



# User Manual

## NAMES 3.0

**Doc-ID** DB.NAMESMAN30.NT  
**Version** 1.1  
**As of** 05.05.2017  
**State** Final Version  
Subject to change without notice

Copyright 2017 NovaTec Kommunikationstechnik GmbH

Forwarding, duplication, utilisation, saving or publication of this document or its contents are neither allowed in excerpts nor completely, unless explicitly permitted in written form.

Infringement obliges to payment of damages.  
All rights reserved.



## CONTENT

1	Introduction .....	6
2	System requirements .....	7
2.1	NAMES execution environment .....	7
2.1.1	Minimum specifications .....	7
2.1.2	Recommended specifications .....	7
2.2	Database server .....	7
2.3	Compatible NovaTec products .....	7
2.4	Compatible client software .....	8
2.5	Network configuration .....	8
3	Installation .....	9
3.1	Running the installer .....	9
3.2	Licence installation .....	13
3.3	Database initialisation .....	15
3.4	Uninstalling .....	16
4	Configuration .....	18
4.1	NAMES configuration file .....	18
4.1.1	Database configuration .....	18
4.1.1.1	Oracle DB 11g .....	18
4.1.1.2	MySQL 5.5 .....	18
4.1.2	Web server configuration .....	19
4.1.2.1	Changing the listen port .....	19
4.1.2.2	Using secure mode (HTTPS) .....	19
4.1.3	Miscellaneous configuration .....	20
4.1.3.1	Storage path .....	20
4.1.3.2	Maximum Java heap size .....	20
4.1.3.3	Target monitoring alert time .....	20
4.2	Logging configuration file .....	20
4.3	Firewall settings .....	21
5	Administration .....	22
5.1	Starting NAMES .....	22
5.2	First login .....	22
5.3	General settings .....	23
5.3.1	Maximum number of simultaneous jobs .....	23
5.3.2	Maximum number of simultaneous logins .....	23
5.3.3	Maximum number of simultaneous reconfigurations .....	23
5.3.4	Keep CDRs .....	24
5.3.5	Keep log entries .....	24
5.4	User management .....	25
5.4.1	Users .....	25

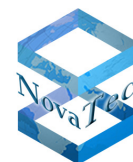


5.4.1.1	Creating a user.....	25
5.4.1.2	Editing a user.....	26
5.4.1.3	Disabling/Enabling a user.....	27
5.4.2	User groups .....	27
5.4.2.1	Creating a user group .....	27
5.4.2.2	Editing a user group .....	28
5.4.2.3	Deleting a user group .....	28
5.5	Role management .....	29
5.5.1	Creating a role .....	29
5.5.2	Assigning permissions to a role .....	30
5.5.3	Deleting a role.....	30
5.6	SNMP configuration .....	30
5.7	Certificate Authority configuration .....	31
5.7.1	General configuration procedure.....	32
5.7.2	Configuring NAMES as a Root CA.....	34
5.7.3	Configuring NAMES as a subordinate CA .....	35
5.7.4	Configuring NAMES using an existing key and certificate.....	36
5.8	SSL contexts .....	36
5.8.1	Creating an SSL context.....	37
5.8.2	Editing an SSL context .....	37
5.8.2.1	Adding a private key and certificate .....	37
5.8.2.2	Replacing a private key and certificate .....	38
5.8.2.3	Adding a trusted certificate authority .....	38
5.8.2.4	Removing a trusted certificate authority.....	39
5.8.3	Setting an SSL context as default context .....	39
5.8.4	Removing an SSL context .....	39
5.9	Managing firmware images, music on hold files and Licence Manager.....	39
5.9.1	Firmware images.....	39
5.9.2	Music on Hold .....	40
5.9.3	Licence Manager .....	42
5.10	Shutting NAMES down .....	43
6	Usage .....	44
6.1	Provisioning .....	44
6.2	Configuring the system .....	47
6.2.1	System Settings .....	49
6.2.1.1	System Information .....	49
6.2.1.2	Network.....	49
6.2.1.2.1	Mode .....	49
6.2.1.2.2	Hostname .....	51
6.2.1.2.3	Single Port .....	51
6.2.1.2.4	MTU (Maximum Transfer Unit) .....	52
6.2.1.2.5	Default Gateway.....	52
6.2.1.2.6	DNS Servers.....	52
6.2.1.2.7	VLAN .....	52
6.2.1.3	NAMES Servers.....	53
6.2.1.4	Time Settings.....	54



6.2.1.4.1	Time zone .....	54
6.2.1.4.2	Daylight Savings Time .....	54
6.2.1.5	Monitoring .....	55
6.2.1.5.1	Parameterless alarms.....	55
6.2.1.5.2	CPU usage Alarm.....	56
6.2.1.5.3	Call Setup Time Alarm .....	56
6.2.1.5.4	Memory Full Alarm .....	56
6.2.1.5.5	Heartbeat .....	56
6.2.1.5.6	ASR Settings .....	57
6.2.2	Hardware.....	58
6.2.2.1	Chassis .....	58
6.2.2.1.1	Changing the chassis type.....	59
6.2.2.1.2	Slide in cards and daughter boards.....	59
6.2.2.2	Analogue Profiles.....	60
6.2.2.3	VoIP Port Profiles .....	61
6.2.3	Security .....	63
6.2.4	Telephony.....	68
6.2.4.1	Localisation .....	68
6.2.4.2	VoIP .....	68
6.2.4.2.1	SIP .....	68
6.2.4.2.1.1	SIP Codec Mapping.....	68
6.2.4.2.1.2	Global SIP Options.....	72
6.2.4.2.1.3	SIP Timeout Options.....	77
6.2.4.2.1.4	Trunks .....	79
6.2.4.2.2	NAT.....	83
6.2.4.2.3	STUN.....	83
6.2.4.3	ISDN .....	84
6.2.4.3.1	Trunks.....	84
6.2.4.4	Call Routing .....	87
6.2.4.4.1	Trunk groups .....	87
6.2.4.4.1.1	New Trunk Group .....	87
6.2.4.4.1.1.1	New Number Group.....	91
6.2.4.4.1.1.2	New Number .....	94
6.2.4.4.2	All subscribers .....	94
6.2.4.4.2.1	Subscriber group .....	96
6.2.4.4.2.1.1	Creating a Subscriber.....	98
6.2.4.4.2.1.2	Creating a SIP Subscriber.....	102
6.2.4.4.3	Line groups.....	107
6.2.4.4.3.1	New Line Group .....	107
6.2.4.4.4	Adjusting the routing .....	109
6.2.4.5	Call Take Over Groups .....	112
6.2.4.6	Dialling Codes .....	114
6.2.4.7	Synchronisation.....	115
6.2.4.8	Call Data Profiles .....	116
6.2.4.9	Channel Permissions.....	118
6.2.4.10	MLPP .....	118
6.2.4.11	ALCR .....	119
6.2.4.12	Global Options.....	120
6.2.4.13	Bank holidays.....	120
6.2.4.14	Premium Rate Numbers .....	122
6.2.4.15	Network Service Provider .....	123
6.2.4.15.1	Network Service Provider .....	123
6.2.4.15.2	Regional charge categories .....	125
6.2.4.15.3	Time charge categories.....	126



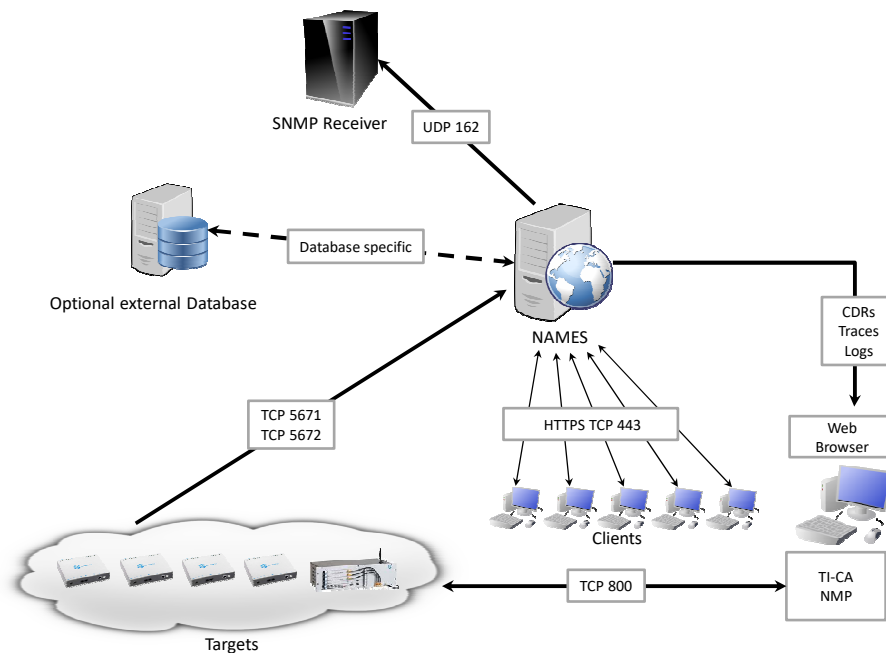


6.2.4.15.4	Assign telephone numbers .....	127
6.2.4.15.5	Call barring .....	128
6.3	Targets .....	129
6.3.1	Editing a target .....	129
6.3.2	Removing a target .....	129
6.3.3	Multiple target actions .....	129
6.3.4	Target details .....	130
6.4	Target groups .....	130
6.4.1	Creating a target group .....	131
6.4.2	Editing a target group .....	131
6.4.2.1	Adding Targets .....	131
6.4.2.2	Removing targets .....	132
6.4.3	Removing a target group .....	132
6.5	Jobs .....	132
6.5.1	Job types .....	132
6.5.1.1	Upload Firmware .....	132
6.5.1.2	Reset .....	132
6.5.1.3	Download Trace Files .....	133
6.5.1.4	Download Log File .....	133
6.5.1.5	Download CDRs .....	133
6.5.1.6	Sign Certificate .....	133
6.5.2	Job states .....	133
6.5.3	Creating a job .....	133
6.5.4	Viewing and modifying scheduled jobs .....	134
6.5.5	Active jobs .....	135
6.5.6	Completed and failed jobs .....	135
6.6	Job Trigger .....	136
6.6.1	Creating a Job trigger .....	136
6.6.2	Edit Job triggers .....	137
6.7	User settings .....	137



# 1 Introduction

The NovaTec Administration and Management Element Server (NAMES) allows you to manage all your NovaTec devices through a central service. It contains functions to assist you with deployment, maintenance, configuration and monitoring. The following image shows NAMES in a typical deployment:



NAMES can and should be used as the central administrative element for any installation of NovaTec devices. Currently additional tools (the NovaTec Maintenance Package, consisting of the NovaTec Trace Info Client and NovaTec Call Server) are required for certain functionalities and are therefore included in the overview above as installed on the client PCs.

The following documentation applies to the fully licensed version of NAMES. For availability of individual features, please see the terms of your licence. The free version of NAMES does not contain any of the following features:

- Scheduled Jobs,
- Triggered Jobs,
- Certificate Authority functions,
- User/role management (only the default user "names" is available),
- SNMP mapping,

Multi-user capability (only one user session at a time).



## 2 System requirements

### 2.1 NAMES execution environment

NAMES is intended to run on physical or virtual servers under a Windows Server operating system. As NAMES is implemented in Java, a Java Runtime Environment is required.

#### 2.1.1 Minimum specifications

At a minimum, the following specifications are necessary to run NAMES:

- 256 MB of free memory,
- 2 CPU cores,
- 256 MB of disk space,
- Windows Server 2008 R2 Standard Edition SP1,
- Oracle Java SE 8 64-bit Runtime Environment, latest update,
- Oracle Java 8 Unlimited Strength Jurisdiction Policy Files.

With these specifications, only a small number of devices (up to about 10) can be administered. A short deletion interval must be used if automatically retrieving CDRs from the devices, as these can quickly fill up hard drive space, depending on the call volume.

#### 2.1.2 Recommended specifications

The following specifications are recommended for small to medium installations (up to about 50 devices):

- 512 MB of free memory,
- 4 CPU cores,
- 1 GB of disk space,
- NTP time synchronisation.

Larger installations require additional resources and should be sized according to specific requirements.

### 2.2 Database server

NAMES will use an embedded database by default. However, the use of an external database is possible and may offer advantages with regard to availability and backup planning. NAMES supports the following external databases:

- Oracle DB 11g,
- MySQL 5.5.

If using Oracle, it is recommended to configure a Unicode character set.

### 2.3 Compatible NovaTec products

NAMES must be used in conjunction with specific versions of NovaTec hardware, firmware and PC utilities. Following versions may be used with NAMES 3.0:

- Hardware: CCU4, CCU6
- Firmware: 00.09.00.xx



- NMP 7.4.x only TI-Client, Call-Server and network services

## 2.4 Compatible client software

The NAMES web user interface was tested with Microsoft Internet Explorer 11 and Firefox. The web framework in use claims to support all relevant modern desktop browsers and spot checks have shown no contrary evidence; however, extensive testing has not been done. While NovaTec welcomes bug reports for non-Microsoft browsers, fixes will at best be provided on a best-effort basis and support may be unavailable.

