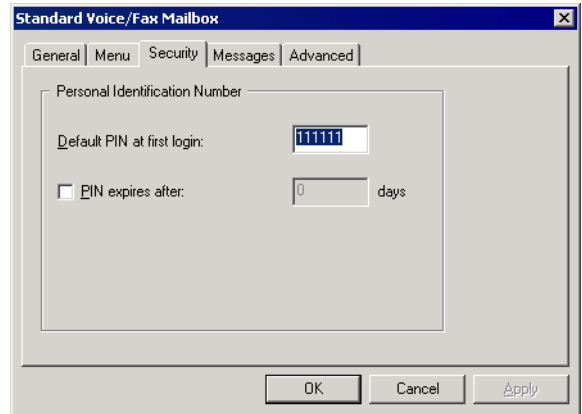
If other times are to be allocated to individual users, this should be done through the user database. Recording times for the individual users can be entered in the database field **MAXRECTIME**. If it is to be used, this database field must be inserted in the user database.

When the option **Limit journal to: ... messages** is activated, the user will be prompted when this limit is exceeded.

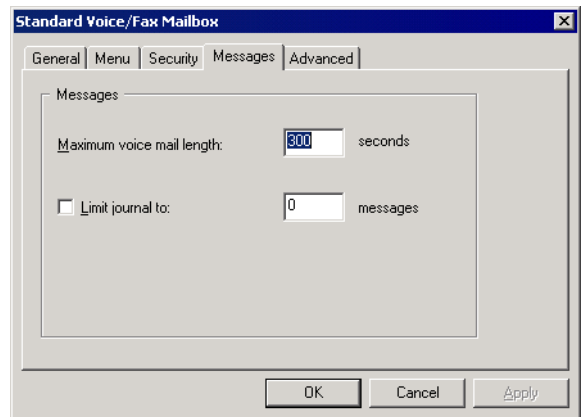
The **Advanced** configurations tab will be used in the future for additional parameters to customized script extensions. Furthermore the following options which cannot be configured in the previous tabs are available:

-askformailbox

If the Standard Voice/Fax Mailbox has already identified the caller on grounds of his transmitted telephone number with switching to the control mode, only the PIN is queried and not the mailbox number. If the mailbox number is to be queried in each case this parameter should be entered.



The image shows a screenshot of the 'Standard Voice/Fax Mailbox' dialog box with the 'Security' tab selected. The 'Personal Identification Number' section contains a text field for 'Default PIN at first login' with the value '111111' and a checkbox for 'PIN expires after' which is currently unchecked. The 'days' field next to it contains the value '0'. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.



The image shows a screenshot of the 'Standard Voice/Fax Mailbox' dialog box with the 'Messages' tab selected. The 'Messages' section contains a text field for 'Maximum voice mail length' with the value '300' and the unit 'seconds'. Below it is a checkbox for 'Limit journal to:' which is currently unchecked, followed by a text field with the value '0' and the unit 'messages'. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

Server Administration

Integrated Services Digital Network (ISDNAPL)

-uocname=<Script Name>

With activated **User Outcall** this parameter must be entered if the protocol name for the Standard Voice/Fax Mailbox does no longer correspond to the default script name mck but has been changed.

Example: -uocname=VOICEFAX

-BeepDe lay=<Time in Seconds>

Time in seconds between the personal announcement and the beep which indicates the start of the recording. This value can be upgraded if you have all subscribers recording an announcement text ending with "Press 0 for connection to the operator...". This parameter can be used to give the caller sufficient time for pressing 0 after the announcement.

Via entry of the mobile phone number or another digital (ISDN) telephone number in the database field **DIRECT-LOGON** the user is automatically logged in at the system when he calls his mailbox from the corresponding telephone.

To get output on the displays of a telephone connected to a Hicom 300 you should set the value **ACLUse (DWORD)** in the registry key **HKLM\Software\PP-COM\MRS\IsdnApl\Vfs** to 1.

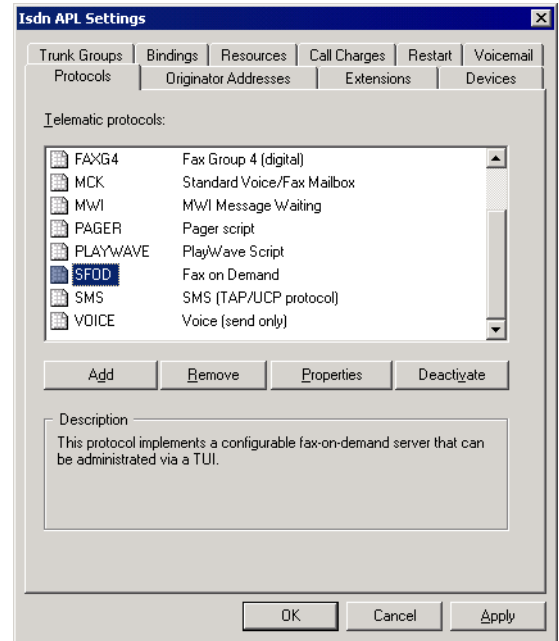
Fax-on-Demand Server

A description of the three modes of this script and the associated options is found in the "Fax-on-Demand Server" section from page 66.

In the script configuration the three standard services of the Fax-on-Demand server are set. You can assign documents an extension number so that these are automatically sent when the number is dialed. Furthermore, polling is enabled via DTMF tones of an MFV compatible telephone. The access numbers to be entered correspond to the numbers required for dialing in into the system. The polling numbers that you enter for specifying the desired documents must originate from the extension number range assigned to the script and must not be identical!

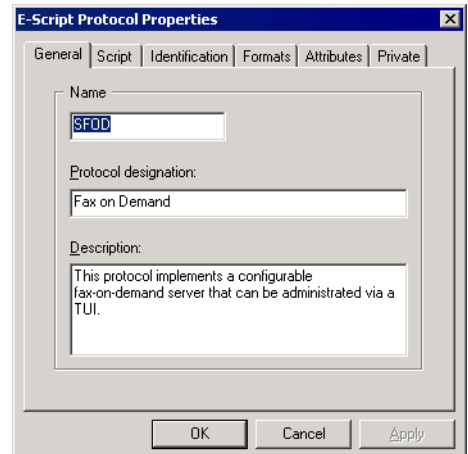
In order to reach the configuration dialog of the Fax-on-Demand server, open the settings dialog of the Telematic APL (ISDN APL) in the MRS Monitor.

In the **Protocols** tab select the Fax on Demand protocol and click on **Properties**.



The configuration dialog of the Fax on Demand protocol opens.

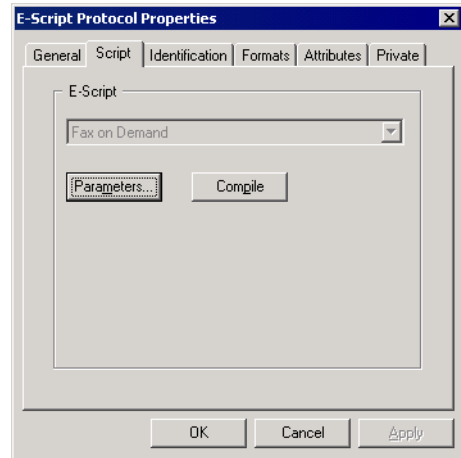
In the **General** tab you can modify the settings for the name, the protocol designation and a supplementing description.



Server Administration

Integrated Services Digital Network (ISDNAPL)

To configure the Fax-on-Demand script, switch to the **Script** tab and in there press **Parameters**.



The Fax-on-Demand script configuration dialog opens.

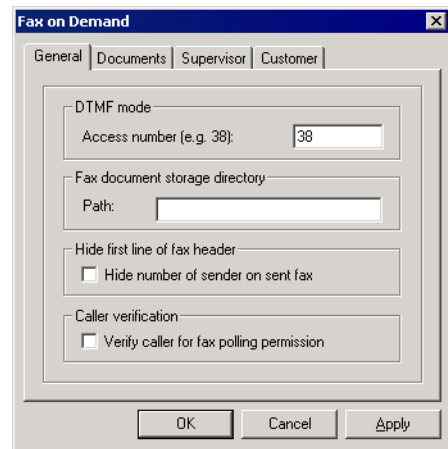
General Tab:

In the **DTMF mode** portion enter the access number via which a user can poll Fax-on-Demand documents in the voice menu operated DTMF mode (see page 68).

If you do not want Fax-on-Demand documents to be stored in the default folder (<MRS Root>\userdata\fod), you can enter the path to another filing directory in the **Fax document storage directory** section.

The option **Hide number of sender on sent fax** under **Hide first line of fax header** prevents an originator information from appearing in the header of the polled fax.

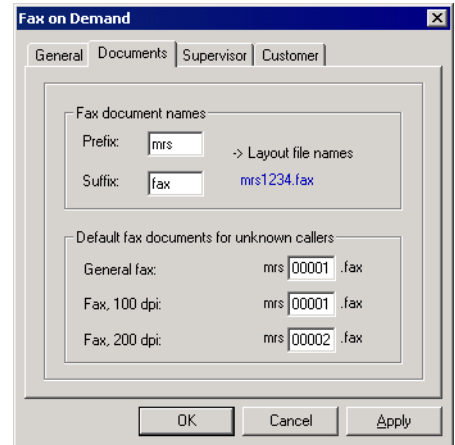
If you only want users entered in the MRS database, and for who the Fax-on-Demand privilege (FAXG3REV) is active, to use the fax polling service, checkmark the **Verify caller for fax polling permission** option. Users not present in the database receive a standard fax document when the option is active (see page 133).



Documents Tab:

The **Fax document names** portion serves to alter the prefix and suffix of the saved Fax-on-Demand documents. Under **Layout file names** you can then see the modifications performed.

Use the **Default fax documents for unknown callers** section to define which fax documents are sent to users unknown to the system. These fax documents are only transmitted when in the **General** tab the **Verify caller for fax polling permission** option is active (see page 132).



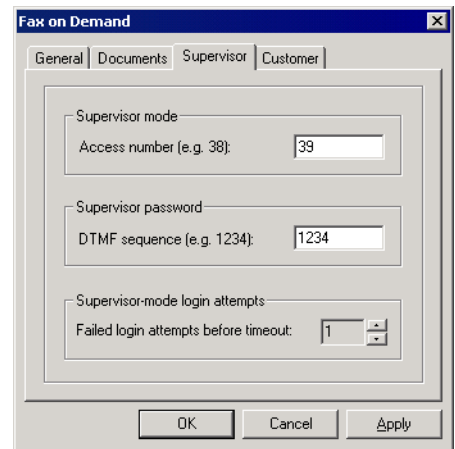
The screenshot shows the 'Fax on Demand' window with the 'Documents' tab selected. The 'Fax document names' section has 'Prefix' set to 'mrs' and 'Suffix' set to 'fax'. To the right, 'Layout file names' shows 'mrs1234.fax'. The 'Default fax documents for unknown callers' section has three entries: 'General fax' with 'mrs00001.fax', 'Fax, 100 dpi' with 'mrs00001.fax', and 'Fax, 200 dpi' with 'mrs00002.fax'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Supervisor Tab:

In the **Supervisor mode** section enter the access number that leads to the voice menu operated supervisor mode (see page 70). In this mode you can file, rename and delete Fax-on-Demand documents.

The password (PIN) to enter the supervisor mode is specified in the **DTMF sequence** field.

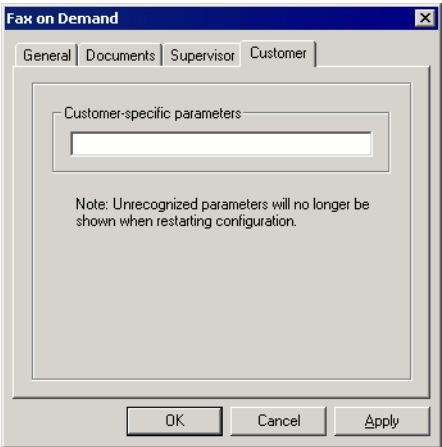
The **Supervisor-mode login attempts** portion serves to define how many login attempts may fail until the system quits the login procedure.



The screenshot shows the 'Fax on Demand' window with the 'Supervisor' tab selected. The 'Supervisor mode' section has 'Access number (e.g. 38)' set to '39'. The 'Supervisor password' section has 'DTMF sequence (e.g. 1234)' set to '1234'. The 'Supervisor-mode login attempts' section has 'Failed login attempts before timeout' set to '1'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Customer Tab:

In the **Customer specific parameters** field you can enter all configurable parameters of the configuration dialog as command line parameters. In the following find a list of the available parameters:



Parameter	Description	Default Setting
<i>check</i>	Activates/deactivates the caller's Fax-on-Demand privilege	false (deactivated)
<i>hideorigin</i>	Activates/deactivates hiding the fax header.	false (deactivated)
<i>path</i>	Sets the path to the fax filing folder	<empty> for default folders
<i>prefix</i>	Sets the prefix for all Fax-on-Demand folders.	prefix=mrs
<i>recdefault</i>	Sets the calling number of the default fax document sent to unknown users.	recdefault=00001
<i>rec100dpi</i>	Sets the calling number of the 100dpi default fax document sent to unknown users.	rec100dpi=00001
<i>rec200dpi</i>	Sets the calling number of the 200dpi default fax document sent to unknown users.	rec200dpi=00002
<i>suffix</i>	Sets the suffix for all Fax-on-Demand documents.	suffix=fax
<i>admin</i>	Sets the access calling number for the supervisor mode.	admin=0

<i>dtmf</i>	Sets the access calling number for the dtmf=0 DTMF mode.
<i>pin</i>	Sets the access PIN for the supervisor mode. pin=0000
<i>tries</i>	Sets the number of tolerated failed attempts tries=1 to log in at the supervisor mode.

Example:

When you enter the command line instruction `hideorigin` in this dialog and save it, the **Hide first line of fax header** option in the **General** tab (siehe page 132) changes.

Message Waiting Indication

The MWI protocol implemented via the MWIISDN.e script for Siemens PBXs transmits information required for setting the LED and the display via the D-channel (Cor-net-N/NQ or QSIG). Depending on the PBX a callback number is required which is dialed when the user presses the activated LED. This callback number is transferred to the script parameter field in the format `CALLBACK=<number>`.

In most cases this number corresponds to the callback access number configured with the TUI used so that you are directly connected to the TUI by the telephone LED for playing back a new message.

This requires further settings with most PBXs. The number e.g. set in the script as callback access and used as callback number in the MWI protocol must be equally administered in the Hicom 300. This is done in the AMO RICHT with parameter PM. Here a maximum of 20 servers that may set MWI can be administered per Hicom.

6.1.1.10 Voice Play-back via Telephone

This protocol enables the output of voice mail messages to the telephone.

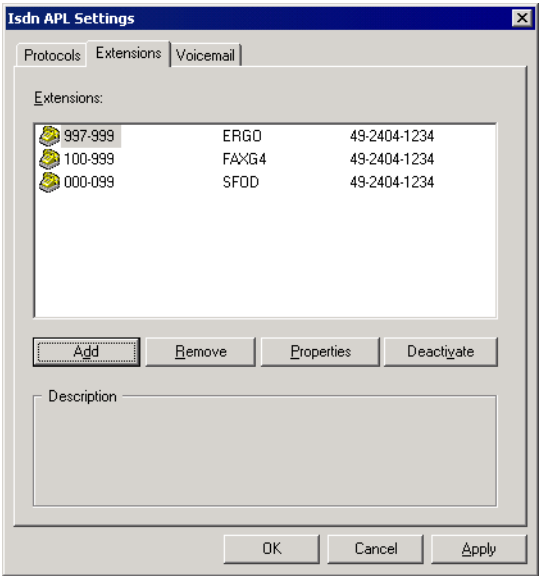
The protocol's configuration tabs **General** and **Repeat Strategy** correspond to those already described with the *Euro-File Transfer Server Protocol*. In the **Private** configuration tab an option is available for the recording of a called party. Settings for this option are described in the *MRS System Architecture*.

6.1.2 Extensions

The assignment of number ranges to the various protocols is accomplished in this dialog. Inbound calls are bound to the various protocols through the use of extension number ranges.

Selection of the buttons **Add**, **Remove**, or **Deactivate** switches-off the selected extension number range while retaining the current configuration.

If a deactivated extension number range is selected, the **Deactivate** button automatically switches to **Activate**, and the extension number range may be reactivated.



Selecting the **Properties** button enables configuration of the various settings for the selected extension number range.

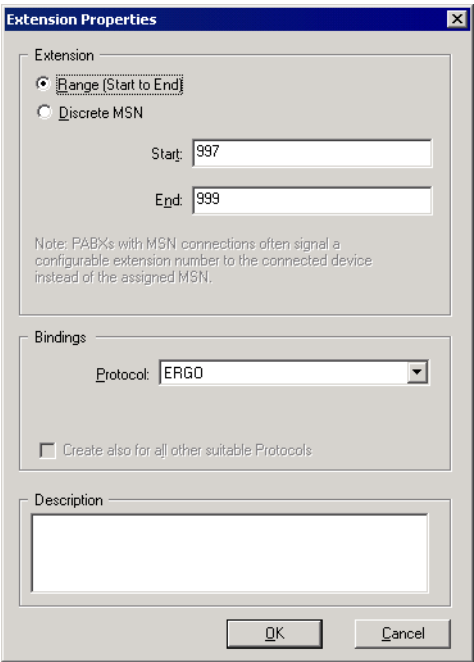
Extension Properties

The **Start** and **End** of a extension number range is defined in the corresponding input field.

If a Point-to-Point connection is not available, but a Point-to-Multipoint is present, a **Discrete MSN** (Multiple Subscriber Number) can be assigned to the protocol instead of an extension number range. The ISDN APL will then only take calls on the MSN for this protocol.

Bindings

In this portion of the dialog number ranges are assigned to installed protocols and OADs. When the service type can be determined from the D-Channel information, it is possible to assign a single extension number range to several services (protocols). This is sup-



ported by the option **Create also for all other suitable Protocols** which automatically assigns analog extension number ranges to installed protocols. These are usually Fax G4 and one protocol including Fax G3 reception, e.g. the **Standard Voice/Fax Mailbox**.

Attention: Since no distinction can be made through the D-Channel information between FAXG3, VFS-Scripts and E-Scripts, a single extension number range may not be used for these services. This also applies the EFT (Euro File Transfer) and MRS SMI protocols.

Description

An optional description for the extension number range can also be entered for display in this dialog.

The following is a description of the Advanced Options.

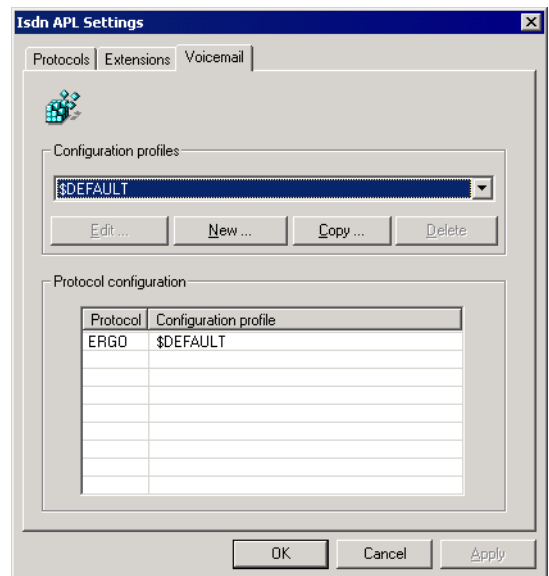
6.1.3 Voice mail

More recent voice mail server such as Ergo, PhoneMail or VMS support a common database layout for functions generally used, so that these configuration data can be globally set here for all these systems. With these global settings **Configuration profiles** can be created that are assigned to the respective protocols in the **Protocol configuration** section.

A voice mail server need not use all setting options offered but when a corresponding function is intended, it is set here.

The default settings in the \$DEFAULT profile cannot be modified so that you can always return to them.

To select other settings either choose, modify and subsequently save an existing profile under a new name by means of **Copy...** Or generate a configuration profile from scratch via **New...** Existing profiles with the exception of \$DEFAULT can be modified with **Edit...** or removed with **Delete**. A profile consists of the configuration tabs described in the following.



6.1.3.1 General Settings

First you can enter a **Profile name** under which this configuration profile can be assigned to a protocol at a later date.

All greetings recorded by the user or system greetings recorded by the administrator are normally stored in the `vmdata` subdirectory in the `\\<MRS>\userdata` structure. The `userdata` directory is shared under the name `MrsUserdata$`. Various voice mail systems could thus use a common directory or an individual one each by specification of another directory under **Voice mail data path**.

The user is warned by a beep that he or she has only a few seconds left for finishing a recording. This acoustic alarm can be replaced with an individual greeting in the **Alternative warn prompt** field.

The screenshot shows a Windows-style dialog box titled "General Settings" with a close button (X) in the top right corner. The dialog has two tabs: "General settings" (selected) and "Messaging settings". Under "General settings", there are three main sections: "Profile name" with a text input field; "Voicemail data path" with a text input field containing "\\GUSTAV\MrsUserdata\$\vmdata" and a "Browse ..." button; and "Alternative warn prompt" with a text input field and a "Browse ..." button. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

6.1.3.2 Messaging Settings

Inbox Settings

With quotas activated in the MTA you can by means of **Quota threshold** enter a value in percent from which the user is warned by the TUI that his or her quota will soon expire. Note that this option in True Unified Messaging environments, where the Microsoft Exchange or Lotus Notes message store is used, is considered useless since the MTA quota function does not monitor this external message store.

In **Max. Inbox documents** the number of messages offered by the TUI is restricted. Depending on the sorting set in the WebAdmin you always receive the first n messages with n corresponding to the value set here.

Options

Here you can **disable** the features **SMS notification** and **distribution lists**.

The screenshot shows a 'Messaging settings' dialog box with three tabs: 'Recording settings', 'Security settings', and 'Call transfer settings'. The 'Security settings' tab is active, showing 'General settings' and 'Messaging settings'. Under 'Inbox settings', 'Quota threshold (in %)' is set to 0 and 'Max. Inbox documents' is set to 100. Under 'Options', there are two unchecked checkboxes: 'Disable SMS notification' and 'Disable distribution lists'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

6.1.3.3 Recording Settings

Here you can default set the maximum recording length to limit the file size.

Max. length of name recording refers to a voicebox owner's name that can be recorded to be played back to a caller. This helps the caller to make sure that he or she has dialed the correct number.

Max. length of announcements limits voice box owners in their recording of announcements via the TUI.

Max. length of messages is a default setting referring to a caller. The caller can leave a message but will be interrupted after the period set here. Shortly before the recording time is up, the caller receives a warning.

Via **Min. length of any recording** you can set a minimum period that a recorded message, name greeting or greeting must have lasted before it is stored. In this way no new message is stored when the caller e.g. has immediately hung up again.

The screenshot shows a 'Recording Settings' dialog box with a blue title bar and a close button. It has two main tabs: 'General settings' and 'Messaging settings'. Under 'General settings', there are three sub-tabs: 'Recording settings' (selected), 'Security settings', and 'Call transfer settings'. The 'Recording settings' tab contains four settings, each with a text input field and a spin button: 'Max. length of name recording (in sec)' with a value of 10, 'Max. length of announcements (in sec)' with a value of 60, 'Max. length of messages (in sec)' with a value of 300, and 'Min. length of any recording (in ms)' with a value of 0. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

6.1.3.4 Security Settings

The **Min. telephone password (PIN)⁹ length** determines the minimum number of digits that a new PIN must have. A PIN should be long enough to increase security but short enough to be kept in mind.

Via **Number of stored telephone passwords (PIN)** the system encodes and stores a number of PINs previously used. These PINs are checked when the current PIN is modified so that a real new one must be entered instead of e.g. toggling between to old ones. Entering 0 disables the function.

In **Telephone password (PIN) expiration** you can enter a number of days after which a PIN is considered invalid and the user is prompted to enter a new one. Entering 0 disables the function.

By means of **Max. tolerated login failures** you can specify a value from which measures set in the **Sanctions...** section are to become active. Furthermore the system hangs up when the value has been reached so that a call needs to be repeated. If the **Lock voicebox** option was set then, redialing is impossible and the voicebox must first be unlocked again by the administrator.

In the **Default PIN** field you can allocate a PIN for a user to perform the first login. In most cases the user is then prompted to specify an individual PIN.

The screenshot shows a dialog box titled "Security settings" with a close button (X) in the top right corner. The dialog has a tabbed interface with four tabs: "General settings", "Messaging settings", "Recording settings", and "Security settings". The "Security settings" tab is currently selected. Inside the dialog, there are several configuration options, each with a text input field and a small up/down arrow button:

- Min. telephone password (PIN) length:** The input field contains the value "5".
- Number of stored telephone passwords (PIN):** The input field contains the value "0".
- Telephone password (PIN) expiration:** The input field contains the value "0".
- Max. tolerated login failures:** The input field contains the value "3".
- Default PIN:** The input field contains the value "0000".
- Sanctions on too many invalid logins:** This section contains a checkbox labeled "Lock voicebox", which is currently unchecked.

At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Apply".

9. Personal Identification Number, occasionally also called telephone password.

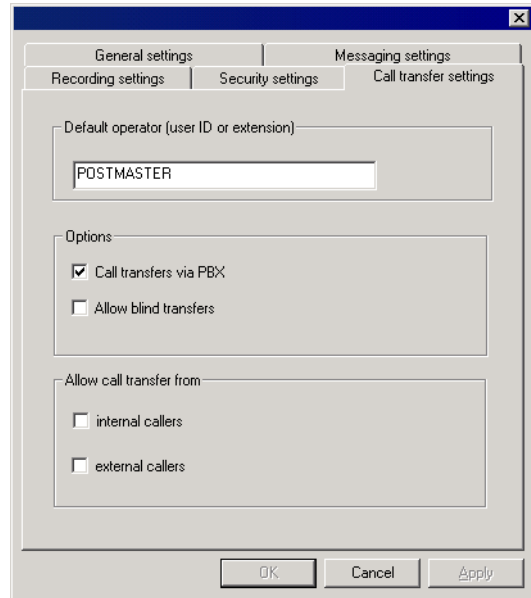
6.1.3.5 Call Transfer Settings

A caller may be put through to the **Default operator**. The corresponding extension or user ID must be entered here for this purpose. In the latter case the associating telephone number is taken from the user database.

Using the **Call transfers via PBX** option, call forwarding is performed in the telephone system. This is not always possible so that this option must not be set then and call transfers are realised via a second B-channel on which the MRS Server dials out.

Via **Allow blind transfers** you can activate this type of forwarding. With a blind transfer the target is not checked for availability so that the caller either receives a busy sign or is even routed to the voice mail system in the user's mailbox again that he or she wanted to be put through to.

The **Allow call transfer from internal callers/external callers** option is used to decide whether a caller can be routed to a stand-in or to the operator. A voicebox owner can appoint a stand-in to who a caller is automatically put through after calling the corresponding menu command. Alternatively a default operator can be made available for callers that do not want to leave a message but immediately get in touch with the callee. The permission to that is given through activation of the corresponding option for internal and/or external callers.



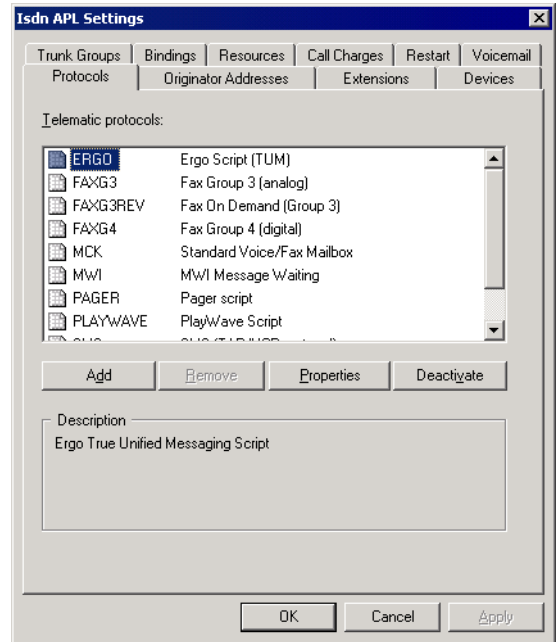
The screenshot shows a dialog box titled "Call Transfer Settings" with a close button (X) in the top right corner. The dialog has four tabs: "General settings", "Messaging settings", "Recording settings", and "Security settings". The "Call transfer settings" tab is currently selected. Inside the dialog, there is a section labeled "Default operator (user ID or extension)" with a text input field containing the text "POSTMASTER". Below this is a section labeled "Options" containing two checkboxes: "Call transfers via PBX" (which is checked) and "Allow blind transfers" (which is unchecked). At the bottom of the dialog is a section labeled "Allow call transfer from" with two checkboxes: "internal callers" (unchecked) and "external callers" (unchecked). At the very bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

In the following find the **extended settings** of the ISDN APL.

6.1.4 Telematic Protocols

The Advanced Option settings for the various ISDN protocols corresponds with those described in the section for Telematic Protocols at the beginning of this chapter. Two further options are also available for the protocol settings, but a modification of the default settings are normally not required.

These options include the supported formats and protocol attributes.

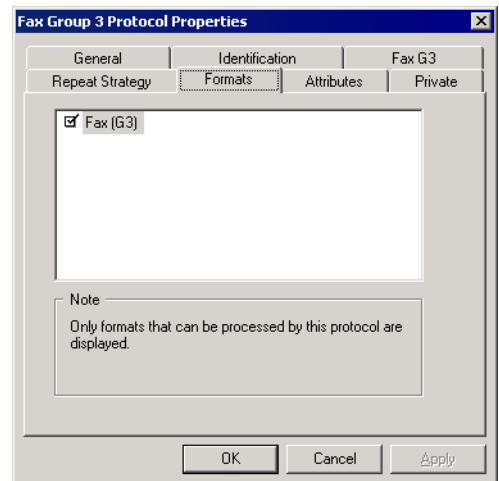


Formats

In this dialog the various file formats are displayed which are supported by the individual protocols. The MRS Server makes the necessary conversion (when possible) to one of the formats listed here for outgoing transmissions.

If a conversion is not possible, an error report would be generated by the server informing the user that document could not be sent by the selected protocol.

Since files sent using the Euro-File-Transport are in a binary form, no conversions are necessary.

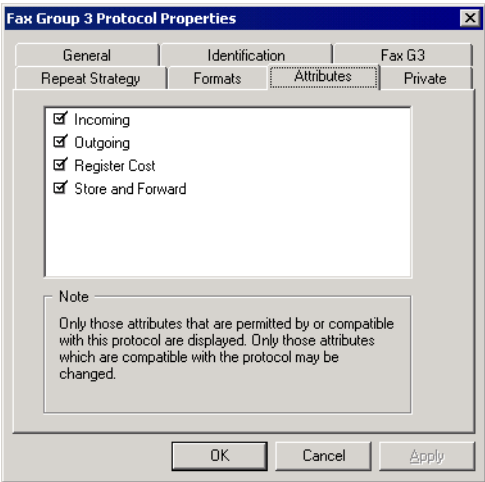


Attributes

In this dialog protocol attributes are displayed and can be activated or deactivated by clicking on the entry.

If for example the Outgoing attribute were to be deactivated, only incoming documents would be processed by the protocol.

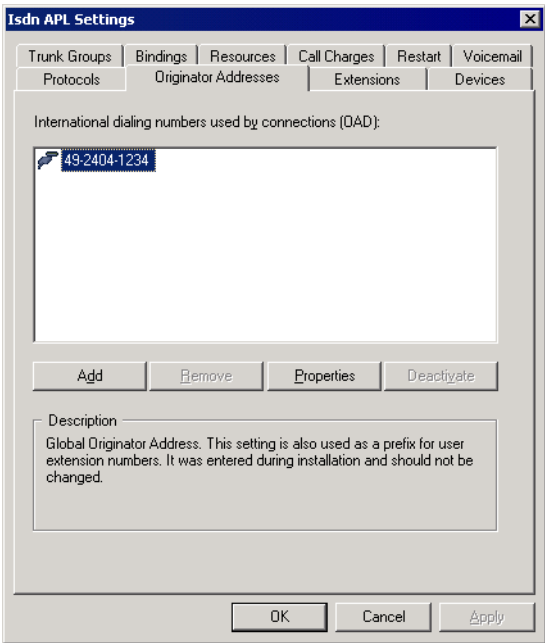
In most cases these settings should not be modified by the user.



6.1.5 Originator Addresses

Originator addresses (OADs) used by the ISDN APL that differ from those of the global configuration are assigned in this dialog. The first calling number displayed is always the global OAD which is, for example, used for normalization by the server. It must correspond to the system calling number without extensions so that normalization can be correctly performed for CTI.

If the OAD to be used by the ISDN APL deviates from the system calling number, thus for example contains a cross connection number, another OAD must be added here and the line bundles and extension ranges linked to this OAD.



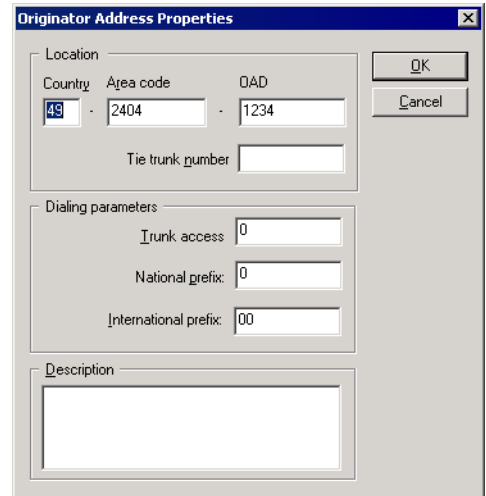
Extension numbers are administered through use of the **Add**, **Remove**, **Activate**, and **Deactivate** buttons. The **Deactivate** button turns into **Activate** when you dial a deactivated originator address.

The individual settings of extension numbers can be configured through use of the **Properties** button. If a direct connection is made to the telephone exchange, the number should be entered and no entry should be made in the field **Tie trunk number**. With connections to the PBX that are made over a cross-connection the ISDN APL's behavior is that of a sub-system. In this case the cross-connection number is to be stated if it is transmitted by the PBX. In most cases configuration already occurs internally in the PBX and specifying the cross-connection number can be omitted. Via the **Line Bundles** tab these numbers are bound to a logical line bundle which in turn belongs to a physical ISDN connection.

Furthermore the trunk access as well as national and international prefixes can be set for the calling number.

Finally an optional description for the extension can also be entered for display in this dialog. In this way maintenance personnel can be provided with important information.

The ISDN APL interprets numbers with more than 9 digits as a number in an international format. If when selecting a number with such a format, an error should occur, the global originator address (first OAD) should be checked for accuracy. A logging monitor to display the topic **DIALINFO** of the ISDN APL and for activation of all filters can be configured in the MRS Monitor.



The image shows a Windows-style dialog box titled "Originator Address Properties". It contains several input fields and buttons. The "Location" section has three fields: "Country" (with a dropdown menu showing "49"), "Area code" (with the value "2404"), and "OAD" (with the value "1234"). Below these is a "Tie trunk number" field. The "Dialing parameters" section has three fields: "Trunk access" (with the value "0"), "National prefix" (with the value "0"), and "International prefix" (with the value "00"). At the bottom is a "Description" section with a large text area. On the right side of the dialog are "OK" and "Cancel" buttons.

6.1.6 Extensions

The Advanced Option settings for the Extension number ranges corresponds with those described in the section for Telematic Protocols at the beginning of this chapter.

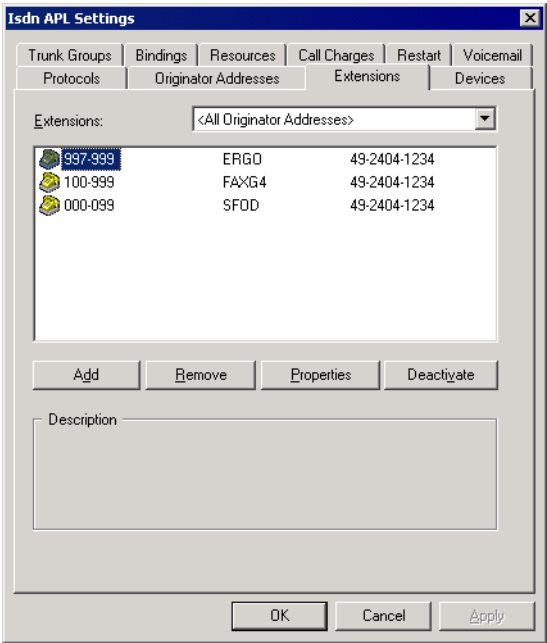
 In contrast to the normal settings configuration menu, extension numbers for Originator Addresses other than that of the MRS Server can be configured. The extension range is selected and subsequently **Properties** button.

Advanced Options

The extension properties provide the following additional options which cannot be set with normal configurations.

If the option **Allow variable length** is activated numbers dialed from outside the system may be of a variable length. If the extension number range is defined as 6 digits in length e.g. 700000 to 999999, then any inbound call with 1 to 6 digits beginning with 7 and extending to 999999 would be forwarded according to the implemented *Routing Rules*.

The option **Allow superfluous** digits ignores any additional digits that are inputted after the actual number. This could apply for the extraneous numbers 500, 50123, etc. for the user with the extension number 50. Without this option the ISND APL would be unable to ascertain a user for the inbound routing, or refuse to take the call. The interaction between the options **Allow superfluous** and **Allow variable length** is presently unknown!



6.1.7 Devices

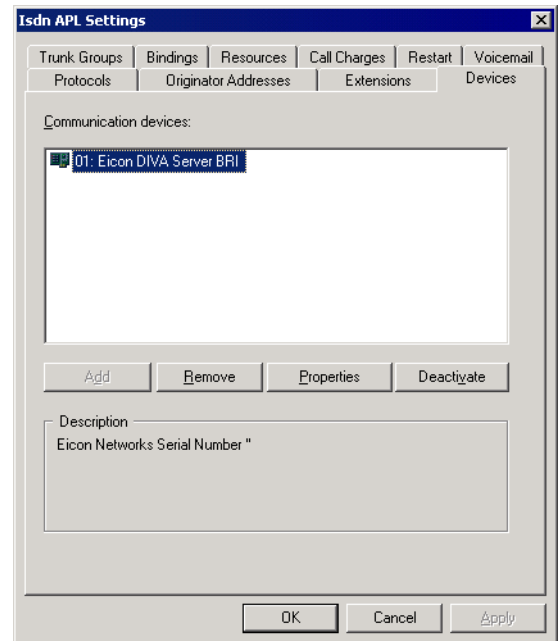
This configuration tab displays all ISDN boards installed in the MRS Server and supported by the ISDN APL. An automatic hardware recognition is performed for this purpose. The **Add** button is therefore with the ISDN APL never selectable.

Hardware supported by the ISDN APL and their individual performance features can be found in the release notes of the MRS Server or the Hardware Compatibility List (HCL).

Devices that are already installed can be either **Deactivated** or **Removed** through selection of the appropriate button. The ISDN APL independently deactivates a

previously configured board not found with a restart. This occurs on grounds of the assumption that a hardware failure may have happened and thus the comprehensive configuration files are to be saved. If, however, the board has actually been removed, you can delete the configuration data associating this board via **Remove**. This option is only available with deactivated boards since physically existing boards would be added with the next restart by the automatic hardware recognition and removing were thus pointless.

Selection of a specific device and subsequently the **Properties** buttons, enable the configuration of **Number of physical Channels** (B-channels) and **Number of built-in Fax G3 Resources**.



Server Administration

Integrated Services Digital Network (ISDNAPL)

Via the **Properties** button you can specify the **Number of physical channels:** (B-channels) and the **Number of built-in Fax G3 channels:** for the selected device. The last-mentioned is performed because with supported, active ISDN boards for Fax G3, the corresponding hardware modules must partly be integrated in the ISDN board.

The number of physically present channels may be divided in **logical trunk groups** to which various protocols may be bound. Here only the number of the required subdivisions is specified and the precise assignment of the single channels can then be performed in the **Trunk Groups** configuration tab later.

Additionally, a portion of the extension number can be ignored by **Incoming Calls**. Example:

The number 49-1234-5678-xx is given. The delivered extension information is 5678123, which is interpreted as the complete number 49-1234-5678-5678123. In this case the first four digits (5678) must be ignored.

If the option **Automatic number identification with external prefix** is activated, the individual extension (Automatic Number Identification [ANI]) would be returned with the number of pre-configured digits outside dialing number. This information is used for a uniform acquisition of billing data.

Note: To view the complete incoming number a Logging Window should be opened in the MRS Monitor. The Topic **DialInfo** from the ISDN APL should be copied (drag&drop) to this window and the filter conditions set to debug information.

With **Outgoing Calls** it is possible to insert digits to a dialing number. If for example a PBX system has two cross connections 82 and 83, then a call from 8247 to 8311 is simply transferred internally and not through the public exchange. Numerous PBX systems do not have this function, and in such a case the call must be routed through the public exchange, and therefore these prefixed digits. In a case such as this, the number of prefixed digits must be entered here.