## 2.5 Network configuration

NAMES makes extensive use of network communication. This means, that for correct operation, the required connections must be able to be established, and bandwidth may become a limitation, especially in installations with many devices.

All ports can be configured freely, however it is generally recommended to use the default ports, if possible. For details about default port numbers and connections, please see the document „IP Port Matrix“ available from the download section of our homepage (<http://www.novatec.de/cms/en/Downloads/Downloadarea.html>).



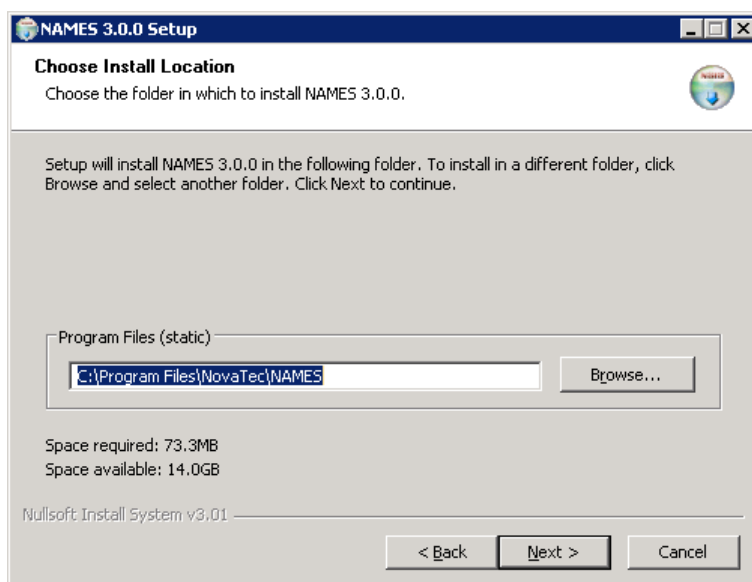
## 3 Installation

### 3.1 Running the installer

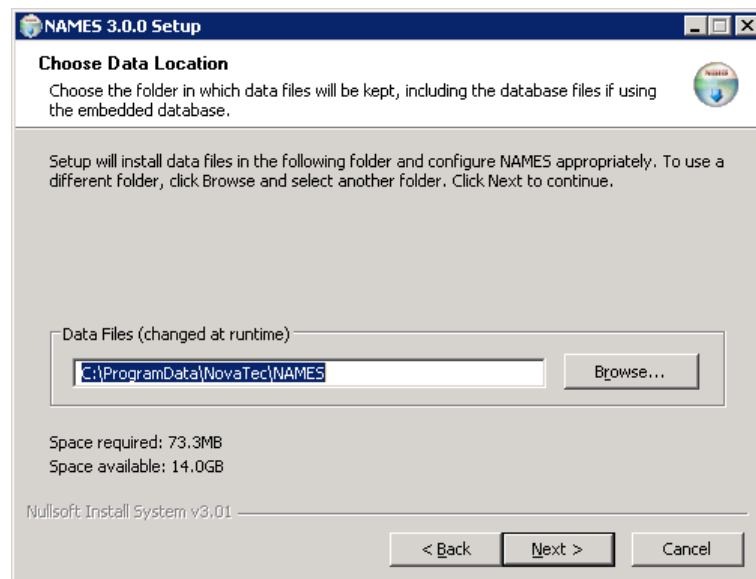
To install NAMES begin by running the provided installer file. The following dialogue box appears:



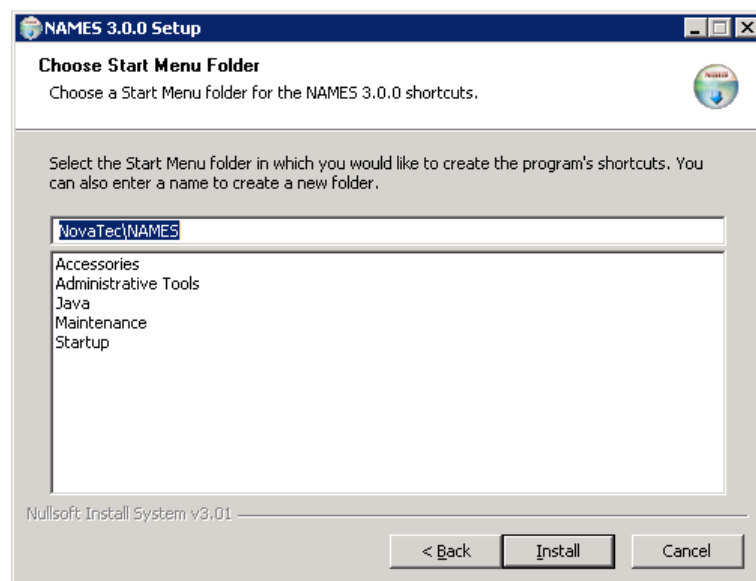
After selecting „Next“ choose the installation folder for NAMES.



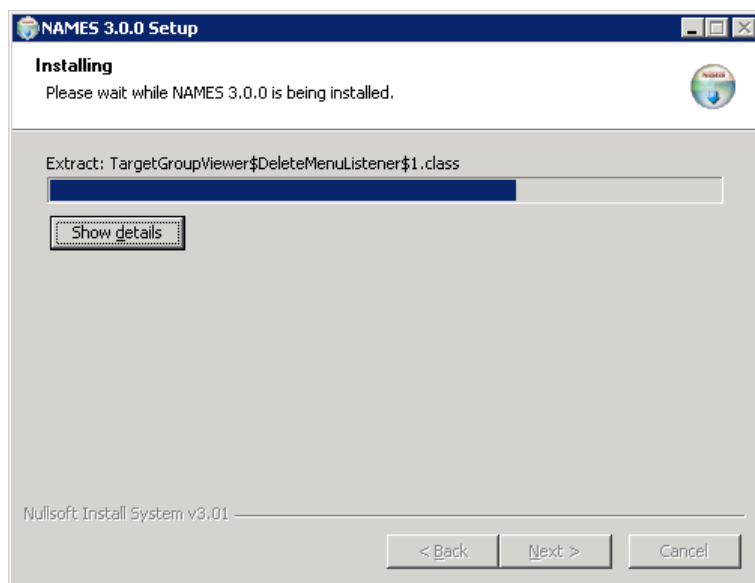
Files that normally don't change during the operation of NAMES are placed into the installation folder, like executables, libraries, resources and configuration files. Files that may change during operation, like the embedded database files and logs, are placed in the data folder, which can be configured on the next page:



After configuring the folders for program and data files, you choose the start menu folder:

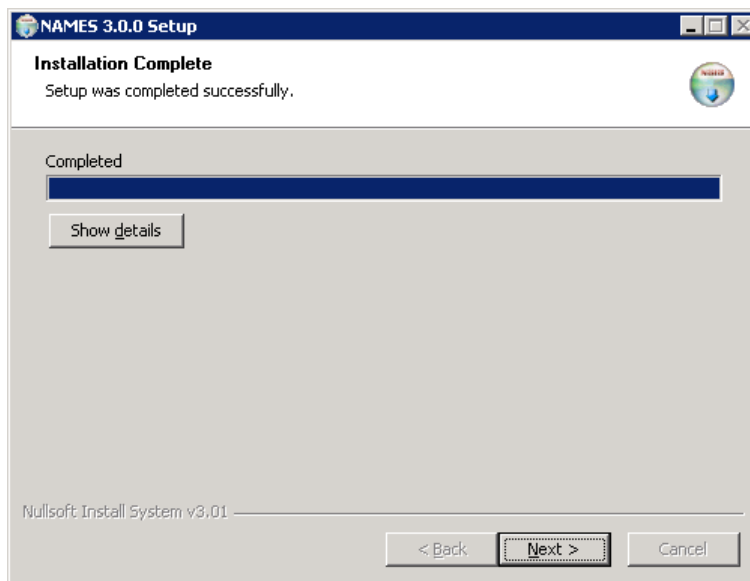


This is the final step before the installation starts, so ensure all settings are correct before clicking „Install“. The installer will proceed to complete the necessary installation steps, including installation of a Microsoft Visual C++ Redistributable and the licencing files, including an evaluation licence.

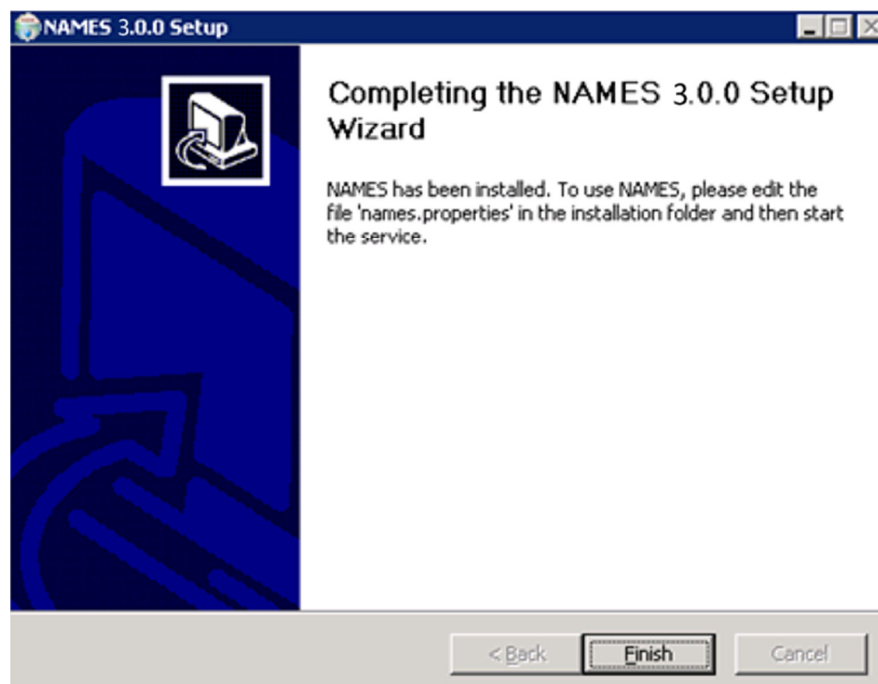


The installation of the licencing mechanism will require a separate acknowledgement:

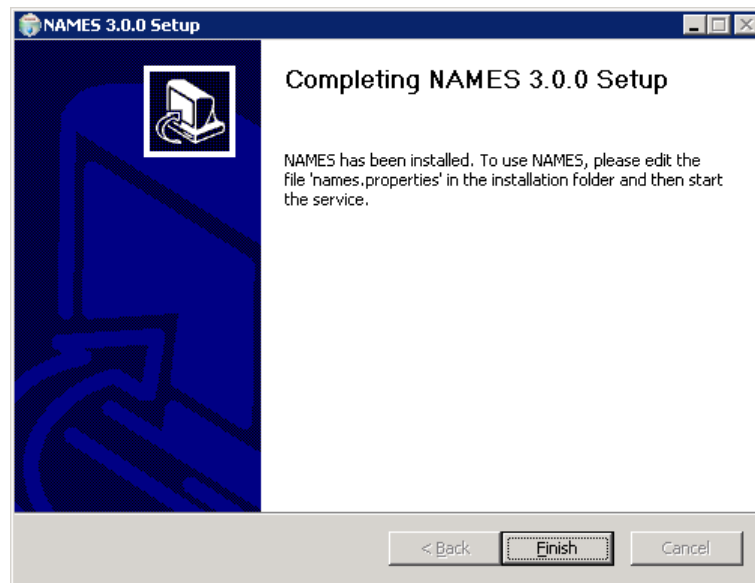
After clicking „OK“ the installation will complete.



Clicking „Next” takes you to the final screen of the installer that describes which steps need to be taken next.







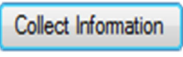
If you wish to use the embedded database and do not want to use HTTPS to access the web UI, NAMES is ready to use. You can manually start the service from the Windows service management UI (see section 5.1) or restart the system. After every system restart, NAMES will start automatically.

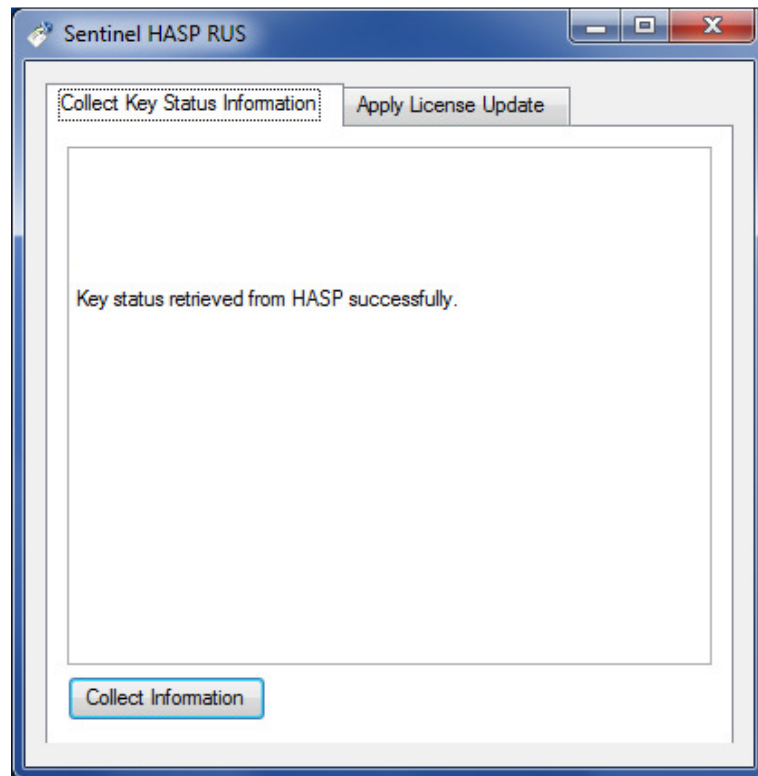
## 3.2 Licence installation

NAMES is installed with a 60-day evaluation licence. Apart from the limited evaluation period, this licence also contains other limitations, such as the number of devices that can be managed. For production use, a perpetual licence has to be installed.