Properties of Eicon DIWA Server BRI

Device

Number of physical channels: 2

Number of logical trunk groups: 1

Number of built-in Fax G3 channels: 2

Incoming calls

Number of leading digits to be ignored: 0

☐ Automatic number identification with external prefix

Outgoing calls

Number of trailing digits to be included: 0

OK Cancel Analog

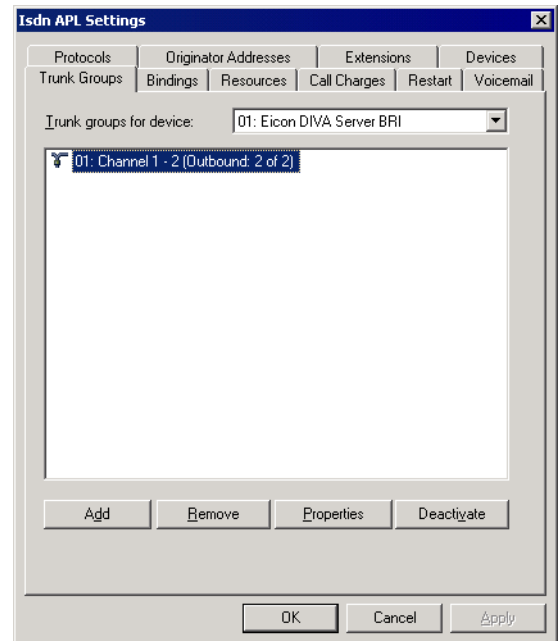
6.1.8 Trunk Groups

The logical line bundles of all installed devices are displayed in this dialog.

The display is switched between the various devices with the pull-down menu **Trunk groups for device:**. All logical line bundles allocated to the device are displayed in the center window.

The user can **Add**, **Remove**, **Activate**, or **Deactivate** lines. The buttons adapt automatically to the different line states.

The number of lines displayed is restricted to the number specified in the license key.



Lines can be configured by selecting a line and subsequently the **Properties** button.

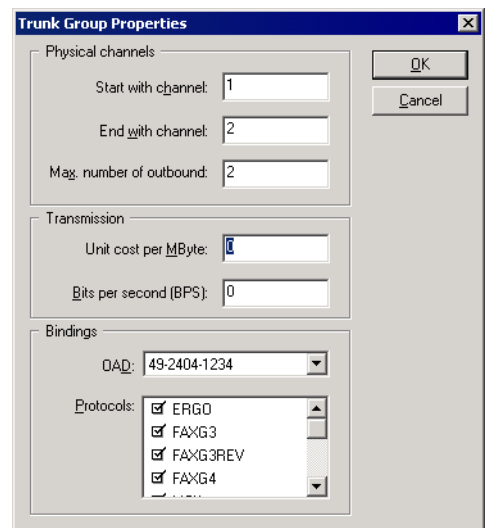
Access to Physical Channels

In this dialog B-Channels are assigned to logical line bundles and the maximum number of outgoing connections configured.

Physical channels can be divided into several sub-groups e.g. a S_{2m}-board with 30 channels. The second option Max. number of outbound enables the reservation of channels so that channels are also available for inbound traffic.

Transfer Information

The **Unit cost per MByte:** and the **Bits per second(BPS):** can be individually assigned to all lines within this portion of the dialog.



Cost effective and fast lines are preferred by the ISDN APL.

Bindings

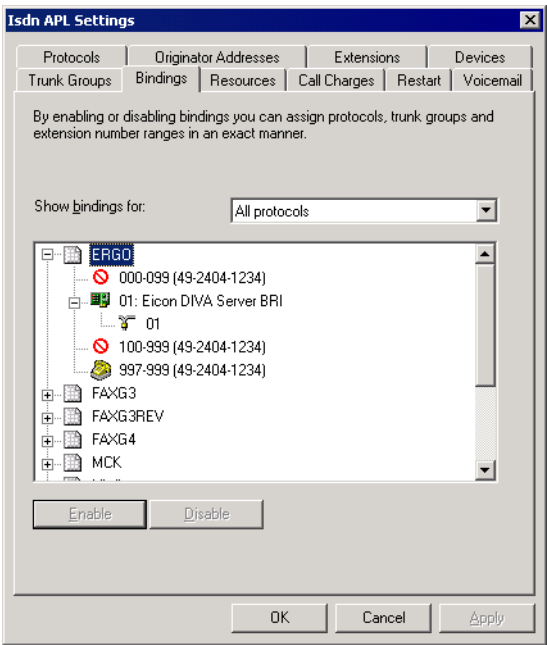
In this portion of the dialog line bundles are assigned an Originator Address (OAD) and a supported protocol bound to them. This assignment must match the originator address assigned to both extension ranges. Clicking on the box proceeding the protocol name you can disable a protocol so that this protocol is not handled via this line bundle.

6.1.9 Bindings

Bindings can be displayed either by **Protocol**, **Line**, **Extension Range**, or **OAD**.

Selected entries in the display can be switched on or off through selection of the **Enable** or **Disable** buttons.

The opposite dialog displays the line bundle of the ISDN board that is bound to the Ergo protocol. Furthermore you see the three configured extension ranges of which one has been assigned to the Ergo protocol, one has been bound to Fax G4 and one to the fax polling server. Corresponding to the Ergo protocol the last ones are displayed deactivated. Thus you have here a good overview of all settings and the available or used resources.



6.1.10 Resources

Hardware

In this section the number of line (B-Channel), voice (corresponds with number of lines by ISDN), and fax resources are entered.

Under **Detected hardware:** the maximum number of resources determined by the hardware recognition is displayed. On the left you find the maximum number of resources to be used by the ISDN APL which must not exceed the number of resources acquired per license. This number to be specified here can be smaller than the number of licenses actually acquired. In this way, with a distributed installation, you can assign resources to another ISDN APL on another computer.

DTMF Recognition

DTMF recognition is always done per software with the ISDN APL. Other telematic APL which use this configuration menu may allow an individual setting of this option.

The screenshot shows the 'Isdn APL Settings' dialog box with the 'Resources' tab selected. The dialog has a title bar with a close button. Below the title bar is a tabbed interface with tabs for 'Protocols', 'Originator Addresses', 'Extensions', 'Devices', 'Trunk Groups', 'Bindings', 'Resources' (selected), 'Call Charges', 'Restart', and 'Voicemail'. A yellow gear icon with a keyhole is next to a text box that says: 'Enter the total number of resources to be reserved and DTMF recognition type. The information provided here will be compared with the license key information.' Below this is a section titled 'Hardware' containing a table with two columns: 'Total no. of resources reserved' and 'Detected hardware:'. The table has three rows: 'Line resources' with values '2' and '2', 'Voice resources' with values '2' and '2', and 'Fax resources' with values '2' and '2'. Below the table is a section titled 'DTMF Recognition' with two radio buttons: 'Hardware' (unselected) and 'Software' (selected). At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

Hardware	
Total no. of resources reserved	Detected hardware:
2	2
2	2
2	2

DTMF Recognition

☐ Hardware

☒ Software

OK Cancel Apply

6.1.11 Charges

Charge costs are internally computed by the PBX. Therefore, ensuing charges must be assigned to either the user initiating the transaction, or to a cost center. Assigning costs to the initiating user is done through use of the data transferred over the D-channel of the ISDN. Therefore, the CLI is correspondingly adapted.

Charge Pulse Information

When the option **Evaluate call detail information** is activated, ensuing transmission costs are compiled. For this purpose, the charge pulse information of the telecommunications service provider is required. In most cases charges are already evaluated in the PBX so that this option can be deactivated then.

The **Currency units per pulse** field contains the price per pulse in the local currency. In Germany, for example, an entry of 12 units per pulse would correspond to 12 Euro-cent. Depending upon where the PBX was purchased or leased, the base price per pulse is pre-programmed, so that a setting of only 1 is required in this field.

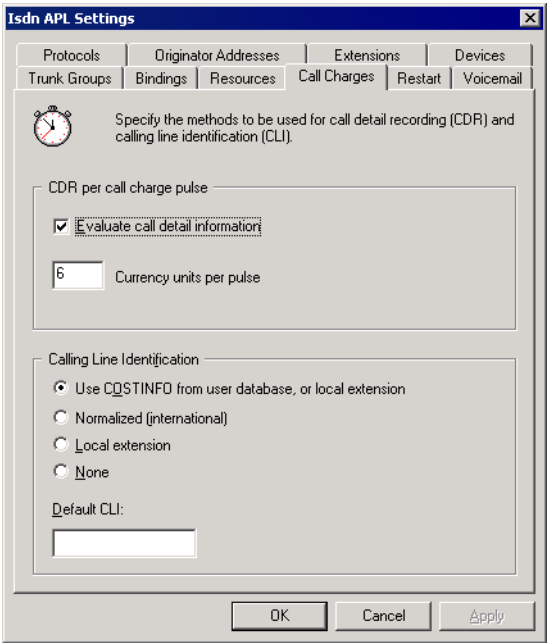
It should be noted that the pulse data delivered by some service providers is less than accurate. If e.g. a discount is given for calls longer than three minutes this would be reflected in the monthly invoice and not in the charge per pulse.

Calling Line Identification

The Calling Line Identification (CLI) can be used by the PBX for billing. For this purpose the CLI can also be manipulated. Through use of the option **Local Extension** the users extension number is taken from the user database.

The user's CLI can also be used in an internationally normed form when the option **Normalized (international)** is activated.

Next you can use the **COSTINFO** field from the user database instead of the normal user extension number. For purposes of billing, users can be grouped together since this number, in contrast to the extension number, must not be unique. Therefore, the



option **Use COSTINFO from user database, or local extension** must be activated. If the field **COSTINFO** is empty, the local extension number will be used.

When the option **None** is activated, either 0 is delivered as the CLI so that no individual billing by the PBX is possible, or , alternatively, a fixed originator ID can be set in the option **Default CLI:**, so that a single originator ID is given for all users. In this case, all costs ensuing from the MRS Server would be booked by the PBX to a single account.

In addition to its use for billing purposes, the CLI is also used by the PBX for initiating outgoing calls.

6.1.12 Restart

Additional Logging Topics

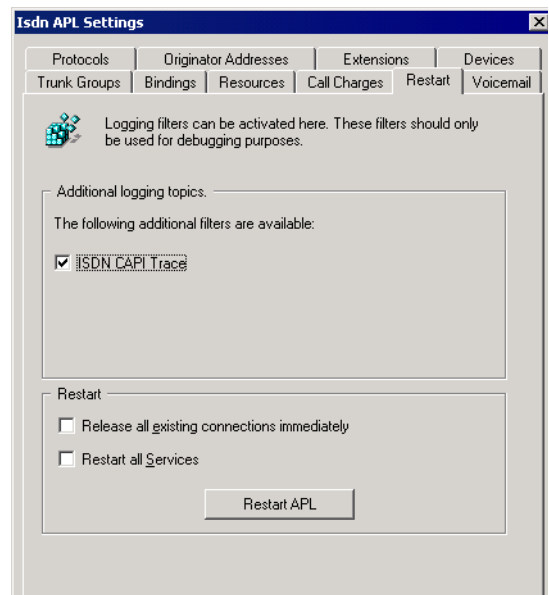
In this section the **ISDN CAPI Trace** can be activated. Due to an increase in server load, this function should only be used when acute problems occur.

As soon as the ISDN CAPI trace has been activated a separate logging window can be configured in the MRS Monitor for the topic “CAPI Trace”.

Restarting APL

Through selection of the **Restart APL** button the ISDN APL is shut down and subsequently restarted automatically. After the button has been selected the ISDN APL no longer accepts calls and executes the shut-down as soon as all lines have been released. Through use of the option **Release all existing connections immediately**, an immediate shut-down can be initiated. This option automatically terminates all connections regardless of their state, and any data being transferred at the time of the shut-down will be lost. If for example a fax message is being transferred at the time of the shut-down it must be retransmitted at a later time.

If the option **Restart all Services** is selected, all CAPI drivers would also be shut-down and restarted. This is only possible for ITK ISDN cards.



6.1.13 General Voice Mail Settings

The extended settings for the general voice mail settings correspond to those of the normal settings (see page 137).

6.2 Ergo Configuration

6.2.1 Generals

After the installation the configuration data specified there are valid for the extension range.

The service access numbers (control mode, answering machine mode and express mode) are automatically generated from the first the calling numbers of the extension range.

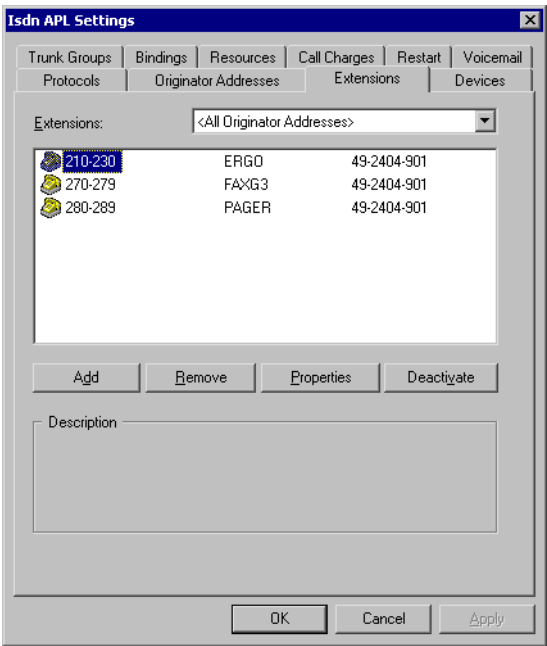
For all other configuration values reasonable defaults are used.

Modifying the default configuration values occurs via the voice mail profile settings and the corresponding Ergo script dialogs.

The ERGO script as protocol always runs in a telematic APL context. Therefore ERGO configuration tabs are reached when you open one of these APLs' settings dialogs.

The MRS Monitor must first be started for these administrative settings. In the "Modules of..." monitor window branch to the  **<Settings>** path and further e.g. to the **IsdnApl**  **IsdnApl** directory. There you can open the configuration tab for the corresponding APL with a doubleclick on  **Set Advanced Options**.

In the "IsdnApl Settings" window now open either select the **Voicemail** or **Protocols** tab, depending on whether you want to edit the voice mail profiles or the telematic protocol settings. The voice mail profile settings via which generic settings, recurringly used by various voice mail systems, are performed, are described on page 137ff).

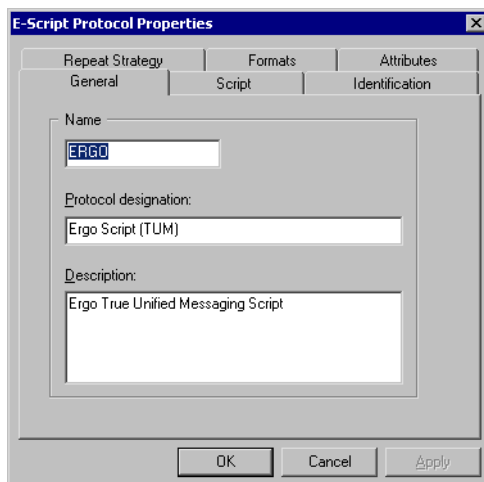


6.2.2 Settings

The voice mail script settings are reached in the “Isdn APL Settings“ via the **Protocols** tab. The window should already display the Ergo script in the list of available protocols. If it is missing, press **Add** and select “Ergo Script (TUM)” to integrate it subsequently.

When the Ergo script has been integrated in the list of telematic protocols, select the Ergo entry with a click and press **Properties** button to be taken to the E-protocols configuration tabs.

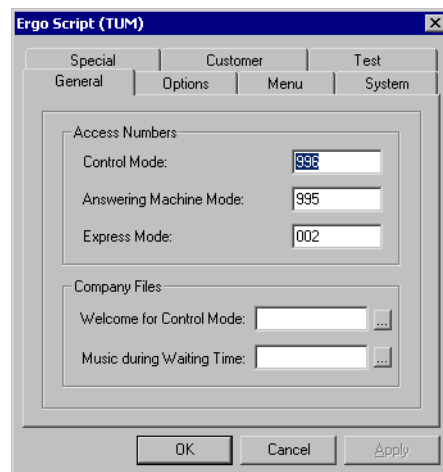
The dialog open now displays in the **General** tab the name, protocol designation and a short description of the protocol. Switch to the **Script** tab. In there press the **Parameter...** button to reach the Ergo configuration tabs.



6.2.3 Ergo Configuration Tabs

6.2.3.1 General

In the **Access Numbers** section of the first tab you can edit access numbers, already specified in Setup, for the single modes. During the installation the first three numbers of the defined extension range were assigned as access numbers for ERGO. Definition of calling numbers for the control, answering machine and express mode is required when redirected numbers are used. In this case users have assigned their telephone number as voice mail number and redirect their telephone to the number of the answering machine mode. This is not necessary when extension ranges are available since then each user has a separate calling number for their mailbox.



Under **Company Files** you can select a new welcome message next to “Welcome for Control Mode” that will be used instead of the default greeting. Open the browse dialog and select the corresponding PCM-file from the following path: `<MRS Install>\res\E\ergo\<Language>`.

As in TUM (True Unified Messaging) environments— depending on system load – the response time to mailbox queries may take some time, a tune will be played during waiting times. Thus the user is informed that he/she is still connected to the system and the entries are being processed. You may select a waiting tune under **Music during Waiting Time** (proceed as described under “Welcome for Control Mode“).

6.2.3.2 Options

In the **Options** tab you activate or deactivate the following functions. After the installation, all standard functions as well as special functions, that were installed then, are already preset.

Activated Standard Functions

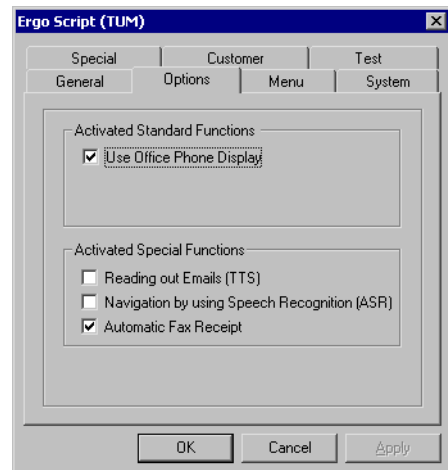
- **Use Office Phone Display:** Determines whether texts are to be send to the displays of called telephones. This function should be deactivated when a PBX not supporting a display is used.

Activated Special Functions

- **Reading out Emails (TTS, Text-to-Speech):** Serves to activate or deactivate the function of having e-mails read out by a speech converter upon message query for all users.

Remark: If you want to have e-mails read out, a license for the speech converter and another one for release in the MRS systems needs to be purchased in addition to the standard MRS scope of delivery. The speech converter derives from a third supplier (for example Speechworks Speechify) but is also directly available via Cycos.

- **Navigation by using Speech Recognition (ASR, Automatic Speech Recognition):** For future implementation of menu operation per voice input. This feature activates or deactivates menu operation per voice input for all users. Functions are then triggered through articulating the desired command instead of pressing a key (DTMF command).



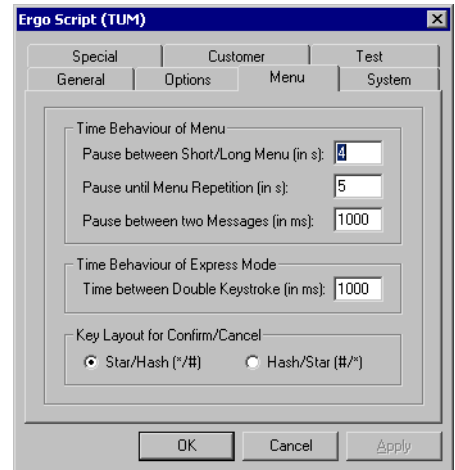
- **Automatic Fax Receipt:** Deactivate this checkbox if you want to suppress automatic fax message receipt. Otherwise fax messages are automatically transmitted to the user's mailbox (or telephone) when a fax tone is recognized.

6.2.3.3 Menu

In this configuration tab the menu time behaviour is set. Additionally you can customize the interval in which the two DTMF entries have to be made to directly call an originator. Furthermore you can exchange the functional allocation of the star (*) and number sign key (#). In this way it is possible to react to operating conventions of voice mail systems that probably need to be replaced.

The following parameters can be set:

- **Pause (in seconds) between the short/long menu:**
After the complete output of system greetings in a menu, a more detailed system greeting is automatically switched to after the pause you have specified here. The adjustment range is between 1 s and 99 s, the value default set with the installation is 4 s.
- **Pause (in seconds) until menu repetition:**
Once the short and subsequently the long menu have been played completely, the output procedure starts all over again after a break. The time between repetitions can be modified here. The adjustment range is between 1 s and 99 s, the default value is 5 s.
- **Pause (in milliseconds) between two messages:**
This concerns the time span between the end of the message just played and the output of the next message. The adjustment range is between 0 and 9999 ms, the default value is 1000 ms.
- **Time Behaviour of Express Mode:**
In express mode you can press an arbitrary key during message output to skip to the next message. With two keystrokes in succession (in a specific interval), a connection to the originator is immediately established. To distinguish both types of entry, the first one is followed by a short waiting period and if no second keystroke occurs, the function first mentioned is triggered. You can determine the waiting period here. The adjustment range is between 0 and 9999 ms, the default value is 1000 ms.



Remark: If this value is set to 0, no connection can be established to the originator – when you press a key the next message is immediately switched to.

- **Key Layout for Confirm/Cancel**

Is used to exchange the star key/number sign key function. Per default you can confirm entries with the star key and cancel current operations via number sign. If, however, you prefer the converse behaviour, the key behaviour can be exchanged here (thus: number sign → entry confirmation and star key → exit).

6.2.3.4 System

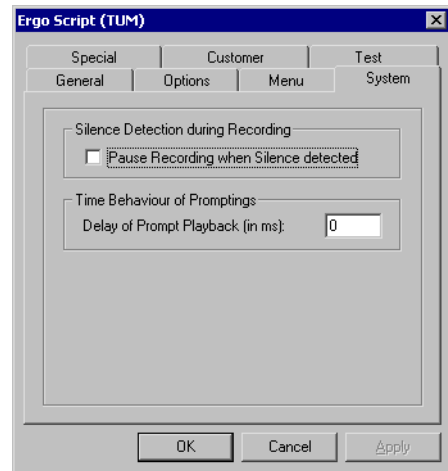
In the “System” tab further configurations can be performed to allow system fine tuning.

- **Silence Detection during Recording**

The associating checkbox serves to define whether or not the system is to automatically stop the recording after it has detected that no further input is made. In this way you can reduce the file size of a voice message as breaks do no longer occupy any storage capacity then. To resume recording you need to enable the corresponding functional key.

- **Time Behaviour of Promptings**

The value in the **Delay of Prompt Playback (in ms)** entry field allows fine tuning the greeting start. With some types of PBX it may occur that greetings immediately played after a key entry are cut off a bit when their output begins. In order to make shure that the entire greeting can be listened to, you can set a suitable delay period (adjustment range is from 0 to 9999 ms). The default set value is 0 which means that no delay is intended.



6.2.3.5 Special

Use this tab to set further special functions.

Activated Special Functions

- **Use ANI as Box Number during Login**

Enabling this function allows to define an easy procedure for all users to access their own mailbox. ERGO first determines the number of the calling device (ANI). If you dial into the control mode using your own telephone, ERGO will look up the corresponding mailbox number of this user and use it automatically (usually, you would be prompted to enter the box number first). Thus, you do not have to enter the mailbox number manually, only the access PIN has to be entered. If the calling device has been defined by the user as “trusted“, even entering the PIN becomes unnecessary – you may access the control mode directly without further inputs.

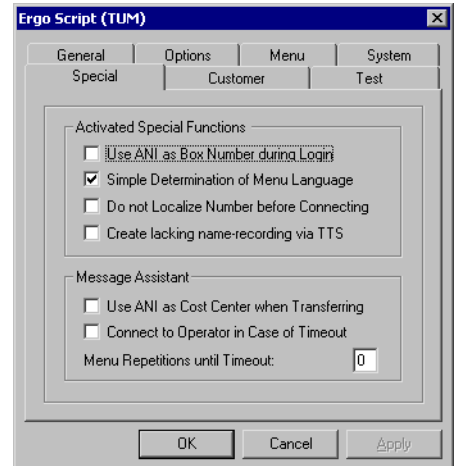
- **Simple Determination of Menu Language**

This function allows you to determine by which criteria the menu language is selected in case of a call. If it is activated, the default language is always used first in the control and answering machine mode. After login, ERGO will switch to the language selected by the user for his/her mailbox. If the mailbox is accessed directly, the language configured for this mailbox will be used (if no language was selected, the default setting will be used).

If this function is not selected explicitly, ERGO will try to offer the appropriate menu language depending on the access mode or the selected mailbox. If the number of the caller is not transmitted, ERGO will use the default language. If the caller's number is transmitted, ERGO connects the number to a known user and derive the language settings from there. If this is not possible (user unknown), the country code will be used to select the language (for example if the ANI starts with 49..., German is selected, 33... corresponds to French).

- **Do not Localize Number before Connecting**

In general, all numbers are localized internally before they are sent as dial information (for example to avoid that a connection that could be established internally is routed as external call). This option forces ERGO to ignore this localization and to dial the number directly.



Message Assistant:

If the user has configured his/her mailbox in a way that the message assistant is activated instead of using it as answering machine only, the behaviour of the message assistant can be determined by means of two variables.

- **Use ANI as Cost Center when Transferring**

With a transfer the mailbox number is normally passed on as caller to the PBX so that this number is used for billing. This is the default setting since the mailbox owner must configure the numbers where a transfer can be made to. With this option you can have a caller's number transferred to the PBX so that his/her number is used for billing.

- **Connect to Operator in Case of Timeout**

A caller uses a telephone that does not support DTMF dialing or where DTMF dialing has been disabled. He/she calls a mailbox whose user activated the message assistant. As he/she cannot make any entries that will be recognized by the system, a solution has to be found for not losing this call. By default, the system behaviour is designed in a way that this caller will be prompted to leave a message after a certain number of menu repetitions (via a timeout routine). If this function is activated, the call will be redirected to an operator after the preset number of menu repetitions.

- **Menu Repetitions until Timeout**

Use this field to enter the number of menu repetitions until the call will be disconnected (timeout).

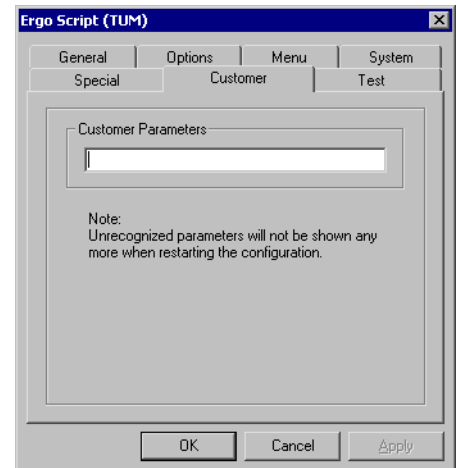
Attention: Leave this value to the default setting ("0"). Usually, a caller without DTMF compatible telephone will not listen to the menu more than once as soon as he/she realizes that ERGO does not expect any input from him/her.

6.2.3.6 Customer

In this tab you can enter customer-specific parameters.

For the time being the following parameter entries are available: *-extended*, *-pga* and *rmtopic* and the five parameters (*prs=*, *recplen=*, *recplvl=*, *recslen=*, and *recslvl=*) used to detect a momentary break (Silence Detection Parameters).

Remark: If several parameters are used simultaneously, they are entered in a row, separated by a blank. Entered invalid parameters are ignored and not displayed when this configuration tab is called again.



-extended

This parameter serves to release the setting options of the extended mode for all users. In this mode you can use far reaching mailbox options per telephone keypad if no client is available at the respective workplace.

-pga (Pre-Greeting-Announcement)

With this parameter string you can implement an additional welcome message for external, inbound calls. In this way you can have e.g. a company greeting played before the ERGO voice system answers the call and customers are thus immediately informed that they are connected to the right company. The associating company-specific greeting is not included in the ERGO scope of delivery. If required you need to generate such a greeting yourself. Some important remarks on this:

- The greeting file to be implemented must be generated in the PCM format
- Its name must definitely be `pregreetingann.pcm` since only a greeting file with this name is played at this point.
- The directory where this greeting file must be stored is `<MRS Install>\res\e\ERGO` and then in the folder according to the selected language (for example: `american`, `british`, `french`, or `german`).

-rmtopic (Remove MRS Monitor Topic)

If the MRS Server is set up completely, it may happen that no topic entry for ERGO monitoring can be created (in the "Components of `<MRS-Server Name>`" dialog) as their number is limited (max. 20). This parameter string lets you setup the MRS Server in a way that it removes some existing topics from the **IsdnApl** branch (or **DlgApl**)

and replace them by ERGO as topic. This allows you to monitor ERGO's activities in a logging window.

prs=<value in 1/10 seconds> (Pre Recording Silence)

In some system environments it may happen that a signal tone (beep) at the end of the recording is stored together with the recording. This can be avoided by entering a suitable value after this parameter. That means, the end of the recording will be mute for the time set.

recplen, **recplvl**, **recslen** and **recslvl**

Since with recording the electric parameter for volume depends on the recording/playback components used (respectively their driver), a volume adaption may be required. The impulse length that must at least be available for starting a recording can be additionally influenced. The following four parameters are used to detect speaking or silence for starting or stopping a recording. In this way recording times are limited so that no unnecessarily large recording files are generated. The problem is to select the corresponding levels in a way that speaking is unambiguously detected, but e.g. line and background noise is interpreted as silence. The thresholds for length and peak level, required to detect breaks, can be adapted here.

recplen=<Value> (**recplen** stands for Record Peak Length)

Defines the minimum pulse length of a signal in order to be detected as such.

Default: 64

Value range: 0 to 4000

recplvl=<Value> (**recplvl** stands for Record Peak Level)

Defines the minimum peak level of a signal for starting a recording. The higher a peak level is selected, the louder a person must speak to start a recording. The value range for the entry is between 0 and 4000, with 4000 representing the maximum peak value. When the entry value is divided by 40, you receive the level value in percent (in relation to the maximum value).

Default: 32

Value range: 0 to 4000

recslen=<Value> (**recslen** stands for Record Silence Length)

Defines in milliseconds the minimum impulse length a break must have for stopping a recording .

Default: 3000

Value range: 0 to 4000

recslvl=<Value> (**recslvl** stands for Record Silence Level)

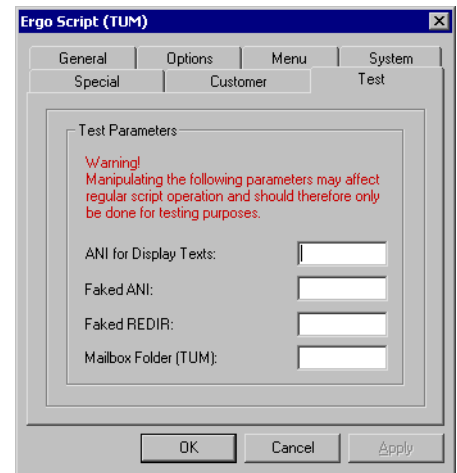
Defines the minimum peak level a break must have for stopping a recording. The higher the “silence level” is set, the louder a person must speak for not stopping the recording. The value range for the entry is between 0 and 4000, with 4000 representing the maximum silence value. When the entry value is divided by 40, you receive the level value in percent (in relation to the maximum value).

Default: 32

Value range: 0 to 4000

6.2.3.7 Test

This tab is intended for entering test parameters



Please enter parameters carefully. Nonsensical entries may hamper regular ERGO operation or make it even impossible.

The entry fields have the following significance:

- **ANI for Display Texts:**

In this field you can enter a telephone number as address for all display texts (intended for general function checks).

- **Faked ANI:**

To serve testing purposes an arbitrary number, automatically interpreted by the system as recognized calling number for every further call, can be entered here.

- **Faked REDIR:**

Another field for testing purposes in which you can specify, similar to the faked ANI, a redirected number for call rerouting.

- **Mailbox Folder (TUM)**
Here you can explicitly define the output mailbox folder for True Unified Messaging (TUM) by entering its name.

6.3 Dialogic (DlgAPL)

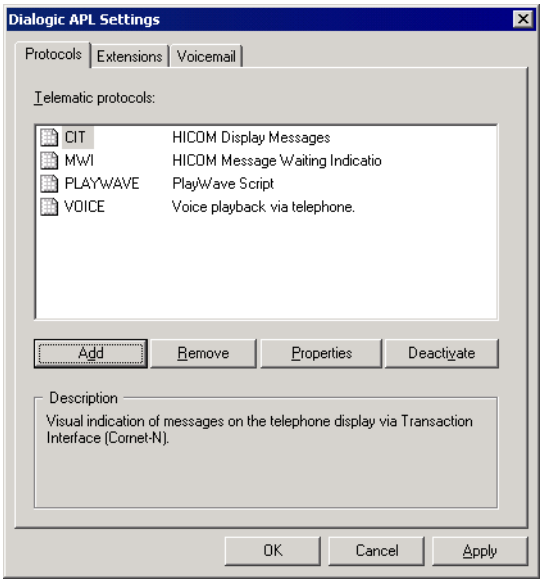
The Dialogic APL provides the integration between the Dialogic communication hardware and the MRS Server. Dialogic is one of America's leading manufacturers in the area of computer supported telephony and fax.

The configuration of the Dialogic APL is done through the MRS Monitor. The basis for the configuration is taken from the Teleconfig Library, which provides a uniform method of configuration for all telematic services. The Dialogic APL configuration is started by double clicking on the **Set Options** entry found under **Settings** in the module window of the MRS Monitor. Under the option **Set Advanced Options**, further settings for the APL configuration are available, but in most cases these options under normal configuration are sufficient.

6.3.1 Telematic Protocols

All telematic protocols installed on the MRS Server and supported by the Dialogic APL are displayed within this configuration tab.

New protocols can be included in the list through selection of the **Add** button. Protocols no longer required are removed through use of the **Remove** button or disabled through the **Deactivate** button. Once a protocol has been deactivated and later reselected, the **Deactivate** button would toggle to **Activate**. The Dialogic APL supports the Fax G3 protocol for transmission and receipt of fax documents, Fax G3 reverse polling from a Fax-on-Demand Server, voice message playback over a telephone, Message Waiting Indication over Cornet-N to a Siemens Hicom PBX, and various script based protocols such as the Fax-on-Demand (FOD, see page 66 and page 130), or the modern voice mail system Ergo (see individual manual).



Operation and configuration of these protocols correspond to the description given with the ISDN APL. Described here are therefore only the special Dialogic APL protocols that are added with connecting a Hicom PBX via a special Cornet-N Layer, only available via Siemens.

Note that for technical reasons the Dialogic APL does not support old scripts in the VFS language.

Selection of the **Properties** buttons enables the user to display and modify configuration parameters of the selected protocol.

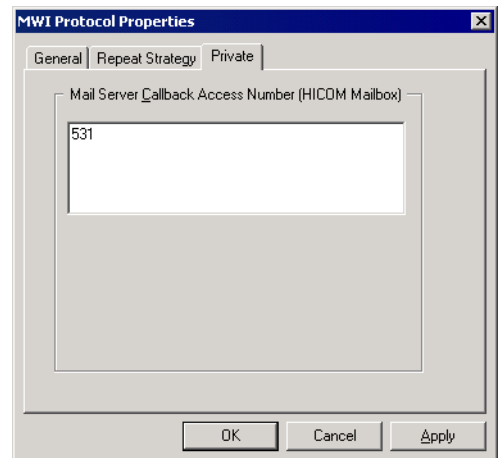
6.3.1.1 Hicom Message Waiting Indicator

This protocol offers users a method for optical signalization of new inbound messages to Hicom System Telephones. A prerequisite for this functionality is the Cornet-N Layer which can only be obtained from Siemens.

The configuration tabs **General**, **Repeat Strategy**, **Formats**, and **Attributes** correspond principally to those described with the ISDN APL. Here as well attribute and supported format settings are only possible via extended settings.

Private

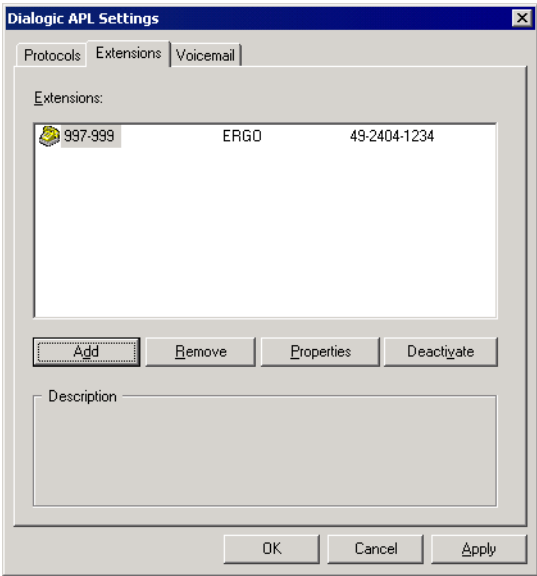
In this configuration tab, the ring-back number of the Hicom Mailbox is entered. In most cases, this is the number of the cross-connection followed by a 1, so that the Hicom can switch through.



6.3.2 Extensions

In this configuration tab, number ranges are assigned to the individual protocols. Incoming calls are bound to the various protocols through the use of these number ranges. New ranges can be added, removed, activated or deactivated through selection of the appropriate button. Configuration parameters of the number ranges are retained even when they are deactivated.

Configuration of the various number range parameters is made through selection of the **Properties** button.



Extension Properties

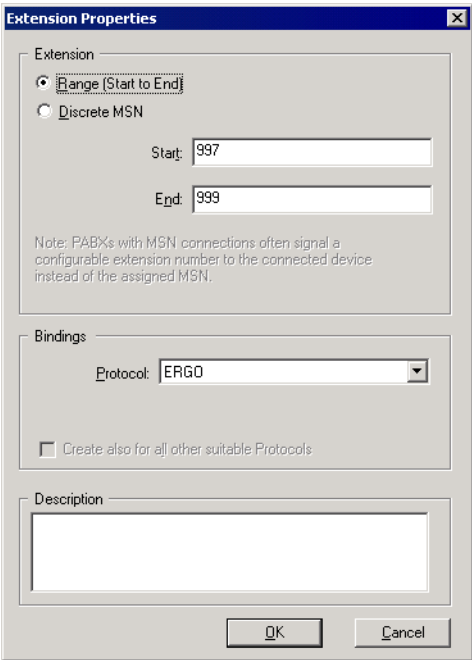
Beginning and end numbers of the number range are defined in the fields **Start** and **End**.

If a Point-to-Point connection is not available, but a Point-to-Multipoint is present, a **Discrete MSN** (Multiple Subscriber Number) can be assigned to the protocol instead of an extension number range. The Dialogic APL will then only take calls on the MSN for this protocol.

With analog boards no extension range specification is made and the corresponding line directly connected to an analog OAD to be correspondingly configured.

Bindings

OADs are assigned to the installed **Protocol** in this section of the configuration tab.



Description

An optional text description may be given to the number range in the portion of the configuration tab.

6.3.3 General Voice Mail Settings

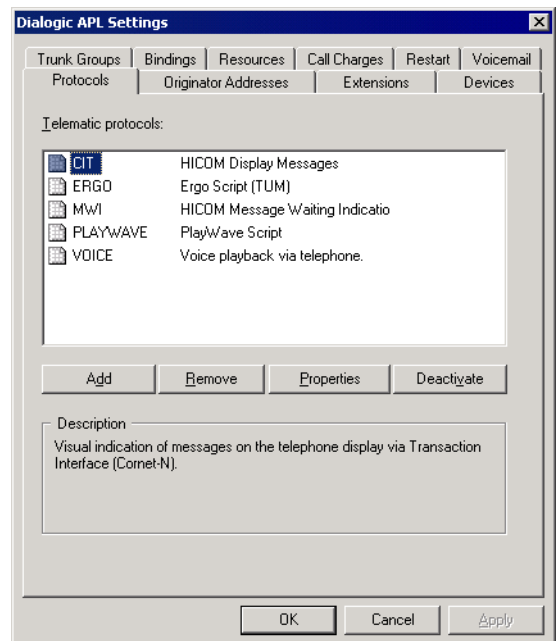
The general voice mail settings correspond to those described with the ISDN APL. (siehe page 137).

In the following you find the **extended settings** of the Dialogic APL.

6.3.4 Telematic Protocols

The Advanced Option settings for the various ISDN protocols correspond with those described in the section for Telematic Protocols at the beginning of this chapter. Two further options are also available for the protocol settings, but a modification of the default settings are normally not required.

These options include the supported formats and protocol attributes. The configuration of these protocol attributes is the same as those in the ISDN APL.