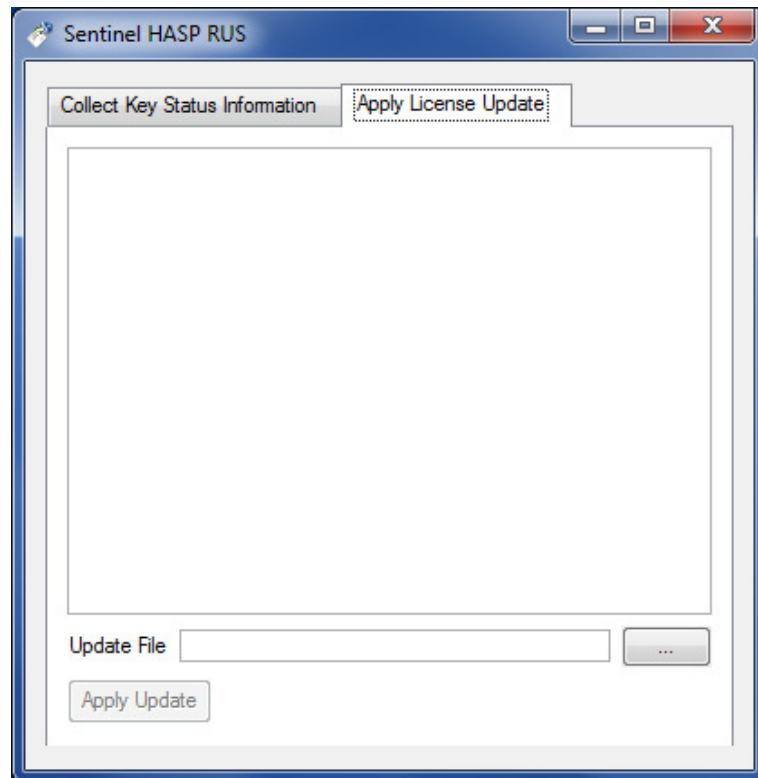
The licencing system in use requires the user to use a licencing tool to collect certain system information into a file, which must then be sent to NovaTec e.g. via email. The information contained in the file is used to create an individualised licence, which is sent back to the client who then has to install it using the same tool.



The process is as follows:

1. Run the application „NAMES License Tool“ in the NAMES installation folder. A window with two tabs will appear. The first tab, which is selected by default, allows you to collect the licence information.
2. Click the  button and then select a location and name for the generated system information file. The tool will inform you that the key status was successfully retrieved:



- 3.** Send the generated file (e.g. info.c2v) to your sales contact at NovaTec with the order number for your NAMES licence purchase. If you have not purchased a NAMES licence yet, contact a sales representative for licensing terms.
- 4.** NovaTec will generate a licence file (e.g. customer.v2c) and return it to you.
- 5.** Run the "NAMES License Tool" again. This time, select the second tab which allows you to apply the licence file:



6. Click the  button. A file selection dialogue will open, allowing you to select the file with the licence information sent to you by NovaTec.
7. Finally, click the  button. The licence is now installed and ready to be used. If NAMES is running, restart NAMES to load the new licence information.

### 3.3 Database initialisation

If using an external database, the database structure (tables and some basic database rows) must be imported. If using the embedded database, this step is not required, as the installed database comes prepared with this structure.

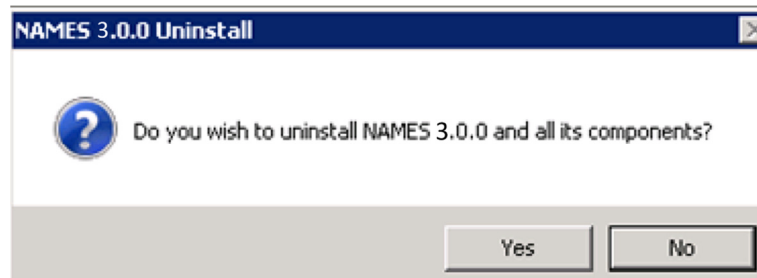
The NAMES installation folder contains two SQL scripts for the two supported external database systems. Select the file appropriate to the database in use (either names-oracle.sql for Oracle DB 11g or names-mysql.sql for MySQL 5.5) and import it into the schema (Oracle) or database (MySQL) that you wish to use for NAMES.

For security reasons, it is recommended to use a separate database user for NAMES. This database user should have all permissions on the corresponding schema/database, except table create/drop privileges, as these are not required for normal operation. Database import operations, and later database upgrades, where necessary when upgrading NAMES, can be carried out with a privileged user that can create, alter and drop tables.

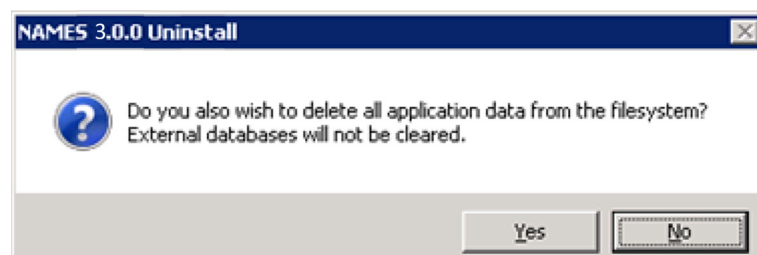
After setting up the database, the correct connection information must be provided to NAMES. See section 4.1.1 for further information about configuring NAMES database connectivity.

## 3.4 Uninstalling

If required, NAMES can be uninstalled by selecting the „Uninstall“ option from the „Start Menu“ folder selected or created during installation (default: NovaTec\NAMES). After starting the uninstaller, you are first prompted to confirm that you really wish to uninstall NAMES:



After selecting „Yes“, the uninstaller will ask you whether you also wish to remove the data folder, which contains logs, templates and the embedded database, which, if in use, will contain all NAMES runtime data such as configured targets, system configurations etc.. These files will be irrevocably deleted if you select „Yes“, so ensure that you have made a backup of these files if you wish to have access to the data at a later point of time:



The uninstaller also reminds you that, should you be using an external database, you will need to drop any data from this database manually. The uninstaller will then proceed to remove the installed files, services, registry settings and shortcuts from the system. Should any files remain in the installation folder (user created files such as Java key stores, backup copies of configuration files etc.) after the uninstallation is completed, the uninstaller will list them and ask you whether you want these files to be removed as well.

After successfully removing NAMES from the system, the uninstaller will show a confirmation screen:



The uninstallation has now been completed.



## 4 Configuration

### 4.1 NAMES configuration file

The main configuration file for NAMES is the file `names.properties` in the installation folder (default: `C:\Program Files\NovaTec\NAMES`). This file contains configuration settings for the NAMES database, for the embedded web server and for the Java Runtime Environment, as well as some other important start up settings.

The configuration file contains extensive commentary, including the default settings for each setting.

#### 4.1.1 Database configuration

If using the embedded database (the default), no further configuration is necessary. To switch back to the embedded database after using an external database, simply comment out all the database configuration directives by prefixing them with a hash mark (#).

To use an external database, the correct connection settings for the database in use must be made. To do this, uncomment the corresponding lines and replace the default setting with the setting you want to change it to.

##### 4.1.1.1 Oracle DB 11g

To configure the Oracle DB 11g connection, make the following configuration settings:

```
database_type = oracle
database_url = jdbc:oracle:thin:@<Hostname/Address>:<Port>:<System Identifier>
database_username = <Username>
database_password = <Password>
database_schema = <Schema>
```

Replace the placeholder text in above example with the corresponding information for your Oracle database. For example, if you are running a database on the server with the hostname `oracle` on the port `1521` with the System Identifier (SID) `ORCL`, and you have prepared a user with the name `names` and password `secret`, using their own schema, configuration should be as follows:

```
database_type = oracle
database_url = jdbc:oracle:thin:@oracle:1521:ORCL
database_username = names
database_password = secret
database_schema = NAMES
```

NAMES will automatically transform the schema name into uppercase internally, as required by Oracle DB 11g. You may therefore also enter the schema name in lowercase, however entering it in uppercase is recommended for consistency.

##### 4.1.1.2 MySQL 5.5

To configure the MySQL 5.5 connection, make the following configuration settings:

```
database_type = mysql
database_url = jdbc:mysql://<Hostname/Address>:<Port>/<Database>
database_username = <Username>
```



```
database_password = <Password>
database_schema = <Database>
```

Replace the placeholder text in above example with the corresponding information for your MySQL database. Please note that MySQL uses the terms „database“ and „schema“ interchangeably. For example, if you are running a database on the server with the hostname `mysql` on the port `3306`, have created a database with the name `namesdb` and prepared a user with name `names` and password `secret` and read/write access to this database, configuration should be as follows:

```
database_type = mysql
database_url = jdbc:mysql://mysql:3306/namesdb
database_username = names
database_password = secret
database_schema = namesdb
```

### 4.1.2 Web server configuration

The embedded web server need not be configured if you wish to run it in the default unsecured HTTP mode on the default port of `80`. If you wish to enable HTTPS or use a non-standard port, you have to configure the webserver.

#### 4.1.2.1 Changing the listen port

If you simply wish to change the port used for incoming connections from the default `80`, make the following setting:

```
webserver.port = <Port>
```

Replace `<Port>` with the port number you wish to use. Setting the port to `0` will cause NAMES to use the default port, depending on whether HTTPS is configured or not.

NAMES will listen on all available network interfaces.

#### 4.1.2.2 Using secure mode (HTTPS)

In order to secure the web UI of NAMES, you must first generate a pair of keys and acquire a certificate for your webserver. The key and certificate must then be placed in a Java key store with the name `keystore.jks`, while the root certificate of the issuing PKI as well as any other trusted root certificates must be placed in a key store with the name `truststore.jks` in the NAMES installation folder.

How to generate the key and acquire the certificates depends on your PKI and security policies and is beyond the scope of this document. If in doubt, please consult with your resident security expert.

The key stores may be created and populated with any appropriate tool, including the Java key tool contained in the standard JRE distribution and graphical tools such as the free KeyStore Explorer. When importing the private key, ensure that the password for the key and the key store password are identical and that only one key and certificate pair is contained in the key store.

Once the `keystore.jks` files have been placed in the installation folder make the following settings:

```
webserver.secure = 1
webserver.keystore_password = <keystore.jks Password>
```

The NAMES web server will now run on port `443` by default, which is the well-known port for HTTPS. If you wish to use a non-standard port instead, configure a different port as described above.



## 4.1.3 Miscellaneous configuration

### 4.1.3.1 Storage path

The storage path is the path to the data folder. During installation, this is automatically set to the path you selected; changing this is only necessary if you decide to move your data folder. To move your data folder, stop the NAMES service, move the data folder to its new location, set the `storage_path` setting to the new location and restart NAMES.

### 4.1.3.2 Maximum Java heap size

Depending on the size of your installation and how you use NAMES, a large amount of memory may be required. By default, the maximum heap size of NAMES is limited to 512 MB, which is sufficient for most small to medium installations, but may cause out-of-memory conditions for certain memory-intensive operations (mainly XML imports with embedded base64-encoded binaries such as configurations, firmware etc.).

To allow NAMES to use more memory, change the `memsize` setting. For example, to allow NAMES to use up to 1GB of Java heap memory, make the following setting:

```
memsize = 1G
```

Note that the actual Java process size will exceed the configured limit, as memory for other parts of the Java virtual machine is also needed; the heap size is the main determining factor for the Java process size. NAMES will normally start with a lower process size, but will grow, possibly up to the limit, during use.

### 4.1.3.3 Target monitoring alert time

NAMES monitors the target systems using regular time events sent by the systems. You can configure how many time events a system is allowed to miss before it is considered offline and a SNMP trap is generated. It is recommended to set this to two or even three, as time events may be delayed on occasion. To configure the maximum number of missed time events, make the following setting:

```
max_missed_timeevents = <Number of Max Missed Time Events>
```

## 4.2 Logging configuration file

Configuration for the logging system (`log4j`) is stored in the file `log4j.properties`. The settings in this file apply to the NAMES error and debugging log as well as the accounting log. It is possible to configure log levels for various NAMES components as well as which appenders (log sinks; anything from a simple file appender through to a remote logging server) these logs should be sent to.