6.3.5 Originator Addresses

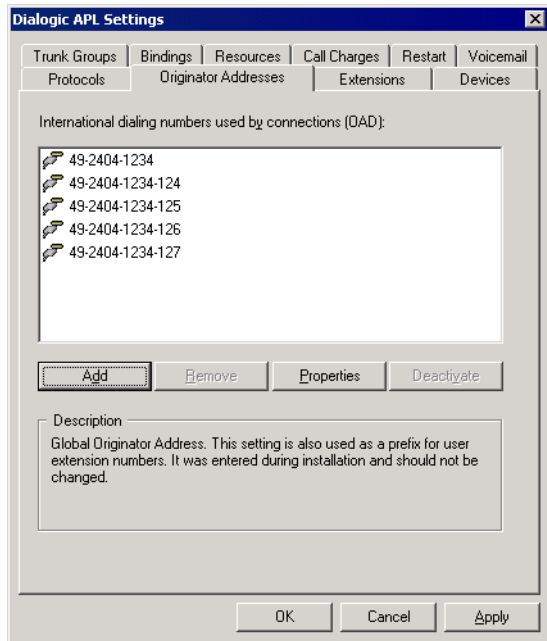
If deviating from the globally configured extension additional addresses (OADs) are used by the Dialogic APL, they are to be specified here. The first calling number displayed is always the global OAD that the server, for example, uses for normalizing. This OAD must correspond to the system calling number without extensions, so that for CTI, normalizing can be performed correctly.

If the OAD to be used by the Dialogic APL deviates from the system calling number, thus for example contains a cross-connection number, another OAD must be added here and the line bundles and extension ranges bound to this OAD. The Dialogic

APL supports analog boards as well. For these the entire calling number must be entered here since with an analog connection no extensions are possible.

Via **Add**, **Remove**, **Deactivate** and **Activate** you can – as already seen with the other dialogs – administer addresses. The **Deactivate** button turns to **Activate** when you select a deactivated originator address.

By means of the **Properties** button you can modify the individual components, various external prefixes and the optional extension description.



6.3.6 Extensions

The Advanced Option settings for the Extension number ranges correspond with those described in the section for Telematic Protocols at the beginning of this chapter.

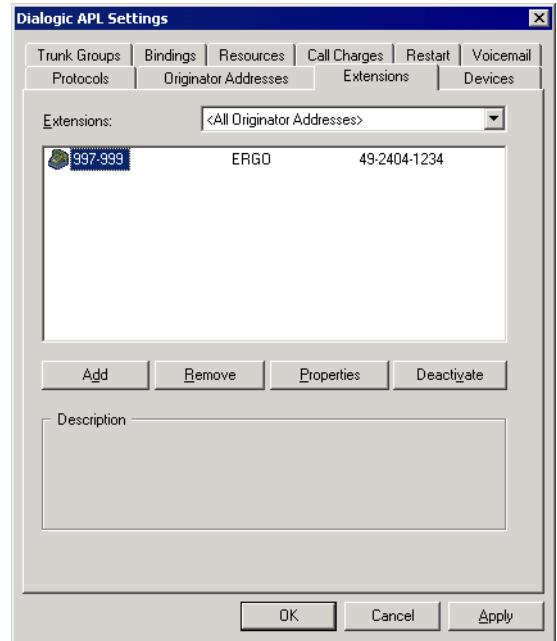
In contrast to the normal settings configuration menu, extension numbers for originator addresses other than that of the MRS Server can be configured. Select the desired number from the top right pull-down list.

Advanced Options

If the option **Allow variable length** is activated numbers dialed from outside the system may be of a variable length. If the extension

number range is defined as 6 digits in length e.g. 700000 to 999999, then any inbound call with 1 to 6 digits beginning with 7 and extending to 999999 would be forwarded according to the implemented *Routing Rules*.

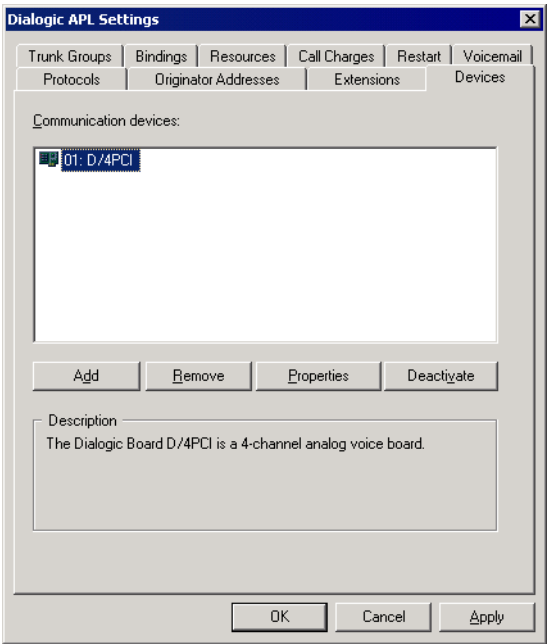
The option **Allow superfluous** digits ignores any additional digits that are inputted after the actual number. This could apply for the extraneous numbers 500, 50123, etc. for the user with the extension number 50. Without this option the Dialogic APL would be unable to ascertain a user for the inbound routing, or refuse to take the call. The interaction between the options **Allow superfluous** and **Allow variable length** is presently unknown!



6.3.7 Devices

Newly installed hardware communication devices which are supported by the Dialogic APL can be **added** through the use of this configuration tab. Existing devices can be removed, deactivated, resp. activated with the options available in the tab.

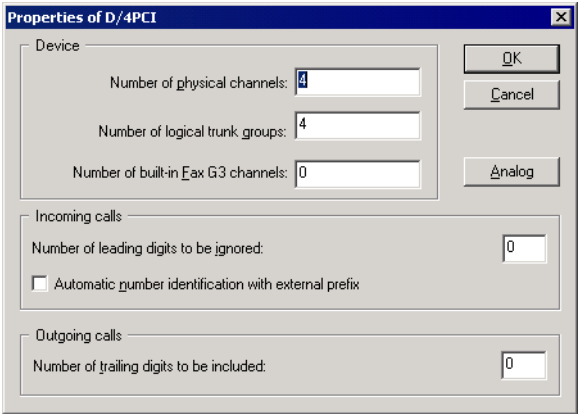
The Dialogic APL supported hardware always appears updated with the respective supported features in the MRS Server release notes resp. in the Hardware Compatibility List (HCL).



Through selection of the **Properties** button, the **number of physical channels** and **number of built-in Fax G3 channels** can be entered.

The number of physically present channels may be divided in **logical trunk groups** to which various protocols may be bound. Here only the number of the required subdivisions is specified and the precise assignment of the single channels can then be performed in the configuration tab **Trunk Groups** later.

Additionally, portions of the extension can be ingnored with **Incoming calls**.



Example:

The number 49-1234-5678-xx is given. The delivered extension information is 5678123, which is interpreted as the complete number 49-1234-5678-5678123. In this case the first four digits (5678) must be ignored

If the option **Automatic number identification with external prefix** is enabled, the originator number (Automatic Number Identification (ANI)) is prefixed and delivered to the exchange by the device.

With **Outgoing Calls** it is possible to insert digits to a dialing number. If for example a PBX system has two cross connections 82 and 83, then a call from 8247 to 8311 is simply transferred internally and not through the public exchange. Numerous PBX systems do not have this function, and in such a case the call must be routed through the public exchange, and therefore these prefixed digits. In a case such as this, the number of prefixed digits must be entered here.

The **Analog** button is only active when an analog Dialogic board type D/41E-PCI or D/120JCTLS is used. With this button you call a configuration dialog in which you can configure the so-called VMle interface (**Voice Mail Interface extended**) which is a Dialogic APL component. This interface is required for use of a voice mail system (e.g. ERGO) with the above analog Dialogic boards.

Contrary to digital connections (ISDN), no D-channel is available for transmitting connection information (e.g. Automatic Number Identification (ANI) or Dialed Number Information System (DNIS) with analog connections. Therefore this information is transmitted to the Dialogic APL after a successful connection set-up by the PBX¹⁰ in the form of DTMF tone sequences.

The VMle interface interprets these tone sequences and subsequently they can be processed by the Dialogic APL.

The DTMF tone sequence transmitted by the PBX is structured as follows:

<code><ANI Number><DNIS Number>

Example: <***1><024041234><02415678>

Analog Configuration of D/4PCI

Select Topic: VoiceMail interface

VoiceMail Interface

Code length: 4 Fill: *

ANI length: 6 Fill: *

DNIS length: Min: 2 Max: 8

'Private' number default: 000000

'Length exceeded' default: 011111

'Not available' default: 022222

Time: 99 100ms IDD: 20 100ms

If DNIS is missing: 100

Justification: ☐ Left ☒ Right

Default

Ok Cancel

10. The PBX used must support the VMle interface (e.g. Siemens HiCom)

The `<code>` field contains a number for identifying an incoming call (e.g. an internal call has number 1, an external one number 2). The `<ANI Number>` field contains the caller number (if it is transmitted) and the `<DNIS Number>` field contains the number dialed by the caller.

To configure the VMle interface you need to select the **Voice Mail interface** option in the **Select Topic:** section first. Now the script configuration tab is displayed. The settings that can be performed in this dialog must be identical with the PBX settings. Using the **Default** button the entire dialog is filled in with default settings or set back to the original state.

Code length:	Here you set the number of digits the <code><code></code> string is to have. Default: 4
Fill:	The character entered here fills blanks in the <code><code></code> and in the <code><ANI Number></code> string. If for example the <code><code></code> string contains only one digit, the remaining digits are filled with the character specified here (e.g. ***1). Default: *
ANI length:	This field serves for entering the number of digits the <code><ANI Number></code> string is to have. This specification effects the numbers to be entered in the 'Private' number default , 'Length exceeded' default : and 'Not available' default : field. If, for example, you enter 3, the calling numbers in the above fields may only be three-digit (e.g. 011 with 'Length exceeded' default :). Default: 6
DNIS length:	With this parameter you can use the Min: and Max: fields to set the minimum and maximum length of the <code><DNIS Number></code> string. Default: Min=2, Max=8
'Private' number default:	In this field you specify the <code><ANI Number></code> string to be used if a caller has suppressed transmission of his or her calling number. The length of the number entered here must be identical with the setting in the ANI length: field. Default: 000000
'Length exceeded' default:	The number entered here is used as <code><ANI Number></code> string, when the transmitted calling number exceeds the length set in the ANI length: field. The length of the entered number must be identical with the setting in the ANI length: field. Default: 011111
'Not available' default	When an error occurs during the caller number transmission, the number entered here is used as <code><ANI Number></code> string. The length of the entered number must be identical with the setting in the ANI length: field. Default setting: 022222

- Time (x100ms)** The value entered here defines the period in which the complete DTMF tone sequence must be transmitted from the PBX to the Dialogic APL. The value must be multiplied by factor 100ms. Default setting: 100 x 100ms = 10 seconds
- IDD (x100ms)** The value entered here defines the period in which two digits from the DTMF tone sequence each must be transmitted from the PBX to the Dialogic APL. The value must be multiplied by factor 100ms. Default setting: 20 x 100ms = 2 seconds
- If DNIS is missing** When no value has been entered in the *<DNIS Number>* string (the number dialed by the caller is unknown or missing), the number entered here is used. This can be for example a collective number of the ERGO voice mail system. Default: 100
- Justification:** Here you can determine whether the numbers in the DTMF tone sequence fields are to be formatted right or left justified. Default: Right
Example: right justified = ***3 / left justified = 3***

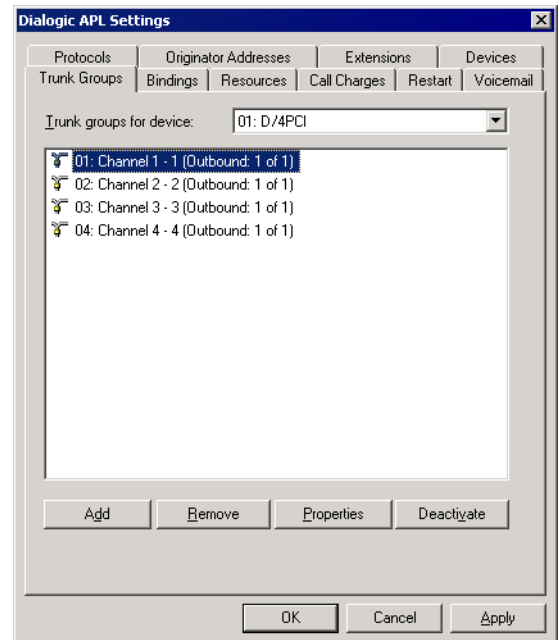
6.3.8 Line Bundles

All available lines for the installed devices are displayed in this dialog.

The display is switched via selection in the **Trunk groups for device:** pull-down menu so that all lines of the associating devices can be seen.

Lines can be **added**, **removed**, **activated** or **deactivated** through use of the buttons in the lower portion of the dialog.

The number of lines displayed in this dialog is restricted to those resources contained within license key entries for a maximum number of lines.



Selecting the **Properties** button enables the configuration of the Line Bundles.

Physical channels

In this dialog B-Channels are assigned to logical line bundles and the maximum number of outgoing connections configured.

Physical channels can be divided into several sub-groups e.g. an S_{2m}-board with 30 channels. The second option Max. number of outbound enables the reservation of channels so that channels are also available for inbound traffic.

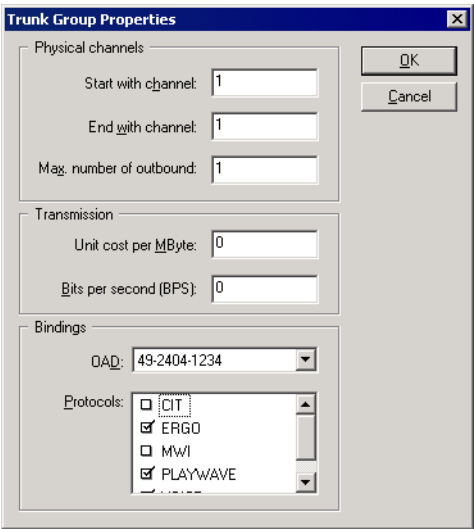
Transmission

The **Unit cost per MByte:** and the **Bits per second (BPS)** can be individually assigned to all lines within this portion of the dialog.

Cost effective and fast lines are preferred by the Dialogic APL.

Bindings

In this portion of the dialog line bundles are assigned an Originator Address (OAD) and a supported protocol bound to them. Clicking on the box proceeding the protocol name deactivates a protocol for this connection.

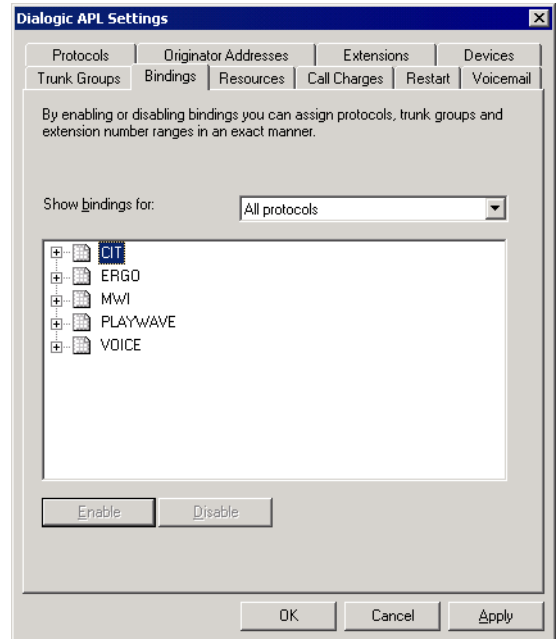


6.3.9 Bindings

Bindings can be **shown** either by Protocol, Line, Extension Range, or OAD.

Selected entries in the display can be switched on or off through selection of the **Enable** or **Disable** buttons.

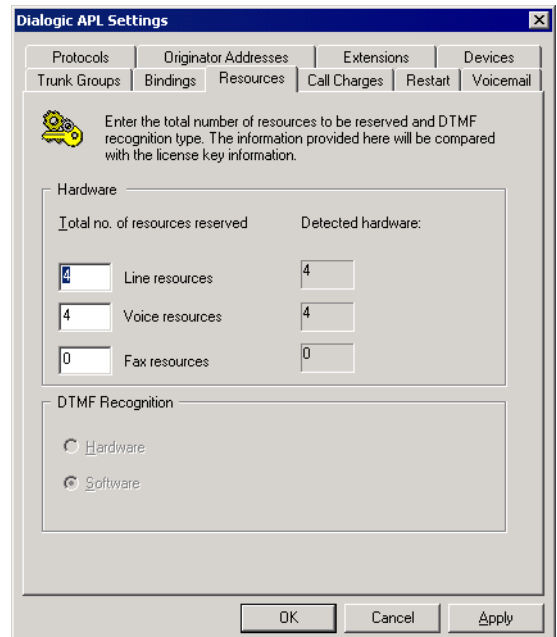
A good overview is provided in this dialog for all settings and available resources.



6.3.10 Resources

Hardware

In this section the number of lines (B-Channel), voice resources (Dialogic) and fax resources (Gamma Fax) are entered. Under **Detected hardware:** the number of these resources determined by the hardware recognition is displayed. The **Total no. of resources reserved** column features the number of resources to be used by the Dialogic APL which must not exceed the number of resources acquired per license. In this way you can, with a distributed installation, assign resources to another Dialogic APL on another computer.



DTMF Recognition

DTMF recognition can be performed either by the hardware or by software through the Dialogic APL. Since DTMF recognition by the Dialogic card has proven to be extremely reliable, it is recommended that the hardware method of recognition be used for this option. Another point in favor of the hardware method is the computation bound process involved with the software method.

6.3.11 Charges

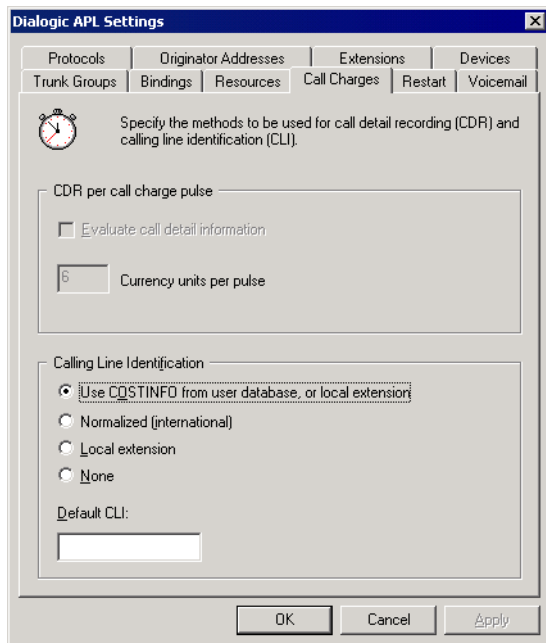
Charge costs are internally computed by the PBX. Therefore, ensuing charges must be assigned to either the user initiating the transaction, or to a cost center. Assigning costs to the initiating user is done through use of the data transferred over the D-channel of the ISDN. Therefore, the CLI is correspondingly adapted.

Charge Pulse Information

Via the option **Evaluate call detail information** you can have the ensuing transmission costs collected by the MRS Server. For this purpose, the charge pulse information of the telecommunications service provider is required. In most cases the charges incurred are already evaluated in the PBX so that this option can then be deactivated.

The **Currency units per pulse** field contains the price per pulse in the local currency. In Germany for example, an entry of 12 units would mean 12 Eurocent per pulse. Some PBXs deliver the charges in the respective currency already so that a setting of only 1 is required in this field.

It should be noted that the pulse data delivered by some service providers is less than accurate. If e.g. a discount is given for calls longer than three minutes this would be reflected in the monthly invoice and not in the charge per pulse.



Calling Line Identification (CLI)

The Calling Line Identification (CLI) can be used by the PBX for billing. For this purpose the CLI can also be manipulated. Through use of the option **Local extension** the users extension number is taken from the user database.

The user's CLI can also be used in an internationally normed form when the option **Normalized (international)** is activated.

Next you can use the **COSTINFO** field from the user database instead of the user's normal extension. For purposes of billing, users can therefore be grouped together since this number, in contrast to the extension number, must not be unique. Therefore, the option **Use COSTINFO from user database, or local extension** must be activated. If the field **COSTINFO** is empty, the local extension number will be used.

When the option **None** is activated, either 0 is delivered as the CLI so that no individual billing by the PBX is possible, or, alternatively, a fixed originator ID can be set in the option **Default CLI**, so that a single originator ID is given for all users. In this case, all costs ensuing from the MRS Server would be booked by the PBX to a single account.

In addition to its use for billing purposes, the CLI is also used by the PBX for initiating outgoing calls.

6.3.12 Restart

Services

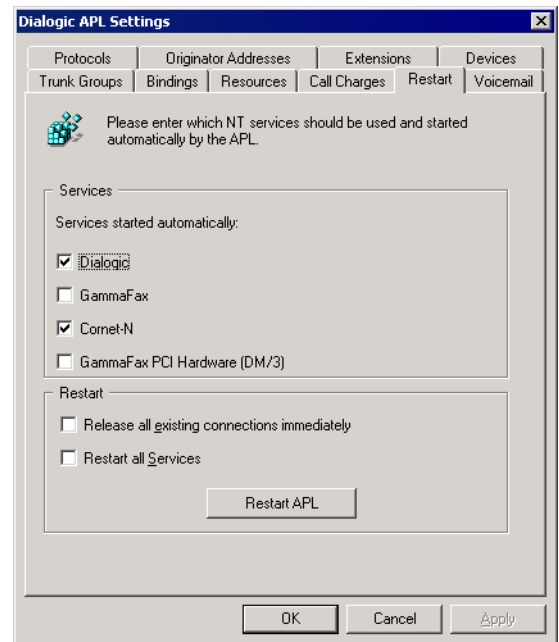
The following Windows NT services are used and automatically started by the Dialogic APL:

- **Dialogic**

Dialogic service is automatically started when this option is enabled. This service is a mandatory requirement.

- **Gamma Fax and GammaFax PCI Hardware**

Start the GammaFax service. This service may only be selected when a GammaFax board type DM/3 or CP-12 is used. For Dialogic boards type BRI2VFD and D80-PCI GammaFax is not required since these boards have internal fax functionality.



- **Cornet-N**

It is assumed that the Dialogic APL is configured for use of the Cornet-N protocol.

Restart

The Dialogic APL is automatically shutdown and restarted through use of the button **Restart APL**. Normally the Dialogic APL accepts no new inbound traffic once the button has been depressed and executes a restart as soon as all (in and outbound) lines have been released. Enabling the option **Release all existing connections immediately** causes all open connections to be immediately cut-off (both in and outbound traffic) when initiating a restart.

If the option **Restart all Services** is enabled, other services (Gammafax and Cornet-N) are automatically shutdown and restarted with the Dialogic APL.

6.3.13 General Voice Mail Settings

The general voice mail settings correspond to those described with the ISDN APL (see page 137).

6.4 Message Transfer Agent (MTA)

The MTA is the central router, through which all messages in the MRS System must pass. The default configuration of the server is sufficient for most applications. If any modifications to the system must be made, these should only be implemented by an individual that is extremely familiar with the system. This is especially valid when making any alterations in the *Routing Rules*. A detailed description of the *Routing Rules* can be found in the *MRS System Architecture*.

The configuration is performed from the MRS Monitor. The configuration dialog is started by double clicking on the **Set Options** entry in the Modules window under **<Settings>**.

6.4.1 Automatic Maintenance

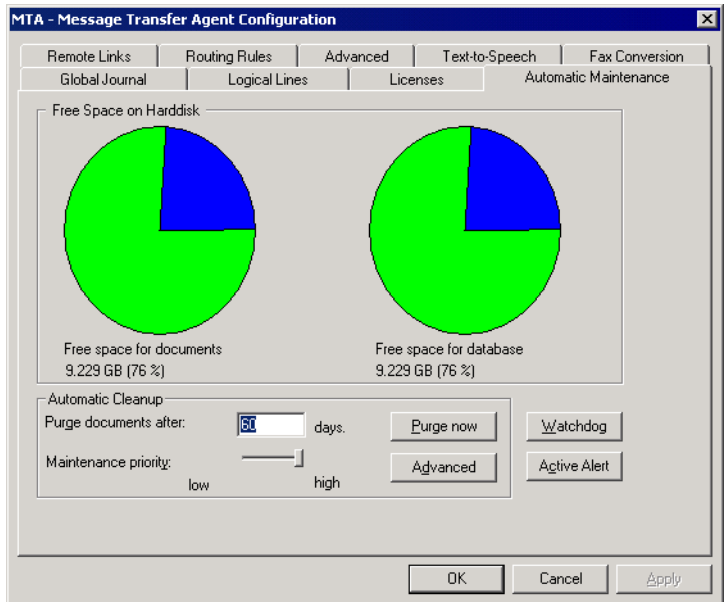
The circles display the amount of available free storage space for documents and the database.

Automatic Cleanup

This option allows the server to remove any MRS documents which exceeded the specified time limit. Through use of the **Purge now** button an immediate setting

modification can be triggered as well. This is especially useful with acute shortage of storage space. Otherwise a modification would not take effect until the next performance of the corresponding maintenance script job.

With the **Maintenance priority** option these purge operations and all other routine maintenance jobs are executed with the set priority. If computation bound processes such as simultaneous voice mail user service occur along with the maintenance script, a low priority should be chosen.



Further maintenance options are available for the maintenance script through selection of the **Advanced** button. These options greatly influence the amount of free storage space on the server.

Remove Database Entries and Documents

Transaction processes as well as individual documents are purged through the activation of the various options in this section of the dialog.

Maintenance Cleanup Options

☐ Remove Database Entries and Documents

☐ Remove CIT indication after: 0 days
Script variable: \${LifeTimeService}

☐ Remove pass-through documents after: 0 days
Script: \${LifeTimePassthrough}

☐ User defined parameter: 0 days
Script: \${LifeTimeUserdefined}

Compression

☐ Representation and voice compression after: 0 days
Script: \${LifeTimeCompress}

Do Not Compress (DNC-Driver) 8000 Hz Mono **Codec >>**

Remove Documents

☐ Purge e-mail after: 0 days
Script: \${LifeTimeEmail}

☐ Purge outbound documents after: 0 days
Script: \${LifeTimeOutbound}

☐ Purge inbound documents after: 0 days
Script: \${LifeTimeInbound}

Jobs **Stop Jobs** **Reload Script** **OK** **Cancel**

- **Remove CIT indication after... days**

Each CIT notification of new inbound messages is equivalent to that of a transmission job for MRS Server. CIT notifications are used for activating signal lamps on the users telephone by new inbound messages. This option deletes the document as well as any corresponding database entries.

- **Remove pass-through documents after... days**

This option deletes all documents transmitted from one non-interactive service to other non-interactive services. Non-interactive services consist of those services where documents are not actively deleted by the originator e.g. Fax G3, voice, or SMTP.

- **User defined parameter:**

This option sets the variable `$(LifeTimeUserDefined)`, which is used in user defined deletion actions of maintenance scripts.

Compression

The option **Representation and voice compression after...days** deletes any conversions created for delivery to the various client types, while retaining the original document. Additionally, through use of the **Codec** button, an audio codec can be configured, that the original voice file is compressed. These files can be played-back at a later time, but in their compressed form, require less system resources (harddisk storage space).

Remove Documents

These options remove the original document from the database and in some instances, insert an administrative notification. The information in the journals remain intact so that e.g. billing data can be evaluated.

- **Purge e-mail after ...days**

This option deletes email messages. These could be for example, documents sent from one mail gateway to another.

- **Purge outbound documents after ... days**

Outbound documents e.g. fax documents would be deleted when the expiration time has elapsed.

- **Purge inbound documents after ... days**

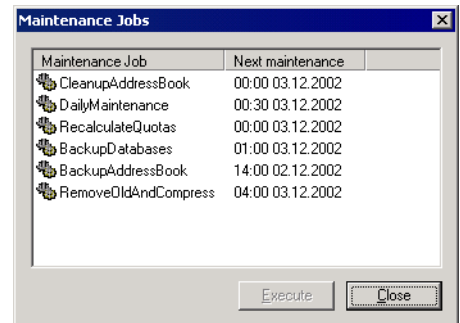
Inbound documents e.g. fax documents would be deleted when the expiration time has elapsed.

Maintenance Jobs

Jobs defined in the various maintenance scripts are displayed in this dialog along with their upcoming execution time.

An immediate execution of the job is possible through selection of the job and subsequent selection of the **Execute** button.

Selection of the **Close** button returns the user to the Maintenance Clean-up Options dialog.



Maintenance Job	Next maintenance
CleanupAddressBook	00:00 03.12.2002
DailyMaintenance	00:30 03.12.2002
RecalculateQuotas	00:00 03.12.2002
BackupDatabases	01:00 03.12.2002
BackupAddressBook	14:00 02.12.2002
RemoveOldAndCompress	04:00 03.12.2002

Stop Jobs

Via this button you can terminate all currently running maintenance script jobs.

Reload Script

If you have modified the maintenance script, press this button to reload it so that the modifications are copied. Note that with an MRS Server update a modified script would be overwritten again with the script default version. To avoid this the modified version should be stored under a different name in the directory <MRS Root>\res\maint\. This new name with complete path specification should then be entered in the registry value MaintenanceScript in key HKEY_LOCAL_MACHINE\SOFTWARE\PP-COM\MRS\MTA.

Watchdog

Several surveillance functions can be set here.

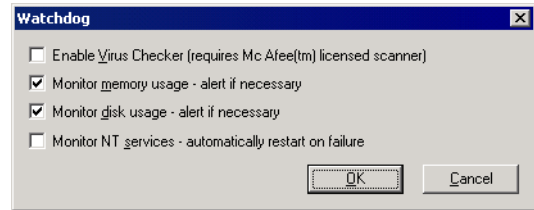
The memory usage (RAM) and the hard disk capacity can be placed under surveillance, so that in the event of a critical decrease in capacity an appropriate warning would be generated.

MRS Services can also be monitored at the process level, and restarted in the event of a termination. This requires a bit of manipulation in the Windows NT Registry and is explained in the *MRS System Architecture*.

Additionally, all binary files that are received either as attachments to a document or through an Euro file transfer, can be scanned for viruses using the Network Associates¹¹ Virus Scanner. If a virus is detected, the infected file is replaced with a text document containing an appropriate warning and the originator's name. The virus scanner supports among other things the search in ZIP archives and macro viruses.

To activate the virus scanner the Command Prompt version¹² must be installed in the directory <MRS Root>\Res\VirScan, thus copy Scan.exe (version 4.0.2 to 4.50 are currently supported) along with the required DLLs and current *.DAT files to this directory. The virus scanner must be licensed!

If in addition to binary files also text files are to be checked for viruses, the value VirusCheckFileFormats must be adapted in the Windows NT registry database. More information is found in the *MRS System Architecture*.



11. Formerly McAfee.

12. The software to be installed is "McAfee VirusScan for Command Line". "McAfee VShield", "McAfee GroupShield" or "McAfee VirusScan Antivirus-Software for Windows 95, Windows 98, Windows NT Workstation v4.0 and Windows 2000" are **not** supported.

Active Alerts

Through the use of active alerts, the surveillance of all log messages to the MRS Monitor is possible. By applying various search criteria to the messages, warnings can be generated, routine status reports containing all error messages can be sent or a notification can be written in the Windows event log.

Before active alerts can be used, the global filter in the MRS Monitor must be configured for their use. This is performed much in the same manner as with the global log files. Messages will only be generated when one of the filter conditions specified here has been satisfied. Under **Log Intervals**, the **Interval in days between log messages:** is entered. **Minimum time in seconds between alert messages:** is also defined in this portion of the dialog. This entry prevents reoccurring reports from being continuously sent.

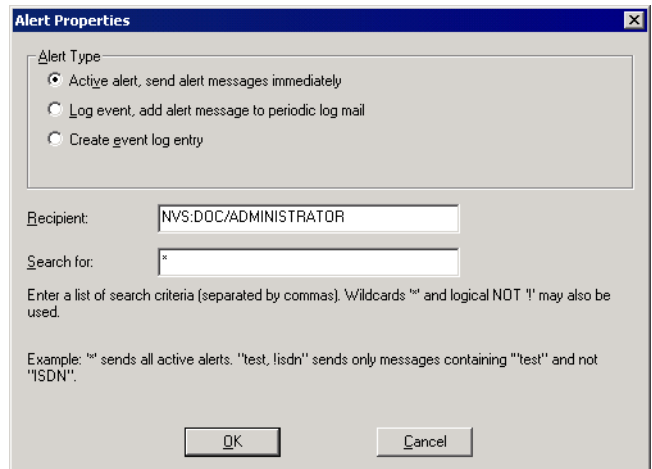
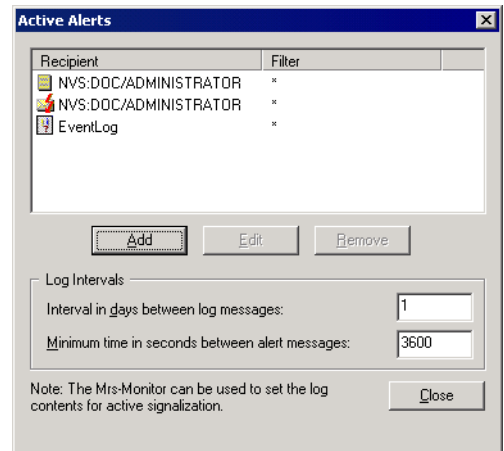
If the **Alert Type** for a combination of recipient and filter setting is set to **Active Alert**, a message is immediately sent when such a log notification occurs.

Log events are compiled and sent at regular intervals.

For **Event Log Entries** no recipient can be defined since the entry is generated in the Windows event log. This alert type is suitable e.g. for further editing by an SNMP management tool.

Any MRS address can be used as the **Recipient:** for these notifications.

In the **Search for:** field search criteria are defined that must be present in a message before the message is transmitted. An asterisk (*) encompasses all messages configured within the MRS Monitor, whereas an exclamation mark (!) followed by a term

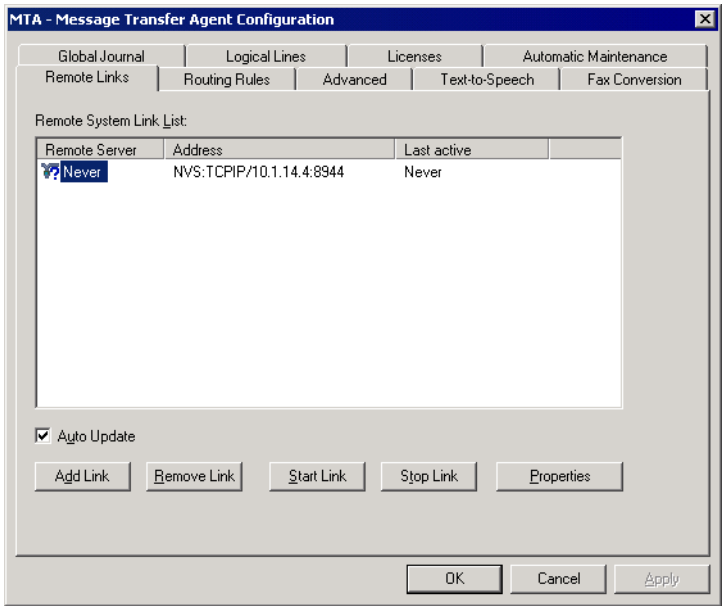


specifies that the term is not present in the message. Numerous search criteria may be entered when separated by a comma.

If the prompt program log server is started from within the MRS SDK Utilities external Windows NT events can also be incorporated into reports.

6.4.2 Remote System Links

Connections to remote servers can be configured or removed from the **Remote Links** tab. Under the dialog entry **Last active** the functionality of connection can be checked. Through use of the buttons **Start Link** and **Stop Link**, selected connections can be dynamically stopped or started during the operational mode of the server.



The option box **Auto Update** ensures that the data displayed in the window is always current.

New connections are inserted in the dialog through use of the **Add Link** button. Configuration of the new link is described in the following paragraphs. Existing links can be removed by selecting the link and subsequent selection of the **Remove Link** button.

The most important entry to mention in the **Remote System Link Properties** dialog is the **Address:** of the other MRS Server. The address of other MRS Servers is given here. The service of this address must be a SMI Transport. For a more detailed description of these transports refer to the section on “SMI Transport (Remote System Links)” section from page 58, “ISDN SMI Transport (Remote System Links)” section from page 66, and “SMI Transporter” section from page 204.

The screenshot shows the 'Remote System Link Properties' dialog box. It has a title bar with a close button. The fields are as follows:

- Server:** Never
- Password for DDC on remote server:** A text field containing 'xxxxxx'.
- Address:** NVS:TCPIP/10.1.14.4:8944. Below it, a note says '(Remote server NVS Address, e.g. NVS:TCPIP/mrserver.ppcorn.com)'. There is a small 'x' icon to the right of the text field.
- Poll rate (sec):** 86400
- Timeout (sec):** 600
- Retries (n):** 5
- Protocols:** A text field. Below it, a note says '(Protocol import list - when empty import all e.g.: NVS:FXG3.1,NVS:SERVER,NVS:SMS)'. There is a small 'x' icon to the right of the text field.
- ☒ Synchronize local server clock with remote server
- ☒ Replicate remote correlation data to local server
- Replication:** A section with a title bar. Inside, it says 'The following information can be replicated to the local server:'. There are four checkboxes: ☒ User data, ☐ Distribution lists, ☐ System masks, and ☐ Only users with SYNC<node>. There is a small 'x' icon to the right of the section title.
- Buttons:** OK and Cancel.

In the **Protocols:** entry field you can either import all protocols from the remote server (empty field) or specific ones. All lines (protocols) of the remote MTA not having the *Local* attribute can be imported. More than one protocol may be entered when separated by a comma.

If in the MTA configuration tab **Advanced** the validation for remote connections has been activated, a password must be entered for each connection and this password must also be entered on the remote server. For this purpose a pseudo user account must be defined on the remote server with the name of this MRS Server as user ID and the password assigned to the server must be entered here. See also page 58. Assign the following privileges to this user account:

- **Trusted Domain Privilege**
All jobs from the foreign system receive the privileges of this user account and additional privileges must be assigned so that e.g. a fax may be sent via the remote system. This is easiest accomplished by assigning a user group to the user account.

Global Alias Editor

This privilege is required for correlation data exchange (see further below). Thus remote system users on the individual MRS Server can for example be automatically defined as contacts.

Server Administration

Message Transfer Agent (MTA)

In the dialog entry **Poll rate**, the time interval is given in seconds. A value of 60 denotes that a connection will be attempted every 60 seconds. The value in **Timeout** is the amount of time between connection attempts if the connection attempt results in a failure. **Retries** is the number of times an attempt is made before a remote system link is deactivated.

If the option **Synchronize local server clock with remote server** is activated, the clock of the server making the remote connection will be set to that of the remote system. This could be of interest when establishing a remote system link to a server equipped with an atomic clock (DCF-77).

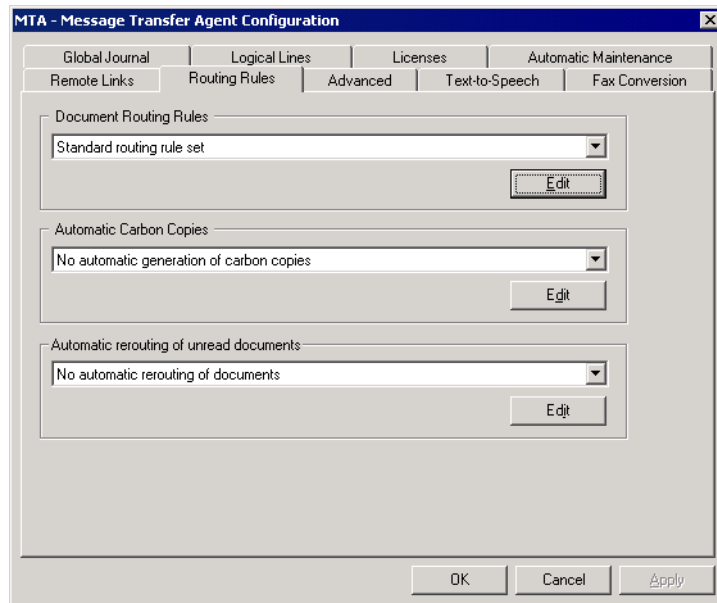
The address directories (Correlation Database) of both systems can be replicated. It is possible to overwrite the information on the local system with that of the remote system, so that the user administration of both systems occurs on the remote system. The amount of information to be replicated can be selected via the checkboxes **User data**, **Distribution lists**, **System masks** and **CTI Journals**.

Please note that with the **Only users with SYNC<Node>** option only user accounts for which a corresponding switch has been set are replicated. This switch must first be inserted in the user database mask each. A database field of the CHAR type with length 1 (switch) must be created on the remote server for this purpose. Using this option the MRS Server name may only consist of a maximum of 11 characters instead of 15. If the individual server was named DOC, a database field called SYNCDOC had to be installed on the remote server.

Since a remote system link is unidirectional, the settings must be performed on both MRS Servers.

6.4.3 Routing Rules

Routing Rules determine the behavior of the MTA.



Document Routing Strategy

In most cases, documents are routed over the address book of the MRS Server (default routing rules). Therefore, the user database must be provided with the appropriate information for this task (user database, see page 22ff).

The fax-server inbound routing strategy is different from the default routing rules insofar as a special rule for networking voice mail servers is omitted.