In default post-installation configuration, all modules are set to log level „WARN“ and full accounting logs are active. The log files `names-log4j.log` and `accounting.log` in the subfolder `log` of the NAMES data folder, as chosen during installation, are used as output.

For more complex configurations, please refer to `log4j` documentation or consult with NovaTec.

**Warning:** Setting some modules to `DEBUG` or even `TRACE` log levels will produce very large amounts of log information which may slow execution speed to a point where normal operation is not possible. These log levels should only be set if requested by a NovaTec service technician for troubleshooting purposes.





## 4.3 Firewall settings

If using a firewall on the host on which NAMES is installed (the Windows Firewall is enabled by default) or on another system between the NAMES server and the client PCs, a firewall exception has to be configured. At the least, an exception allowing incoming connections to the configured NAMES web UI port (80 by default) has to be present. Additional firewall exceptions are required for incoming connections to configured CallHome Servers (see section **Fehler! Verweisquelle konnte nicht gefunden werden.**).

It might also be necessary to configure firewall exceptions for connections originating from NAMES and going to the target devices.

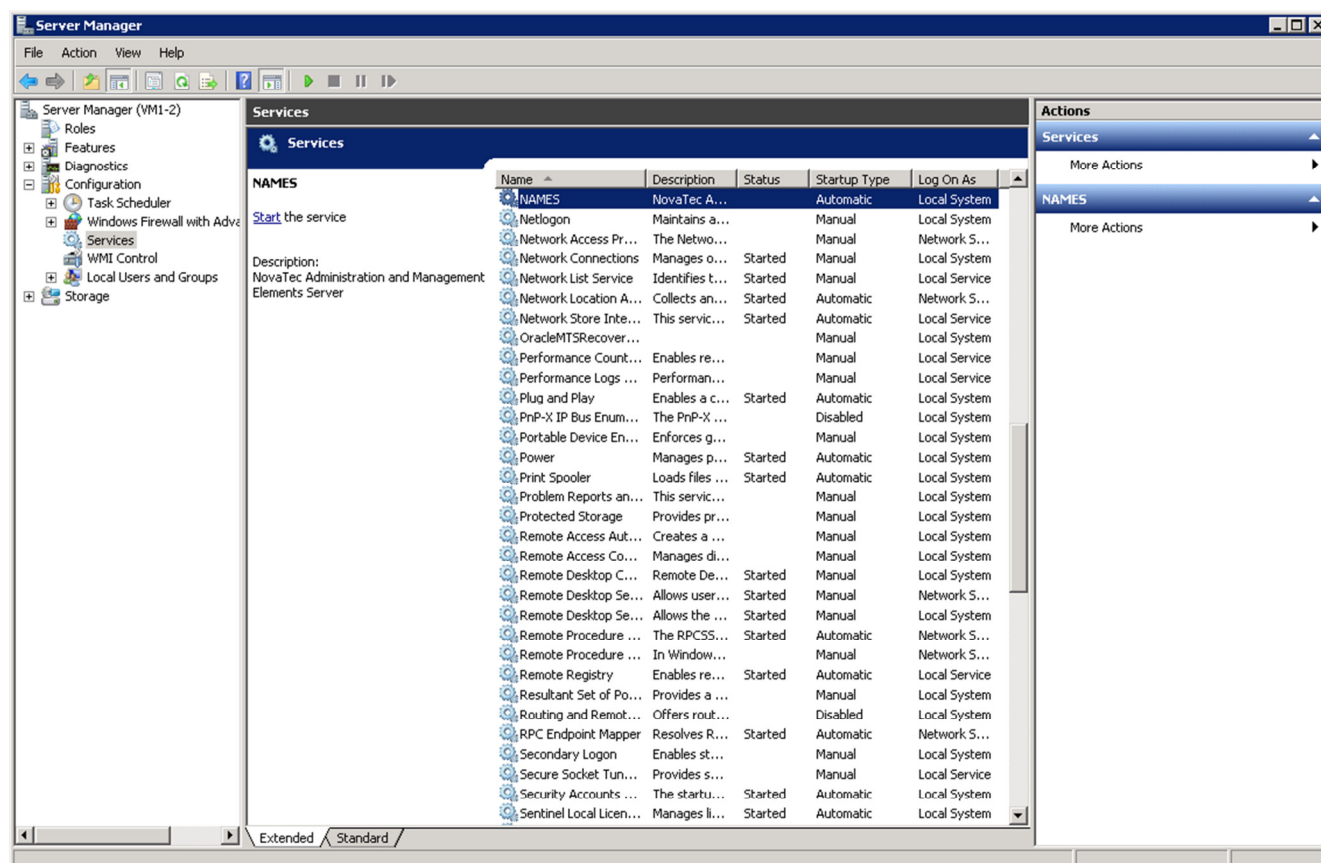
How these exceptions are configured depends on the firewall product(s) you are using and the structure of your network; further explanation is beyond the scope of this document. For default port numbers, please refer to the document „IP Port Matrix“, which is available on NovaTec’s website under download/handbooks (<http://www.novatec.de/cms/en/Downloads/Downloadarea.html>).

## 5 Administration

### 5.1 Starting NAMES

NAMES is installed as a service. This means that it is not started like a normal application, but is managed by the system. During installation, NAMES is configured to run automatically at system start-up, so you will normally not need to explicitly start NAMES. However, if you have just installed NAMES and a condition occurs which prevents NAMES from running (such as the database being unavailable) or you manually shut NAMES down, you will have to start NAMES manually.

To do this, you should generally use the Server Manager UI, where you can find the item „Services“ under „Configuration“:



Select the NAMES service from the list and click the „Start“ link. Please note that, though the start-up progress window appears only briefly, at that point of time only the Java Virtual Machine has been started, the start-up process of the actual application is still ongoing. It will take a little longer – up to a minute or two – until the NAMES web UI is available.

### 5.2 First login

To log in to the NAMES web GUI open your browser and navigate to the address where NAMES is installed. You will be asked for your login data:

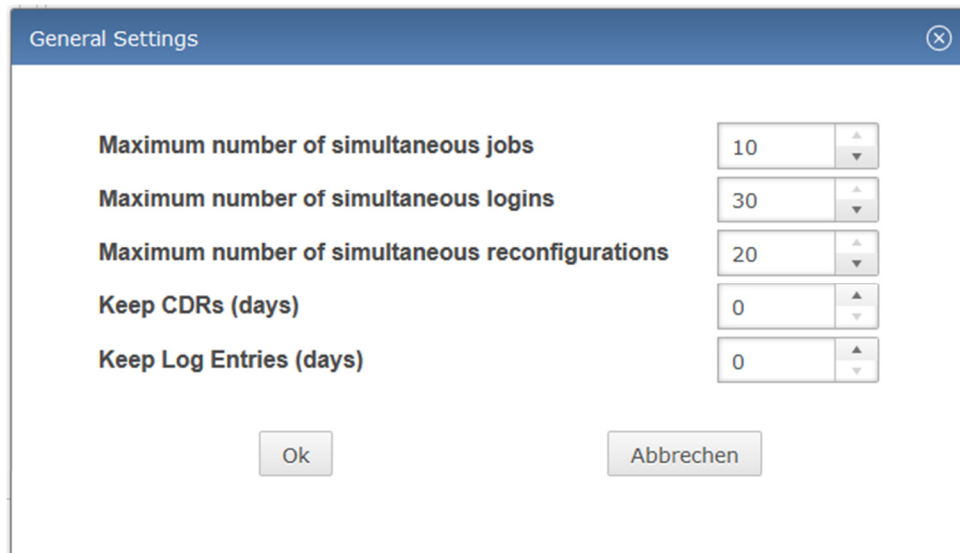
Name	<input type="text" value="names"/>
Password	<input type="password" value="....."/>
	<input type="button" value="Login"/>

After database installation, a single administrative user with name `names` and password `names` is present. Use this login data when logging in to NAMES for the first time.

After logging in, it is recommended to immediately change the `names` user's password as described in section 6.7 below.

## 5.3 General settings

In the „General Settings“ dialogue, you can set a number of miscellaneous parameters:



The dialog box titled "General Settings" contains five settings, each with a text label and a numeric input field with up/down arrows:

Maximum number of simultaneous jobs	10
Maximum number of simultaneous logins	30
Maximum number of simultaneous reconfigurations	20
Keep CDRs (days)	0
Keep Log Entries (days)	0

At the bottom are two buttons: "Ok" and "Abbrechen".

### 5.3.1 Maximum number of simultaneous jobs

This setting specifies how many jobs NAMES may run at the same time. The maximum setting is currently limited to ten simultaneous jobs. You may wish to reduce this if bandwidth limitations lead to poor performance or you want to reduce NAMES bandwidth usage.

### 5.3.2 Maximum number of simultaneous logins

This setting specifies how many users may use the NAMES web UI at the same time. The default is 30 (the maximum setting available), but it can be reduced if server performance is not sufficient with that number of simultaneous users.

### 5.3.3 Maximum number of simultaneous reconfigurations

This setting refers to the reconfiguration feature of NAMES, which allows other applications to use NAMES' SOAP interface to reconfigure specific settings on a target. Full documentation on this feature is available on request.



### 5.3.4 Keep CDRs

This setting controls how long CDRs are kept before being automatically deleted from the database. The default setting is 0, which means „never delete CDRs“. If you are regularly downloading CDRs from your systems, especially if using automated CDR downloads, it is recommended to ensure that CDRs are regularly removed from the database. This may be accomplished through an external mechanism, e.g. if you wish to archive old CDRs, or through NAMES' automated deletion system.

If this setting is set to any number larger than 0, NAMES will regularly delete any CDRs that are older than this number of days.

### 5.3.5 Keep log entries

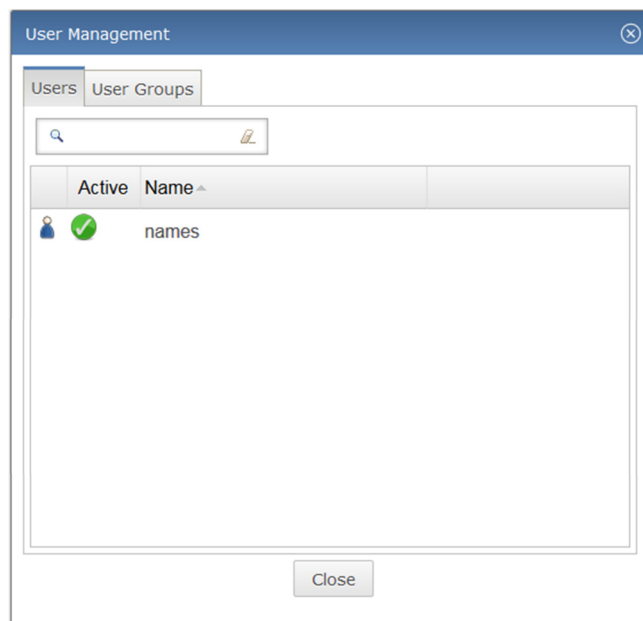
This setting is the equivalent to „Keep CDRs“, except it applies to system logs which have been downloaded from the targets. These logs are saved in the NAMES database and, similarly to CDRs, will need to be deleted on occasion. The default setting is also 0.

## 5.4 User management

NAMES has an integrated user management system, which is the base for the AAA (authentication, authorisation and accounting) system. You can create users, assign them to groups, assign roles (more on roles in section 5.5) to users or groups and disable users. Users cannot be deleted or renamed, as this can lead to ambiguity or lack of traceability in the accounting logs.