The SAP inbound routing forwards all messages to an SAP R/3 system which is in charge of inbound routing by assigning the corresponding information such as fax number to the users. Note that SAP inbound routing must at any rate be adapted since the routing rules must also contain the individual token of the connection to the SAP R/3 system which cannot be added automatically. See "SAP R/3 Gateway (SAPR3APL)" on page 263.

of the **SAP routing rules** and the **FMS routing rules** (fax server) do not differentiate from that of **standard routing rules** through the MRS address book. Therefore in this case the routing strategy used last will be displayed,

If an individual modification to the routing rules is required, then changes must be made directly in the Windows NT registry. This can be accomplished by selecting the **Custom defined routing rules** and then editing the routing rules through use of the **Edit**

button. Modification of the routing rules should only be attempted by someone with well-founded knowledge of the routing rules and their effect on the operation of the total system. A detailed description is found in the *MRS System Architecture* manual.

Automatic Carbon Copies

Every incoming fax document can be routed to a printer as an automatic copy. The only requirements for this procedure is an installed Print APL and a printer connected to the system.

Through use of the option **Incoming faxes are copied to the default printer**, all incoming fax documents are copied to the default printer of the Print APL.

With the option **Incoming faxes are copied to a user defined printer**, incoming fax documents are only copied when a printer name is present in the user database field **PRINTER** of the recipient.

In the option **Custom carbon copy rules**, administrators can define their own rules for carbon copies. Selecting the **Edit** button calls up the built-in editor for creating custom rules. As previously mentioned, modification of the routing rules should only be attempted by persons with a well founded knowledge of the routing rules.

This option is deactivated when the option **No automatic generation of carbon copies** is selected.

Time Triggered Document Routing

Incoming documents that are not read by the recipient within a specified time limit can be rerouted to another user (e.g. Postmaster). Through use of the option **Incoming documents are automatically rescheduled to a Postmaster if not read**, all documents (fax, voice, EFT-files) will be rerouted to the Postmaster if not read within a 10 day period. During the MRS Server installation the Postmaster is given as default recipient for unread documents.

The option **Custom rescheduling rules** enables administrators to define their own rules for the rerouting of unread documents. Selecting the **Edit** button calls up the built-in editor for modifying the *Awake Rules*. Modification of the *Awake Rules* should only be attempted by persons with a well founded knowledge of all *Rules*.

Through use of the option **No automatic rescheduling of documents**, the *Awake Rules* are deactivated. In lieu of data protection prescription, this option should remain active.

6.4.4 Advanced

In the configuration tab **Advanced**, parameters for various options can be set.

The screenshot shows the 'MTA - Message Transfer Agent Configuration' dialog box with the 'Advanced' tab selected. The tabs include Global Journal, Logical Lines, Licenses, Automatic Maintenance, Remote Links, Routing Rules, Advanced, Text-to-Speech, and Fax Conversion. The 'CIT - Message Waiting Indication' section has a checked 'Enable CIT signalization' checkbox. Below it are two radio buttons: 'Send dynamic text message as CIT' (selected) and 'Send voice message as CIT'. A 'CIT Cache' button is to the right. The 'Message:' field contains the text '{ORNAME}: {SUBJECT,30} {DIGEST,120}'. The 'User Quota' section has an unchecked 'Activate user quota checking' checkbox and a checked 'Count outbound documents for quota calculation' checkbox, with a note below. The 'Remote System Links' section has a checked 'Use authentication for Remote System Links' checkbox. The 'Performance' section has a checked 'Optimize Scheduling Queue' checkbox. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

CIT – Message Waiting Indication



If you use the Notification APL for message waiting indication, the CIT signalization must be deactivated here! This is done automatically with the Notification APL installation. The administrator need not configure the Notification APL. Merely the user must decide via the Web Administrator in which way they want to be notified.

Here you can **enable CIT signalization** via the kernel and select the type of signalization.

Send dynamic text message as CIT allows transmission of a configurable text message over a text capable protocol (e.g. SMS). The text is entered in the **Message** field and may contain the following variables:

Variable	Significance
{DATE}	Date

Server Administration

Message Transfer Agent (MTA)

Variable	Significance
{DIGEST[, <Max>]}	A portion of the text message is embedded in the CIT notification. The maximum length of this option can be set through the optional entry <Max>. The algorithms that forms the digest attempts to filter-out unnecessary information from the text. This could be e.g. empty lines, greeting macros, etc.
{FORMAT}	Inbound message format (e.g. voice, fax, or email) independent of the inbound service used.
{ORGNOME[, <Max>]}	A readable version of the originator address. If the message originator is contained within the alias database, the name of the originator could appear instead of the fax number. The maximum length of this option can be set through the optional entry <Max>.
{ORGNODE}	Incoming service
{ORGUSER}	Originator address
{RECNAME[, <Max>]}	A readable version of the recipient address. message. The maximum length of this option can be set through the optional entry <Max>.
{RECNODE}	Target service
{RECUSER}	Recipient address
{SUBJECT[, <Max>]}	Subject line of the message. The maximum length of this option can be set through the optional entry <Max>. If the actual length of the subject line is greater, it will be cut-off and “...” suffixed to entry.
{TIME}	Time

The option **Send voice as CIT message** enables the transmission of voice files over the ISDN voice protocol. This protocol is also used for setting and resetting indicator lamps on telephones connected to an Integral PBX from Bosch-Telecom. After selecting this option the path to the * . PCM voice file is entered that is to be used for notifications.

Protocols used for setting and resetting indicator lamps (e.g. CIT over the Hicom PBX from the V.24 APL) should be of the type text since no actual message is being sent.

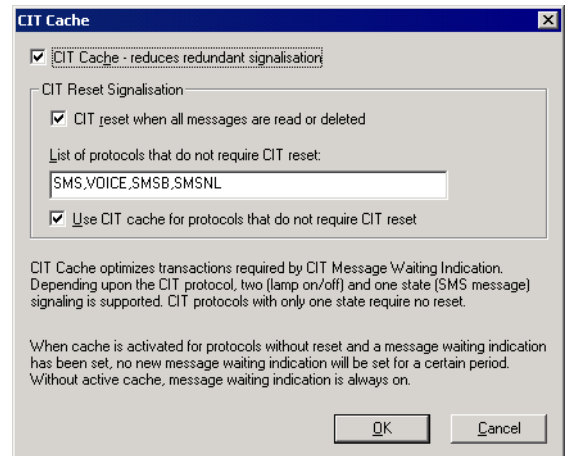
For the kernel the transmission job acts as a trigger for setting or resetting the indicator lamps.

These entries can also be made depending on the user. Enter the file containing the individual text resp. voice file of the respective user in the database field **CITFILE**. Text files must be suffixed with **TXT** for this purpose. The files are stored in the MRS Server's **UserData** directory tree and entering files is thus performed in relation to this directory. This feature enables among other things various language versions of the CIT notification.

If user-dependent CIT files are to be used, the value **CitUserBasedMessage** in the registry key **HKLM\PP-COM\MRS\MTA\CIT** must additionally be set to 1.

The number of transaction required for CIT signaling can be optimized in the **CIT Cache** dialog.

Depending upon the CIT protocol, two (lamp on/off) and one state (SMS message) signaling is supported. When the CIT cache is deactivated, a notification is sent for every new inbound message. When CIT cache is activated, and a message waiting indication has been sent, no new message waiting indications will be sent for a brief period of time.



A counter based CIT is activated when the option **CIT reset when all messages are read or deleted** is selected. Counter based CIT differentiates itself from the previously described CIT in that MRS caches the number of new messages that have not been read in the database field **NEWMSGs**. The CIT signal is then reset when this number returns to 0. The option CIT Cache should not be activated with counter based CIT.

User Quotas

Quotas are normally used to restrict the amount of resources (e.g. hard disk storage space) allotted to a user. Access to these resources are denied when users have exceeded the amount of resources allocated to them. There are however conceptual differences between quotas used on a file server and those of a mail server.

Users on a mail server have only a limited amount of control over the use of resources. Their actions (sending messages) and those of others (receiving messages) tax the amount of resources allotted to them. It is therefore possible that a user may not be

able send a message while either several large messages, or simply too many messages have been received.

How do Quotas function?

Two database fields are used: QUOTA and QUOTAUSED. The field QUOTA contains the amount of allocated resources in Bytes. An entry of zero in this field indicated an unrestricted amount of resources. The amount of used resources is written to the field QUOTAUSED. The value in QUOTAUSED is compared with that in QUOTA when a message is sent, and if the document size plus the amount in QUOTAUSED is greater than the value in QUOTA, the message will not be sent. This condition will remain until the user deletes a portion of their in or outbound messages. Receipt of inbound messages is always possible.

Outbound documents may also be included in QUOTAUSED computations. The activation of this option causes an asynchronous update of quota data which may take several hours to complete.

Remote System Links

When the option **Use authentication for Remote System Links** is activated a password is required as validation for each remote system link. A secure connection is guaranteed through the use of this option.

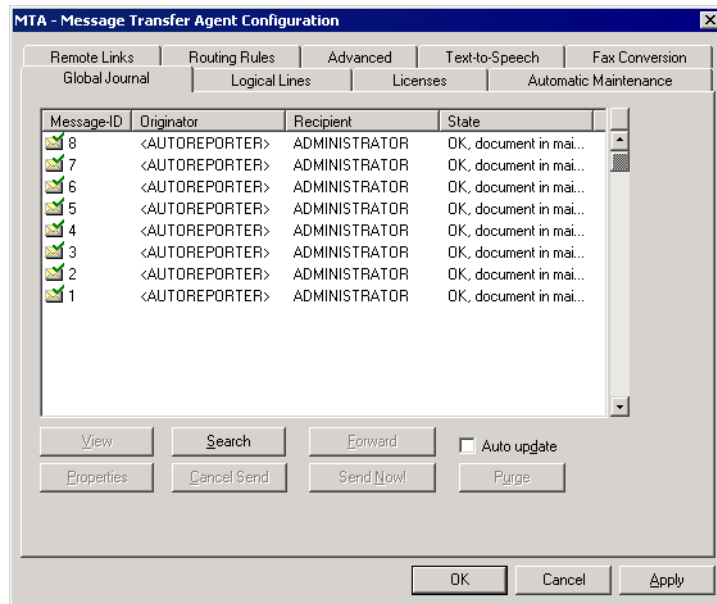
Optimization

The option **Optimize Scheduling Queue** activates an algorithm which optimally reassigns all lines. Disadvantage: This algorithm is extremely computation bound.

Attention: Since the MTA immediately reassigns all free lines when this option is used, it is possible that during the expansion of fax distribution lists, no free lines are available for inbound traffic. This can be avoided by defining certain lines for inbound traffic only.

6.4.5 Global Journal

The global journal displays information over in and outbound messages from the MRS Server.



Messages can be sorted either by Message ID, originator, recipient, or document state. Message sorting is accomplished by clicking with the mouse pointer on the corresponding field in the header.

Various message operations can be performed through use of the buttons in the lower portion of the dialog. The message ID is selected and subsequently the desired operation. When the user possesses the appropriate authority, a document viewer can be started through use of the **View** button. Selecting the button **Properties** displays the contents of the internal journal database fields and the PMF system fields of the selected entry. Transmission jobs that are still in the MTA queue can be removed with the **Cancel Send** button. These messages are identifiable by the clock symbol. As soon as a message has been transferred to another APL, the **Cancel Send** option is no longer available. **Send Now!** immediately transmits messages that are still found in the MTA queue. The option **Forward** allows messages to be forwarded to other users. The user currently logged-in must possess read privileges before they can forward a document. The option **Purge** replaces the contents of the message with the text “document already deleted by administrator”. Through this the journal entry remains and therefore the information over the transaction is retained, but the storage space required by the document is drastically reduced.

The option **Search** allows the user to search for either a message ID, originator, recipient, or a state. The results of search requests are displayed at the top of the global journal.

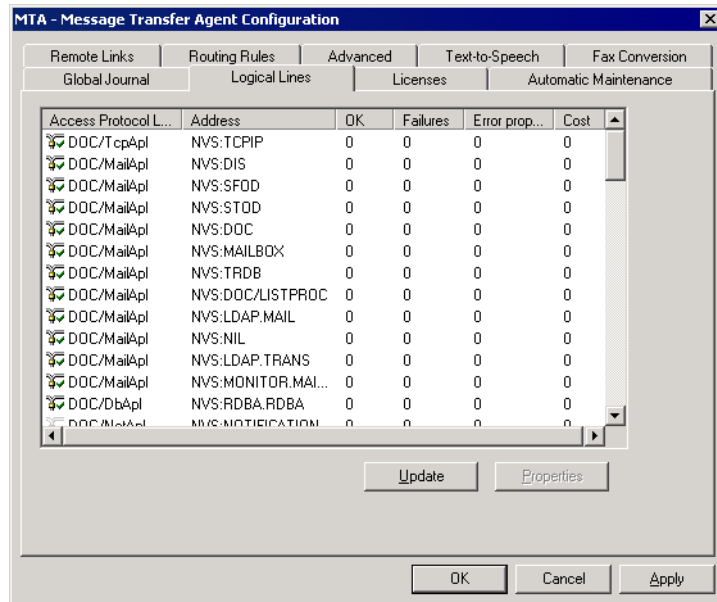
When the option **Auto update** is activated the journal is updated in a real time mode. This option should not be activated for those users that have a relatively slow RAS connection to the MRS Server.

A message status is represented by the corresponding icon. Possible icons and their meaning:

Icon	Significance
	This message has an invalid status! One possible reason could be an APL crash during a transmission process so that the kernel has consequently not received a status report.
	The message has been transferred to an APL or to another MRS Server per Remote System Link; up to now no final report has been received.
	The message is queuing up (in a waiting loop) to be transmitted to an APL.
	Successful message transmission according to status report.
	Message delivery could not be executed or an error occurred during the transmission according to status report.
	Successful message transmission according to status report. The mail is now intended for automatic deletion. See “Automatic Cleanup” on page 179.
	Message delivery could not be executed or an error occurred during the transmission according to status report. Furthermore the message is now intended for automatic deletion. See “Automatic Cleanup” on page 179.
	The message has been transferred to an APL or to another MRS Server per Remote System Link; up to now no final report has been received. Furthermore the message is now intended for automatic deletion. See “Automatic Cleanup” on page 179.
	The target APL has already returned a report on this message, however, this report is still queuing up (in a waiting loop) and has not been delivered to the sending APL yet.

6.4.6 Logical Lines

All logical lines registered within the MTA are displayed in the configuration tab **Logical Lines**. All information, attributes and options are displayed for a selected line through use of the **Properties** button.



In the **Logical Lines Properties** dialog all relevant attributes can be viewed for a logical line and those of lines imported over a remote system link.

Line traffic directions can be defined for the individual logical lines through the option **Line enabled for outbound transactions**. Lines are either defined as bi-directional or explicitly for inbound traffic only.

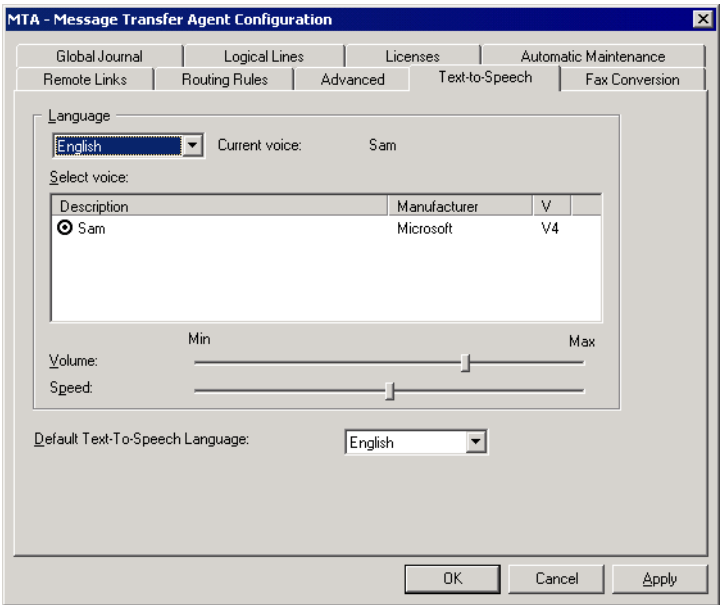
Through use of the option **Line usage preference**, values can be assigned to lines which determine the priority of their usage. Taking advantage of this possibility, a Least Cost Routing configuration can be easily setup for transmission jobs over various lines to various sites. In a like manner a fall-back strategy can be developed for remote system links. If for example a remote system link is normally established over a TCP/IP connection through the Internet, a second line over an ISDN connection could be configured using a lower line priority which would only be used in the event of an Internet interruption or when the amount of data to be transferred is too large.

The MTA is equipped with a cache in which all line information is stored. Through this cached information the MTA is aware of all lines and their properties at the start of the server. Included in this cached information are the attributes and characteristics of lines imported over a remote system link.

Statistical information and dynamic error probabilities are also displayed within the dialog.

6.4.7 Text-to-Speech

Text messages can be converted to voice messages over the Microsoft SAPI version 5.1 interface for speech synthesis.



Therefore, a Text-to-Speech module¹³ that conforms to SAPI standards and provides a speaker in the respective language must be installed and Text-to-Speech and the corresponding TTS language added as supplementary MRS features.

Subsequently select a **Voice** for each of the supported **Languages** in this tab. MRS tries to recognize the language of the text to be put out and takes the speaker set for the recognized language for conversion. If no language has been recognized, the **Default Text-To-Speech Language** set here is used. The **Volume** and **Speed** of the voice playback can be set through use of the sliders.

13. Since MRS 5.0 for example ELAN has been supported, with 5.1 also Speechify by Speech works which requires considerably more resources but offers a much better voice quality.

6.4.8 Fax Conversions

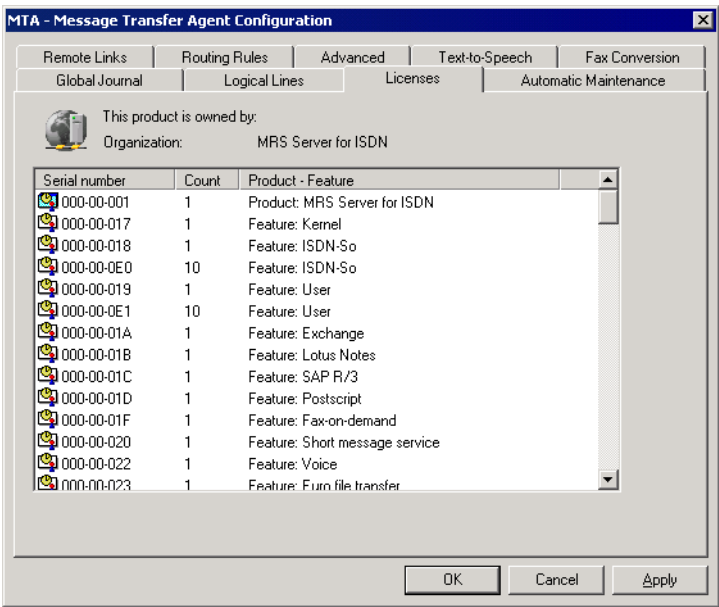
These settings determine the appearance and format of fax documents that arrive as text documents on the MRS Server which converts them into fax messages for transmission..

The image shows a screenshot of the 'MTA - Message Transfer Agent Configuration' dialog box, specifically the 'Fax Conversion' tab. The dialog has a title bar with a close button. Below the title bar is a tabbed interface with the following tabs: 'Global Journal', 'Logical Lines', 'Licenses', 'Automatic Maintenance', 'Remote Links', 'Routing Rules', 'Advanced', 'Text-to-Speech', and 'Fax Conversion'. The 'Fax Conversion' tab is selected. The settings are organized into three sections: 1. 'Font for Text-to-Fax Conversion': Includes a 'Type:' dropdown menu set to 'Courier New', a 'Size:' dropdown menu set to '11', and a 'Weight:' dropdown menu set to 'Normal'. 2. 'Resolution': Includes a 'Fax G3' dropdown menu set to '200*200 dpi' and a 'Fax G4' dropdown menu set to '200 dpi'. 3. 'Paper Settings for Text-to-Fax Conversion': Includes a 'Format:' dropdown menu set to 'A4', four margin input fields (Left margin: 1.00, Top margin: 1.00, Right margin: 1.00, Bottom margin: 1.00), and a 'Units:' dropdown menu set to 'inch'. At the bottom right of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

Firstly, the utilized type of **Font for Text-to-Fax Conversion** can be set via **Type:**, **Size:** and **Weight:**. Next the **Resolution** for **Fax G3** resp. **Fax G4**, appropriate for such a conversion, should be set. Lastly, the paper size and the margins must be entered under **Paper Settings for Text- to- Fax Conversion**. For margin entries you can default set the **Units:**.

6.4.9 Licences

In this configuration tab the serial number of the product as well as product features are displayed..



6.5 Mail APL

6.5.1 Printer Embedded Codes

By means of printer embedded codes you can place information in a document to be evaluated by the MRS Server without any special installations on the client computers. Only a corresponding PostScript printer on the MRS Server is used as network printer by the clients.

The printer “HP LaserJet III PostScript Plus v2010.118” which is included in the Windows scope of supply and connected with the “MRS Server Fax Monitor” port

must be installed on the MRS Server. You can select an arbitrary printer name that ends with “EC” for “Embedded Codes”. For example “MRS Server Printer with EC”. “EC” must be preceded by a blank.

The Mail APL evaluates the embedded codes contained in the PostScript code of the print output and replaces these with blanks in the hardcopy. The embedded codes must be set in Courier font which is a so-called native font with printers and is thus maintained as text in the PostScript hardcopy which is required for recognizing and filtering the codes at a later date.

The following embedded codes are supported with the precise syntax being configurable in each case. You can either select one of the preconfigured versions or define entirely new ones. This example corresponds to one of the available presets:

Embedded Code Example

@FAX=263/@

@SMTP=xy@unbekannt.de/@

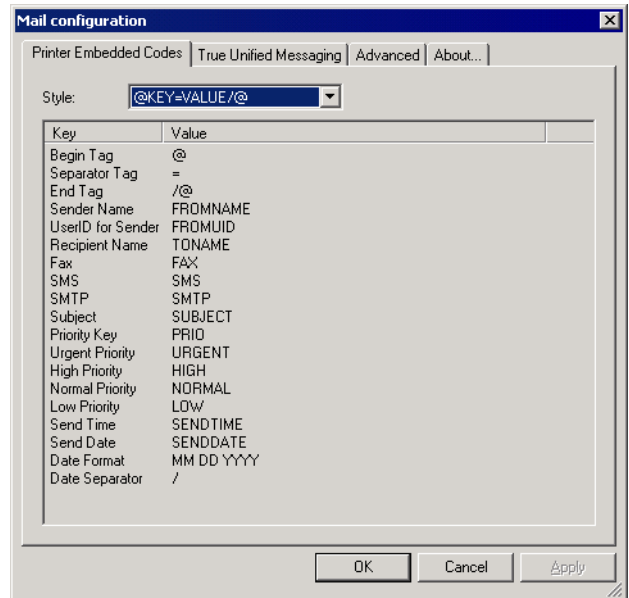
@FROMUID=MAM/@

Significance

Recipient fax number.

Recipient Internet e-mail address.

Individual MRS user ID.



Embedded Code Example	Significance
@FROMNAME=Mark Maier/@	Individual name resp. originator name.
@SENDTIME=13:30:00/@	Send time for delayed transmission.
@SENDDATE=17.06.2001/@	Send date for delayed transmission.
@PRIO=normal/@	Message priority
@SUBJECT=Testing PEC/@	Message subject. With fax this can be displayed on the optional cover page.
@TONAME=Thomas Crown/@	Recipient name.

You can define an arbitrary number of different fax and Internet e-mail recipients per embedded code in a document. Each specified recipient receives a copy of the message then.

The syntax of an embedded code thus reads:

<BeginTag> <Token> <Separator> <Content> <EndTag>

<BeginTag>

Example: "@"

<Token>

The following tokens are available: FAX, SMTP, FROMUID, FROMNAME, SENDTIME, SENDDATE, PRIO, SUBJECT, TONAME.

<Separator>

Default: "="

<Content>

Depending on the *<Token>* used, the corresponding content is here entered by the user. See above table.

<EndTag>

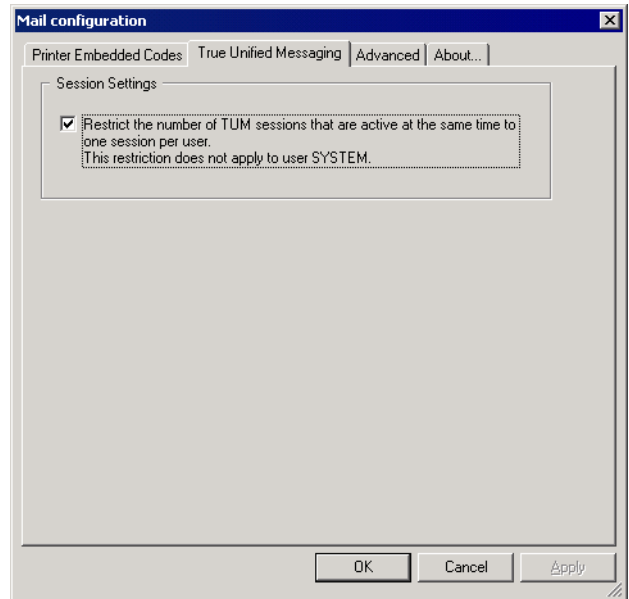
Example: "/@"

6.5.2 True Unified Messaging

The option **Restrict the number of TUM sessions that are active at the same time to one session per user** prevents a mailbox from being simultaneously accessed via several telephones per TUI. Thus the option is basically a locking mechanism.

Other TUM providers e.g. for Lotus Notes or Microsoft Exchange have default set this restriction to a TUM session.

The user **SYSTEM** is a user automatically defined by the system with a minimum of privileges and is exclusively used for access per TUM. With TUM a new message must always be generated by a user. Therefore a TUI accessing a message per TUM always specifies this user when a caller leaves a message.



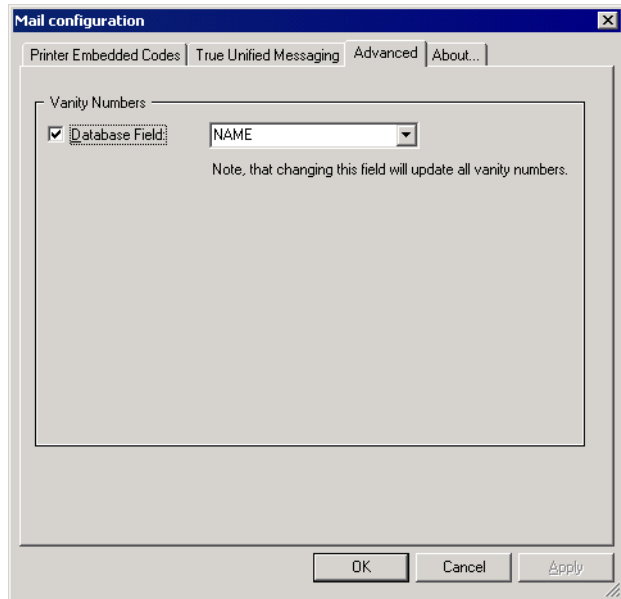
6.5.3 Vanity Numbers

In addition to digits you also find characters printed on modern telephone device keys. So you can also memorize numbers in the form 0700 CYCOS AG instead of cryptic telephone numbers such as 0700-2926724. Such character representations of telephone numbers are called vanity numbers.

The MRS Server can use such character combinations for dialing by converting from a database field to be specified, containing a digit/character

sequence, into another database field. The **Database Field** for this conversion can be selected here from the fields NAME and VM_HI_DSP_NAM (alternative name for representation in a Hicom telephone display; is used, for example, by the VMS voice mail system). The converted result is then found in the VM_VANITY field of the correlation database. This field can now be used by client applications such as e.g. a voice mail system.

The assignment of characters and digits on the keys has been standardized by the ITU. However, there are two recommendations for this assignment: Option A and B.



Option A

1	2 ABC	3 DEF
4 GHI	5 JKL	6 MNO
7 PQRS	8 TUV	9 WXYZ
0		

Option B

1 QZ	2 ABC	3 DEF
4 GHI	5 JKL	6 MNO
7 PRS	8 TUV	9 WXY
0		

In practise, option A occurs the most, therefore it is used by the MRS Server. The MRS Server additionally contains a conversion table that places some special characters on certain characters, thus converting them into the digits assigned to the characters.

Since the correlation database contains the entries in the OEM font (codepage 437), this assignment occurs for characters with a value greater than or equal to 128 to the ASCII characters A to Z.

The following table contains the assignment:

Decimal	OEM	Assigned	Decimal	OEM	Assigned
128	Ç	C	146	Æ	AE
129	ü	UE	147	ô	O
130	é	E	148	ö	OE
131	â	A	149	ò	O
132	ä	AE	150	û	U
133	à	A	151	ù	U
134	å	A	152	ÿ	Y
135	ç	C	153	Ö	OE
136	ê	E	154	Ü	UE
137	ë	E	159	f	F

Decimal	OEM	Assigned	Decimal	OEM	Assigned
138	è	E	160	á	A
139	ï	I	161	í	I
140	î	I	162	ó	O
141	ì	I	163	ú	U
142	Ä	AE	164	ñ	N
143	Å	A	165	Ñ	N
144	É	E	225	ß	SS
145	æ	AE			

Note that all characters not specified here, except A to Z, are not copied. The names “Doe, John“, “DoeJohn“ or “DOEJOHN“ thus result in the same number.

Since the assignment of vanity numbers to users e.g. via the user name cannot be unique, a corresponding selection mechanism in a client application must consider this and, with choosing via a user name, offer all users for selection that have been assigned the same vanity number by conversion.

6.6 Microsoft Exchange Gateway (ExchAPL)

Exchange 5.5 Gateway configuration is described in the *MRS and Microsoft Exchange* manual. Exchange 2000 Gateway configuration is described in the *MRS and Microsoft Exchange 2000* manual.

6.7 SMI Transporter

A SMI transport is used when a SMI interconnection is made between two servers (Remote System Link), or when a connection is created between a client and a server. In addition to those listed here, there are other SMI transporters such as the ISDN APL. Those listed here are generally used for in-house connections (LAN) and have no further telematic functions.

6.7.1 Named Pipes (PipeAPL)

The Named Pipes APL is a transport based on Named Pipes. This transport can be used under the Windows NT platform for connecting the MRS Server to a system. Additionally, the MRS Client can be connected to a server through the use of a Named Pipe.

Configuration of the Named Pipes is not necessary since all required settings are made during the installation of the selected network protocol under Windows NT.

Named Pipes were created for the Internal Process Communication (IPC) in the LAN Manager. They are present as soon as a network protocol is installed under Windows NT. A common protocol on both client and server is a prerequisite for the connection over a Named Pipe. Several advantages to Named Pipes under Windows NT are:

- Implementation as a file system (NPFS), where joint features from the Windows NT file system such as caching are automatically used.
- Connection to the local computer does not run over the network interface. This is the only transport with which the MRS Windows Client can be connected to a MRS Server, when both are installed on the same computer.
- Named Pipes, as with every other network protocol, can also be used over the Remote Access Service (RAS) of Windows NT.

6.7.2 SPX (SPXAPL)

The SPX APL is a SPX based transport. MRS Servers under Windows NT can be connected to other systems using this transport. In addition, the MRS Windows client can be coupled to a server using the SPX transport.

A configuration of this transport is not necessary since all required settings were performed during the Windows NT *NWLink IPX/SPX compatible transports* network protocol installation.

The SPX transport was developed for applications in local networks (LAN).

6.7.3 TCP/IP (TCPAPL)

The TCP/IP APL is a TCP/IP based transport. MRS Servers under Windows NT can be connected to other systems using this transport. Remote system links with a NVS Server running in QNX (real time operating system) can be made using the TCP/IP transport.

The MRS Windows client can also communicate with a MRS Server using a TCP/IP transport. Since TCP/IP is a protocol which is used in wide area networks (WAN) such as the Internet, communication between servers (or client and servers) could also be worldwide if an Internet connection is available.

A configuration of this transport is in most cases not necessary since all required settings were performed during the Windows NT *TCP/IP network protocol* installation.

6.7.3.1 Firewall

After it's installation, the TCP/IP firewall is disabled. This enables access from every computer to the MRS Server over the TCP/IP protocol.

If access is to be denied to specific computers or networks, this can be accomplished by forming a reference from the IP-Net-network address and Netmask. Through this reference, access can either be granted or denied. A description of the access type can also be given for easy identification.

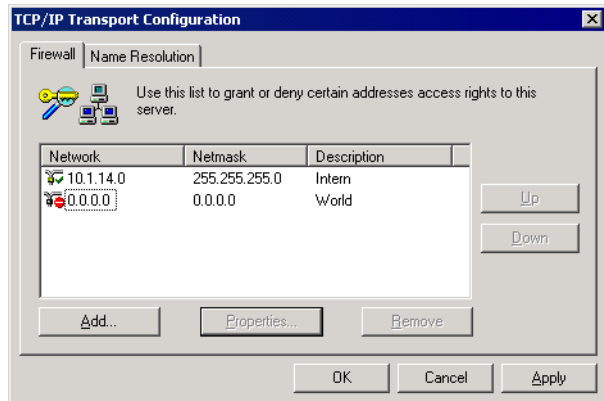
As soon as an entry is present in the dialog window, the behavior of the TCP/IP APL changes so that every computer (or network) must now be explicitly granted access to the server. In most normal cases only computers and networks that are allowed access to the MRS Server will appear in the dialog window.

The reference list is sequentially searched from the first entry until a match is found. If a single computer from a network is to be allowed access to the server but the rest of its network denied access, then the computer reference must be inserted in the list prior to that of the network. By selecting the **Add** button, new references may be added to the list. After selecting a reference and subsequent selection of the **Properties** button, characteristics of the address may be viewed or modified. Selecting the **Remove** button deletes the selected entry from the reference list. Repositioning an access reference within the list is accomplished through the use of the buttons **Up** and **Down**.

New settings are activated as soon as the **OK** or **Apply** buttons are selected. All changes to the settings are dynamically integrate, so that a restart of the TCP/IP APL is not necessary.

Example

In the following examples an activated entry (access granted) is displayed with a "+" and a deactivated entry (access denied) through an "X".



- If access to the MRS Server is to be explicitly granted to all IP-addresses, then the following should be inserted into the reference list:

	IP-Address	Netmask
+	0.0.0.0	0.0.0.0

- To deny access to all IP-addresses the following entry is inserted into the reference list.

	IP-Address	Netmask
X	0.0.0.0	0.0.0.0

- A Class C network exists which has been divided into two logical networks. The “upper” network and the “rest of the world” are to be denied access to the server.

Class C Network: 194.77.158.0, Netmask: 255.255.255.0

Lower Network: 194.77.158.0, Netmask: 255.255.255.128

Upper Network: 194.77.158.128, Netmask: 255.255.255.128

The reference list then has the following entry:

	IP-Address	Netmask
+	194.77.158.0	255.255.255.128

- A Class C network exists which has been divided into two logical networks. The “upper” network and the “rest of the world” are to be denied access to the server with the exception of one MRS Server within the upper network which is to be used for a remote system link.

Class C Network: 194.77.158.0, Netmask: 255.255.255.0

Lower Network: 194.77.158.0, Netmask: 255.255.255.128

Upper Network: 194.77.158.128, Netmask: 255.255.255.128

MRS Server in upper Network: 194.77.158.155

The reference list then has the following entries:

	IP-Address	Netmask
+	194.77.158.0	255.255.255.128
+	194.77.158.155	255.255.255.255

- In a Class C network all computers are to be granted access with the exception of one, and worldwide access is also to be deactivated.

Class C Network: 194.77.158.0, Netmask: 255.255.255.0

Computer denied access: 194.77.158.166

The reference list now has the following entries:

	IP-Address	Netmask
X	194.77.158.166	255.255.255.255
+	194.77.158.0	255.255.255.0
X	0.0.0.0	0.0.0.0

Since all addresses that do not fall within the range of those through the combination of IP-address and Netmask will be denied access, the last entry may be omitted:

	IP-Address	Netmask
X	194.77.158.166	255.255.255.255
+	194.77.158.0	255.255.255.0

6.7.3.2 Name Resolver

The name resolver of the TCP/IP APL is by default always activated. This means that every IP-address which attempts to make a connection to the MRS Server is queried through *Reverse Name Resolving*.

If individual computers within a local network are assigned IP-address through DHCP, these addresses should be entered in the Name Resolver's list, and the Name Resolver then deactivated.

Since the configuration in this dialog corresponds to that of the Firewall, a short description of the differences between the two are outlined in the following:

Selection of the **Add** button in the tab **Name Resolver**, calls up a dialog in which a reference to an IP-address, netmask, and description may be entered. The option **Reverse resolve the specified IP addresses** can either be switched on or off for the specific reference.

In contrast to the Firewall, the standard behavior of the Name Resolver is to resolve all IP-addresses. This behavior remains constant, even for those IP-addresses not entered in the list when a computer or network is listed.

6.7.4 Remote System Links

The SMI protocol is used for internal communication between MRS Servers and Clients. A connection between MRS Servers through SMI is called a *Remote System Link*. All SMI transports can also be used for connections between two servers.

Remote system links are configured over the MTA settings. See page 184.

6.8 Internet Email, POP3/IMAP4 Server and POP3 Mail Import (SMTPAPL)

A description of the services implemented through the SMTP APL can be found on page 78ff of this manual. Configuration of the SMTP APL, as with all other APLs, is done through use of the MRS Monitor. In the Modules window of the MRS Monitor the entry **Settings** should be selected and subsequently **SmtplApI/Settings.SMTP** (Simple Mail Transfer Protocol) Server

6.8.1 SMTP (Simple Mail Transfer Protocol) Server

The SMTP Server enables receiving and sending of email messages via the Internet protocol Simple Mail Transfer Protocol (SMTP). For send operations some additional configurations can be performed in the **Outbound Mail** configuration tab.

General Settings

The TCP/IP Host name of the MRS Server (including the domain), is used as the default entry in the field **Host name:**. This entry is used for creating the originator address. If the Host name was not included, and only the domain given, the MRS originator address generated by the SMTP gateway would be `user@domain` instead of `user@host.domain`. This address, as well as other user specific data,

can be individually configured for the user within the MRS user database. Enter the complete SMTP address of the respective user in the SMTP field of the user database. This address is also used for inbound routing to the users.

The **SMTP port:** entry determines which port is used by the SMTP APL for in and out-bound email traffic. The default setting is 25, but when used behind a firewall, another setting may be more appropriate.

The screenshot shows the 'Internet Mail Configuration' dialog box with the 'SMTP Server' tab selected. The dialog has a title bar with a close button. Below the title bar are four tabs: 'Secure Sockets', 'Formats', 'POP3 Mail Import', and 'SMTP Server'. The 'SMTP Server' tab is active. The main area contains the following fields and options:

- Version 5.10.112 (w/IN-NT) Release Build 3333
- Host name: ☒ Use ESMTP delivery reports
- SMTP port: ☐ Use BIND address:
- E-mail section:
 - ☒ Enable inbound mail
 - Inactivity timeout for mail receipt:
 - Max. no. of concurrent inbound connections:
 - ☐ Use sender addresses to authorize gateway access
 - ☐ Autolearn names of senders in user database
 - ☒ Enable client authorization

At the bottom are three buttons: 'OK', 'Cancel', and 'Apply'.

Server Administration

Internet Email, POP3/IMAP4 Server and POP3 Mail Import (SMTPAPL)

The option **Use ESMTP delivery reports** activates delivery confirmations (Delivery Status Notifications), an SMTP protocol extension (Extended SMTP). The arrival of emails at the MRS Server is thus confirmed to originators with ESMTP. This extended service functions only when this SMTP protocol extension is also available to the recipient.

In the **Use BIND address:** field you can enter the IP address the SMTP server then binds itself to. This is normally the computer's default TCP/IP address. With a multi host system having several IP addresses the desired one can be specified here.

Incoming Mails

Via **Enable inbound mail** the gateway for incoming SMTP messages is activated. Receiving mails then occurs simultaneously through the maximum number of channels specified in **Max. no. of concurrent inbound connections:**.

In the dialog field **Inactivity timeout for mail receipt:**, the time is given in seconds after which a transmission is terminated should an error occur.

The transmission privileges of the message originator can be checked when the option **Use sender addresses to authorize gateway access** is enabled. If the recipient address of a transmission job was e.g. NVS:FAXG3/1234567890@domain.com the originator of this job must have Fax G3 transmission privileges.

Upon activating this option a pseudo user with the SMTP identifier and the privileges "Internet Mail", "Trusted Domain", "e-mail" and USER is automatically defined. Without this pseudo user the SMTP APL is not enabled to forward external messages to internal users. In the event that a user with this identifier already exists when this option is activated, a malfunction might be the result since this user is not automatically assigned the above privileges then.

When the option **Autolearn names of senders in user database** is enabled, an entry is automatically created in the user database using the originator address of incoming messages. Attention should be given to the fact that these automatically generated entries lead to a relatively fast expansion of the user database. Also the following conceivable scenario may cause problems: Someone has sent himself a message from his private Internet account to the company he works for. Two entries with the same name exist in the user database. Now if someone does not know a recipient's alias (username) and tries to find this recipient using the full name both addresses would be displayed. The message might then inadvertently be sent to the private address instead of the company account.