**The paid version of NAMES 3.0 allows the creation of multiple users and user groups. In the free version of NAMES 3.0 only the default admin user „names“ is available.**

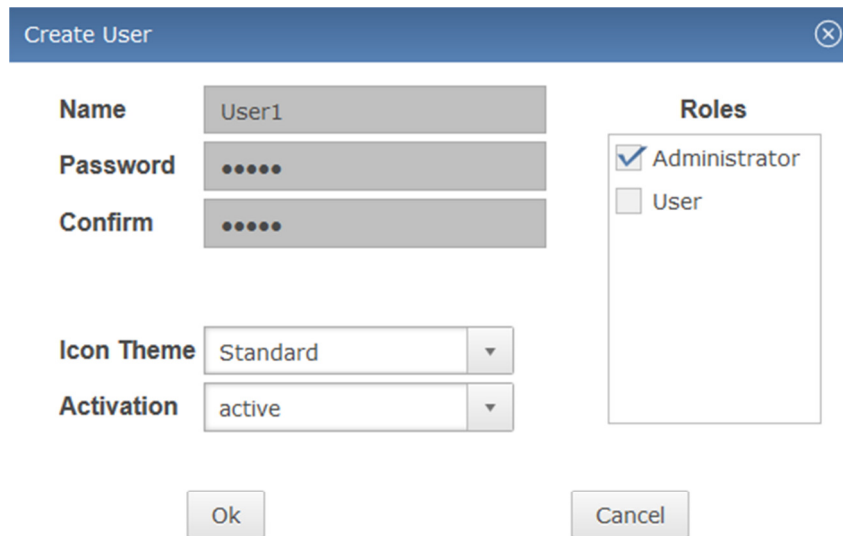
The User Management UI is available from the maintenance menu:



### 5.4.1 Users

#### 5.4.1.1 Creating a user

To create a user, right-click in the user table to bring up the context menu, and select „Create“. The user creation dialogue is displayed:



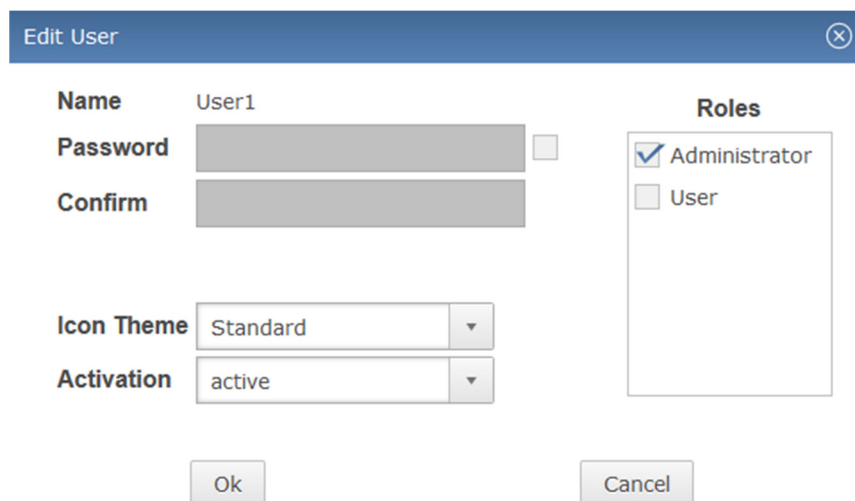
The 'Create User' dialog box has a blue header bar with the title 'Create User' and a close button. It contains several input fields: 'Name' with the value 'User1', 'Password' and 'Confirm' fields both showing five dots, 'Icon Theme' with a dropdown menu set to 'Standard', and 'Activation' with a dropdown menu set to 'active'. To the right, under the 'Roles' section, there are two checkboxes: 'Administrator' (checked) and 'User' (unchecked). At the bottom, there are 'Ok' and 'Cancel' buttons.

Some changes may require a re-login for activation.

You must enter a user name and initial password for the new user. You can also explicitly assign a role to the user at this stage, though this is not required. Changing the „Activation“ setting allows you to create users that are disabled, for example to reserve a certain user name.

#### 5.4.1.2 Editing a user

To edit a user, right-click the user in the User Management UI and select „Edit“ from the context menu. The user edit dialogue is displayed:



The 'Edit User' dialog box has a blue header bar with the title 'Edit User' and a close button. It contains several input fields: 'Name' with the value 'User1', 'Password' and 'Confirm' fields both showing five dots, and a small square checkbox to the right of the 'Password' field. 'Icon Theme' has a dropdown menu set to 'Standard', and 'Activation' has a dropdown menu set to 'active'. To the right, under the 'Roles' section, there are two checkboxes: 'Administrator' (checked) and 'User' (unchecked). At the bottom, there are 'Ok' and 'Cancel' buttons.

Some changes may require a re-login for activation.

The user edit dialogue allows an administrator to change all the settings that were previously set in the user creation dialogue. To change a user's password, the checkbox next to the password entry field must be checked. Typing into the password field will automatically check the box. For security reasons, the password field will always be blank when the dialogue loads.

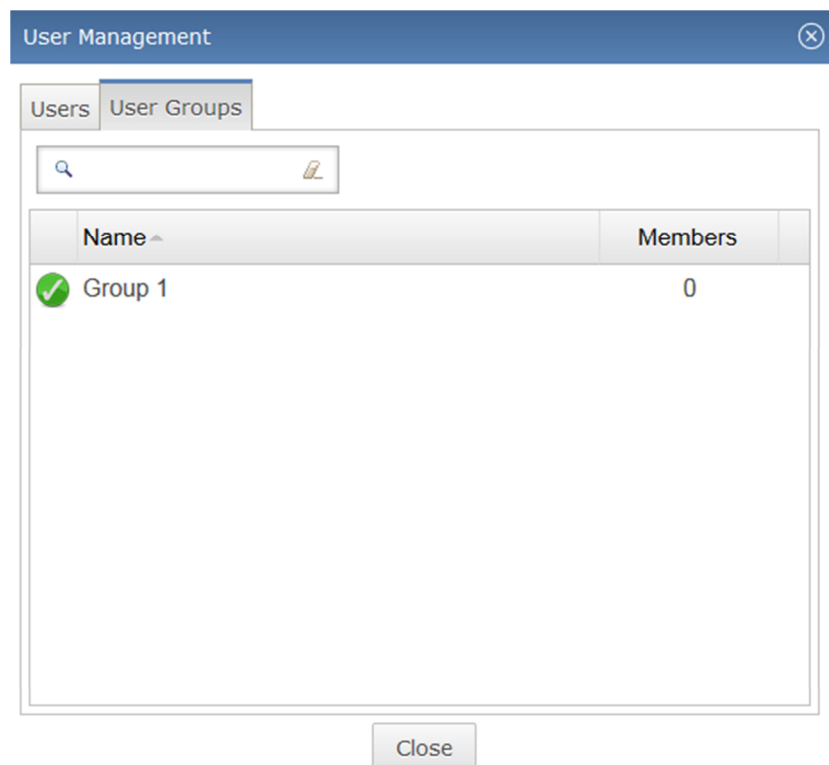
### 5.4.1.3 Disabling/Enabling a user

Users may be disabled and will then no longer be able to log in to NAMES. This is achieved by editing the user (see 5.4.1.2) and setting the activation status to „inactive“. To re-enable the user, set the activation status back to „active“.

## 5.4.2 User groups

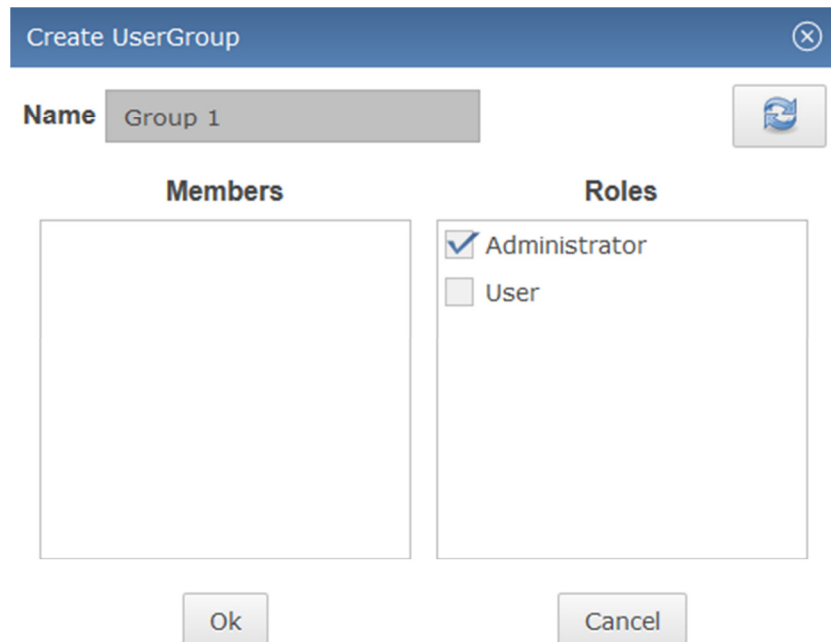
User groups are an entirely optional element of user management. If you wish, you can assign your users to certain user groups. Users will inherit any roles assigned to their groups.

User groups are managed through the User Management UI, which is opened by clicking on „User Management“ in the „Maintenance“ menu. Switching to the second tab in the User Management UI displays the User Group UI:



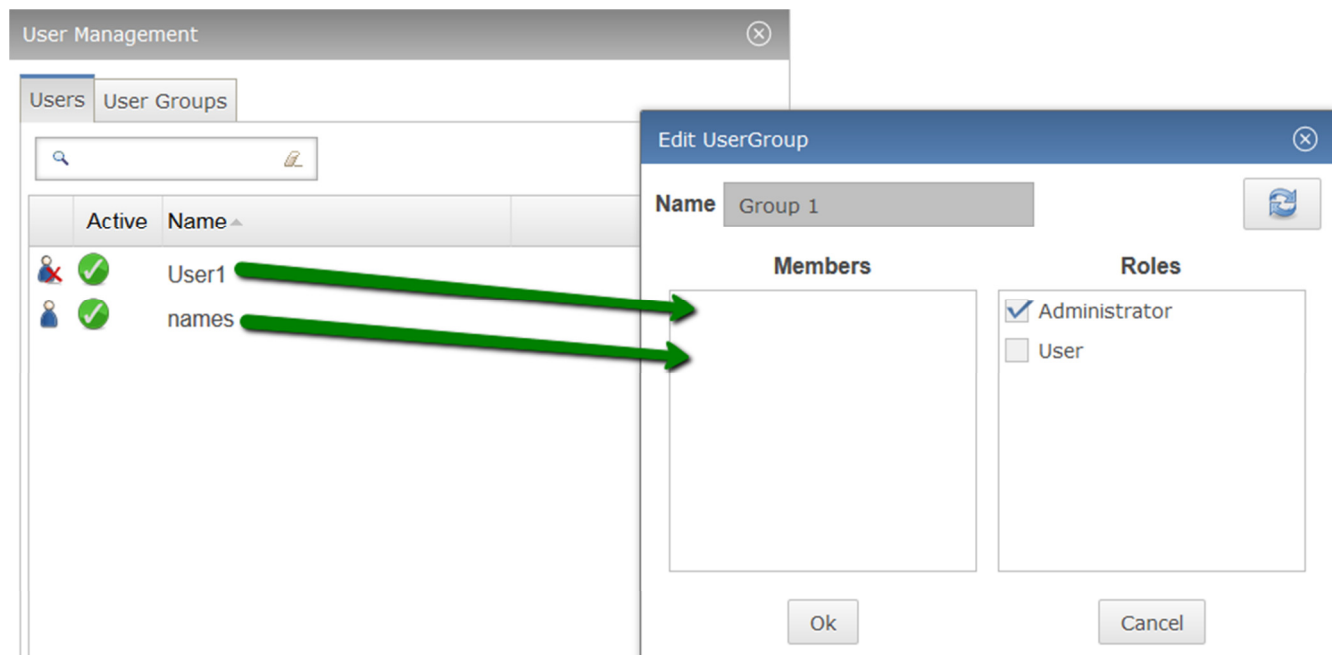
### 5.4.2.1 Creating a user group

To create a user group, right-click in the user group table and select „Create“. The group creation dialogue is displayed:



The 'Create UserGroup' dialog box has a title bar with a close button. It contains a 'Name' field with the text 'Group 1' and a refresh icon to its right. Below the name field are two columns: 'Members' (an empty box) and 'Roles' (a list with 'Administrator' checked and 'User' unchecked). At the bottom are 'Ok' and 'Cancel' buttons.

You must enter a name for the new group. Roles can be assigned as needed. Members can be assigned to the group through drag and drop from the User Management UI:



The 'User Management' window shows a 'Users' tab with a table of users. The table has columns 'Active' and 'Name'. Two users are listed: 'User1' and 'names', both with active status icons. Two green arrows point from the 'User1' and 'names' rows to the 'Members' box in the 'Edit UserGroup' dialog box, which is overlaid on the right side of the window. The dialog box is identical to the 'Create UserGroup' dialog, showing 'Group 1' as the name and 'Administrator' as the selected role.

Click OK to save the group.

#### 5.4.2.2 Editing a user group

The name, members and roles of a user group can be edited by right-clicking the user group in the list and selecting „Edit“ from the context menu.

#### 5.4.2.3 Deleting a user group

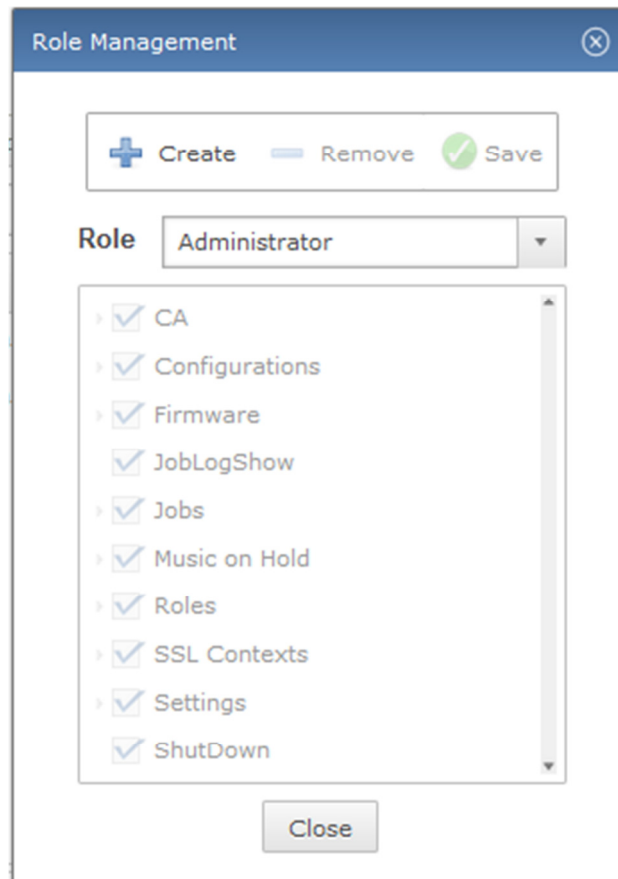
To delete a user group, right-click the group in the list and select „Delete“. You will be prompted to confirm deletion. Once confirmed, any users inheriting roles from the group will lose those roles.



## 5.5 Role management

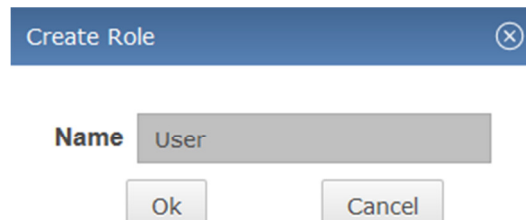
In NAMES, a role is defined as a collection of individual permissions that can be assigned to a user or user group. The default role „Administrator“ has all permissions and cannot be deleted. Additional roles with reduced permissions may freely be defined.

To open the Role Management GUI, select „Role Management“ from the „Maintenance“ menu:



### 5.5.1 Creating a role

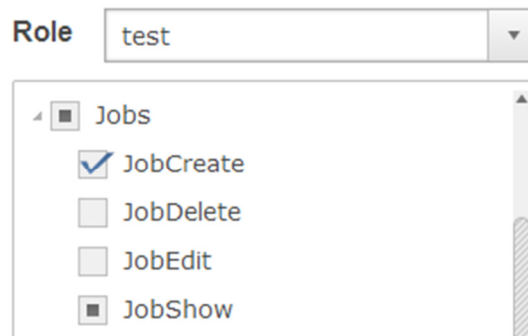
To create a role, click the „Create“ button. The role creation dialogue is displayed:



Enter a name for the role and click „OK“. The role is created.

## 5.5.2 Assigning permissions to a role

To assign permissions to a role, select the role you wish to modify from the „Role“ combo box. The currently assigned permissions are displayed in a tree structure, with different permissions (create, read, update, delete) for the same object type collected under a common heading:



The checkboxes are tri-state, and the meaning differs slightly between permissions and group headings:

- ☐ The permission is not granted / no permissions are granted.
- ☒ The permission is granted / all permissions are granted.
- ☐ The permission is implicitly granted / some permissions are granted.

Implicit permissions result when a permission that is explicitly granted requires another permission to work properly. In the above example, to be able to create a job, you must also be able to view the job list.

After adjusting the permissions as required, click the „Save“ button to persist your changes.

## 5.5.3 Deleting a role

To delete a role, select the role you wish to remove from the combo box and click the „Remove“ button. You will be prompted to confirm the deletion.

## 5.6 SNMP configuration

NAMES can send SNMP traps/notifications to a network monitoring tool to alert you about various events and conditions, ranging from NAMES start up and shutdown through loss of database connectivity to various target events (CallHome Events) which are mapped to SNMP.

In order to send SNMP traps to your monitoring tool, the correct settings must be configured in the „SNMP Configuration“ dialogue available from the „Maintenance“ menu:



SNMP Settings ✕

✓ Save Settings 🔄 Send Test Trap

Version	Version 1 ▾
IP Address	127.0.0.1
Port	162 ▲ ▾
Community	public
Send Inform	<input type="checkbox"/>
Security Level	No Auth / No Privacy ▾
User Name	user
Password	
Auth Protocol	SHA-1 ▾
Privacy Protocol	AES-256 ▾
Receiver Engine ID	

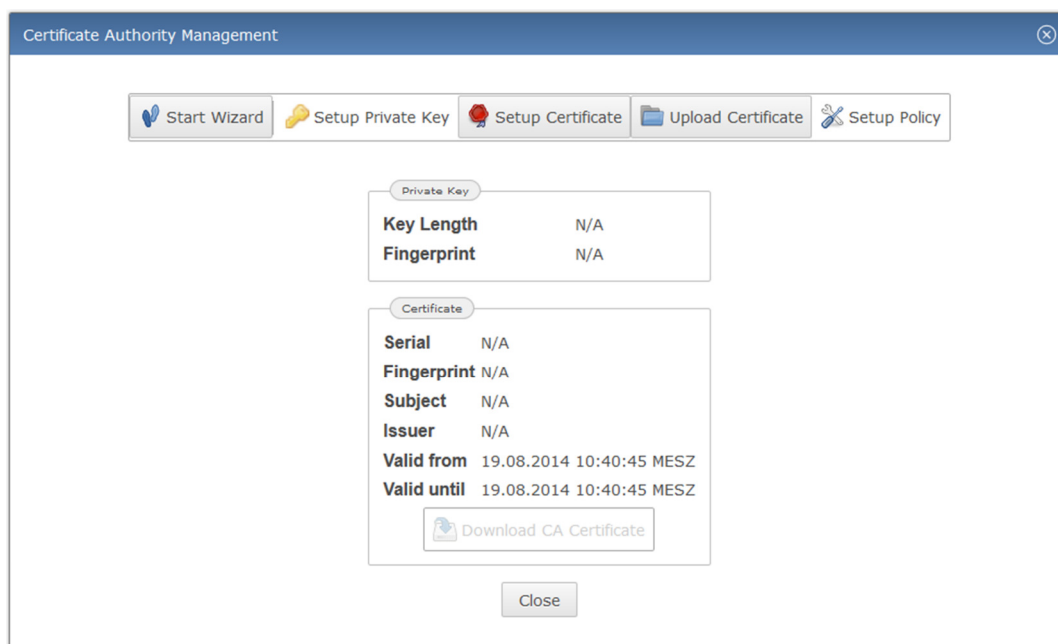
Close

The settings should be configured to match the network monitoring system in use. Some settings are enabled and disabled depending on other settings, primarily the SNMP version, as not all settings are required or supported for all versions.

## 5.7 Certificate Authority configuration

To use the „Sign Certificates“ job to provide a TLS-enabled target with the certificates required for secured operation, the integrated NAMES certificate authority must first be configured properly. Properly configuring both the targets and NAMES for TLS-secured operation requires a working knowledge of asymmetric encryption, PKIs and TLS. Providing this is outside the scope of this document; it is recommended that administrators acquire this knowledge from other sources.

To configure the built-in certificate authority (key, certificate, signing policy) open the „Certificate Authority“ dialogue from the „Maintenance“ menu:

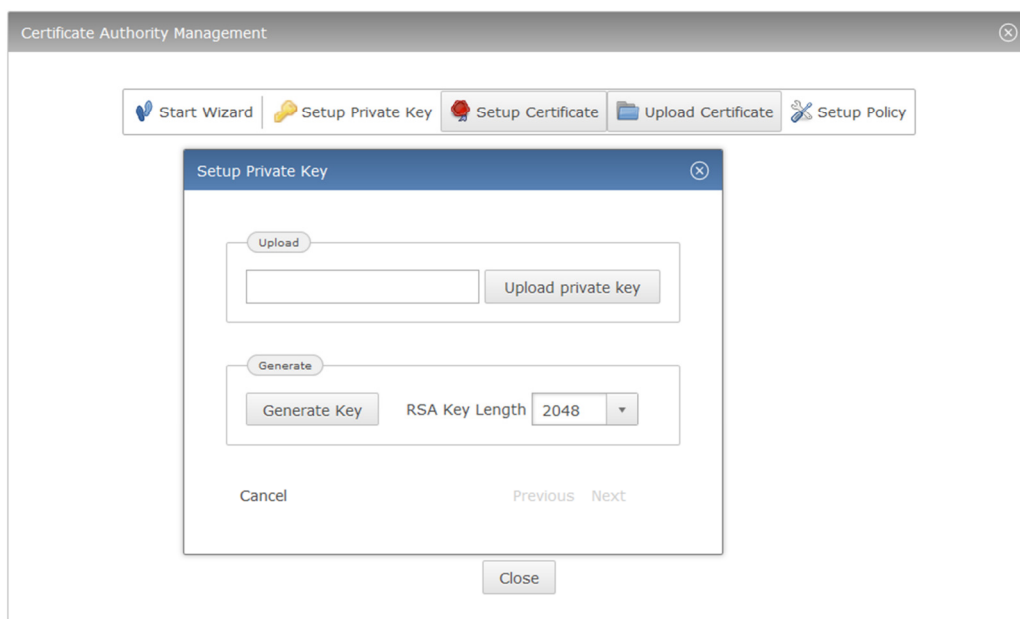


This dialogue shows information about the currently configured RSA key and matching certificate. To begin configuring the certificate authority, either click the „Start Wizard” button to be guided through the configuration, or use the other buttons to directly open the section you wish to configure. In the following description screenshots from the wizard mode will be used, the resulting dialogues are however identical to the individually selected dialogues except for the buttons at the bottom.

There are a number of different ways to configure your certificate authority, both with regards to how key and certificate material is acquired and whether NAMES is integrated into an existing PKI or is configured as a root certificate authority.

### 5.7.1 General configuration procedure

In all scenarios, the certificate authority key and certificate as well as signing policy must be configured. The first step is always to configure the key:



The key can either be uploaded in the form of an unencrypted PEM-encoded RSA key, or generated by NAMES. When generating a key, you can select a key length of 1024, 2048 or 4096 bits. Depending on the selected length of the key and random chance, generation of an appropriate key may take some time.

After configuring the key, a matching certificate has to be configured. For details of how to configure the certificate, see sections 5.7.2 to 5.7.4.

Finally you have to configure the signing policy. The signing policy determines both: Which distinguished names the certificate authority will accept in a certificate signing request and for how many days the issued certificates will be valid.



Setup Policy

Policy

Email	<input type="radio"/> Match	<input type="radio"/> Supplied	<input checked="" type="radio"/> Ignore
Common name	<input type="radio"/> Match	<input checked="" type="radio"/> Supplied	<input type="radio"/> Ignore
Country name	<input type="radio"/> Match	<input type="radio"/> Supplied	<input checked="" type="radio"/> Ignore
State/Province	<input type="radio"/> Match	<input type="radio"/> Supplied	<input checked="" type="radio"/> Ignore
Locality name	<input type="radio"/> Match	<input type="radio"/> Supplied	<input checked="" type="radio"/> Ignore
Organization name	<input checked="" type="radio"/> Match	<input type="radio"/> Supplied	<input type="radio"/> Ignore
Organizational unit	<input type="radio"/> Match	<input type="radio"/> Supplied	<input checked="" type="radio"/> Ignore

Policy

Client validity (days)

720

Apply Settings

Close

For each distinguished name component, it can be specified whether the value in the request has to **match** the corresponding value in the certificate authority's certificate, simply be **supplied** but can have any value or is completely **ignored** and thus may also be unset.

### 5.7.2 Configuring NAMES as a Root CA

The simplest way to configure NAMES is as a Root CA. Begin by generating a RSA key and then generate a self-signed certificate. To do this, you will need to enter the distinguished name of the certificate authority you are setting up in the „Setup Certificate“ dialogue. Select how long the self-signed certificate should be valid and finally click the „Generate Self-Signed“ button:



Setup Certificate

Distinguished Name

Email

Common name

NAMES-CA

Country name

DE

State/Province

NRW

Locality name

PB

Organization name

NovaTec

Organizational unit

Labor

Certificate Signing Request

Download CSR

Self-Signed Certificate

Generate Self-Signed

Certificate Validity

730

Cancel

Previous

Next

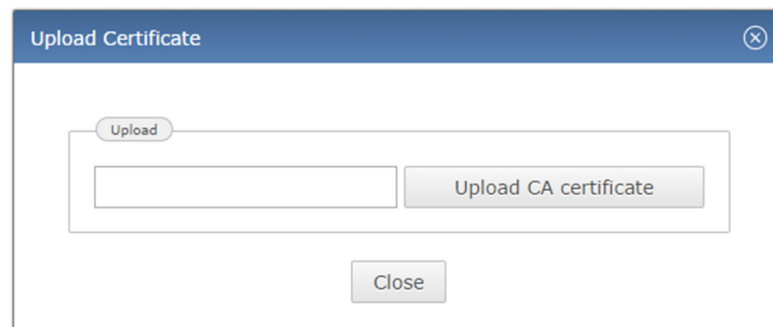
The generated certificate will be sent to your browser for use in other applications' trust stores. It can be re-downloaded later from the CA information dialogue. For security reasons, generated RSA keys cannot be downloaded from NAMES.

After configuring your policies as described above, your CA is ready to use. Please note that the NAMES CA can only be used to issue certificates to NovaTec devices, not to other devices or software tools. You will therefore need another CA to issue certificates to these and will have to configure trust relationships accordingly.

### 5.7.3 Configuring NAMES as a subordinate CA

When using NAMES with an existing PKI, it may be more convenient to configure it as a subordinate certificate authority under the existing hierarchy. To accomplish this, proceed as in section 5.7.2 above, but do not generate a self-signed certificate. Instead, click the „Download CSR“ button in the „Setup Certificate“ dialogue to generate a Certificate Signing Request.