Enable client authorization activates another ESMTP feature, namely the AUTH token, which serves to authorize the SMTP originator by means of a password, is sent to the client in this case. Via this AUTH token the connected client is informed that the SMTP

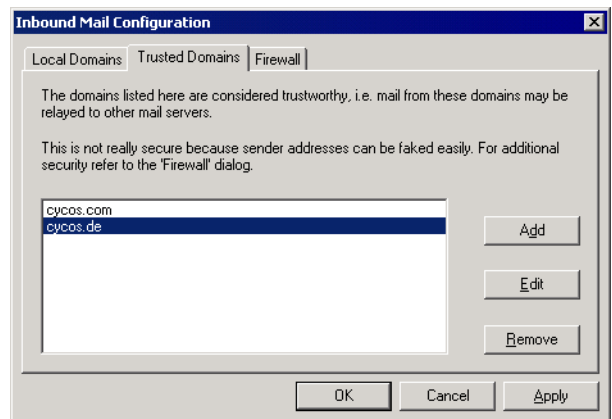
server has this feature so that the client can use it. Several processes are supported then.

For the CRAM-MD5 process the SMTP APL must know the user password in the clear text. This, however, is not possible with the default database entry **PASSWORD**. Therefore the database **POP-PASSWORD** is taken which, using this feature, should be added to the user database with type **CIPH, CHAR** and a reasonable password length (app. 40 characters). With the **PLAIN** and **LOGIN** processes the **PASSWORD** entry is used as alternative if the **POP-PASSWORD** database field is not available or empty. The **LOGIN** process is used for example by Outlook Express and Outlook.

Please note that a possibly desired authorization against the SMTP server cannot be explicitly configured in the Netscape Messenger. The Netscape Messenger automatically uses the **PLAIN** process if it is offered. In the event that you do not want an explicit authorization by means of a password here, deactivate the **AUTH** function via the Registry.

Selecting the **Advanced** button enables the entry of local and trusted domains.

Messages are never forwarded to other Internet Hosts from within a **Local Domain**. Messages are only transmitted internally within these domains. If the local domain has an **MX-Record** which points to the **MRS Server**, it will automatically be considered to be a local domain and must not be entered as such.



Through an entry in **Trusted Domains**, SMTP messages can be routed to non-local users. Messages from non-authorized originators will be disregarded, without any notification to the sender.

Since recipient addresses in the Internet are easily feigned, further security measures should be set in the configuration dialog of the **Firewall** tab so that the server is not used as a relay station. Hereby access to the SMTP APL can explicitly be permitted or refused for certain IP networks. This corresponds to the firewall handling for the TCP/IP APL described on page 205.

Some mail servers do not allow receiving messages from a mail server that is classified as so-called Open Relay via which messages can thus be sent by everyone. Such

Server Administration

Internet Email, POP3/IMAP4 Server and POP3 Mail Import (SMTPAPL)

an Open Relay is at any rate a security problem enabling so-called spammers to send their mails via the individual mail server. In this way companies can incur considerable costs as the spammer simply sends one mail with the complete recipient list to the Open Relay which subsequently routes the message to all recipients at the company's expense! For this reason we recommend to globally block relaying here and to give explicit permission only for networks where it is desired. Blocking receipt of mails from an Open Relay is normally done via lists available in the Internet. Whether the individual mail server is an Open Relay can be checked e.g. under <http://www.abuse.net/relay.html>.

Relay Authentication Strategie

Relaying means transmission of a message via another SMTP server. Direct delivery to the target SMTP server would be normal, but the originators may be behind a firewall or on-line only for a short while. Therefore they possibly transfer their emails to an SMTP server that is on-line permanent so that this server then sends the messages to the target SMTP server. In this case the MRS SMTP server would act as so-called Relay Host, defining via the following strategy when it can be used by an originator for message transmission.

- If neither firewall nor Trusted Domain entries have been defined, each originator is considered local and may thus use the SMTP server as relay.
- Firewall entries are compared with the originator's physic IP address; Trusted Domains with the "Mail From" entries in the email header. If at least one firewall entry has been defined, all incongruous originators and those that match a corresponding exclusion entry of the firewall entries are considered not local unless they have an entry as Trusted Domain. Originators not local must not use the SMTP server as relay.
- Through a successful verification by means of AUTH command or "SMTP after POP/IMAP", the originator is also considered local except he or she would be excluded via a firewall entry.

6.8.2 Outgoing Emails

In the dialog entry **Send mail via relay host:**, an optional Host address (TCP/IP) may be entered where messages are to be rerouted. This is common practice e.g. when the MRS computer cannot fully access the Internet but can reach another SMTP server that takes over this function. This could be for example a firewall which is used to protect the company's network from Internet intrusion.

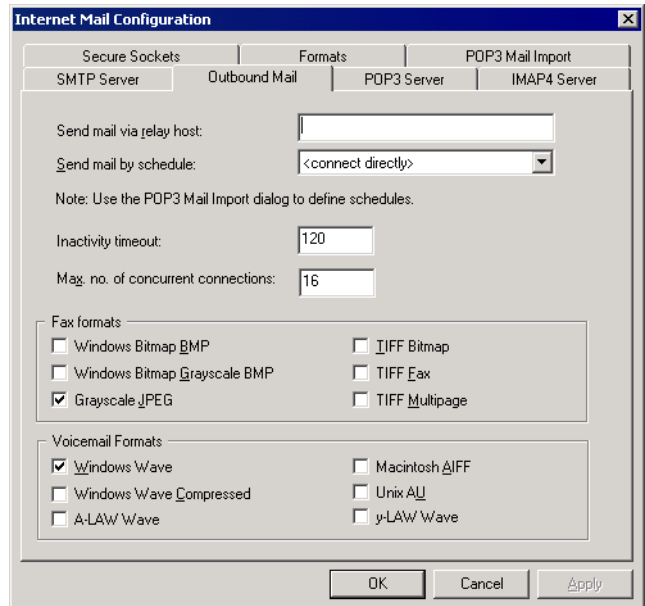
The option **Send mail by schedule:** allows the selection between a

direct network connection or that of one defined in the user database. For user defined connections, a time-plan can be assigned to users in the configuration tab **POP3 Mail Import**. In this constellation, a PPP-Connection is established through the Windows NT RAS service. Outbound Internet email messages are then sent over this connection. Outgoing Internet email messages are sent immediately when a direct network connection (dedicated line, etc.) or equivalent Internet connection is used. This happens either directly or indirectly through the Relay Host which was entered in this dialog.

After lapse of the time specified under **Inactivity timeout:** the server closes an inactive outgoing connection.

Max. no. of concurrent connections: is the number of send jobs that can be carried out parallel. This value should not be measured too high if the available band width is relatively small. Otherwise the send processes are increasingly cancelled owing to timeouts as the receiving party had to wait too long.

If required, outbound fax and voice messages can be converted into one or more formats to be selected under **Fax Formats** resp. **Voice Mail Formats**. It goes without saying that this only applies to rerouted or directly sent documents and not to attachments of normal emails.



Server Administration

Internet Email, POP3/IMAP4 Server and POP3 Mail Import (SMTPAPL)

6.8.3 POP3 Server

The option **Enable POP3 server** activates the POP3 server on the port listed in the field **POP3 server port**:

In the **Client inactivity timeout**: field you can enter the time in seconds after which the POP3 server terminates transmission in case of irregularities.

For connections to the client the **Max. no. of messages per poll**: can be set as well as the **Maximum messages size**: in the appropriate fields provided in the **POP3 Server** configuration tab. An

entry of zero in **Maximum messages size**: denotes that the set amount of messages can, regardless their size, be transferred in one go. If **Max. no. of messages per poll**: were set to zero, *no* messages would be transmitted any more!

Max. no. of concurrent connections: limits the number of POP3 clients that can simultaneously access the server.

Via **Flag as read after retrieval** you can inform the MRS Server that polled messages are flagged as read on the server as soon as they have been polled via a POP3 client. Since there is no further interaction between the POP3 client and the POP3 server after message polling, this is the only way to indicate these messages accordingly. Otherwise polled messages would be considered unread and thus new with a later access to the individual mailbox via another client (IVR system, Lotus Notes, Microsoft Exchange etc).

The screenshot shows the 'Internet Mail Configuration' dialog box with the 'POP3 Server' tab selected. The 'POP3 server' section contains the following settings:

- ☒ **Enable POP3 server**
- Client inactivity timeout:** 30 seconds
- Max. no. of messages per poll:** 64
- Maximum message size:** 0 bytes
- Max. no. of concurrent connections:** 16

A note states: 'Note: Specifying 0 as the maximum message size disables message size restrictions.'

POP3 server port: 110

☐ **Flag as read after retrieval**

Buttons at the bottom: OK, Cancel, Apply.

6.8.4 IMAP4 Server

Selecting the option **Enable IMAP4 server** activates the IMAP4 server on the port indicated in the field **IMAP4 server port**:

With the IMAP4 protocol, documents remain on the server and only header information is fetched at login. Since only a small amount of data is being transferred, restrictions required by POP3 servers becomes unnecessary.

In the option **Client inactivity timeout**, the time is entered in seconds after

which the IMAP4 server terminates a connection if no data are transferred to and from the client any more. The presetting is 666 seconds which is a bit more than the Microsoft Outlook standard poll rate, querying new messages every 600 seconds.

Max. no. of concurrent connections: restricts the number of IMAP clients that may simultaneously access the server.

Individual folders can be configured as a repository for transmitted and deleted messages. The names of these folders should be entered in the **Folder for sent items** field.

In the **Mailboxes that should not be copied automatically** field you can specify the MRS Server folder name for which MRS is to ignore a copy command. Note that for example Outlook provides a setting called 'Save copies of messages in Sent Items folder' (found via **Tools→Options...→Preferences→E-mail Options...**), via which copies of the sent documents are automatically generated. But since the MRS Server has a corresponding folder for all outgoing documents, these copies are pointless. In particular when access is made via older IMAP clients that can handle folders only restrictedly or not at all, documents are displayed twice since these clients display all documents from all folders in a flat view. Thus if the user performs the above setting, they can have the copy command ignored by the MRS Server.

The screenshot shows the 'Internet Mail Configuration' dialog box with the 'IMAP4 Server' tab selected. The 'IMAP 4 server' section includes a checked 'Enable IMAP4 server' checkbox, a 'Client inactivity timeout' of 666 seconds, a 'Max. no. of concurrent connections' of 16, an 'IMAP4 server port' of 143, and a 'Folder for sent items' set to 'Sent items'. Below this is a section titled 'Mailboxes that should not be copied automatically' with a text input field and 'Add', 'Edit', and 'Remove' buttons. The bottom of the dialog features 'OK', 'Cancel', and 'Apply' buttons.

Server Administration

Internet Email, POP3/IMAP4 Server and POP3 Mail Import (SMTPAPL)

6.8.5 Secure Sockets

Via the **Enable Secure Sockets** you can activate an SSL ciphering (Secure Sockets [SSL/TLS]) for IMAP, POP, SMTP sending and receiving. The ports used are default set to those used by Outlook 2000, thus for POP3 Port 995 and for IMAP4 Port 993.

For SMTP sending and receiving the START-TLS command is supported. The options **verify client certificates** resp. **verify server certificates** enable you to check the certificates of the respective receiving

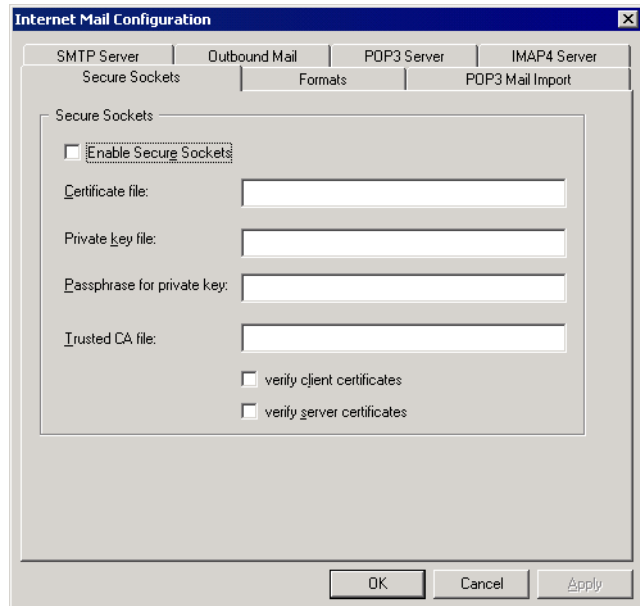
stations for the case that the SMTP APL acts as client, thus sends messages, as well as for the case that it is server and receives messages.

With secure sockets activation the entries **Certificate file:**, **Private key file:**, **Passphrase for private key:** and **Trusted CA file:** must contain reasonable values. To obtain the required data proceed analog to the Web APL:

You need a certificate of an internationally accepted CA (Certificate Authorities). Such a CA is for example Verisign (www.verisign.com), who are, however, among the most expensive. Follow the procedure described by the respective CA to receive the certificate.

Enter the **Certificate file:** obtained from the CA, the **Private key file:** and the **Passphrase for private key:**. The password must at any rate be entered via the configuration tab here since it is stored in the registry enciphered. The term "Passphrase" is to point out that a whole sentence rather than a simple password should be used to enhance security.

Demanding the certificate or creating a simple test certificate for viewing the basic functionality requires the **OpenSSL** program which is found in the `<MRS Install>\SDKTools` directory.



Example of the creation of a self-signed certificate to be used for test purposes to check the basic SSL functionality:

```
openssl req -x509 -newkey rsa:1024 -keyout key.pem  
-out req.pem -config config
```

Two files are generated, the **Private key file** `key . pem` and the **Certificate file** `req . pem`. Copy these files to `<MRS Install>\res\SMTPAPL\`.

How to obtain an officially signed certificate?

You need a private key and a certificate request. The latter one is usually sent to the CA that signs this certificate with your private key. First generate some random numbers required for private key generation later on:

```
openssl md5 * > rand.dat
```

Next create the private key upon which its password is specified. This password should be a longer phrase, for example a sentence:

```
openssl genrsa -rand rand.dat -des 1024 > key.pem
```

or, if you want to use “triple DES”:

```
openssl genrsa -rand rand.dat -des3 1024 > key.pem
```

Now the private key `key . pem` has been generated. Keep the specified password (phrase) well in mind as without it the private key cannot be used. Furthermore create a backup copy of the private key and keep it in a safe. Never pass the private key on to anyone else! If you should lose it, the certificate signed with it cannot be used any more.

Finally generate a certificate signing request to be transferred to the CA. The CA then sign the request and send back a certificate which can be used with the previously generated private key:

```
openssl req -new -key key.pem -out csr.pem -config config
```

`key . pem` is the above generated private key and `csr . pem` the desired certificate request. During the generation you are queried for the following information:

- Country code. It consists of two letters and has been standardized by ISO (e.g. de for Germany, au for Australia, gb for Great Britain, mx for Mexico, etc.)
- Full country name.
- Name of the city resp. town.
- Name of the organization. This should be the organization that owns the domain name.
- Name of the individual department (e.g. marketing, sales, etc.)
- The qualified host name of the individual SMTP site (e.g. mail.cycos.com).

Internet Email, POP3/IMAP4 Server and POP3 Mail Import (SMTPAPL)

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBETCBvA1BADBMXQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0ZTEh
MB8GA1UEChMYSW50ZXJxZXQvV2lkZ210cyBqdHkgTHRkMRAdBgYJKoZIhvcNAQkB
FgFgMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAL6nPTY3avNgbubx+ESmD4LV1LQG
fcSh8nehEOIxGwmbCPlrhTP87PaAOXvgPvRQUjCGStrlQsd8lcYVvK0aytNUCAwEA
AaAAAOAGCSqGSIb3DQEBAUAAOEAxCSa8eXgbG2ZhVyFkRvRi4vT8haN39/Qjc9
BrRh2n0TKGfMct9h+1Xx0wNRQY/SIGV1y3+3abNiJmJBWnJ8Bg==
-----END CERTIFICATE REQUEST-----
```

```
[ req ]
default_bits                = 1024
default_keyfile              = privkey.pem
distinguished_name          = req_distinguished_name
attributes                  = req_attributes
x509_extensions             = v3_ca

dirstring_type              = nobmp

[ req_distinguished_name ]
countryName                 = Country Name (2 letter code)
countryName_default         = AU
countryName_min             = 2
countryName_max             = 2

localityName                = Locality Name (eg, city)

organizationalUnitName      = Organizational Unit Name

commonName                  = Common Name (eg, YOUR name)
commonName_max              = 64

emailAddress                = Email Address
emailAddress_max            = 40

[ req_attributes ]
challengePassword           = A challenge password
challengePassword_min       = 4
challengePassword_max       = 20

[ v3_ca ]
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer:always
basicConstraints = CA:true
```

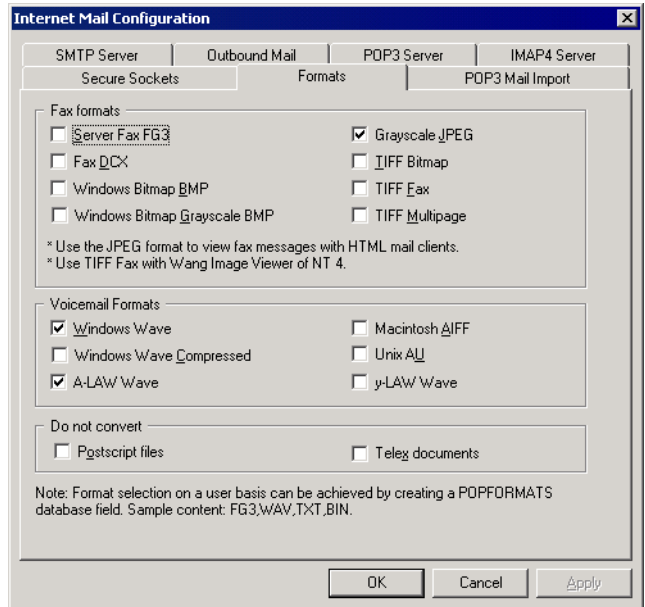
6.8.6 Formats

In the configuration tab **Formats**, various file formats can be given for fax and voice services for display by either a POP3 or IMAP4 client.

Clients whose format is not supported by the MRS Server would be converted (when possible), to one of the selected file formats.

If Postscript or telex files can be displayed by the client a conversion to either a graphic or text format should be included.

The following **Fax Format** are available:



Format	Description
Server Fax G3	Cycos fax format (MRS Viewer).
Fax (DCX)	Multi-page PCX graphic format. Used by Microsoft fax.
Windows Bitmap BMP	Individual fax pages are converted to a Windows Bitmap.
Windows Bitmap Grayscale BMP	Individual fax pages are converted to a Windows Bitmap, where a grayscale interpolation is performed.
Grayscale JPEG	Fax data is converted to a 9 color JPEG grayscale format. This format is suitable for viewing with HTML mail clients.
TIFF Bitmap	Individual fax pages are converted to a standard TIFF Bitmap.
TIFF Fax	Fax data is converted in accordance with TIFF standards.
TIFF Multipage	Fax data is converted in accordance with TIFF standards (multi-page).

Server Administration

Internet Email, POP3/IMAP4 Server and POP3 Mail Import (SMTPAPL)

The following **Voice Mail Formats** are available:

Format	Description
Windows Wave	Windows Sound Format
Compressed Windows Wave	Compressed Windows Sound Format. The audio codec used to compress these files is configured in the MTA settings. The appropriate codec to play-back compressed files is also required on the client computer.
Macintosh AIFF	Audio format used predominantly on Apple computers.
Unix AU	Unix audio format.

6.8.7 POP3 Mail-Import

The Windows NT remote data transmission service (RAS) must be installed prior to the use of this service.

6.8.7.1 New Database Fields

Four new database fields must be installed in the user database for use with the POP3 Mail-Import service. The fields are described in the following table:

Database Field	Significance
PMI - SCHEDULE	Schedule name (see below). This schedule determines at which time a connection to the POP3 server is established.
PMI - USERNAME	User name for which mail is fetched from the POP3 server. If no entry is given the MRS login name will be used.
PMI - PASSWORD	User login password for the POP3 server.
PMI - HOSTNAME	POP3 server Hostname.

These fields may contain either a pseudo account through which all user mail is retrieved or user specific data for a user account on a POP3 server. A combination of both these possibilities is also possible. The MRS Server recognizes pseudo accounts through the empty user database field **GROUP**.

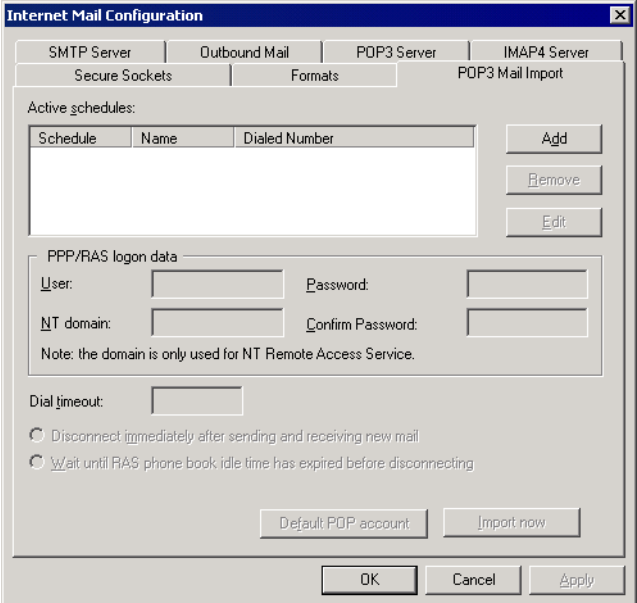
The SMTP APL searches the user database for users with the field **PMI - SCHEDULE** and imports their Internet email in accordance with the scheduling data.

6.8.7.2 Active Schedules

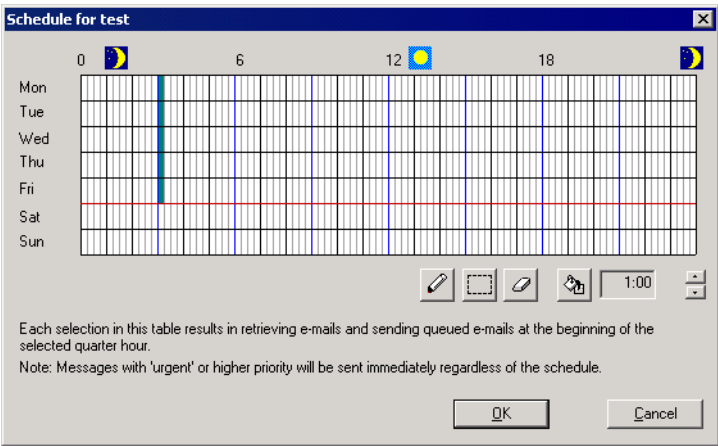
New Schedules can be inserted through selection of the **Add** button. The new schedule must be assigned a name and a dialing number from the RAS telephone book. The new schedule must then be assigned to a minimum of one user before it can be executed.

To delete an existing schedule simply select the schedule and subsequently the **Remove** button.

After the creation of a new schedule, the times at which it is executed must be entered. This is done through selection of the **Edit** button. Connections are established through the Remote Access Service (RAS) during the times marked within the scheduling table. Throughout the duration of the connection email messages are sent and fetched for the various users.



The 'Internet Mail Configuration' dialog box has several tabs: SMTP Server, Outbound Mail, POP3 Server, and IMAP4 Server. The 'POP3 Server' tab is active, showing sub-tabs for 'Secure Sockets', 'Formats', and 'POP3 Mail Import'. The 'Active schedules:' section contains a table with columns 'Schedule', 'Name', and 'Dial Number'. To the right of the table are 'Add', 'Remove', and 'Edit' buttons. Below this is the 'PPP/RAS logon data' section with fields for 'User:', 'Password:', 'NT domain:', and 'Confirm Password:'. A note states: 'Note: the domain is only used for NT Remote Access Service.' Below that is a 'Dial timeout:' field and two radio buttons: 'Disconnect immediately after sending and receiving new mail' (selected) and 'Wait until RAS phone book idle time has expired before disconnecting'. At the bottom right are 'Default POP account' and 'Import now' buttons. The main dialog has 'OK', 'Cancel', and 'Apply' buttons at the very bottom.

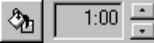


The 'Schedule for test' dialog box displays a scheduling grid. The top horizontal axis shows time in hours (0, 6, 12, 18) with moon icons indicating night. The vertical axis lists days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun). The grid consists of 24 columns (hours) and 7 rows (days). A vertical blue bar is highlighted in the first column (00:00-01:00) for Monday. Below the grid are icons for editing (pencil, eraser, lasso, hand) and a '1:00' time interval selector. Text at the bottom explains: 'Each selection in this table results in retrieving e-mails and sending queued e-mails at the beginning of the selected quarter hour. Note: Messages with 'urgent' or higher priority will be sent immediately regardless of the schedule.' 'OK' and 'Cancel' buttons are at the bottom right.

Server Administration

Internet Email, POP3/IMAP4 Server and POP3 Mail Import (SMTPAPL)

The function of the individual buttons is described in the following table:

Button	Significance
	Assigns “Pen” characteristics to the cursor. The individual fields of the scheduling table can be marked or unmarked.
	This button enables the selection of a range within the scheduling table. The functions of the following two buttons can be applied to the area within marked range or to that outside the range.
	Deletes either the complete schedule, or that within resp. outside the marked range.
	After a time interval assigned (in the example a connection is attempted every 60 minutes (1:00)), the left-hand portion of the button (fill icon) is selected. The complete schedule or that within resp. outside the marked range can then be filled using the fill tool. The complete schedule or the area within resp. outside the marked range would be filled, beginning at 00:00 (12 o'clock midnight) with the selected time interval. Using this method, an hourly POP3 Mail Import can be easily configured.

PPP/RAS Logon Data for <Schedule>

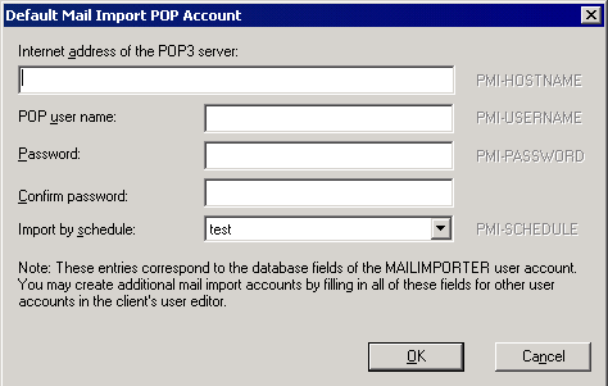
Users and their password can be assigned to every schedule. The password is entered for the user and subsequently confirmed through a second entry of the password. This account data is used for establishing a PPP connection. The optional **NT Domain** is only used when a connection to another Windows NT computer is required to exchange email messages with a POP3 server within that Windows network.

The option **Dial timeout:** defines the amount of time after which a connection attempt is terminated due to the non-establishment of a connection. A redial attempt will not be executed.

An existing RAS connection can either be immediately terminated through use of the option **Disconnect immediately after sending and receiving new email**, or after expiration of the configured RAS inactivity time when the option **Wait until RAS phone book idle time has expired before disconnecting** is selected. It should be noted that even though the first option is somewhat more cost effective, it does not take into consideration that other data transfer activities may be occurring during the connection time. An *immediate termination* of the RAS connection does exactly what it implies regardless of any other background activities. In the case of the inactivity times, a reasonable amount of time should be given for Windows NT RAS services.

Through selection of the button **Default POP account** POP3 servers and POP user names with their corresponding password can be entered. Internet mail for this account would be fetched according to the times stipulated in the schedule entered in the field **Import by schedule**.

When the button **Import now** is selected a connection attempt is immediately executed. Internet email for those users whose database contains an entry for the selected schedule in the field **PMI-SCHEDULE** will be fetched once the connection has been established.



The dialog box is titled "Default Mail Import POP Account". It contains the following fields and labels:

- Internet address of the POP3 server:** A text input field with the label **PMI-HOSTNAME** to its right.
- POP user name:** A text input field with the label **PMI-USERNAME** to its right.
- Password:** A text input field with the label **PMI-PASSWORD** to its right.
- Confirm password:** A text input field.
- Import by schedule:** A dropdown menu with "test" selected, and the label **PMI-SCHEDULE** to its right.

Below the fields, there is a note: "Note: These entries correspond to the database fields of the MAILIMPORTER user account. You may create additional mail import accounts by filling in all of these fields for other user accounts in the client's user editor."

At the bottom right, there are two buttons: **OK** and **Cancel**.

6.9 Web Server (WEBAPL)

In front of the Web APL is a complete HTTP 1.0 Web Server which is used as an interface for the administration of user data, and access to user mailboxes via any HTML browser (e.g. Netscape Navigator, Microsoft Internet Explorer). The complete integration of the E-Script language on the server enables the realization of almost any scenario over a HTTP connection. The HTML pages sent to the Web Client contain MRS specific data which is delivered by the E-Script. This could be for example user fax documents, or the inbound journal.

Besides the Web Server functionality the Web APL can also work as Web Client, controlled by other MRS components via transactions to automatically poll HTML pages from any Web Server. The information contained in these pages can be processed per script to e.g. readout certain stock exchange quotations.

6.9.1 HTTP

In the configurations tab **HTTP** the **Bind address:** is entered in the **TCP/IP** section of the menu. This is of interest to the administrator when more than one IP address is available for the server.

The **HTTP port:** entry determines which port is used by the Web Server for queries and replies. Default settings is port 80.

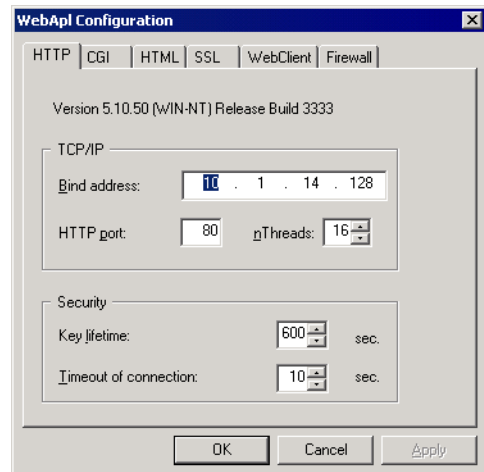
The number of **nThreads:** defines number of Web Clients which may simultaneously access the Web Server.

Security

Users are validated as with the MRS Server, by entering their account name and corresponding password. After the validation has been completed a key is issued by the MRS Web Server which is valid for subsequent queries by the user. After the **Key lifetime:** has expired, the key loses its validity and the user must login again to receive a new key. The value of **Key lifetime:** is given in seconds.

This process increases the access security by decreasing the probability of manipulation on the URL which contains the key.

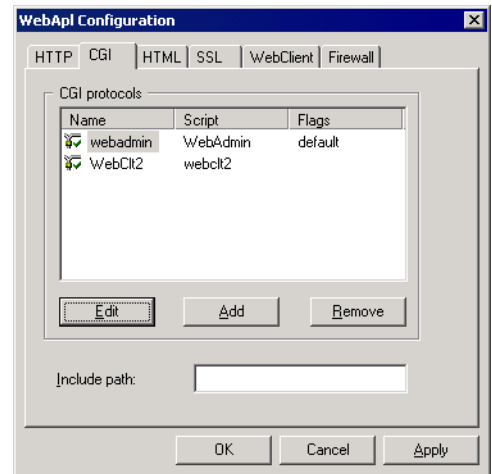
If no data is currently being transferred, the connection to the Web Client will be released after the expiration of the value **Timeout of connection:**. This value is also given in seconds.



6.9.2 CGI

In this configuration tab the protocols provided by the Web APL are entered. For each protocol a **CGI E-Script** must be given which executes the dynamic replacement in the sent HTML pages. This could be for example, the current inbound journal of the logged-in user. If one of these scripts is uncompiled, the **Include path**: to the E-Header Files needs to be specified as well. So this is only necessary with locally written E-Scripts.

Via **Edit**, **Add** and **Remove** the configuration of existing protocols can be altered, new protocols be added or existing ones be removed again.



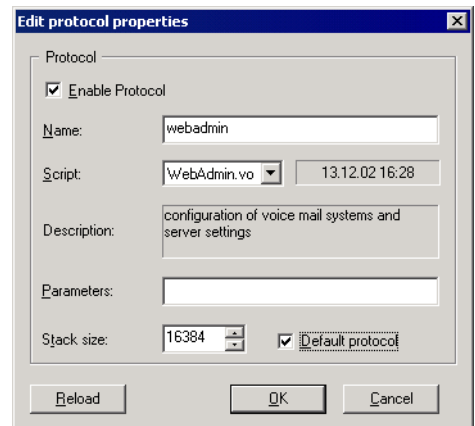
Editing/Adding

Via **Script** one of the installed scripts is entered. In the case of a file with the extension *.vo, this is a previously compiled file, and the date and time of its creation is displayed in the opposite field.

Above the script the **Name** of the protocol is given. Thus various protocols can be installed based on one E-Script. Depending on the **Params** entered, these protocols show a different behaviour. In case of the WAP-Script, however, dependencies, which directly reference the protocol name, exist in the HTML pages and partly also in the script itself. The result is that with the WAP-Script the protocol name must correspond to the file name: WAPCGI. Such dependencies can unfortunately also occur with other scripts so that you should always take the file name as protocol name first and not try other names until this works.

If the script is an E-Script not previously compiled, it can be **Reloaded** after an alteration.

The **Stacksize** refers to the Virtual Machine which executes the E-Object Code. If the E-Scripts have not been locally written for the Web APL, this value should not be changed.



One of the protocols is the **Default protocol** which is automatically called when you address the Web Server, thus open e.g. a page of the type `www.cycos.com` in the individual Web Browser. The other protocols can be addressed by affixing the protocol name in the following manner:

`www.cycos.com/cgi_bin/<Protocol>`

The WAP script as WAP protocol is a special case here since it calls *.wml pages and as only one script of this type exists up to now, you can omit the `cgi_bin` and directly call e.g. the page `www.cycos.com/wap` via a WAP compatible mobile phone to poll your e-mails. In this case `wap.wml` exists as a file referring to the actual WAP script.

You can manually generate a corresponding HTML forwarding page for each protocol here to enable users to call the protocols via

`www.cycos.com/<Protocol>`

The contents of these files would then include a meta tag of the following type as it is also used in the `index.htm` for the default HTML page:

```
<meta http-equiv="Refresh" content="0; URL=/cgi_bin/WebClt2/start">
```

Please note that the specification of the protocol in the URL must precisely correspond to the name of the protocol as it has been configured in the Web APL, thus upper and lower case must be correct as well. If you made a mistake here, the referenced page would not be found and the Web APL would call the default set protocol.

6.9.2.1 WAP Protocol

The WAP protocol must be installed from the `Projects\E\WAPClient` folder found on the Add-On-CD. You can configure it then via **Add**.

Enter the protocol name ("wapcgi" in this case) in the entry line **Name**. Thereunder the description "wapcgi.vo" is selected in the pulldown menu **Script**. The entry that now appears in the **Description** field is a short indication of the script function. Additional entries can now be made in the **Params** line. Via this entry field various script parameters can be adapted. For this purpose several parameters can set in juxtaposition separated by a blank. The following parameters can be specified:

Parameter	Significance
<code>graphics=on</code> or	Image transmission activated

Parameter	Significance
graphics=off	Image transmission switched off (default set) Remark: 1. Image transmission is very time consuming and therefore expensive (connecting time) 2. With different types of mobile phones and activated image transmission problems may occur depending on the installed WAP browser version.
wmlc_site_maxsize=n	n indicates the maximum size of the WMLC page in bytes. The default value is 1200 bytes. Via this setting the representation quality, which also depends on the mobile phone display version, can possibly be improved.
inbox_maxcount=n	This parameter limits the maximum number of inbox messages (= n) pollable per mobile phone. The default value is 300. If message loading is too time consuming then this value should be reduced.
cti_jrn_days=n	The value n represents the number of days for which unanswered calls are listed from the CTI journal in retrospective. The default value is 7 (days).
cti_jrn_count=n	Maximum number of CTI entries to be registered. The default value is 250 and should not be modified.

Now this protocol needs to be activated via the **Enable Protocol** checkbox so that the settings come into effect after **OK** has been selected. The opposite illustration shows the described entries and settings for the WAP protocol. After these have been accomplished you are automatically taken back to the “WebApl Configuration” window. In there the additional entry “wapcgi” is found in the “CGI Protocols” field. Confirm the configuration with **OK** once again.

The screenshot shows a Windows-style dialog box titled "Define a new protocol". It contains the following elements:

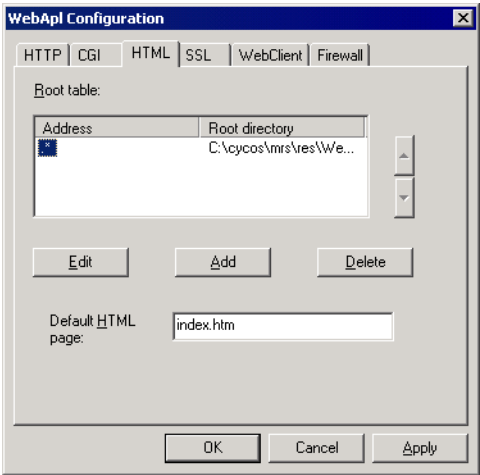
- Title Bar:** "Define a new protocol" with a close button (X).
- Protocol Section:**
 - ☒ **Enable Protocol**
 - Name:** wapcgi
 - Script:** wapcgi.vo (with a dropdown arrow)
 - Timestamp:** 29.11.02 9:06
 - Description:** MRS WAP-Service
 - Parameters:** inbox_maxcount=100
 - Stack size:** 8192 (with a spinner)
 - ☐ **Default protocol**
- Buttons:** Reload, OK, Cancel

6.9.3 HTML

Through use of the **Root Table**, various directories can be given, to which individual addresses are assigned. In this way numerous www sites under various addresses may be hosted (Web Hosting).

The buttons **Edit**, **Add** and **Delete** can be used for the configuration of addresses and start directory.

Addresses are given in regular expressions. The following table provides an overview of the elements which make-up a regular expression:



Element	Description
.	Corresponds to all characters with the exception of a line feed.
*	Corresponds to none or several copies of the previous expression.
[]	A character class which corresponds to those characters contained within the brackets. If the first character in the brackets is a '^' (not) then all characters within the brackets are excluded. A range can be given through the use of a hyphen '-'. Example: [a - z])
+	Corresponds to one or several copies of the previous expression.
?	Corresponds to none or one copy of the previous expression.
	Corresponds to the previous or the following expression.
()	Used to group a series of regular expression to form a new regular expression.
[:<ctype> :]	Another method of representing a character class. This representation can also be used in the character classes described above. <ctype> may be one of the following expressions:
alnum	Corresponds to [0 - 9 A - Z a - z]
alpha	Corresponds to [A - Z a - z]
cntrl	Corresponds to all ASCII characters with a value less than 0x20.

Element	Description
digit	Corresponds to [0-9]
graph	Corresponds to all printable characters.
lower	Corresponds to [a-z]
print	Corresponds to graph and ' ' (space)
punct	Corresponds to [!.,:;]
space	Corresponds to [\f\n\r\t\v]
upper	Corresponds to [A-Z]
xdigit	Corresponds to [0-9A-Fa-f]

All other characters represent a regular expression. The backslash is used before a special character (*,&,#, etc.) to portray a normal character. If a backslash is to be used in an expression as a backslash, it must be given twice (e.g. \\).

Example:

Expression	applies to
. *	all arbitrary character strings
**	exactly two asteriks
www\\.cycos\\.com	www.cycos.com

Additionally, addresses are processed from the top of the table until a match is found for the requested address. Therefore, the order in which addresses appear in the table is important. The order can be rearranged with the arrow on the right hand-side of the menu.

The **Default HTML page** is sent to the Web Client when no other is explicitly requested. This is normal by the first request since in most cases only the web address (for example www.cycos.com) is given.

The HTML file referenced here normally contains a special HTML tag that forwards to one of the installed protocols, thus for example:

```
<meta http-equiv="Refresh" content="0; URL=/cgi_bin/WebClt2/start">
```

Please note that the specification of the protocol in the URL must precisely correspond to the name of the protocol as it has been configured in the Web APL, thus upper and lower case must be correct as well. If you made a mistake here, the referenced page would not be found and the Web APL would call the default protocol if it has been defined.

6.9.4 SSL

In this dialog you can configure the Secure Socket Layer protocol (SSL). The protocol's primary purpose is to enable a safe and particularly private communication between two applications. In this case the two applications are the Web Server realized by the Web APL and the Web Browser employed by the user.

Consequently, with active SSL connection, e.g. the password transmission for polling individual messages can no longer be read by the administrator in charge of the systems used for the message transfer.

To **Enable Secure Sockets** a certificate by an internationally recognized CA (Certificate Authority) is required. Such a CA is e.g. Verisign (www.verisign.com), however, also one of the most expensive. In order to obtain a certificate you should follow the procedure issued by the individual CAs.

Enter the **Certificate file:**, received from the CA, the **Private key file:** and the **Passphrase for private key:** and subsequently specify the **HTTPS port:** via which safe access to the Web Server is to occur. Default port is 443.

For the requisition of the certificate or to create a simple test certificate which can be used to become familiar with the basic functionality, the program **OpenSSL**, to be found in the SDKTools directory, is required.

Example of the creation of a self-signed certificate to be used for testing resp. checking the basic SSL functionality:

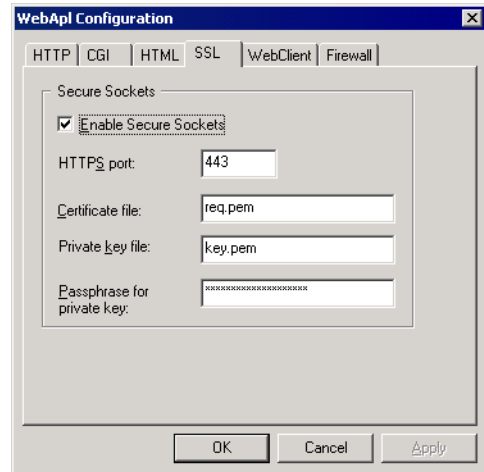
```
openssl req -x509 -newkey rsa:1024 -keyout key.pem  
-out req.pem -config config
```

Two files are generated: the **Private key file:** `key.pem` and the **Certificate file:** `req.pem`. These files must be copied to `<MRS Root>\res\WebAPL\`.

Obtaining an officially signed certificate

A private key and a certificate signing request are needed. The request is usually sent to the CA that signs the certificate with its private key. First some random numbers are generated which are needed for the private key generation at a later time:

```
openssl md5 * > rand.dat
```



Next generate the private key and specify its password. This password should be a longer phrase, e.g. a sentence:

```
openssl genrsa -rand rand.dat -des 1024 > key.pem
```

or, if “triple DES” is to be used:

```
openssl genrsa -rand rand.dat -des3 1024 > key.pem
```

Now the private key `key.pem` has been generated. The password (phrase) should well be kept in mind as without it the private key cannot be used. Additionally a backup copy of the private key should be created and kept best in a safe deposit. The private key is never passed on to anyone else! If it gets lost the certificate signed with it is no longer usable.

Finally a certificate signing request is generated and passed on to the CA. The authority signs the request and sends back a certificate that can be used in combination with the previously generated private key:

```
openssl req -new -key key.pem -out csr.pem -config config
```

Here `key.pem` is the above generated private key and `csr.pem` the desired certificate signing request. During the generation process you are prompted for the following information:

- The country code. It consists of two characters standardized by the ISO (e.g. de for Germany, au for Australia, gb for Great Britain, mx for Mexico, etc.)
- Full name of the respective country.
- Name of the city resp. town
- Name of the organization. This should be the organization owning the domain name.
- Name of the individual department (e.g. marketing, sales, etc.)
- The qualified host name of the individual Internet site (e.g. `www.cycos.com`). This name must correspond to the planned https-URL.

If you are queried for “extra attributes” simply ignore it. The `csr.pem` contents should about look like this:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBETCBvAIBADBXMqswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0
ZTEh
MB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMRAdBgYJKoZIhvcN
AQkB
FgFgMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAL6nPTy3avNgbubx+ESmD4LV
1LQG
fcSh8nehE0IxGwmCPlrhTP87PaA0XvGpvRQjCGStrlQsd8lcYVvk0aytNUC
```

Server Administration

Web Server (WEBAPL)

```
AwEA
AaAAMA0GCSqGSIB3DQEBBAUAA0EAXcMsa8eXgbG2ZhVyFkRVrI4vT8haN39/
QJc9
BrRh2n0TKgfMcT9h+1Xx0wNRQ9/SIGV1y3+3abNiJmJBWnJ8Bg==
-----END CERTIFICATE REQUEST-----
```

Example of a configuration file that makes the OpenSSL program query the above mentioned values. As the case may be, copy it as config file to the SDKTools directory.

```
[ req ]
default_bits             = 1024
default_keyfile           = privkey.pem
distinguished_name       = req_distinguished_name
attributes               = req_attributes
x509_extensions          = v3_ca
dirstring_type           = nobmp

[ req_distinguished_name ]
countryName              = Country Name (2 letter code)
countryName_default      = AU
countryName_min          = 2
countryName_max          = 2

localityName             = Locality Name (eg, city)
organizationalUnitName   = Organizational Unit Name

commonName               = Common Name (eg, YOUR name)
commonName_max           = 64

emailAddress             = Email Address
emailAddress_max         = 40

[ req_attributes ]
challengePassword        = A challenge password
challengePassword_min    = 4
challengePassword_max    = 20

[ v3_ca ]
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer:always
basicConstraints = CA:true
```

6.9.5 Web Client

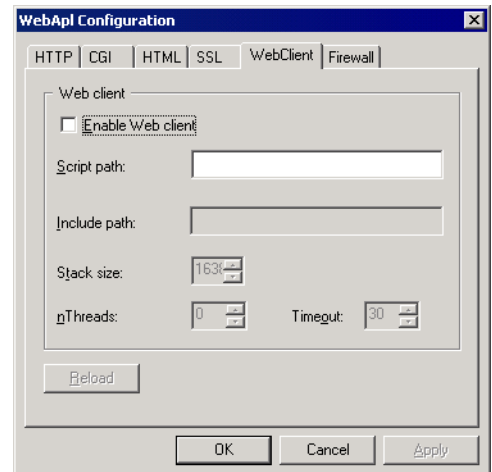
The Web Client fixedly integrated in the Web APL is controlled via transactions from another APL. Do not confuse it with the Web Client implemented as CGI protocol. This is to say that the Web APL acts as Web Client and, for example, controlled by transactions, polls pages from another Web Server and evaluates these with the script specified here to return corresponding information. An example were the regular polling of stock exchange quotations

These transactions are passed on to a dedicated E-Script which executes the

instructions. The E-Script is entered under **Script path:**, and under **Include path:** the path to the E-Header Files used is defined. You should pay attention to the fact that when started the Web APL automatically regards all scripts found in the `... \res\WebAPL\` directory as CGI scripts. In so far the script for the Web Client should not be stored in this directory but e.g. in `... \res\WebAPL\Client\`.

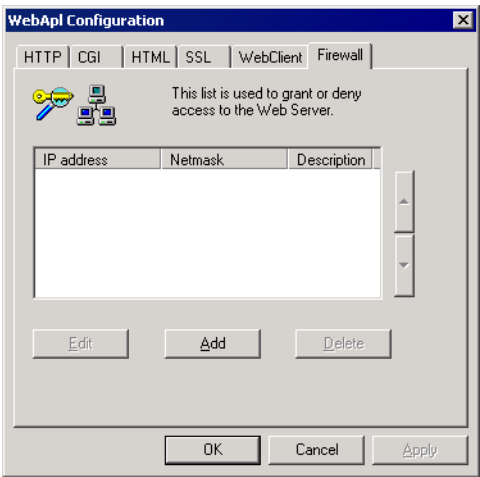
The **Stack size:** refers to the Virtual Machine that executes the E-Object Code. Via **nThreads:** the number of connections simultaneously established by the WebAPL is specified. In **Timeout:** the period is set (in seconds) after which a connection is released when no data are received from the addressed server anymore.

More information on the functions used by the here required E-Script is found in the *E Programming Language* manual.



6.9.6 Firewall

Via this configuration tab additional safety measures can be taken. For certain IP networks access to the Web Server can explicitly be allowed or denied. Handling is the same as with the TCP/IP APL firewall described on page 186.



6.10 Modem (V24APL)

Clients and servers can be coupled to the MRS Server over the V.24 APL. The V.24 APL also enables transmission and reception of fax G3 documents over Class 2 fax modems. Polling of fax documents is also possible from Fax on Demand servers.

Other protocols are available for Short Message Service (SMS), and Message Waiting Indicator signaling for new inbound messages.

As with all other configurations, these are performed with help of the MRS Monitor. In the **Modules** window under **Settings** the **V24APL** configuration dialog is selected with a double click of the mouse pointer.

6.10.1 Identification

In this dialog default settings for fax transmissions can be configured, e.g. **Originator Name:** and **Originator ID:**. These are included in the header of every fax transmission when no entry is present in the user database.

In the dialog entry **Continuation message for interrupted faxes:**, a text message is inserted in the page header informing the recipient that the fax transmission is being continued. In the dialog entry **Default fax recipient:**, the user name is entered who would receive all incoming fax documents. This entry is required since analog modem technology prohibits direct inward dialing/routing to various users.

The button **Restart V.24 APL** is used for executing a restart of the V.24 APL. This option should only be used as a “last resort” when the modem blocks or can only be addressed after manually switching it off and on. Since the modem is not recognized as cleared and re-initialized by the V.24 APL after a hardware reset, a restart of the V.24 APL must be executed.

The screenshot shows the 'V.24 Configuration' dialog box with the 'Identification' tab selected. The dialog has four tabs: 'Identification', 'Protocols', 'Devices', and 'Bindings'. The 'Identification' tab contains a text box for 'System Name' with the value 'DOC', a text box for 'Originator Name' with the value 'Sample Corp.', and a text box for 'Originator ID' with the value '+49 1234 567890'. Below these is a section titled 'System Settings' which includes a text box for 'Continuation message for interrupted faxes' with the value 'Continuation of an interrupted message' and a text box for 'Default fax recipient' with the value 'POSTMASTER'. At the bottom of the dialog is a button labeled 'Restart V.24 APL'. The 'OK', 'Cancel', and 'Apply' buttons are at the very bottom.

Field	Value
System Name	DOC
Originator Name	Sample Corp.
Originator ID	+49 1234 567890
Continuation message for interrupted faxes	Continuation of an interrupted message
Default fax recipient	POSTMASTER

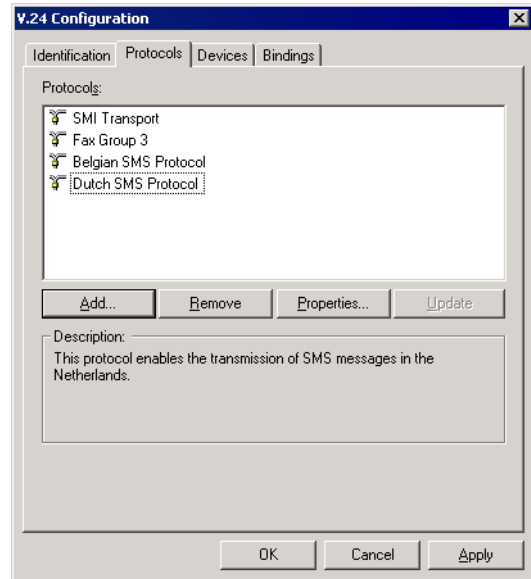
6.10.2 Telematic Protocols

In the configuration tab **Protocols**, all installed protocols are listed that can be used with the various devices. Through use of the button **Add**, new protocols may be inserted into the list. Protocols that are not included in the standard package can be installed from disk. Removal of a selected protocol is done with the button **Remove**. The protocol can be easily re-inserted in the list at a later time.

Some protocols require further configuration in order to function properly. Settings for the installed protocols can be configured through use of the **Properties...** button.

The various international SMS protocols require the access numbers of the various GSM Service providers, over which SMS short messages are transmitted over a modem. The **Originator ID** may also be entered and is displayed to the recipient of an SMS message.

Control sequences for Message Waiting Indicators used in the **Hicom CIT Message Waiting** protocol can be entered in the **Properties** dialog.



6.10.3 Devices

In a manner similar to that of the protocols, devices (modems) connected to a serial port can be added or removed with the **Add...** and **Remove** buttons. Various standard modems as well as a serial-line for connecting computers is included in the standard delivery. If a modem is used which is not included in the standard delivery, an adapted driver-script may be installed from disk.

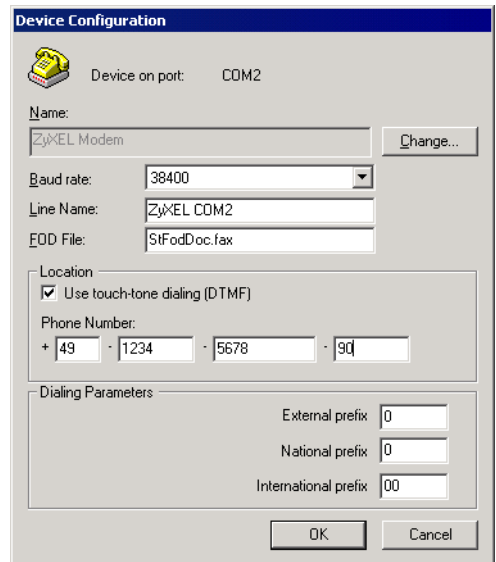
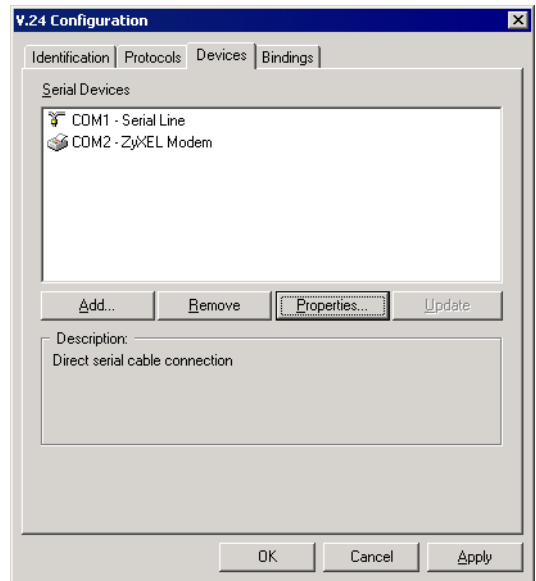
The type of device can be easily recognized by the symbol preceding the device name. The printer symbol indicates a fax-modem, a telephone denotes that the device is a data-modem, and the line with a node indicates a serial line.

Configuration of the various devices is done through use of the **Properties...** button.

The **Change...** button allows the modification of driver-scripts, if e.g. new devices connected are to the serial port. In the dialog entry **Baud rate**: the transmission speed between the computer and the modem is defined. The value entered here should always be higher than actual transmission speed so that any on-line data compression can be executed.

The description entered in the dialog entry **Line Name**:, will be displayed in the MRS Monitor.

Since direct inward dialing is not supported by analog modem lines, only one document per modem may be used as a **FOD File**: for fax on demand applications. This file, as with those of ISDN fax on demand applications, must be stored in the directory `\user-data\sfd\faxfiles\`.

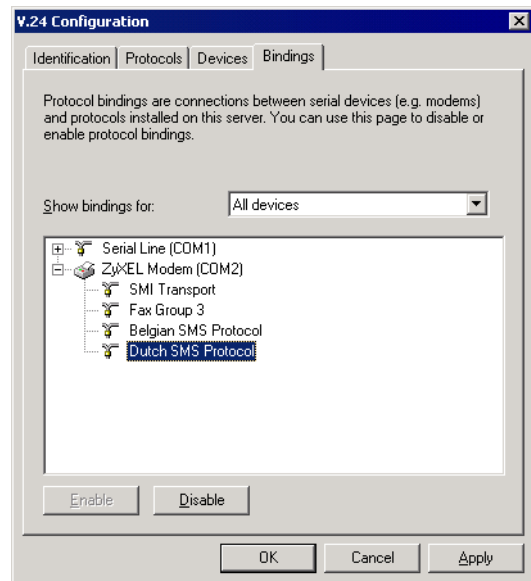


In the **Dialing Parameters** section the **External prefix** do be dialed for external connections, the area code for local calls (**National prefix**) and an international dialing number (**International prefix**) can be entered in the appropriate fields. The last two entries are required for correct dialing within the area code and for international calls. Pulse or tone (DTMF) dialing can be selected with the option **Use touch-tone dialing (DTMF)**. In the **Phone Number:** field the complete dialing number is given in international notation. The first entry is the country code without any proceeding zeros, then the area code (also without proceeding zeros), the telephone number, and the extension number of the modem.

6.10.4 Bindings

In the configuration tab Bindings, protocols are bound to the various serial devices. At first all protocols are bound to each device that is installed and supported. In the event a device should not support a specific protocol, the protocol can be selected and disabled through use of the **Disable** button. In the illustration, the SMI Transport for the *Siemens SMS box for GSM* is easily recognizable as being disabled. In a like manner the protocol can be reactivated through selection of the protocol and subsequent selection of the **Enable** button.

In the field **Show bindings for:** the display is either sorted by devices or protocols in the window.



6.11 GammaFax (GammaAPL)

The Gamma APL provides the integration between the analog Dialogic communication hardware and the MRS Server. Dialogic is one of America's leading manufacturers in the area of computer supported telephony and fax.

The TeleReg-API is used for the configuration of the Gamma APL, and provides a uniform operation and configuration of telematic APLs. Therefore some configuration tabs contain only a few options since the Gamma APL does not require the options otherwise available in these tabs. Operation thus corresponds mostly to the ISDN or Dialogic APL configuration tabs.

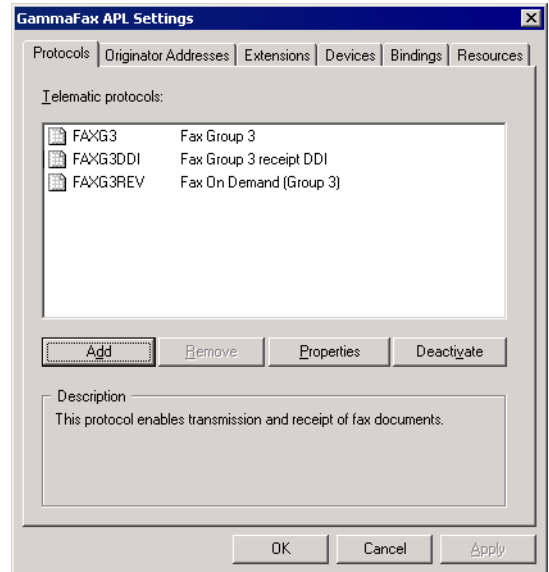
6.11.1 Telematic Protocols

All telematic protocols installed on the MRS Server and supported by the Gamma APL are displayed within this configuration tab.

New protocols can be included in the list through selection of the **Add** button. Protocols no longer required are removed through use of the **Remove** button or disabled through the **Deactivate** button. Once a protocol has been deactivated and later reselected, the **Deactivate** button would toggle to **Activate**. The Gamma APL supports the protocols Fax Group 3 and Fax Group 3 Reverse Polling by fax-on-demand servers. Additionally a variant for Fax G3 with Direct Inward Dialing (DID) is

available. This protocol, however, can only be used for inbound fax documents and also requires a CPD/220 board employing a method common in the U.S. to automatically pass through extension numbers with analog connections.

Selection of the **Properties** buttons enables the user to display and modify configuration parameters of the selected protocol.

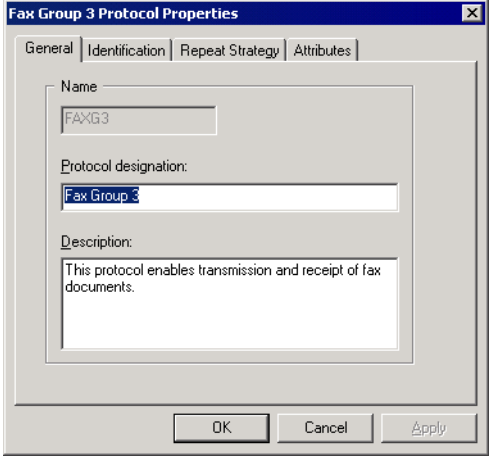


6.11.1.1 Fax Group 3

General

The protocol elements are displayed here. These are the protocol **Name** for addressing the protocol, a descriptive **Protocol designation**: for display in the MRS Monitor and optionally a detailed protocol **Description**:

The protocol name is specified with the installation and cannot be modified any more.

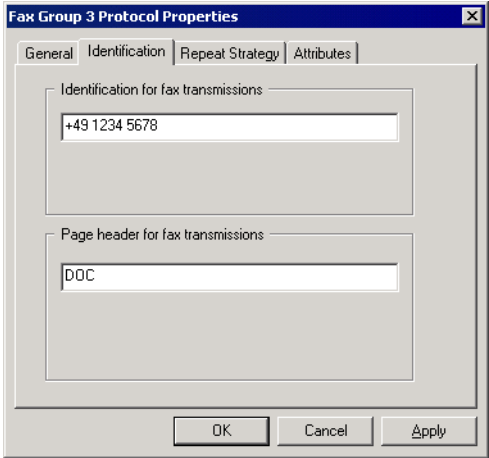


The dialog box 'Fax Group 3 Protocol Properties' has four tabs: General, Identification, Repeat Strategy, and Attributes. The General tab is active. It contains three text input fields: 'Name' with the value 'FAXG3', 'Protocol designation:' with the value 'Fax Group 3', and 'Description:' with the text 'This protocol enables transmission and receipt of fax documents.' At the bottom are three buttons: OK, Cancel, and Apply.

Identification

If a Fax G3 identification or headline is required, other than that given in the global configuration of the MRS Server, these can be entered in the fields **Identification for fax transmissions** and **Page header for fax transmissions**.

Personalized user identifications and page headlines found in the user database will always be used as default.



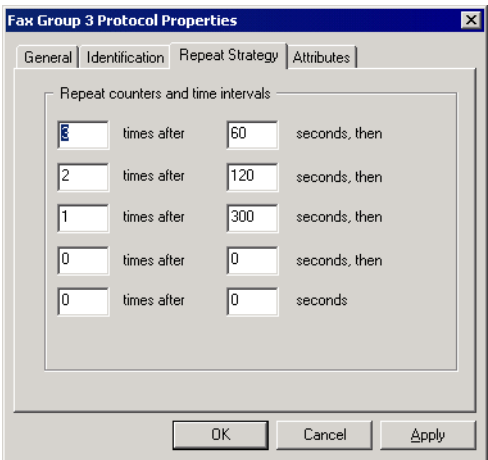
The dialog box 'Fax Group 3 Protocol Properties' has four tabs: General, Identification, Repeat Strategy, and Attributes. The Identification tab is active. It contains two text input fields: 'Identification for fax transmissions' with the value '+49 1234 5678' and 'Page header for fax transmissions' with the value 'DOC'. At the bottom are three buttons: OK, Cancel, and Apply.

Repeat Strategy

Under **Repeat counters and time intervals** the number of redial attempts and the intervals between them are defined. In the column on the left hand side the number of repeats and opposite the associating intervals are entered.

Up to five different counters with varying intervals to be executed in succession can be specified.

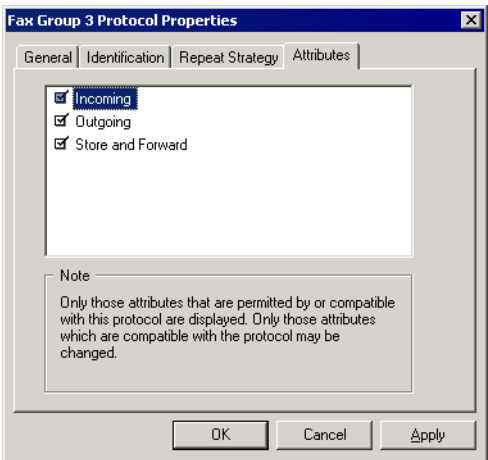
This tab is not available with the “Fax G3 with DID Receipt” protocol since this protocol only serves fax receipt and consequently a repeat strategy for outgoing fax documents is not required there.



Attributes

In this configuration tab, attributes are displayed for the protocol. These attributes can be switched on or off by placing or removing a check in the box preceding the attributes name.

If for example the attribute **Outgoing** was deactivated, incoming fax documents could be received, but no fax documents sent.



6.11.1.2 Fax Group 3 Polling

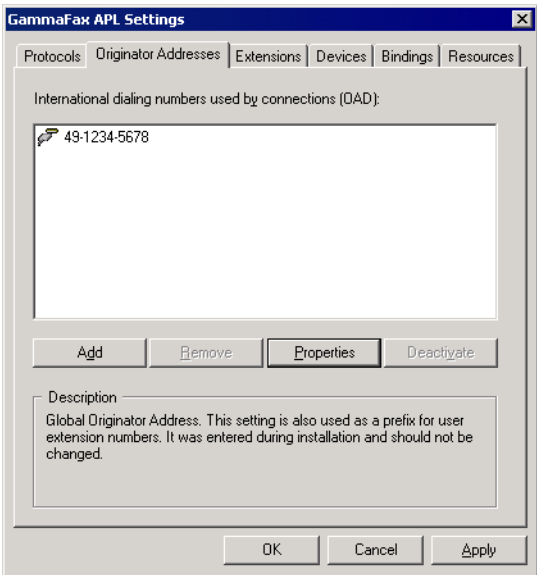
The configuration dialogs for this protocol are comparable to those found in the Fax Group 3 Protocol. The descriptions contain in configuration tabs **General**, **Identification**, and **Repeat Strategy** are similar to those found above.

6.11.2 Originator Addresses

Originator Addresses different to that of the globally configured OAD of the Gamma APL, are displayed in this configuration tab.

Addresses can be **added**, **removed**, **activated** or **deactivated** through use of the appropriate button contained in this dialog.

Configuration of the various dialing parameters is made through selection of the **Properties** button. Optional OAD descriptions may also be entered in the properties dialog. The description is then displayed in this configuration tab when the corresponding OAD is selected with the mouse.

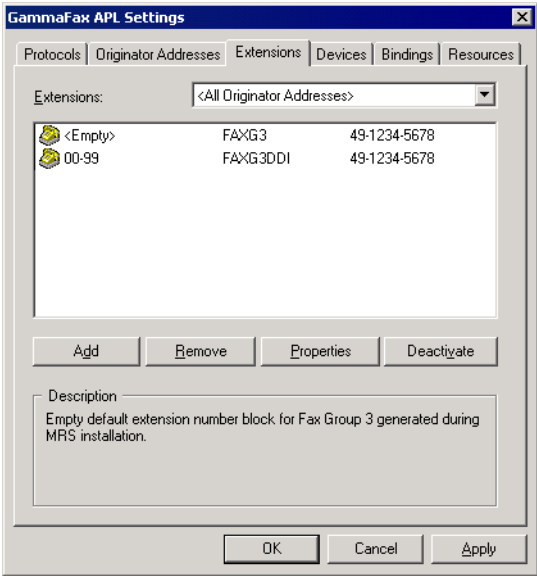


6.11.3 Extension Number Ranges

In this configuration tab, number ranges are assigned to the individual protocols. Incoming calls are bound to the various protocols through the use of these number ranges. New ranges can be **added**, **removed**, **activated** or **deactivated** through selection of the appropriate button. Configuration parameters of the number ranges are retained even when they are deactivated.

Configuration of the various number range parameters is made through selection of the **Properties** button.

In most cases the Gamma APL is assigned an Empty number range, and the extension number of the Postmaster account assigned as Fax G3 number. Only



through the use of the CPD/220 board with DID support can an extension number range be assigned and inbound fax documents routed directly to the recipient.

Number ranges

Beginning and end numbers of the number range are defined in the fields **Start:** and **End:**. If the option **Allow variable length** is enabled, numbers called from outside may be of variable length. The extension number range entered defines the length of an extension number. With a range from 700000 to 999999, the extension number range combinations 7-9, 70-99, ..., and 700000-999999 are possible (up to 6 digits).

The option **Allow superfluous digits** ignores any additional digits that are inputted after the actual number. This could apply for the extraneous numbers 500, 50123, etc. for the user with the extension number 50. Without this option the Gamma APL would be unable to ascertain a user for the inbound routing, or refuse to take the call. The interaction between the options **Allow superfluous digits** and **Allow variable length** is presently unknown!

It should be observed that only the GammaLink fax board CPD/220 supports Direct Inward Dialing (DID). Therefore, all other boards that call over the trunkline must wait for the fax recognition tone and the extension dialed per DTMF. For a professional fax solution this method cannot be implemented, and it is therefore suggested not to specify an extension range and to assign the extension (OAD) allocated for the GammaLink board to an operator account that routes incoming fax documents to the actual recipient.

Extension number ranges may be used with the Gammalink CPD/220 (with DID support) and fax documents routed directly to the recipients workplace.

Bindings

OADs are assigned to the installed **Protocol** in this section of the configuration tab.

Extension Properties

Extension

☒ Range (Start to End)

☐ Discrete MSN

Start: 00

End: 99

☐ Allow variable length

☒ Allow superfluous digits

Bindings

OAD: 49-1234-5678

Protocol: FAXG3DID

☐ Create also for all other suitable Protocols

Description

Empty default extension number block for Fax Group 3 (DID) generated during MRS installation.

OK Cancel

Description

An optional text may be given to the number range in the **Description** portion of the configuration tab. The description is displayed in the Extension Properties configuration tab when you select the number range with the mouse.

6.11.4 Communication Devices

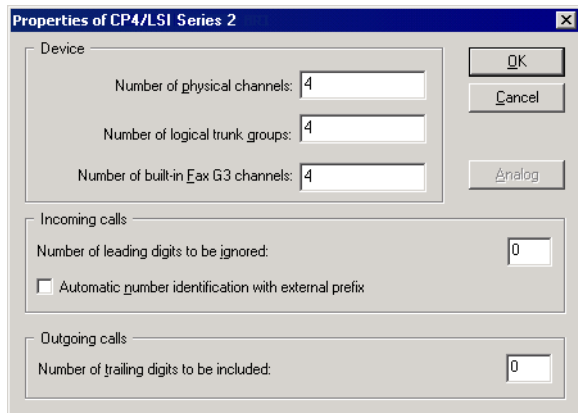
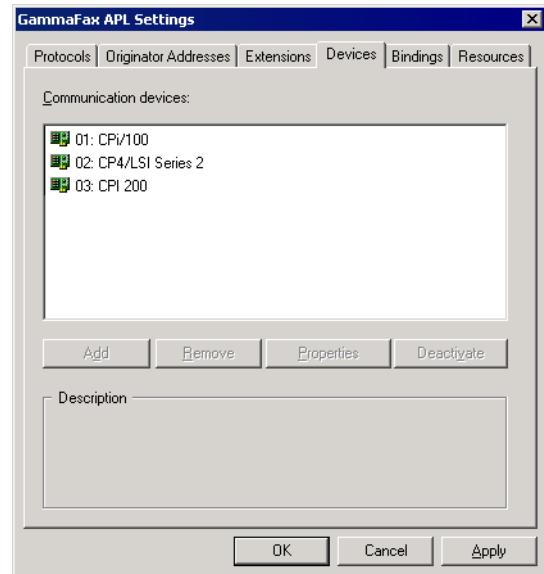
Newly installed hardware boards supported by the Gamma APL can be **added** in this configuration tab. Existing devices can be removed, deactivated, resp. reactivated.

The following GammaLink boards are currently supported:

- CPi/100 (ISA, 1 Fax Channel)
- CPi/200 (ISA, 2 Fax Channels)
- CP4/LSI SERIES II (ISA, 4 Fax Channels)
- CPi/200 PCI (PCI, 2 Fax Channels)
- CPi/400 PCI (PCI, 4 Fax Channels)
- CPD/220 (ISA, 2 Fax Channels, 2 inbound channels with DID support)

Through selection of the **Properties** button, the **Number of physical channels:** and **Number of built-in Fax G3 channels** can be entered.

The number of physically available channels can be divided into **logical trunk groups**, to which various flexible protocols may be bound. The number of logical trunk groups must not be greater than the number of physical channels.



Additionally, a portion of the extension number can be ignored by **Incoming calls**. This option is only useful when the extension number information to be evaluated over an analog line is subsequently forwarded by the communications board. This is available by boards with DID support.

Example:

The number 49-1234-5678-xx is given. The delivered extension information is 5678123, which is interpreted as the complete number 49-1234-5678-5678123. In this case the first four digits (5678) must be ignored

If the option **Automatic number identification with external prefix** is enabled, the originator's number (Automatic Number Identification (ANI)) is prefixed and delivered to the exchange by the device.

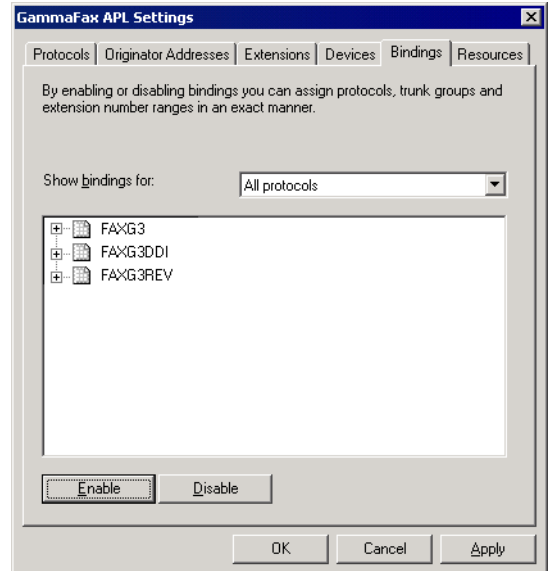
With **Outgoing calls** it is possible to insert digits to a dialing number. If for example a PBX system has two cross connections 82 and 83, then a call from 8247 to 8311 is simply transferred internally and not through the public exchange. Numerous PBX systems do not have this function, and in such a case the call must be routed through the public exchange, and therefore these prefixed digits. In a case such as this, the number of prefixed digits must be entered here.

6.11.5 Bindings

Bindings can be displayed and sorted according to protocols, extension ranges, lines, and originator addresses. Display and sorting criteria is selected from the pull-down list **Show bindings for:**.

The buttons **Enable** and **Disable** can be appropriately used for the selected element.

The display in this window provides a good overview of the interaction between the various resources.



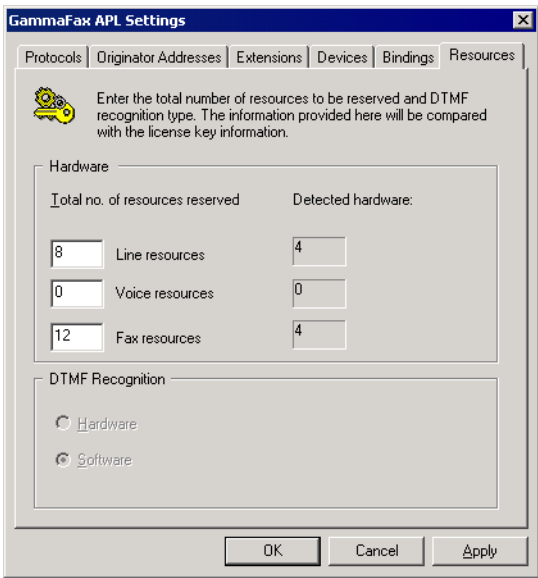
6.11.6 Resources

Hardware

The number of lines, voice (always 0 with the Gamma APL), and fax resources to be used are configured in this tab. In the right-hand portion of the dialog the number of resources detected by the hardware recognition are displayed. Licensed resources are entered in the entry fields on the left-hand side of the dialog. The number of resources entered here may not exceed the number contained in the license key.

DTMF Recognition

DTMF recognition is always per hardware by the Gamma APL. Since the board filters DTMF tones, a software recognition is not possible.



6.11.7 Configuration Examples

6.11.7.1 Channel Reservation for In or Outbound Fax Traffic

Firstly, the configuration which defines how many physical lines/channels are represented by a logical MRS line must be modified. Without this modification a Gamma-Link CP4/LSI board with four channels would be represented as one logical MRS line. Using the menu item **Device→Properties**, the four physical channels can be assigned as four logical MRS lines. For this example two logical lines will be used.

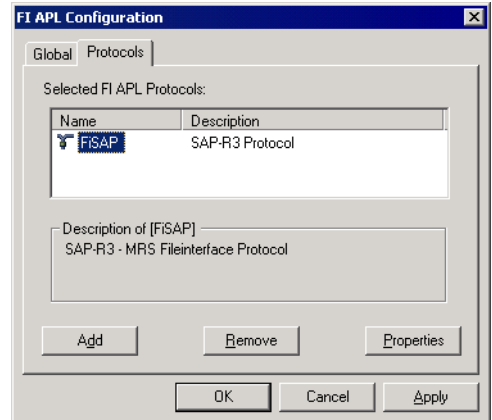
In the MTA configuration tab **Logical Lines**, one of the newly created logical lines for the GammaAPL can now be selected, and option **Line enabled for outbound transmission** deactivated in the **Properties** dialog. This line will now be used only for inbound fax traffic.

The second line must now be configured for outbound traffic only. This is done by deactivating the **Incoming** attribute assigned in the FaxG3 protocol. So that the deactivation of this attribute does not affect the first logical line in this example, a second instance of the protocol must be inserted, renamed, and subsequently bound to the logical line. This protocol must also be handled parallel to that of the FaxG3 protocol in the Routing Rules.

6.12 Gateways over General File Interface (FIAPL)

The File Interface enables MRS transmission and receipt processes over a file interface. For this purpose several special files are installed which contain necessary information over the file structure. Conversely, incoming documents are parsed using an E-Script and a transmission job created for the MRS Server.

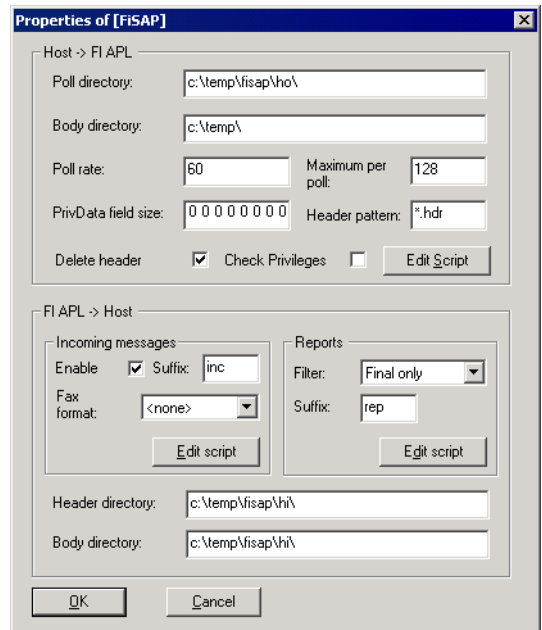
Appropriate definitions exist for gateways to SAP R/3 (see page 80), HP GroupWise (see page 82), HP Open Mail and a connection for the HP Digital Sender (see page 96). File Interface protocols installed on the computer can be added through use of the **Add** button, removed with the **Remove** button, and configured using the **Properties** button in the FIAPL configuration dialog. The number of protocols is restricted to 32.



Host to File Interface APL

In the properties dialog the field **Poll directory:** contains path information for the directory where the host system stores header files which contain the necessary data for transmissions. The field **Body directory:** contains the path information to where the corresponding bodies of the header files are stored.

The interval at which the File Interface APL queries for new incoming documents is given in seconds in the field **Poll rate:**. The **Header Pattern** field defines which header file type is to be searched for in the Poll-Directory. When the **Delete header** option is activated, header files that have been pro-



Server Administration

Gateways over General File Interface (FIAPL)

cessed are removed from the directory. This option should be disabled for debugging purposes only.

By means of **Maximum per poll**: you can define the maximum number of jobs to be read in and processed all at once. This temporarily distributes the load with a very large job.

The field **PrivData field size**: defines the size of individual data fields set by the various scripts, and which are made available at a later time for reporting purposes.

Activation of **Check Privileges** does just that with respect to originator privileges, e.g. whether he or she is authorized to send fax documents.

File Interface APL to Host

In the reverse direction (**FiAPL -> Host**), a **Header directory**: is installed as well as a **body directory**:. A **Suffix** is appended to all header files for incoming messages and reports to the host system. These files are read by the host system and then accordingly processed.

If fax documents are to be transmitted to the host system the file format must be defined in the field **FaxFmt**.

Both the **PrivData field size** entry and the **Edit script** button are used for adaptation of incoming messages and reports, are deactivated when these fields are exported in the E-Script (* .or l), or are assigned a corresponding function.

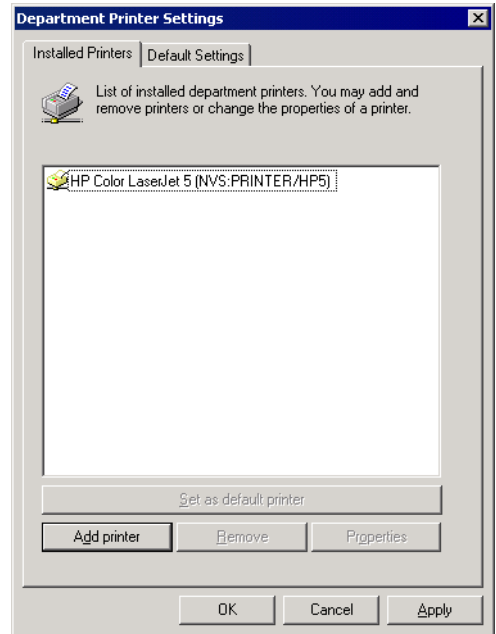
6.13 Department Printer Settings (PrintAPL)

Through use of the Print APL, copies of in and outbound documents can be automatically sent to a printer. As with all other APL's, the Print APL configuration is performed in the MRS Monitor. Under **Settings** the **Print APL** is selected and subsequently **Set Options** with a double click of the mouse pointer.

In the configuration tab **Installed Printers**, all currently installed printers are displayed. New printers are installed through use of the **Add printer** button. Obsolete printers can be removed from the list through use of the **Remove** button.

Default values for all printers are set in the configuration tab **Default Settings**. The default values for individual printers can be modified in the **Properties** dialog of the individual printer.