This CSR then has to be submitted to the root or intermediate CA, under which the NAMES CA is to be inserted. A corresponding certificate has to be issued, taking care to include correct usage restrictions; appropriate information is contained in the CSR, but CA policy may discard the extension requests. Once the certificate has been issued, it has to be uploaded to NAMES through the „Upload Certificate“ dialogue, reached from the „Certificate Authority Management“ dialogue:



The certificate file has to contain the certificate with full verification chain in PEM-encoded format. After configuring signing policy, the certificate authority is ready for use.

#### 5.7.4 Configuring NAMES using an existing key and certificate

If an existing key and certificate are to be reused for NAMES, or key and certificate are to be generated externally, both can be uploaded to NAMES. First upload the key as explained in section 5.7.1, then upload the certificate as explained in section 5.7.3. You may need to convert existing files into the required formats (PEM-encoded, no encryption). Configure the policy and the certificate authority is ready for use.

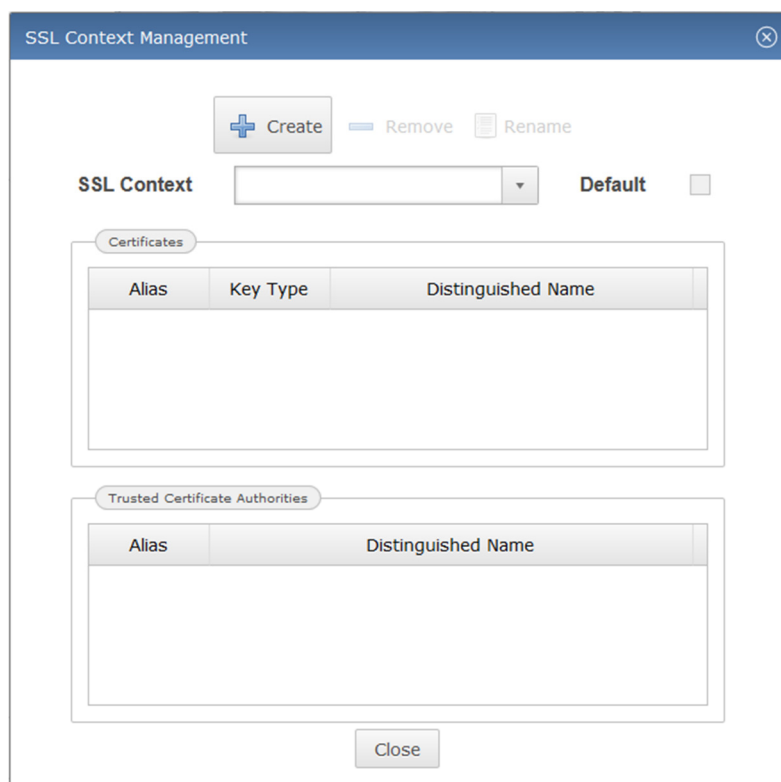
### 5.8 SSL contexts

In order for NAMES to communicate with targets configured for secure maintenance (TLS encrypted/authenticated MNT and/or CH connections), SSL Contexts must be configured. These contexts contain the RSA key used by NAMES, a corresponding certificate and a collection of certificates for all trusted Certificate Authorities. NAMES does not automatically trust its own CA, so you will need to add the certificate for the internal CA even if using NAMES to certify the targets.

You can have multiple SSL Contexts in use at the same time, for example when migrating from one PKI to another, or when using different PKIs for different network segments or clients. The SSL Contexts will later be assigned to specific targets or CallHome servers; a default SSL Context can also be selected.

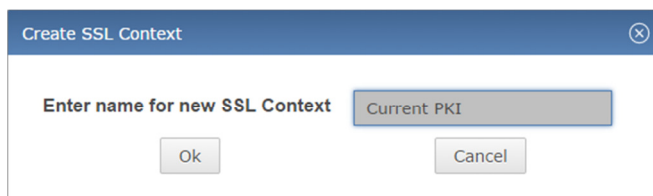
To begin configuring SSL Contexts, select „SSL Contexts“ from the „Gateway Management“ menu:





### 5.8.1 Creating an SSL context

To create a new SSL Context, click the „Create” button. Specify a descriptive name for the new context and click OK:



The new context will now appear in the „SSL Context” combo box and can be edited as described in section 5.8.2.

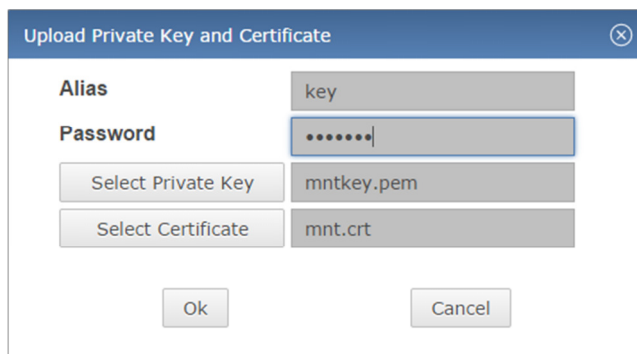
### 5.8.2 Editing an SSL context

Each SSL Context must contain exactly one entry in the „Certificates” table and at least one entry in the „Trusted Certificate Authorities” table. Multiple own certificates are supported in principle, however, as current firmware versions do not supply a list of trusted CAs during TLS handshake, NAMES cannot select an appropriate certificate. To ensure the correct one is used, only one should be configured at a time.

Warning: editing an existing context which is in use by one or more targets/CallHome servers may cause connections to these targets/servers to fail while changes are being made.

#### 5.8.2.1 Adding a private key and certificate

First, right-click in the „Certificates” table and select „Create” from the context menu. The „Upload Private Key and Certificate” dialogue is displayed:



Fill in a descriptive alias for the key pair and then select a private key file and a certificate file for upload. These files must contain an RSA private key and a corresponding certificate, both in PEM format. The certificate file should contain the entire certificate chain without the Root CA certificate if the signing Certificate Authority is not the Root CA. If the key is encrypted, you must also supply the correct password for decryption. Finally, click „OK“ to upload the files.

If the import process was successful an entry containing basic information about key and certificate will be displayed in the „Certificates“ table:

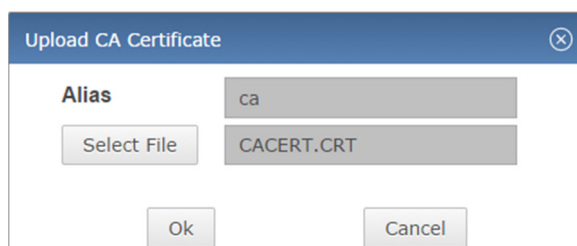
Certificates		
Alias	Key Type	Distinguished Name
key	RSA-1024	CN=MNT, OU=Entwicklung, O=NovaTec, I

### 5.8.2.2 Replacing a private key and certificate

To replace a private key and certificate for an SSL Context, you must first remove the current key and certificate. To do this right-click the entry in the „Certificates“ table and select „Remove“ from the context menu. After removing the current entry proceed as described above.

### 5.8.2.3 Adding a trusted certificate authority

You must add at least one entry to the „Trusted Certificate Authorities“ table. Multiple CAs may be added if necessary, for example if targets are signed by different CAs, but trust the same CA. To add a trusted certificate authority, right-click in the „Trusted Certificate Authorities“ table and select „Create“ from the context menu:



Fill in a descriptive alias (this must differ from any other alias used in the same context, including the alias for the „Certificates“ table entry) and select a PEM-encoded certificate for upload, then click OK.

If the import process was successful, an entry containing basic information about the certificate is displayed in the „Trusted Certificate Authorities“ table:

Trusted Certificate Authorities	
Alias	Distinguished Name
ca	C=DE, ST=NRW, L=Paderborn, O=NovaTec, OU=Entwic

#### 5.8.2.4 Removing a trusted certificate authority

To remove a trusted CA from the list, right-click it's entry in the table and select „Remove“ from the context menu.

#### 5.8.3 Setting an SSL context as default context

You may assign a „Default Context“, which means this SSL Context will be assigned as the context for newly created targets or CallHome servers by default. To choose the default context, simply select the context from the combo box and check the „Default“ check box.

#### 5.8.4 Removing an SSL context

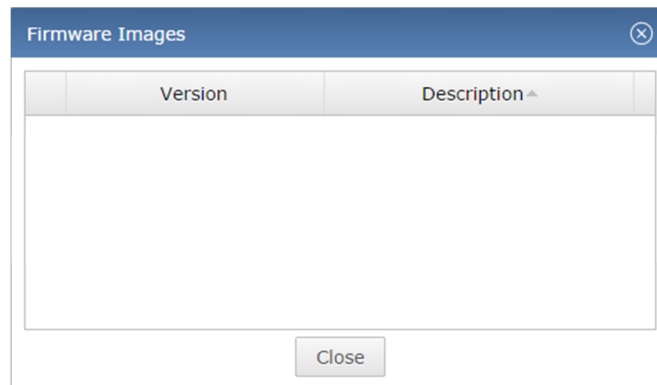
To remove an SSL Context, select the context you wish to remove from the combo box, than click the „Remove“ button at the top. If the „Remove“ button is greyed out, the context is in use and cannot currently be removed. You must first remove the context from any targets and CallHome servers that may be using it.

### 5.9 Managing firmware images, music on hold files and Licence Manager

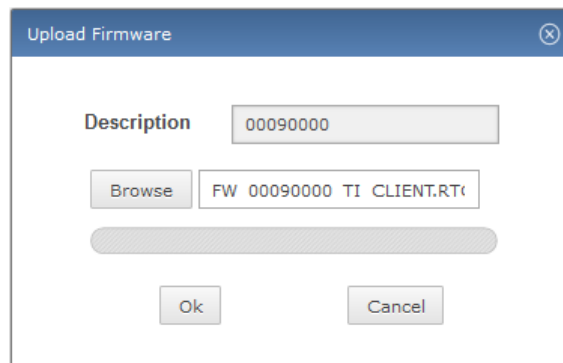
For certain operations binary files need to be uploaded to NAMES first. Specifically these are firmware images, Music on Hold files and licence files.

#### 5.9.1 Firmware images

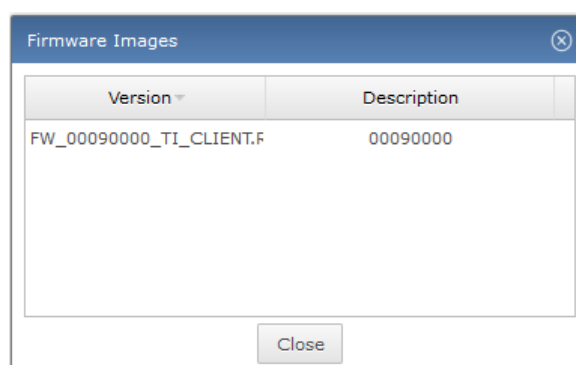
Firmware images are managed through the „Firmware Images“ window, which can be opened from the „Gateway Management“ menu:



To add a firmware image to NAMES for use in „Upload Firmware” jobs, right-click in the table and select „Upload” from the context menu. The „Upload Firmware” dialogue opens. Specify a description for the firmware (for example, the version of the firmware you are uploading) and select the firmware image you wish to upload:



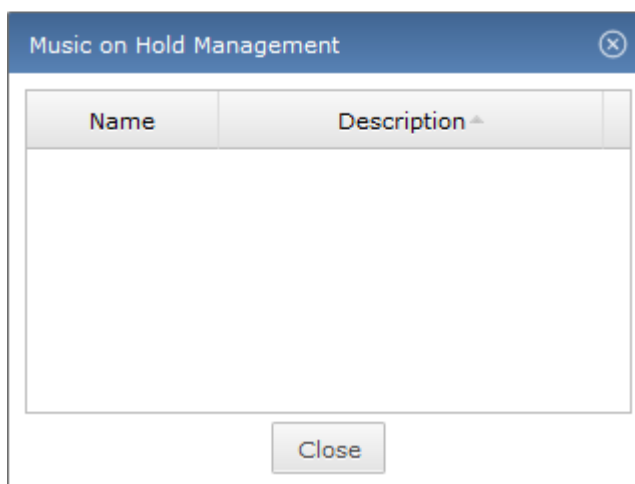
After clicking „OK”, the firmware image will be sent to the NAMES server and stored in the database. It is displayed in the table:



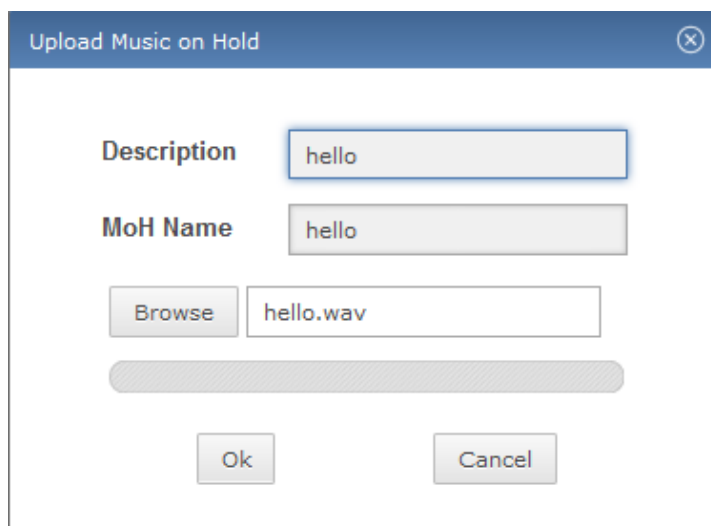
To remove a firmware image from NAMES, right-click the entry in the table and select „Delete”, then confirm the deletion in the following dialogue.