Any one of the installed printers can be declared as the default printer. This printer would then be the default printer used in conjunction with the *Carbon Copy Rules* (e.g. all incoming fax documents are automatically sent to a printer). The yellow printer symbol denotes the current default printer.



Server Administration

Department Printer Settings (PrintAPL)

Number of Copies

The default number of copies to be printed is entered in this field.

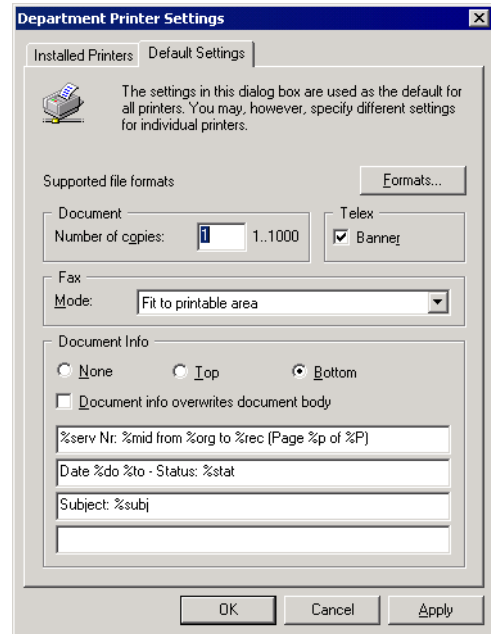
Telex Banner

When activated, a telex banner with the word “Telex” is printed in the right and left-hand margins of the document. The printed document would then have the appearance of a “real” telex message.

Fax Mode

The following conversion options are available for the fax mode:

- **Fit to printable area.** Incoming fax documents are scaled to fit to the printable area of the printer. If a fax document is received whose length exceeds that of the printable area, it will be proportionally reduced so that both the x and y axis fit within the printable area. This setting is generally appropriate for all applications. The one exception is that of continuous form fax documents. If this option is selected, and a continuous form is received (several pages in length), the document would be proportionally reduced and appear as a small stripe when printed.
- **Fit to printer resolution.** Pixel resolution of fax documents are proportionally reduced (or increased) to that of the printer. If a 200 dpi fax is sent to a 600 dpi printer it would be reduced in size by about two-thirds.
- **Fit to width and height.** This option is basically the same as Fit to printable area with the exception that documents exceeding the length of the printable area by 15% are continued on a separate page.
- **Optimize printable area width.** Fax documents whose length does not exceed 5% of the printable area are reduced to fit within the printable area. Fax documents that exceed 5% of the printable area are continued on a second page.
- **Optimize printable area.** Fax documents whose length does not exceed 1% of the printable area are reduced to fit within the printable area. Fax documents that exceed 1% of the printable area are continued on a second page. In some cases, printing outside the printable area may occur, and therefore a loss of document information.



Document Info

In the lower portion of the dialog positions can be defined where document information is to appear. This can either be printed at the **Top**, **Bottom**, or not at all (**None**). If a portion (upper or lower) of the incoming fax document is normally free of text, this area could be used for printing the document information. When the **Document info overwrites document body** option is enabled, document information will be inserted at the selected location and run into the body of the document when necessary.

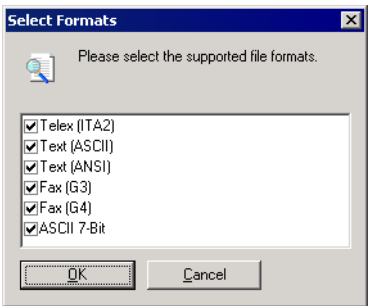
The information that is to be printed can be entered in the four entry fields. The following variables can be used for displaying the document information.

Variable	Significance
%comm	Commentary line.
%cost	Charge costs.
%costid	Cost center.
%do	Date of receipt on server.
%dr	Date of report. The report is generated at the end of the document transmission.
%frm	Format, e.g. Telex, ASCII, fax G3, etc.
%fullname	The complete user name or, if it is unknown, something like 'Unknown User' (language dependent).
%len	Document length in bytes.
%mid	The message ID.
%oid	Originator ID e.g with a fax.
%oorg	Original originator for documents that are rerouted.
%orec	Original recipient for documents that are rerouted.
%org	Message originator.
%p	Actual page number.
%P	Total number of pages in document.
%rec	Message recipient.

Variable	Significance
%rid	Recipient ID e.g with a fax.
%serv	Transport service used.
%stat	Detailed message status.
%subj	Message subject.
%succ	Success or failure of the transmission: Undefined, Unknown, OK, ERROR, REJECT, REPEAT or DELAYED.
%to	Time of receipt on server.
%units	Number of units.
%worg	An attempt is made to find the originator in the user data base. If the originator is found, then the name will be used instead of the fax ID.
%wrec	An attempt is made to find the recipient in the user data base. If the recipient is found, then the name will be used instead of the fax ID.

Supported File Formats

These are the file formats accepted by the Print APL. If the MTA passes on a file for printing, it is converted into one of the printable formats listed here.



Printer Properties

In most cases each printer uses the default settings described above. If this behaviour is not desired, deactivate the **Use default settings** option before performing the desired settings in the bottom portion of the dialog.

The **Printer:** field is provided for entering a line name for the MRS Monitor. In the **Name:** field, the printer name is entered which is found within MRS addressing. This name must also be entered in a user database under **Printer** if this is to be the target device in the *Carbon Copy Rules*.

If documents are to be automatically sent to a departmental printer, then a set of *Carbon Copy Rules* must be defined. The **Routing Rules** configuration tab is found in the **MTA configuration** dialog.

The 'Printer Properties' dialog box contains the following fields and options:

- Printer:** HP Color LaserJet 5
- Address:** NVS:PRINTER
- Name:** HP5
- ☐ Use default settings (with a 'Formats...' button)
- Document** section:
 - Number of copies:** 1 (range 1..1000)
 - Telex** section: ☒ Banner
- Fax** section: **Mode:** Fit to printable area (dropdown menu)
- Document Info** section:
 - Radio buttons: ☐ None, ☐ Top, ☒ Bottom
 - ☐ Document info overwrites document body
 - Fields: %serv Nr: %mid from %org to %rec (Page %p of %P), Date %do %to - Status: %stat, Subject: %subj

Buttons: OK, Cancel

6.14 Hicom Applications Connectivity Link Settings

The Hicom¹⁴ APL enables use of the Applications Connectivity Link (ACL) features of the Siemens Hicom 300 series. These features include switching, call connection, display control, and call forwarding management. Physical coupling is through a **Serial connection via Protum box** or a **LAN connection to WAML module** and TCP/IP protocol, with no appreciable difference in performance between the two connection types. In the lower portion of the dialog the serial port of the server is selected in the option **Use serial port:**, or the **TCP/IP Address of**

The 'Hicom ACL Settings' dialog box has three tabs: 'Hicom Connection' (selected), 'CIT Settings', and 'Phone Monitor'. It contains the following fields and options:

- Text: These settings define how the Hicom system is connected to the server.
- Type** section:
 - Radio buttons: ☐ Serial connection via Protum box, ☒ LAN connection to WAML module
- Use serial port:** COM1 (dropdown menu)
- TCP/IP address of WAML:** fabiola.ppcorn.de

Buttons: OK, Cancel, Apply

14. From MRS 5.1 these functions are possible via the CTI APL as well so that the Hicom APL is only available with already existing installations. Consequently the installation does not offer this APL for direct selection any more but updates only systems that already exist.

Server Administration

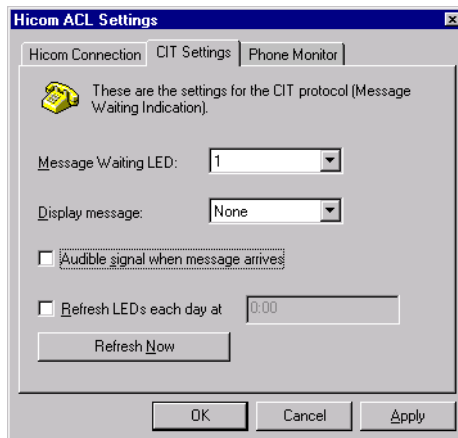
Hicom Applications Connectivity Link Settings

WAML: is entered in the field provided for this purpose. With several connected Hicom 300 systems please consult the *MRS System Architecture*.

The following services are provided by the Hicom APL:

- CIT signalization to LED and/or to the display of digital end devices (Siemens Optiset)
- Terminal device monitoring
- Use of all available performance features and service components through dialog/transaction interface.

The Hicom APL only supports the Hicom 300 series. Support for the Hicom 150 is currently not available.



The Hicom APL logs in the logical line NVS:CIT_HICOM for MWI.

For users that want to have the LED lamp to be configured for MWI at their telephone terminal device, illuminated when new messages come in, CIT_HICOM/<Number> must be entered in the CIT database field. <Number> corresponds to the extension number of the terminal telephone device.

The **Message Waiting LED:** is used for the signalization of new messages to the users telephone. This number should be between 1 and 12. LED's are vertically

arranged and numbered from top to bottom. Only LED's that are not assigned a function from the Hicom PBX may be used for message waiting indicators.

The duration options **None**, **Permanently**, and **Temporary** are available in the pull down list for **Display message:**. Messages are either not displayed (None), displayed until the new message has been read (Permanently), or disappears after approximately 5 seconds (Temporary). Acoustic signalization of new messages can also be implemented through use of the option **Audible signal when message arrives**.

The option **Refresh LEDs each day at ...** resets the telephone LEDs daily to their correct display status. Unfortunately, the Hicom does not register the state of LEDs either by a restart of a assembly unit (or the complete PBX), or by the resetting of a terminal device (pulling the plug out). Since the Hicom does not register when LEDs are again switched on, this information can be refreshed on a daily basis at a specified time. Selecting the **Refresh Now** bottom, executes this action immediately.

In the opposite configuration tab extension number ranges or extension numbers of terminal devices can be entered. selected for **Monitoring** in this dialog. The activity of the devices specified here are kept under surveillance per CTI monitoring.



6.15 Computer Telephony Integration (CTIAPL)

The CTI APL is the centralized CTI transaction provider in the MRS Server. It uses the protocol interfaces from various telephone exchanges and makes their functionality available to all MRS CTI Client applications.

Supported protocol interfaces are:

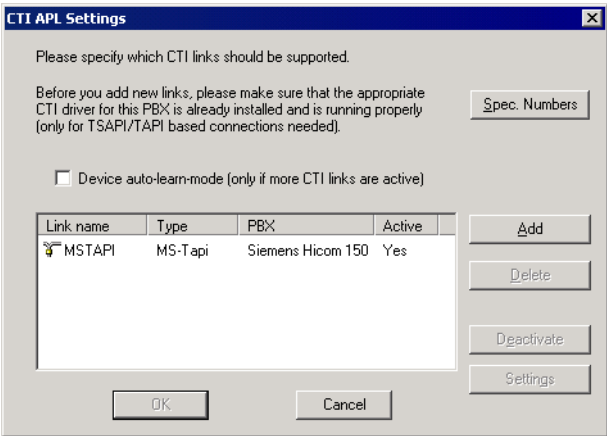
- Computer Supported Telecommunications Applications (CSTA).
Standard-CTI-Interfaces from the European Computer Manufacturers' Association (ECMA). These interfaces are normally provided by the PBX.
- Telephony Services API (TSAPI) from AT&T and Novell. This is principally a software interface based on CSTA.
- Telephony API (TAPI) from Microsoft.

A list of supported/tested PBX's can be found in the hardware compatibility list which is part of the release notes.

6.15.1 Configuration

Configuration on the MRS Server side is done as usual from the MRS Monitor. In the components window simply doubleclick the **Set Options** entry under **CtiApl/Settings**.

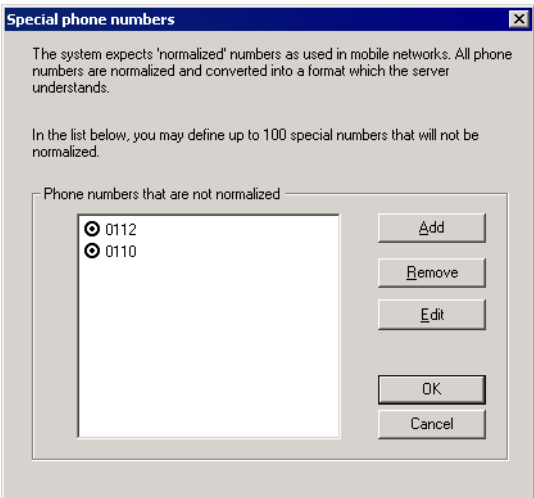
Existing links to PBX's are displayed in the CTI APL Settings dialog. Other links can be inserted through selection of the **Add** button, and existing links removed with the **Deleted** button. The entry "Unknown" may be used for testing purposes of PBX links not previously supported. Our experience has shown that individual adaptations must be made for all PBX's.



Existing links can be activated resp. deactivated through selection of the **Activate/Deactivate** button. This button changes automatically in accordance with the current state of the link.

The **Device auto-learn-mode** option enables the CTI APL to note from which system a specific calling number has been reported when several CTI links to different systems are active. In this way the CTI APL becomes familiar with the entire company network and is eventually able to send corresponding CTI transactions to the correct system.

The **Spec. Numbers** button is used to switch off the MRS Server calling number normalization for certain calling numbers. Up to a certain length the numbers transferred to the MRS Server are considered internal numbers, those exceeding this length are regarded as external numbers. All external numbers receive a canonical format with international code through calling number normalization, thus e.g. 492404123456 with the area code (2404) for Alsdorf and the extension 123456 in Germany (49). If required, external prefixes etc. are added by the MRS Server when the number is dialed. Examples of numbers not to be normalized are emergency call numbers for fire brigade and police



which of course are not handled as local numbers in the sense that they would be preceded by the area code of the MRS Server location. Up to 100 special calling numbers can be entered in this list.

Via **Settings** you are taken to the parameters of the selected links. The configuration options are differentiated on grounds of the link type.

6.15.1.1 Link via TAPI

Unique names are assigned to the PBX link in the **Logical link name:** field. This name is used internally by the server as the class portion of the line name for transaction exchanges with the PBX. In the example displayed here the name of the logical line for this link would be `NVS:CTI.MSTAPI`. Through activation of the **Active** option in the **Message Waiting Ind.** section you can log in another logical line of the CTI APL at the MTA via which users can be noti-

fied about new incoming messages. In case of the Hicom 150 Office from Siemens displayed in this example, one of the LEDs on the telephone terminal device must be configured as “letter box lamp” for the respective user. In the user database field **Message Waiting Indication (CIT)** of the respective user, `MWI/<Number>` needs to be entered. If several PBXs are used at a company with several links to these systems, the class is considered so that the entry for this link is `MWI .MSTAPI/<Number>`.

The **Expert parameters** are described in section 6.15.1.4. page 260.

Monitoring is described in section 6.14.1.5. page 262.

MS-TAPI Properties

Logical link name:

PBX System

Manufacturer	Model
Siemens	HICOM 150 Office...

Message Waiting Ind.

Address: ☒ Active

Configuration

☒ Use all lines

6.15.1.2 Link via TSAPI

The **PBX System:** field contains the name of the PBX connected via this link.

In **Logical link name:** a unique name is assigned to this PBX. The server uses this name internally as the class portion of the line name to exchange transactions with the PBX. In the example displayed here the name of the logical line for this link would be NVS:CTI.TSAPI.

The screenshot shows the 'TSAPI/CTSA Link Properties' dialog box. It contains the following fields and buttons:

- Logical link name:** A text box containing 'TSAPI'.
- PBX System:** A text box containing 'Alcatel 4400'.
- PBX Access** section containing:
 - Login ID:** A text box containing 'MRS'.
 - PBX name:** A text box containing 'ALCATEL#ipbx#CSTA#localhost'.
 - Password:** A text box with masked characters.
 - Confirm password:** A text box with masked characters.
- Buttons:** 'OK', 'Cancel', and '>> Advanced'.

With TSAPI a **Login ID:** is required for access to the PBX by the CTI APL. If this account also requires a **Password**, it must be entered twice for purposes of confirmation. The field **PBX name:** contains a defined name through which the software interface communicates with the PBX. Depending on the PBX type, adaptations to the preset values must be made. The Octopus E-300/800 requires as last portion of this name e.g. the Windows NT name of the MRS Server computer on which the CTI APL runs.

The **Advanced** button enables the configuration of further parameters. These are in particular the maximum values for **Connections:**, **Monitor points:**, **Transactions:** and **Range of numbers:**.

Transactions

In the TSAPI Stack, simultaneous transactions are restricted in a list. Thus this list is static. This parameter specifies the number of transactions that can be simultaneously processed within the TSAPI Stack. The corresponding value affects for example the maximum number of possible monitor points of all simultaneously active TrayPhone applications. For example, if 30 users had activated TrayPhone and added 10 extensions each to their TrayPhone event bar, the simultaneous TrayPhone and computer start would result in 300 transactions in one go. Since in this case the default of 256 were exceeded, only the first 25 users would see all extension statuses in TrayPhone, the 26th user would receive only 6 statuses (the rest of the ex-

The screenshot shows the 'TSAPI/CTSA Advanced Settings' dialog box. It contains the following fields and buttons:

- Maximum Values** section containing:
 - Connections:** A text box containing '256'.
 - Monitor points:** A text box containing '256'.
 - Transactions:** A text box containing '256'.
 - Range of numbers:** A text box containing '100'.
 - Monitor lines:** A text box containing '64'.
 - Open delay:** A text box containing '10' with 'ms' next to it.
- Buttons:** 'OK', 'Cancel', and 'Default'.
- CSTA DLL** section containing:
 - A text box containing 'csta32.dll'.
 - A 'Browse' button.
- Static monitor points** section containing:
 - ☐ Import from user data (field: 'Business phone')
 - ☒ No static monitor points
- Buttons:** 'Expert parameters' and 'Monitoring'.

tensions feature a red exclamation mark to signify that the limit of 256 has been reached), and the remaining users would receive nothing but red exclamation marks.

Range of numbers

Number ranges specify the maximum number of extensions for a static monitor point range. This value must always be smaller or equal to the maximum number of monitor points.

Open delay

With the CTI APL start all monitor points would be set in quick succession which may overstrain the system. You can set a delay here to avoid this behaviour.

The name of the interface library provided by the PBX manufacturer is given in the field **CSTA DLL**. This name is already default set for the selected PBX with the configuration.

In the **Static monitor points** portion the behaviour of the CTI APL is determined when these points are set. In some cases line monitoring is only possible when a monitor point has already been set during the establishment of the connection to the PBX. Here you can decide whether static monitor points

- are to be retrieved from user accounts, thus be set for all users with a number entered in the “Business phone” database field.
- are not to be set at all. This is reasonable e.g. when the PBX can dynamically add numbers.

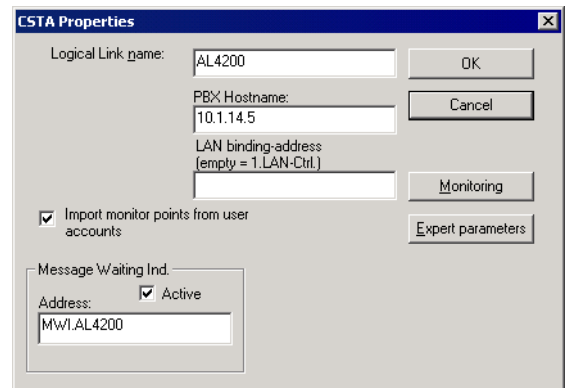
The **Expert parameters** are described in section 6.15.1.4. page 260.

Monitoring is described in section 6.14.1.5. page 262.

6.15.1.3 Link via CSTA

A unique name is assigned to the PBX link in the **Logical Link name:** field. This name is used internally by the server as the class portion of the line name for transaction exchanges with the PBX. In the example displayed here the logical line name for this link would be NVS:CTI.ALCATEL4200.

PBX Hostname: contains the IP address of the PBX via which



In the **LAN binding -address** field you can define via which LAN board the PBX is to be connected. This is only required when more than one LAN board is implemented in the server.

Through activation of the **Active** option in the **Message Waiting Ind.** you can log in another logical line of the CTI APL at the MTA via which users can be notified about new incoming messages by means of a telephone LED. In the user database field **Message Waiting Indication** (CIT) of the respective user, **MWI/<Number>** needs to be entered. If several PBXs are used at a company with several links to these systems, the class is considered so that the entry for this link is **MWI . ALCATEL4200/<Number>**

The **Expert parameters** are described in section 6.15.1.4. page 260.

Monitoring is described in section 6.14.1.5. page 262.

The expert parameters are particularly needed when several PBXs are available, be it with various extension numbers or with the corresponding extension number ranges.

However, an environment with several

260

PBXs and their respective CTI links does not work unconditionally.

As default the **global 'location info'** is used. Through deactivation of this option you can specify an individual extension number for this PBX. For this purpose the fields **Country**, **Area Code**, **Number** and **Tie line number** have been provided. The last one is required for e.g. a networked subsystem. Furthermore an extension number range can be defined in the **Start:** and **End:** fields. This is required exactly and exclusively when there is an additional CTI link to another PBX with the same extension number and a different extension number range. Via the **Always dial area code** option also numbers dialed within the individual area are always prefixed by the corresponding area code. This is required in some countries.

In the **Dialing Parameters** section you can enter the **External Prefix:** as well as the **Country Code:** and the **International Prefix:** to be dialed for this PBX.

In an environment with several CTI links it is ideal when all CTI requests are transferred to the CTI APL in normalized form since otherwise they cannot be assigned to a PBX. In many cases however there is a major system delivering the local resp. internal numbers. The CTI link to this system can be defined as **Link Master** so that all localized CTI requests can be handled via this CTI link.

Most PBXs transmit correct numbers to the CTI APL, thus e.g. 012345678 with 1234 being the area code and 0 the national prefix. Some systems also deliver the dial number prefix, thus in our example 0012345678. To remove the additional 0 you can enter it in the **Additional prefix to be ignored** fields.

If the system delivered the numbers entirely without the preceding 0, thus e.g. 12345678, the corresponding calling number type had to be transmitted by the system as well. Otherwise a correct normalization could not be performed. For example a mobile phone number such as 171-654321 would be handled as international number from the USA if the system did not transmit the calling number type. With a correct calling number type the national prefix would simply be added and the number handled correctly.

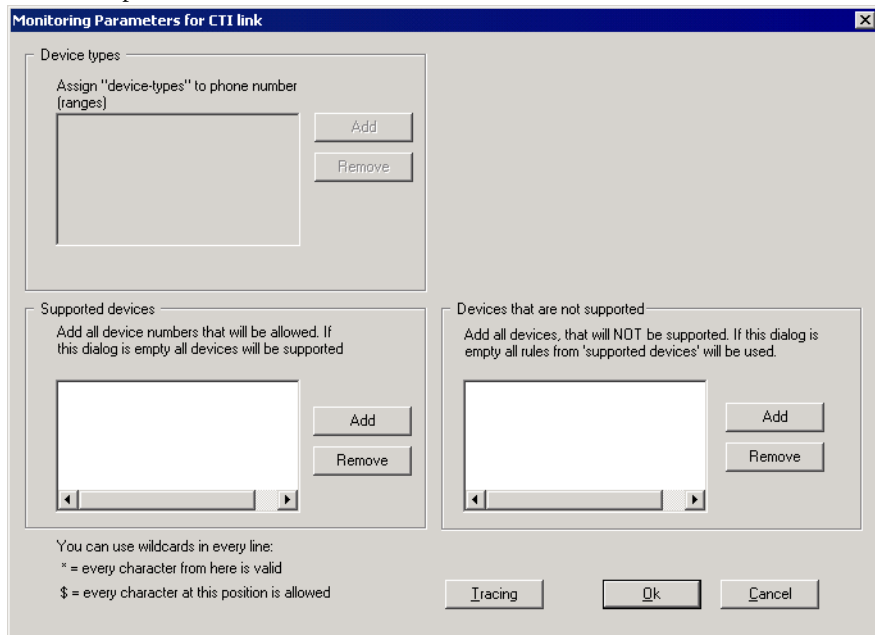
The last field **Minimum length of international numbers** serves the correct assignment of incoming numbers as well. If e.g. local numbers from the individual area are transmitted with external line prefix (example: 054321), this could also be interpreted as a national number with the corresponding area code. As distinctive feature you can enter the minimum length from which such a number is no longer considered a local number from the individual area.

In the **Maximum length for internal numbers** field you can enter the longest internal number. All numbers exceeding the length specified here are considered international calling numbers and normalized accordingly.

Normalize internal numbers is default set. If some CTI client applications are unable to handle normalized calling numbers you can deactivate this switch.

6.15.1.5 Monitoring.

In the Monitoring Parameters for CTI link dialog you can precisely define which terminal devices can and are to be monitored at all. For this purpose enter the corresponding numbers of the terminal telephone devices in the sections **Supported devices** and/or **Devices that are not supported**. The numbers entered may include wildcards so that also number portions can be added.



The dialog box is titled "Monitoring Parameters for CTI link". It contains three main sections:

- Device types:** A section with the instruction "Assign 'device-types' to phone number (ranges)". It features a large empty list box and two buttons, "Add" and "Remove", to its right.
- Supported devices:** A section with the instruction "Add all device numbers that will be allowed. If this dialog is empty all devices will be supported". It features a large empty list box and two buttons, "Add" and "Remove", to its right.
- Devices that are not supported:** A section with the instruction "Add all devices, that will NOT be supported. If this dialog is empty all rules from 'supported devices' will be used." It features a large empty list box and two buttons, "Add" and "Remove", to its right.

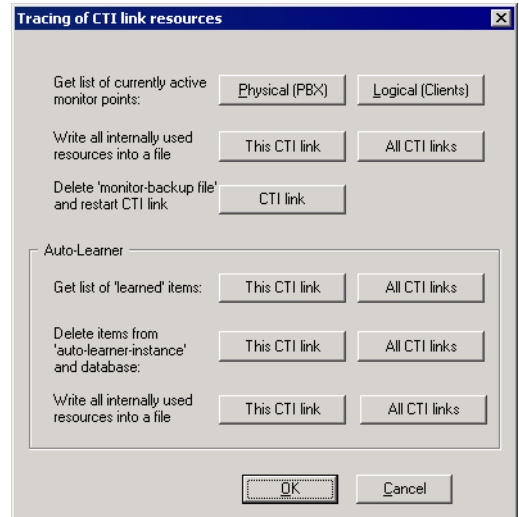
At the bottom of the dialog, there is a note: "You can use wildcards in every line:
* = every character from here is valid
\$ = every character at this position is allowed". To the right of this note are three buttons: "Tracing", "Ok", and "Cancel".

Tracing

The **Tracing** button is used to check, save and delete the resources administered by the CTI APL.

Via **Get list of currently active monitor points** you can query the monitor points actually set in the PBX. You can also check which client applications monitor which terminal devices.

Write all internally used resources into a file enables you to save all resources for more detailed analysis for this or all CTI channels.

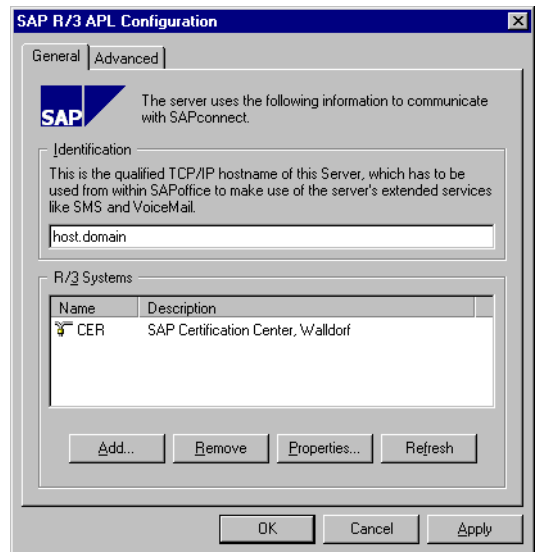


6.16 SAP R/3 Gateway (SAPR3APL)

The configuration in respect to the MRS Server, is as with all other components, accomplished through use of the MRS Monitor. In the Modules window of the MRS Monitor the option **Settings** is selected and subsequently **SapR3ApI/Set Options**.

General Settings

The TCP/IP hostname of the MRS Server is entered in the field **Identification**. SAPoffice user messages are to this TCP/IP address through the Internet Mail service. All services on the MRS Server can be addressed over this address (see page 80). These addresses represent a subset of the address range configured by SAP R/3 for the address type INT (Internet-Mail). These addresses are required for the routing of messages from the SAP R/3 System to the SAP R/3 APL.



Gateways configured to SAP R/3 are displayed with their short name and a description under **R/3 Systems**.

New gateways are inserted through use of the **Add** button. Configuration of the gateway can be done through use of the **Properties** button which will be explained further in this section. Selecting a gateway and subsequently pressing the **Remove** button deletes the gateway from the R/3 Systems list.

System

The SAP R/3 Server is addressed from the MRS Server through an address which is formed from the **Short Name** entered here. In this example the short name is CER so the address

NVS: SAPR3CER/*

would be used for addressing this system. The *Routing Rules* must be manually modified from those addresses formed by the short name, so that document delivery from the MRS Server corresponds to that of the SAP R/3 Server.

The **Description** is used to identify the line in the MRS Monitor.

If the option **Automatically establish the connection to this system by default** is activated, the connection to this system would be established at the system start. The gateway will also be activated.

Should the switch **Activate privilege check for documents that are to be sent** be activated, the document originator must be present in the MRS database and have the corresponding send privilege. One method to copy the originators from the SAP system to the MRS database would be e.g. the option **Activate "autolearn" mode and copy the senders' attributes to the database**. By means of this option the originators are automatically copied from the SAP system to the MRS database and depending on the sent document the fax number and fax ID, the SMTP address or the SMS number is entered. Since no correlation can be recognized between these three document types coming from the SAP system, up to three "Autolearn" user entries would be created in the MRS database.

The screenshot shows the 'SAP R/3 APL System Properties' dialog box. It has three tabs: 'System', 'Server', and 'Client'. The 'System' tab is active. Inside the dialog, there's a section titled 'System Properties' with instructions: 'Enter a short, descriptive name for the R/3 system. This name is used to address an R/3 system. Example: For your sales department's R/3 system you could enter the name 'sales' (w/o quotes).' Below this is a text field for 'Short Name' containing 'CER'. Another instruction follows: 'Enter a description for the R/3 system. Example: For your sales department's R/3 system you could enter the description 'Sales Department' (w/o quotes).' Below this is a text field for 'Description' containing 'SAP Certification Center, Walldorf'. At the bottom, there are three checkboxes: 'Automatically establish the connection to this system by default' (checked), 'Activate privilege check for documents that are to be sent' (unchecked), and 'Activate "autolearn" mode and copy the senders attributes to the database.' (unchecked). At the very bottom are three buttons: 'OK', 'Cancel', and 'Apply'.

The “Autolearn” mode must be activated if canonical addresses (standard presetting under R/3) of the type DE (2404) 123 - 456 are used because replies/documents must be delivered to the SAP user in exactly the same manner. For this purpose the SAP R/3 APL must be able to take this format from the MRS database so that the correct address can be transmitted to SAP R/3. If the numbers are MRS conformably maintained in SAP, the “Autolearn” mode is not required.

Server

These settings are responsible for the receipt of documents and status information from SAP R/3 and their further routing to the MRS Server.

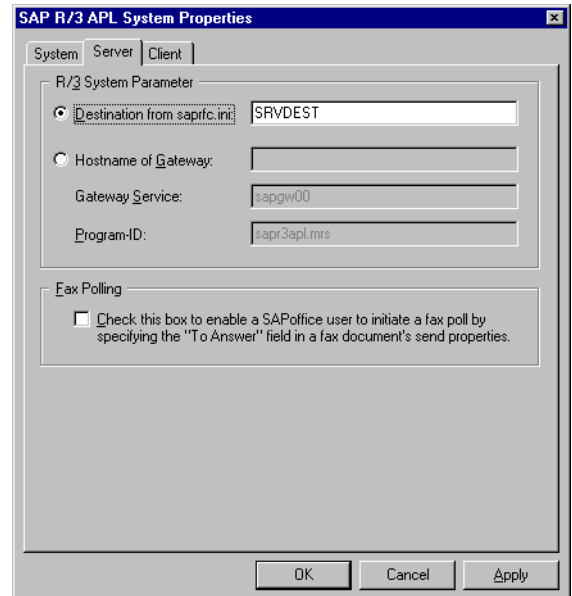
We recommend using the `saprfc.ini` file for the destination. By means of a type R entry an RFC Server can register with an SAP gateway. Subsequently the SAPphone APL as RFC Server waits for RFC calls from this gateway. SAP connect is such a gateway. Later the SAP R/3 APL only needs the RFC destination specification, thus the parameter DEST from the `saprfc.ini` file.

Through use of this SAP standard process, later extensions for the RFC can be simply entered in the `saprfc.ini` file by the SAP administrator. No SAP R/3 APL modifications are necessary to make these extensions immediately usable for the connection. Such extensions can be e.g. “Load Balancing” or “Secure Network Connections”.

This RFC destination is only entered locally in the `saprfc.ini` file on the computer on which the SAP R/3 APL runs.

The following example shows the normally used parameters. An explanation of the various parameters’ effects is found in the `saprfc.ini` file.

```
DEST=SRVDEST
TYPE=R
PROGID=sapconnect.mrs
GWHOST=/H/194.77.158.13/H/147.204.2.232/S/3297/H/cpce601
GWSERV=sapgw13
RFC_TRACE=0
```



The program ID entered here must match the one previously entered with the “sapgui” upon RFC destination configuration.

Alternatively the data rudimentarily required for the destination can also be entered here with the above mentioned flexibility disadvantages.

The TCP/IP hostname of the SAP R/3 Server would be normally entered for **Hostname of Gateway**. Alternatively, a SAP Router String may also be entered here as the hostname. This last method would be used when the SAP R/3 Server can only be addressed through a further SAP Router or SAP gateway.

The **Gateway Service** corresponds to a TCP/IP port. For more information refer to the paragraph on RFC Destinations.

The **Program-ID** corresponds to the configured program ID in SAP R/3 as mentioned earlier in this section.

If the option **Fax Polling** is enabled, SAPoffice users can poll fax documents from a fax on demand server by enabling the “Answer required” option with the transmission job.

Client

The Client settings are responsible for the transmission of documents and status information from the MRS Server to R/3.

We recommend using the `saprfc.ini` file for the destination. Analog to the RFC Server entry an entry of type A is required for the RFC Client. With it you can log in at the R/3 system. Via the RFC Client incoming calls etc are thus passed on to SAPphone. This RFC destination is only entered locally in the `saprfc.ini` file on the computer on which the SAPphone APL runs. The following example shows the normally used parameters. An explanation of the various parameters’ effects is found in the `saprfc.ini` file.

DEST=CLIDEST

TYPE=A

ASHOST=/H/194.77.158.13/H/147.204.2.232/S/3297/H/cpce601

The screenshot shows the 'SAP R/3 APL System Properties' dialog box with the 'Client' tab selected. The 'R/3 System Parameter' section has the 'Destination from saprfc.ini' radio button selected, with the text 'CLIDEST' in the adjacent field. Other fields in this section include 'Hostname of Appl. Server:', 'Hostname of Gateway:', 'Gateway Service:', and 'System Number:'. The 'Logon Data' section contains a note about required information for the RFC client and four input fields: 'Client:' (containing '100'), 'User:' (containing 'MRSC'), 'Password:', and 'Confirm Password:'. At the bottom, there is a checkbox labeled 'Always set EXPRESS flag for incoming SMTP documents.' and three buttons: 'OK', 'Cancel', and 'Apply'.

```
SYSNR=13  
RFC_TRACE=0  
ABAP_DEBUG=0  
USE_SAPGUI=0
```

Alternatively the data rudimentarily required for the destination can also be entered here with the above mentioned flexibility disadvantages.

The TCP/IP hostname of the SAP R/3 Server is normally entered in the field **Hostname of Application Server**. Alternatively, a SAP Router String may also be entered here as the hostname. This last method would be used when a SAP R/3 Server can only be addressed through a SAP router or SAP gateway.

The **Hostname of Gateway** is the TCP/IP hostname of the SAP Gateway. This entry is not mandatory and should only be entered when required.

The **Gateway Service** corresponds to a TCP/IP port. For more information refer to the paragraph on RFC destinations.

The index number of the SAP R/3 Server is entered in the field **System Number**. In most normal cases this would be 0, when not more than one SAP R/3 Server is running on a computer.

The **Signon Data** is required so that the SAP R/3 APL RFC Client can be logged on to the R/3 System through SAPConnect¹⁵. Therefore, the **Client** (client number defined under SAP R/3 with transaction sm59), **User** (user ID defined under SAP R/3 with transaction sm59) and associated **Password** (defined under SAP R/3 with transaction sm59) must be entered in the fields provided for this purpose. The password is entered twice to prohibit any input errors and possible connection errors.

Activation of the option **Always set EXPRESS flag for incoming SMTP documents** notifies the SAP user about newly incoming emails by means of an express message.

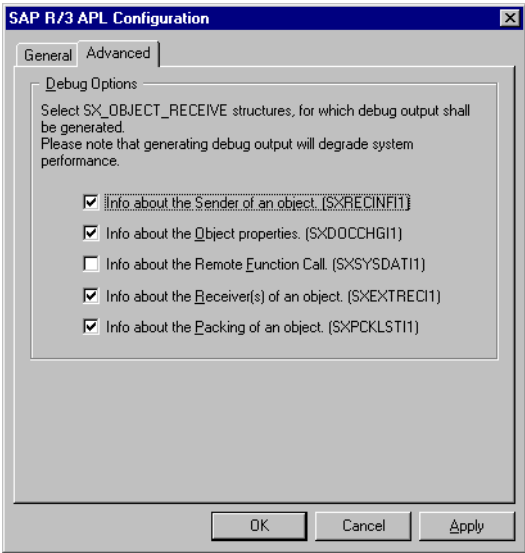
15. SAP R/3 versions earlier than 4.x do not support the immediate verification of Signon Data. This data is verified only after the first transmission of an object.

Advanced

This tab contains the possible debug settings for the SAP R/3 APL, whereby objects delivered by SAP R/3 would contain additional information

For every configurable object information there are three conditions possible. Available are none (empty field), normal (grey check), and detailed information (normal check).

During normal operation debug reports should not be generated since they degrade the systems performance.



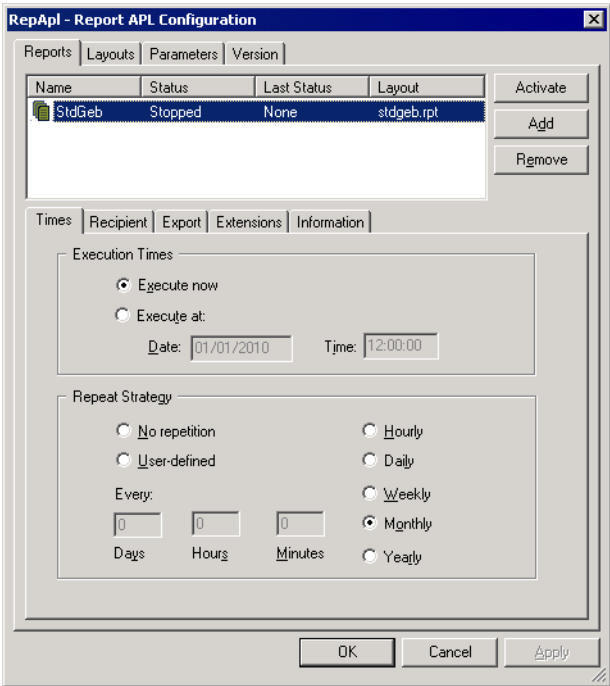
6.17 Creating Reports (RepAPL)

The Report APL provides an easy configurable means for accessing internal MRS Server data. This data is compiled in an easy to read format and can be sent to any MRS Address.

The Report APL uses pre-prepared default layouts for reporting and static editing of data. The MRS Distributor should be contacted if other default layouts are required.

All configured report jobs are displayed in the upper portion of the Report APL Configuration dialog.

The report job can be selected and **activated** so

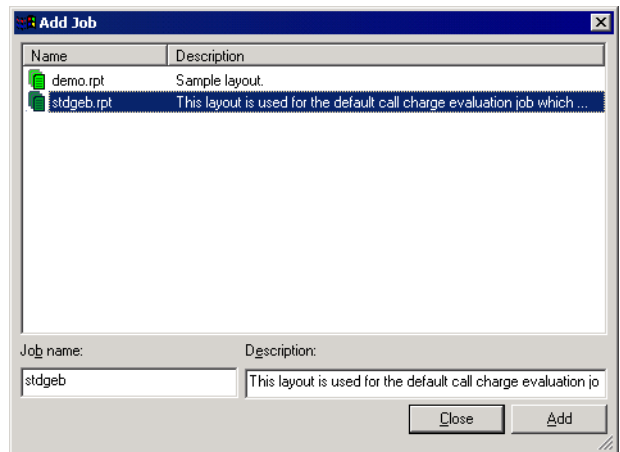


that it is carried out in accordance with the settings that are explained below. When a report job is active, the button changes to **Deactivate**, and can then be used to stop the reporting procedure. Existing report jobs can be deleted by selecting them and subsequently depressing the **Remove** button.

In the lower portion of the dialog the configurations of the selected report job are displayed.

6.17.1 Generating Report Jobs

New report jobs can be created through the use of the button **Add**. The new report job must be assigned a **Job Designation** as well as a **Description**. These are later displayed as **Name** and **Description** for the report job. The layout used for this report job can be selected from the displayed list of installed default layouts. How to add a new default layout is described further below.

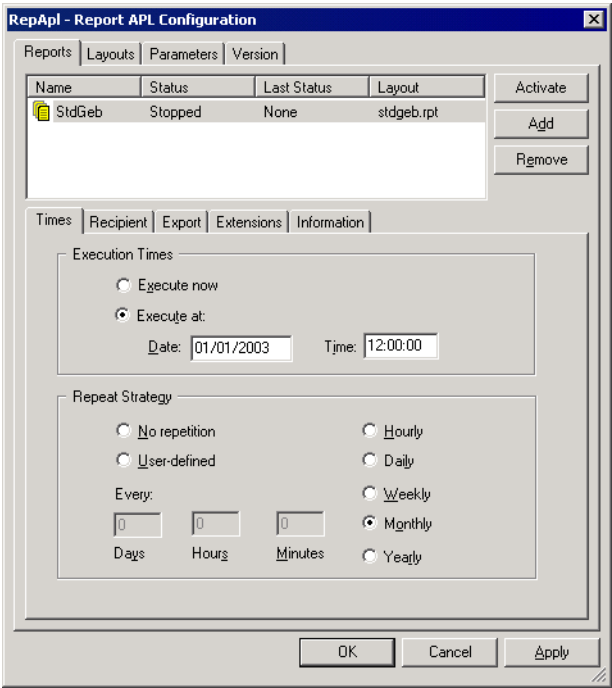


Times

In the dialog tab **Times**, the options **Now** and **Schedule at:** are available for the first-time execution of a report job.

In the dialog section **Repeat**, the frequency at which report jobs are repeated can be configured. The default settings **Hourly**, **Daily**, **Weekly**, **Monthly**, and **Yearly** are available as well as **User Defined** settings

Please make sure that the data are actually available for the defined period.

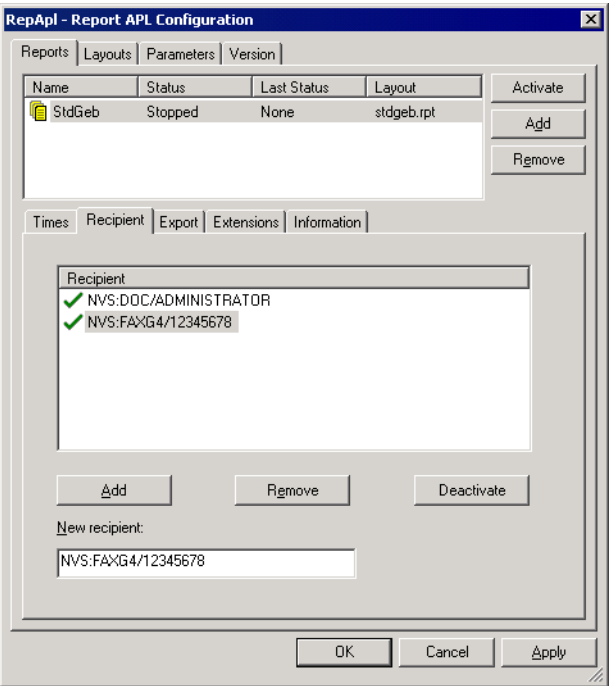


Recipient

Any MRS Address can be used as the **Recipient** for results generated by a report job. New Recipients are entered in the corresponding field, and through the use of the **Add** button, inserted into the Recipient list. The recipient entered should be able to handle the corresponding report format, thus should not be e.g. an SMS address.

Entries in the Recipient list can be deleted through use of the **Remove** button or be simply deactivated through use of the **Deactivate** button.

After a recipient has been deactivated, the buttons change their appearance and recipients can be reactivated through use of the **Activate** button.



Export

In the dialog tab **Export**, the export format of the report job can be configured in the section **Report Format**. The following formats are available for selection: Crystal Report, Rich Text Format (RTF), Hypertext Markup Language (HTML), Tab Separated Values (TSV), Comma Separated Values (CSV), Text WinWord Document, MS Excel 5 Worksheets, Fax G3 and Fax G4 in a proprietary Cycos format, as well as in a TIFF format.

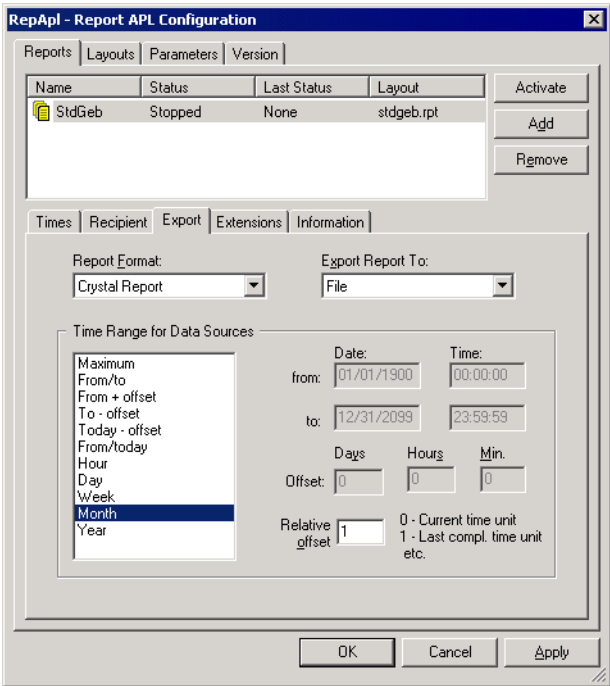
We recommend the native Crystal Report format whose viewer is supplied with the MRS-CD in the

client directory as the export filters of Crystal Reports sometimes do not achieve an optimal result for the other formats. For this reason it is advisable to have the report initially generated in different formats so that the various results can then be checked for a satisfying clarity. Besides, exporting can be performed from within the Crystal Reports Viewer to various target formats as well.

Currently, only files may be given as **Report Target**.

Various time ranges are available in the left side of the section **Time Period for Data Source**. Alternatively, an exact period of time can be defined through the entry fields provided on the right hand side of the section. Depending on the selected time period you either need to enter a fixed or a relative offset on the right. For example a week lasts from Monday 0.00 a.m. to Sunday 12.00 p.m. With 0 as relative offset you would receive a report from last Monday 0.00 a.m. until now; with 1 as relative offset a report from Monday before last, 0.00 a.m., until last Sunday 12 p.m.

Naturally only data available in the database can be exported. If a time period from last year is given, this data must be in the database resp. handed over to the Report APL for this period.



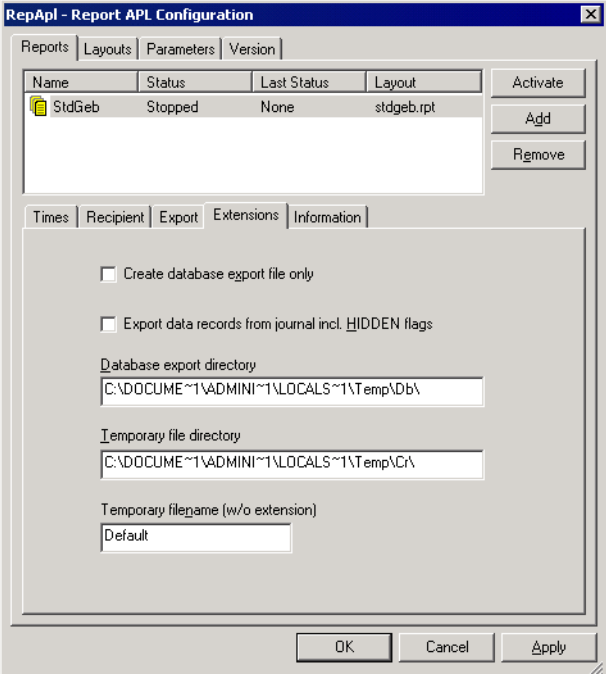
Advanced Settings

The Advanced tab contains configuration settings for database export. However, the export is only needed when a report layout is created with Crystal Reports for the first time. The option **Create Database Export only** enables database export in a DBF format. Additionally this option can be used to regularly export data by means of a job if, with extremely short deletion times, evaluations are to be generated at a later time.

The DBF format is readable by a large number of programs, and could be used e.g. by Excel to display the available data fields. A survey of database fields can be found in the *MRS System Architecture*.

Data records that are flagged with a hidden attribute can also be exported when the option **Export data records with HIDDEN flags from Journal** is enabled. An example are messages generated for CIT notification. These are flagged as otherwise they would be displayed in the user's outbound journal.

Three input fields are provided for entering the paths to the **Database Export Directory**, **Temporary File Directory**, and **Filename for Temporary Files**. No file extension should be given in this last path since the extension is dependent upon the export format.



The image shows the 'RepAPL - Report APL Configuration' dialog box. It has a title bar with a close button. Below the title bar are four tabs: 'Reports', 'Layouts', 'Parameters', and 'Version'. The 'Reports' tab is selected. It contains a table with columns: 'Name', 'Status', 'Last Status', 'Layout', and 'Activate'. There is one row with 'StdGeb' in the Name column, 'Stopped' in Status, 'None' in Last Status, and 'stdgeb.rpt' in Layout. To the right of the table are three buttons: 'Activate', 'Add', and 'Remove'. Below the table are four more tabs: 'Times', 'Recipient', 'Export', and 'Information'. The 'Export' tab is selected. It contains two checkboxes: 'Create database export file only' and 'Export data records from journal incl. HIDDEN flags'. Below these are three text input fields: 'Database export directory' (containing 'C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Db\'), 'Temporary file directory' (containing 'C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Cr\'), and 'Temporary filename (w/o extension)' (containing 'Default'). At the bottom are three buttons: 'OK', 'Cancel', and 'Apply'.

Name	Status	Last Status	Layout	Activate
StdGeb	Stopped	None	stdgeb.rpt	

☐ Create database export file only

☐ Export data records from journal incl. HIDDEN flags

Database export directory
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Db\

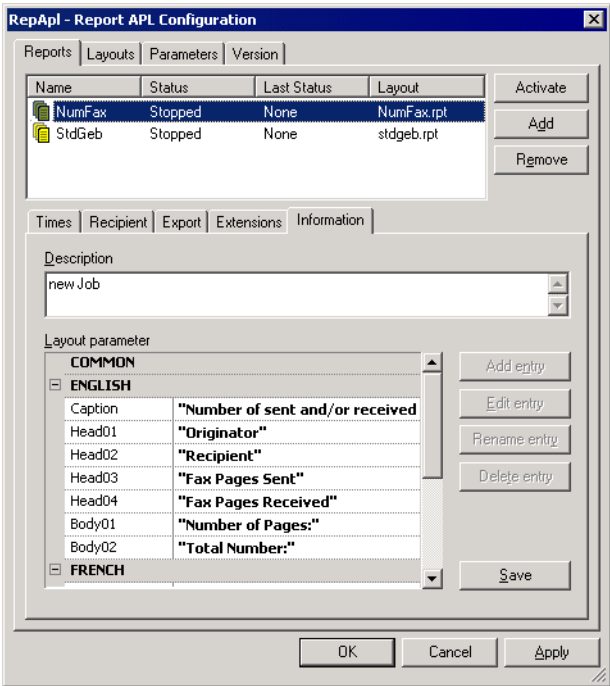
Temporary file directory
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Cr\

Temporary filename (w/o extension)
Default

Information

In addition to the selected report job the **Description**, entered upon the job creation, is displayed here. It can be altered in this tab as well.

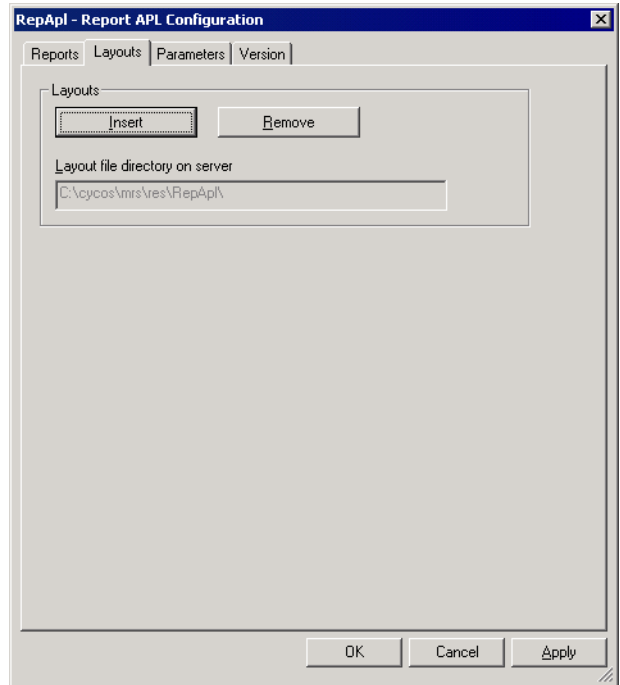
The settings that you can perform in the **Layout parameter** section are the same as described in chapter 6.17.3.



6.17.2 Global Settings

The layout files for the various reports are stored on the MRS Server in the <MRS root>\res\RepApl\ directory per default.

Individually created layouts or new ones received from your MRS Distributor must be copied to this directory.



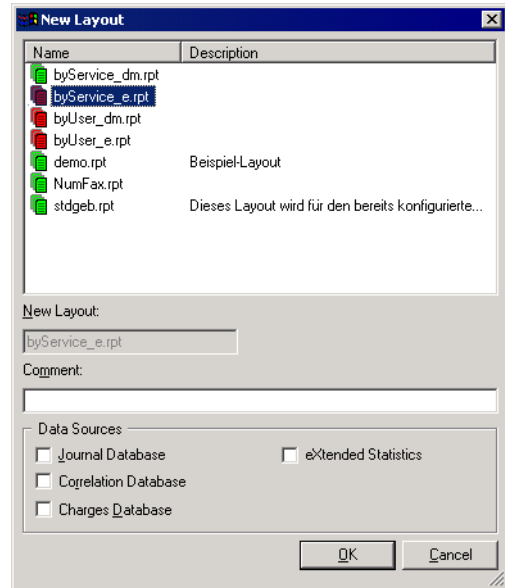
Server Administration

Creating Reports (RepAPL)

Via **Insert** new Report APL layouts can be activated. Active ones or those known to the Report APL have a green indication, all others a red one. Only active layouts can be used for generating a new report job. With **Remove** you can accordingly deactivate layouts known to the Report APL again.

When you select a “red” layout its name is copied to the field under **New Layout:**. The field **Comment:** is used for entering a short description of the layout

Finally the **Data Sources** used by this layout needs to be selected. You can choose from the MRS **Journal**, **Correlation** and **Charges databases** as well as **eXtended Statistics**. The latter one is used by all newer layouts and contains the MRS databases mentioned along with statistic information handed over from the APL to the Report APL. This could be e.g. information on call center operations delivered by the VM APL or information on the capacity of ISDN APL lines etc. Especially when PhoneMail reports are used, activation of this option is mandatory.



6.17.3 Parameters

This tab provides an editor for viewing, editing and modifying global (system wide) charge information. Several buttons are available on the right margin of the editor window. All items of charge information displayed here are stored in the `globals.ini` file found in the `<MRSroot>\res\RepAPL\` directory.

RepAPL - Report APL Configuration

Reports | Layouts | Parameters | Version

PhoneMail

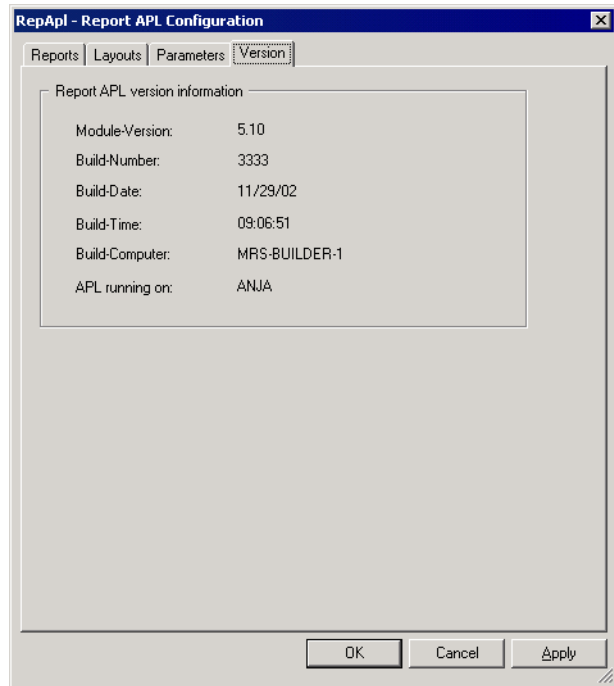
Connect Minutes Into Unit Price	1
Connect Minutes Into Billing Constant	1
Connect Minutes Out Unit Price	1
Connect Minutes Out Billing Constant	1
Message Sent Unit Price	1
Message Sent Billing Constant	1
Message Minutes Unit Price	1
Message Minutes Billing Constant	1

Add section
Rename section
Delete section
Add entry
Edit entry
Rename entry
Delete entry

OK Cancel Apply

6.17.4 Version

In this tab you can see information on the Report APL version currently used. In case of questions or problems concerning the Report APL always state this information.



6.18 Short Message Service (SMSAPL)

The SMS APL serves as interface of the MRS Server to mobile phone networks for sending and receiving SMS (Short Message Service) messages. For this purpose a mobile phone or GSM adapter is connected to the MRS Server via a serial data cable. Data are transmitted to the SMS service center by radio (GSM gateway). This is the difference between SMS transmission via SMSApI and ISDN APL. There the SMS service center of the corresponding mobile phone service provider is reached via the fixed network and receiving SMS messages is impossible.

So that the SMS can be used, the SMS APL must first be installed via the MRS Monitor configuration dialog.

6.18.1 Configuration Steps

1. Connect the mobile phone device with the MRS Server by means of a data cable.
2. Open the SMS APL configuration dialog in the MRS Monitor.
3. Select the mobile phone device from the list.

4. Enter the PIN number for the chip card (if required).
5. Select the serial interface via which the device has been connected.
6. Perform other settings (optional). See configuration options further below.
7. Save settings with **OK**.

6.18.2 Supported Hardware

Mobile phone devices tested and approved by Cynos:

- Nokia 7110
- Siemens M20 GSM Adapter

Mobile phone devices approved by MKS Systems, the original SMS APL producer; not tested by Cynos:

- coM.sat.DATA GSM adapter
- Falcom A2 GSM adapter
- Nokia 6210 mobile phone
- Siemens TC35 GSM adapter
- WaveCom P900 GSM adapter
- WaveCom WMOD2A-G900 GSM adapter
- WaveCom WMOD2B-G900/1800 GSM adapter V4.00.5 or higher
- WaveCom WMOi3 GSM adapter V4.00.5 or higher

6.18.3 Configuration

Type:

Type of mobile phone device.

SIM PIN Code:

PIN number for SIM board.

Serial Interface:

Port number of the serial interface the GSM adapter is connected to.

Postmaster:

ID of the user who receives all SMS messages that arrived without user ID.

Inbox Database Field:

Description of the user database field via which received SMS messages can be assigned to a user.

SMS Center:

Telephone number of the service center via which all SMS messages are to be sent. If the field remains empty, the service center stored on the SIM board is selected. The number is dialed as displayed. Thus no normalization takes place.

Call charges:

Costs that the originator has incurred per SMS message. The amount is written in the charges database per sent SMS message.

Poll Rate:

Time interval in seconds in which the mobile phone device is to be queried for newly received SMS messages.

Send SMS Prefix:

After activating this option you can enter a text that is to precede each outgoing SMS message. Users should be informed about these additional texts so that they can restrict the length of their own messages.

The screenshot shows the 'SMS APL Configuration' dialog box with the following fields and options:

- GSM Adapter:**
 - Type: Nokia 6210 (dropdown)
 - SIM PIN Code: (text field)
- Serial Interface:**
 - Connect through: COM2 (dropdown)
- Global:**
 - Postmaster: POSTMASTER (text field)
 - Inbox Database Field: SMS# (text field)
 - SMS Center: (text field)
 - Call charges: 0 Cent/SMS (text field)
 - Poll Rate: 90 Seconds (text field)
- Messages:**
 - ☐ Send SMS Prefix
 - ☐ Send SMS Suffix
 - ☒ Send Username
 - ☐ Send Subject
 - ☐ Don't delete SMS from SIM

At the bottom right, there is a 'Module: SmsApl' label and 'OK' and 'Cancel' buttons.

Send SMS Suffix:

After activating this option you can enter a text that is to be attached to each outgoing SMS message. Users should be informed about these additional texts so that they can restrict the length of their own messages.

Send Username:

The user ID precedes the SMS message in pointed brackets and is transmitted as well. Users should be informed about these additional texts so that they can restrict the length of their own messages.

Send Subject:

Instead of the message body only the subject is sent.

Don't delete SMS from SIM:

This option is exclusively intended for testing. When activated, read SIM messages remain on the SIM board. This switch should always be deactivated since only limited memory is available on the board.

6.18.4 Sending SMS Messages

SMS messages can be sent from each client. Enter the line `NVS:SMS/<mobile phone number>`. Depending on the client, `NVS:` can be omitted in many cases. If Communications is used as client, addressing is `<mobile phone number>[SMS]`.

Note that, depending on the configuration, either the subject field or the message text is sent as SMS.

SMS message length is restricted to 160 characters, messages that exceed this restriction are not transmitted. Remember that with some configurations also user ID, prefix and suffix may have to be added, so that for the actual message fewer characters are available. If the entire message comprises more than 160 characters, the originator is informed per message that it could not be sent.

6.18.5 Receiving SMS Messages

SMS messages without special recipient ID in the body text are forwarded to the user entered in the **Postmaster** field.

If an SMS message is to be directly sent to a specific user, the message text must contain a coding of this recipient which is prefixed by `*` and suffixed by `#`. The coding can be placed in an arbitrary position within the SMS message body and corresponds to the following pattern:

`<message text>* <recipient>#<message text>`

For example: `*1234#Hello Mr Jones, ...`

The *<recipient>* is now determined via the **Inbox Database Field**:, thus the user is searched for that has the transmitted content displayed in this database field.

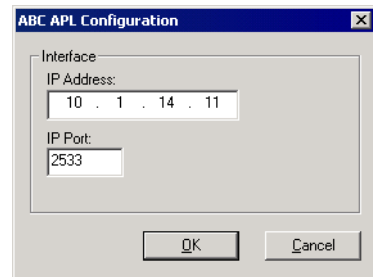
6.19 MWI to Alcatel 4400 (ABCAPL)

The ABC APL serves as interface to the Alcatel 4400 PBX for notifying a user about new messages (MWI). When new messages are available, the LED at the Alcatel system telephone is activated. Reading the messages deactivates the LED again. No further functions are supported.

The name ABC APL derives from the Alcatel protokol ABC-A used. Communication with the PBX occurs via LAN by means of TCP/IP.

So that the Alcatel 4400 MWI service can be used, the ABC APL must first be configured once via the configuration dialog in the MRS Monitor. Proceed as follows:

1. Open the configuration dialog of the ABC APL in the MRS Monitor.
2. Enter the PBX **IP Address** and, if required, the **IP Port** number for the ABC-A protocol. The port number is normally 2533.
3. Save the settings with **OK**.



Prerequisite for message waiting indication is an entry for each user in the **CIT** database field of the correlation database. This entry contains the routing address of the Alcatel PBX for the MTA with the corresponding extension. The MWI address of the ABC APL is: **MWI . 4400**. A complete entry for a user with extension 123 thus reads: **MWI . 4400/123**.

6.19.1 Telephone Display Support

To have the type (e-mail, fax, voice mail, SMS) and number of new messages displayed on the telephone, the **SignalAnyChange** switch must be activated in the Notification APL. This occurs automatically with the initial ABC-A APL start.

Since this mechanism in the Notification APL leads to an increased system load, this switch can be deactivated when this feature is not required.

The text that displays the message type can be modified via the registry.

6.19.1.1 Waiting Message Retrieval

When you press the LED, the correct number of waiting messages is displayed. After pressing the system key under this entry again, the type and number of messages

appears in the display. Putting down the phone or pressing the back key terminates the menu.

Index

A

Access.....	13
Access Authority, Database Fields.....	23
Access Numbers.....	155
Access to Physical Channels	
Line Bundles, ISDNAPL.....	149
Active Alert, Monitor.....	111
Active Alerts	
Automatic Maintenance, MTA.....	183
Active Schedules	
POP3 Mail-Import, SMTPAPL.....	221
Additional Logging Topics	
Restart, ISDNAPL.....	153
Addressing	
MRS.....	14
Administrative Client.....	22
Advanced Options	
DialogicAPL.....	169
Extensions, ISDNAPL.....	146
Advanced Settings	
Creating Reports (RepAPL).....	273
Analog Connections, Telematic Gateways.....	57
Analog Dialogic board.....	171
ANI for Display Texts.....	163
Attributes	
Fax G3, Telematic Protocols, GammaAPL.....	241
Telematic Protocols, ISDNAPL.....	144
Automatic Carbon Copies	
Routing Rules, MTA.....	188
Automatic Cleanup	
Automatic Maintenance, MTA.....	179
Automatic Maintenance, MTA.....	179

B

Backup.....	50
Bindings	
Extension Number Ranges, GammaAPL.....	243
Extensions, ISDNAPL.....	136
GammaAPL.....	245
Line Bundles, ISDNAPL.....	150
Line Bundles, Settings, DialogicAPL.....	174
V24APL.....	238

Body-Directory, HP Digital Sender.....	97
--	----

C

Calling Line Identification (CLI)	
Charges, Advanced Settings, DialogicAPL.....	177
Charges, ISDNAPL.....	152
CGI (Common Gateway Interface)	
WEBAPL.....	225
Channel Reservation	
GammaAPL.....	246
Charge Pulse Information	
Charges, Advanced Settings, DialogicAPL.....	176
Charges, ISDNAPL.....	152
Charges	
Advanced Settings, DialogicAPL.....	176
ISDNAPL.....	152
CIT	
Indication, Settings, MTA.....	189
over ISDN Voice.....	72
over the Siemens Hicom PBX, Telematic Gateways	60
Client	
SAP R/3 Gateway (SAPR3APL).....	266
Client Connections, Database Fields.....	31
Common Gateway Interface (CGI)	
WEBAPL.....	225
Communication Devices	
GammaAPL.....	244
Company Files.....	156
Compression	
Automatic Maintenance, MTA.....	180
Computer Telephony Integration (CTIAPL).....	255
Configuration.....	154
MRS Modules.....	115
Configuration Examples	
GammaAPL.....	246
Configuring a Logging Monitor.....	107
Configuring Line Monitors.....	108
Creating	
Reports (RepAPL), Advanced Settings.....	273
Reports (RepAPL), Export.....	272
Reports (RepAPL), Global Settings.....	275
Reports (RepAPL), Recipient.....	271
Creating Reports (RepAPL).....	268
Times.....	270
CTIAPL (Computer Telephony Integration).....	255

Server Administration

Index

D

Database.....	13
Database Fields	
Significance	23
Deinstallation of Individual Components.....	19
Deinstallation, MRS, Complete.....	19
Department Printer Settings (PrintAPL).....	249
Description	
Extension Number Ranges, GammaAPL	244
Extensions, ISDNAPL.....	137
Devices	
Advanced Settings, DialogicAPL.....	170
ISDNAPL	147
V24APL.....	237
DialogicAPL	
Extension Properties	166
General, DlgAPL.....	164
Line Bundles	
Settings	
Transfer Information	174
Settings	
Charges	
Calling Line Identification (CLI)	177
Charge Pulse Information	176
Devices.....	170
Extensions	169
Line Bundles	173
Bindings	174
Physical Channels	174
Originator Addresses.....	168
Resources	175
DTMF Recognition	176
Hardware	175
Restart.....	177
Restart, Services	177
Telematic Protocols.....	167
Telematic Protocols	
Hicom	
Private.....	165
Directory for Greeting Files	161
DlgAPL (DialogicAPL).....	164
Document Info	
PrintAPL.....	251
Document Routing Strategy, MTA	187
DTMF Recognition	

Resources, GammaAPL	246
Resources, Settings, DialogicAPL	176
DTMF tone sequences	171

E

Editing a Profile	45
EFT Client, Telematic Gateways	65
EFT Server, Telematic Gateways	64
Email Gateways	77
ERGO Script	154
Euro File Transfer (EFT), Telematic Gateways.....	64
Euro-File Transfer	
ISDNAPL.....	116
Euro-File Transfer Client	
Fax G3, ISDNAPL	119
Fax Group 3 Polling, ISDNAPL	121
Fax Group 3, ISDNAPL	118
Fax Group 4, ISDNAPL	121
Fax-Fax-Converter, ISDNAPL	121
ISDNAPL.....	118
Private, ISDNAPL	120
Euro-File Transfer Server	
Configuration Private, ISDNAPL	117
Configuration, Repeat Strategy, ISDNAPL.....	116
General Configuration, ISDNAPL	116
Event Viewer.....	21
Export	
Creating Reports (RepAPL).....	272
Extended Message Reporter Service.....	14
Extended Parameter	161
Extension Number Ranges	
GammaAPL	242
Extension Properties	
Extensions, ISDNAPL	136
Extensions	
Dialogic APL	166
Settings, DialogicAPL	169
Settings, ISDNAPL.....	146

F

Faked ANI.....	163
Faked REDIR.....	163
Fax Conversion, MTA	197
Fax Forward	

Protocol, ISDN (Telematic Gateways).....	61
Server, Telematic Gateways.....	62
Transparent, Telematic Gateways	61
Fax G3	
Telematic Protocols, GammaAPL.....	240
Fax G3 Polling, Telematic Gateways	57
Fax G4, Telematic Gateways	63
Fax Group 3 Polling	
Telematic Protocols, GammaAPL.....	241
Fax Mode	
PrintAPL.....	250
Fax-on-Demand	
Depositing Documents, Telematik Gateways	69
FfuAmt	121
FfuSendErrRep	121
FfuSendMidInId	121
FfuSendOkRep	121
FfuSendRundRep	121
FIAPL	
File Interface APL to Host	248
Gateways over the File Interface.....	247
General	
File Interface APL.....	247
Host to File Interface APL	247
File Formats	
SMTPAPL	219
File Interface	
Protocol, SAP R/3	81
File Interface APL (FIAPL)	247
File Saving.....	50
Firewall	
TCP/IP, SMI Transporter	206
G	
GammaAPL	
Bindings	245
Communication Devices	244
Configuration Examples.....	246
Channel Reservation	246
Extension Number Ranges	242
Description	244
General, (Gamma Fax).....	238
Originator Addresses.....	242
Resources	246
DTMF Recognition	246
Hardware	246
Telematic Protocols	
Fax G3	240
Attributes	241
General Settings	240
Identification.....	240
Repeat Strategy.....	241
Fax Group 3 Polling	241
General	239
GammaFax (GammaAPL).....	238
Gateway Addresses, Database Fields	29
Gateways over the File Interface (FIAPL)	247
General Settings	
Fax G3, Telematic Protocols, GammaAPL	240
SAP R/3 Gateway (SAPR3APL).....	263
SMTP Server, SMTPAPL	209
General User Data, Database Fields	30
Global Journal, MTA	193
Global Settings	
Creating Reports (RepAPL)	275
Greeting File	161
GSM Script, Telematic Gateways	60
H	
Hardware	
Resources, GammaAPL.....	246
Resources, Settings, DialogicAPL.....	175
Header-Directory, HP Digital Sender	98
Hicom	
Message Waiting Indicator, DialogicAPL.....	165
Hicom Applications Connectivity Link Settings	253
Host to File Interface APL	
FIAPL	247
HP Digital Sender	
Configuring a User Pool	97
General.....	96
Hardware Installation.....	96
Sender Protocol Installation.....	97
Software Installation.....	96
HTML	
WEBAPL.....	228
I	
Identification	

Server Administration

Index

Euro-File Transfer Client, ISDNAPL.....	118
Fax G3, Telematic Protocols, GammaAPL.....	240
V24APL.....	235
IMAP4 Server	
General	78
SMTPAPL	215
Incoming Mails	
SMTP Server, SMTPAPL	210
Installation	
of Individual Components	18
Integrated Services Digital Network (ISDN)	61
IntlDialMode	121
ISDNAPL	
Bindings.....	150
Charges	
Calling Line Identification (CLI)	152
General	152
Euro File Transfer Client	
SMI-Protocol	122
Euro-File Transfer	
Configuration, Repeat Strategy	116
General	116
Euro-File Transfer Client	118
Fax G3.....	118, 119
Fax Group 3 Polling	121
Fax Group 4.....	121
Fax Mailbox Administration	
Voice Play-back via Telephone	135
Fax-Fax-Converter	121
Private.....	120
SMS (TAP Protocol)	122
Standard Voice/Fax Mailbox	126
TAP Protocol	
Private.....	123
Euro-File Transfer Server	
Configuration Private	117
Euro-File Transfer Server, General Configuration..	116
Extensions	136
Advanced Options	146
Description	137
Line Bundles	
Access to Physical Channels	149
Transfer Information	149
Originator Address	144
Protocols.....	115

Resources	151
Charge Pulse Information	152
DTMF Recognition.....	151
Hardware.....	151
Restart	
Additional Logging Topics	153
General.....	153
Telematic Protocols	
Attributes	144
Formats	143
General.....	143

K

Kernel.....	13
Key Allocation for Confirmation/Exit	158
Kunde, Konfiguration	161

L

Licences, MTA.....	198
Lightweight Directory Access Protocol (LDAP).....	92
Line Bundles	
Settings, DialogicAPL	173
Line Monitor, Operation Example	111
LinePrefix.....	121
Local Database (Cache)	43
Logging Monitor.....	110
Logging Monitor, Configuration.....	107
Logical Lines, MTA.....	195
Lotus Notes	78

M

Mailbox Folder (TUM)	164
Mailing Lists	93
Main Log File, Monitor	111
Menu Time Behaviour	157
Message.....	13
Message Routing, Database Fields	25
Message Transfer Agent	13
Message Transfer Agent (MTA).....	178
Microsoft Exchange	78
Microsoft Exchange Gateway (ExchAPL)	204
Modem Operation (V24APL)	234
Monitor	
MRS	17

Monitor Options, Standard	109
Monitor, Active Alert	111
Monitor, Haupt-Logdatei	111
Monitor, Line Monitor	110
Monitor, Log-Fenster	110
Monitor, Modules Window	109
Monitor, MRS	105
Monitor, Special Analysis Session	112
MRS	
Addressing	14
MRS Modules	115
MRS Monitor	105
MSP (Service Provider)	43
MTA	
Advanced Settings	189
CIT Indication	189
Optimization	192
Remote System Links	192
Send Voice as CIT Message	190
User Quotas	191
Automatic Maintenance	
Active Alerts	183
Automatic Cleanup	179
Compression	180
Jobs	181
Remove Database Entries and Documents	180
Document Routing Strategy	187
Fax Conversion	197
General	
Automatic Maintenance	179
Global Journal	193
Logical Lines	195
Message Transfer Agent	178
Remote System Link	184
Routing Rules	187
Automatic Carbon Copies	188
Time Triggered Document Routing	188
Text-to-Speech	196
N	
Name Locator	14
Name Resolver	
TCP/IP, SMI Transporter	208
Named Pipes (PipeAPL), SMI Transporter	204
New Database Fields	

POP3 Mail-Import, SMTPAPL	220
NIL Protocol	95
Novell Groupwise	
Addressing	83
O	
Optimization	
Advanced Settings, MTA	192
Originator Address	
ISDNAPL	144
Originator Addresses	
Advanced Option Settings, DialogicAPL	168
GammaAPL	242
Outgoing E-Mail, SMTP Server, SMTPAPL	213
Outgoing Mails	
SMTP Server, SMTPAPL	210

P	
Parameter	
recplen=	162
recplvl=	162
recslen=	162
recslvl=	163
Parameter Entries	161
Pause between short and long menu entries	157
Pause between two Messages	157
Pause until Menu Repetition	157
pga Parameter	161
Phone Display	156
PipeAPL (Named Piped), SMI Transporter	204
Poll-Directory, HP Digital Sender	97
POP3 Mail Import	
General	80
SMTPAPL	209
POP3 Mail-Import	
SMTPAPL	220
POP3 Server	78
POP3 Server, SMTPAPL	214
POP3/IMAP4 Server (SMTPAPL)	209
PPP/RAS Logon	
POP3 Mail-Import, SMTPAPL	222
PrintAPL	
Document Info	251
General (Department Printer Settings)	249

Server Administration

Index

Number of Copies.....	250
Telex Banner	250
Private	
Hicom, Telematic Protocols, DialogicAPL.....	165
TAP Protocol, SMS, ISDNAPL	123
Privileges	35
Customer Specific	42
Protocol Value Digest.....	123
Protocols, ISDNAPL	115

R

Reading out E-mails	156
Recipient	
Creating Reports (RepAPL)	271
recplen= (Parameter)	162
recplvl= (Parameter)	162
recslen= (Parameter)	162
recslvl= (Parameter)	163
Remote System Link, MTA.....	184
Remote System Links	
Settings, MTA	192
Remote System Links (SMI Transport).....	58, 208
Remove Database Entries/Documents, MTA.....	180
Remove Documents	
Automatic Maintenance, MTA.....	181
RepAPL (Creating Reports)	268
Repeat Strategy	
Fax G3, GammaAPL	241
Reports	
MRS User Configuration.....	98
Reports, HP Digital Sender	98
Resources	
Advanced Settings, DialogicAPL.....	175
GammaAPL	246
ISDNAPL	151
Restart	
Advanced Settings, DialogicAPL.....	177
rmtopic Parameter.....	161
Routing Rules, MTA	187

S

SAP R/3	
APL	81
General	80

SAP R/3 Gateway (SAPR3APL)	
Advanced	268
Client.....	266
General.....	263
General Settings	263
Server	265
System.....	264
SAPR3APL (SAP R/3 Gateway)	263
Saving Monitor Layouts.....	108
Script Parameter	155
Security	
WEBAPL	224
Send Voice as CIT Message, MTA	190
Server	
SAP R/3 Gateway (SAPR3APL).....	265
Service Provider (MSP)	43
Configuration	43
Services	
MRS Server.....	57
Settings	
SAP R/3 Gateway (SAPR3APL).....	268
Short Message Service (SMS)	60
Short Message Service (SMS), Telematic Gateways....	66
Silence Detection	158
Simple Mail Transfer Protocol (SMTP).....	209
SMI Transport	
Remote System Links	58
SMI Transport (Remote System Links)	66
SMI Transporter	
General.....	204
Remote System Links	208
TCP/IP	
Firewall	206
Name Resolver.....	208
TCP/IP (TCPAPL)	205
SMI-Protocol, Euro-File Transfer Client, ISDNAPL ..	122
SMS (TAP Protocol), ISDNAPL	122
SMTP (Simple Mail Transfer Protocol) Server	209
SMTPAPL	
File Formats	219
General.....	209
IMAP4 Server	215
POP3 Mail-Import	220
Active Schedules	221
New Database Fields	220

POP3 Server	214
SMTP Server	
General Settings	209
Incoming Mails	210
Outgoing Mails	210
Speech Recognition (ASR)	156
SPX (SPXAPL), SMI Transporter	205
Standard	
Voice/Fax Mailbox.....	72
Start of Individual Components	18
Starting (Server)	17
Stop of Individual Components.....	19
Stopping (Server)	17
Store & Forward Interface.....	43
Supervisor Mode	70
T	
TCP/IP (TCPAPL), SMI Transporter	205
Telematic Gateways	57
Telematic Protocols.....	155
Advanced Option Settings, DialogicAPL	167
Dialogic APL.....	164
GammaAPL.....	239
V24APL	236
Telematic Services, Database Fields	26
Telex Banner	
PrintAPL.....	250
Test Parameter	163
Text to Speech, TTS	156
Text-to-Speech, MTA	196
Time Behaviour in Express Mode	157
Time Triggered Document Routing	
Routing Rules, MTA	188
Times	
Creating Reports (RepAPL)	270
General	270
Toggle Default.....	45
Transactions Interface	43
Transmission	
Line Bundles, Advanced Settings, DialogicAPL	174
Trunk Groups	
Settings, ISDNAPL	149

U

Use of Office Phone Display	156
User Configuration, MRS	98
User Data Administration	22
User Entry	
Example	32
User Profiles	44
User Quotas	
Settings, MTA.....	191

V

V24APL	
Bindings	238
Devices	237
General.....	234
Identification.....	235
Telematic Protocols	236
Vanity Numbers.....	202
VMiE Interface.....	171
Voice (Playback via the Telephone)	
ISDN, Telematic Gateways	66
Voice Play-back via Telephone	
Euro-File Transfer Client, Fax Mailbox Administration, ISDNAPL	135

W

WAP Script	226
WAP Script Parameter.....	226
Watchdog	
Automatic Maintenance, MTA.....	182
Web Server (WEBAPL)	223
WEBAPL	
General (Web Server)	223
Security	224