### 5.9.2 Music on Hold

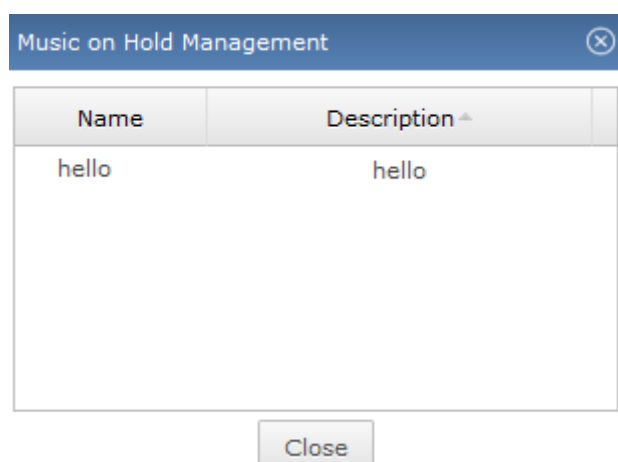
Music on Hold files are managed through the „Music on Hold Management” window, accessible from the „Gateway Management” menu:



To upload a Music on Hold file, right-click and select "Upload".



After entering a description, which can be any text, and selecting the desired music file, click „OK“ to upload the file to NAMES. If the music file is in the correct format (see NovaTec Configuration utility for further details), the file is imported and a new entry appears in the table:

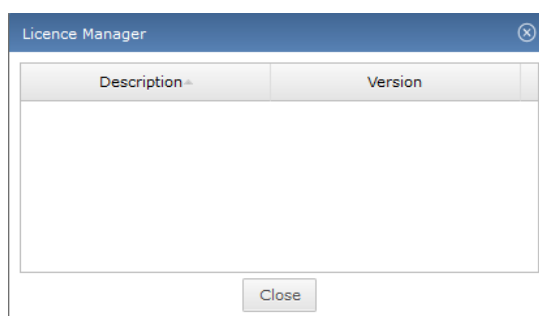


The Music on Hold is now ready for use.

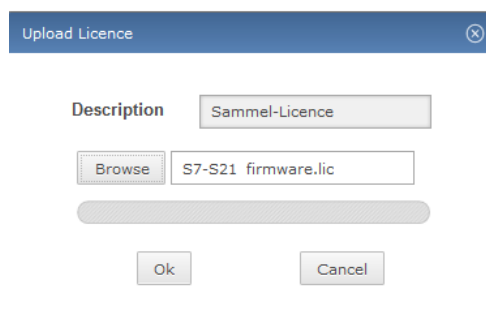
To remove a Music on Hold file from the database, right-click the entry in the table and select „Delete“, then confirm deletion in the following dialogue.

### 5.9.3 Licence Manager

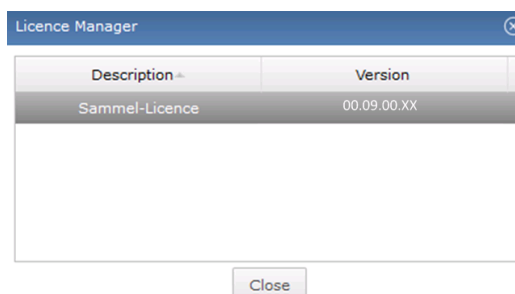
Licenses are managed through the „Licence Manager“ window, which can be opened from the „Gateway Management“ menu:



To add a licence to NAMES for use in „Upload Licence“ jobs, right-click in the table and select „Upload“ from the context menu. The „Upload Licence“ dialogue opens. Specify a description for the licence and select the licence you wish to upload:



After clicking „OK“, the licence will be sent to the NAMES server and stored in the database. It is displayed in the table:



To remove a licence from NAMES, right-click the entry in the table and select „Delete“, then confirm the deletion in the following dialogue.



NAMES will automatically select a licence for use with a device and include it in the configuration. The licence is selected from those available by the device MAC address, the version of the currently installed firmware, whether the number of licenced channels supports the configured amount, and finally by the amount of features licenced.

## 5.10 Shutting NAMES down

To shut NAMES down, you have several options. From the web UI, you can shut NAMES down „gracefully“, which means that no more jobs will be started and the program will exit after all running jobs have been completed, or immediately, which means that any running jobs will be aborted.

To shut down NAMES, select „Server Shutdown“ from the „Maintenance“ menu. The shutdown dialogue will appear:



The „Graceful shutdown“ option is checked by default. To perform an immediate shutdown, aborting all running jobs, deselect the option. After clicking „Yes“, NAMES will shut down either immediately or after all running jobs have finished. As this action also shuts down the embedded web server, no further feedback is provided. The web UI will report that it has lost its connection to the server.

You can also shut down NAMES from the Windows Server Manager UI. This should however only be done as a last resort, if a shutdown through the web UI is not possible.



## 6 Usage

### 6.1 Provisioning

This chapter describes how to provision NovaTec systems with the NAMES 3.0 software. Only CCU4 and later systems are supported.

All NovaTec systems are configured to use DHCP by default. After hardware assembly and initial system boot, the system will query DHCP. The response must contain option 129 with the IP address of the NAMES server. The default host name of the system is "novatec<MAC Address>" (e.g. "novatec8058C5000123").

If the DHCP query is successful, the device will attempt to connect to NAMES. Depending on the NAMES security settings, a new entry may be created if the device is unknown, using the System ID (either the CCU serial number or the backplane ID) as its name.

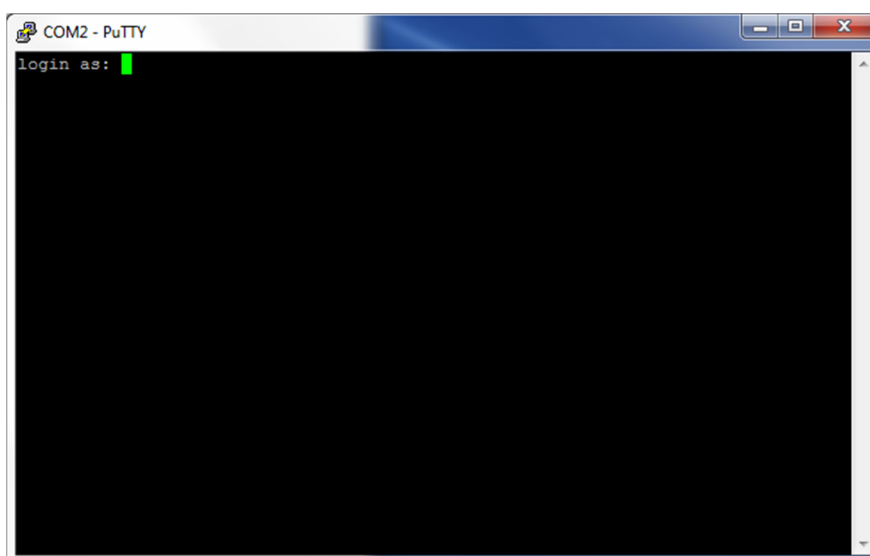
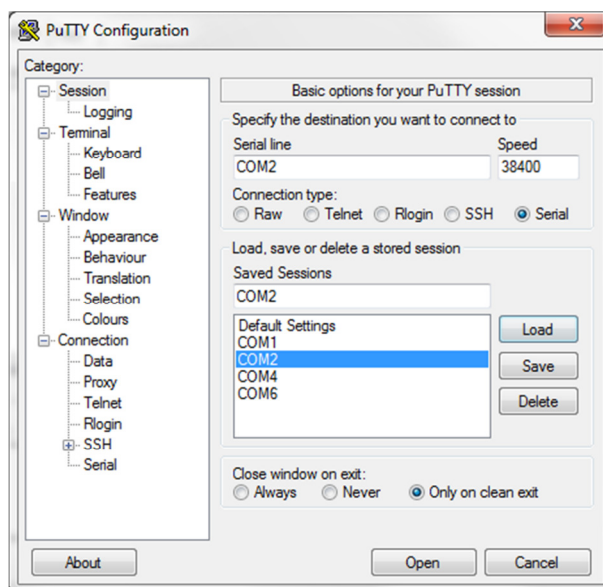
The screenshot shows the 'Targets' tab of the NAMES 3.0 software. It displays a table with two entries, each preceded by a green checkmark icon. The table has columns for Name, Address, and Backplane.

Name	Address	Backplane
000000C12B0	192.168.200.250:800	000000C12B0
1F5050-137-1241-R2B	192.168.100.1:800	000014870D37

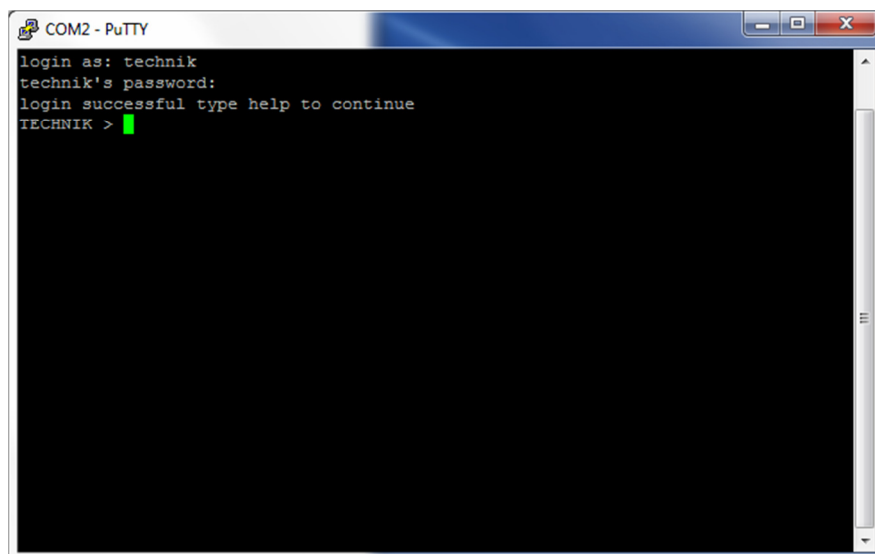
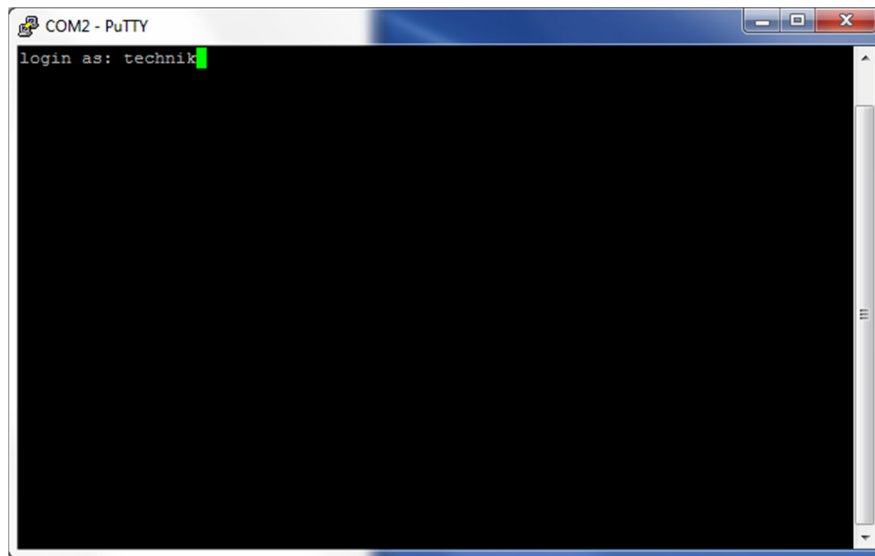
If the network configuration and NAMES IP address cannot be retrieved via DHCP, it must be manually configured through the USB console connection.

The system acts as a USB serial device; when plugged into a Windows PC, it will automatically be assigned as a COM port. Using this COM port, a serial console connection to the device may be established with a serial terminal utility such as PuTTY.





When prompted for the user name, enter „technik“. The default password is empty; when prompted for a password, press return.



The command

`„netconf -i 192.168.1.10 -n 255.255.0.0 -g 192.168.0.1 -s“`  
sets the system IP address, the netmask and the default gateway address and saves them.

Details:

<code>„netconf -i xxx.xxx.xxx.xxx“</code>	temporarily sets the system IP address.
<code>„netconf -n xxx.xxx.xxx.xxx“</code>	temporarily sets the netmask.
<code>„netconf -g xxx.xxx.xxx.xxx“</code>	temporarily sets the default gateway address.
<code>„netconf -s</code>	saves the temporary values as new values. The LAN link will automatically be cycled to activate the new settings. If the system is currently in the default configuration, the settings will remain active after a system restart.
<code>„netconf“</code>	displays the current and new settings.



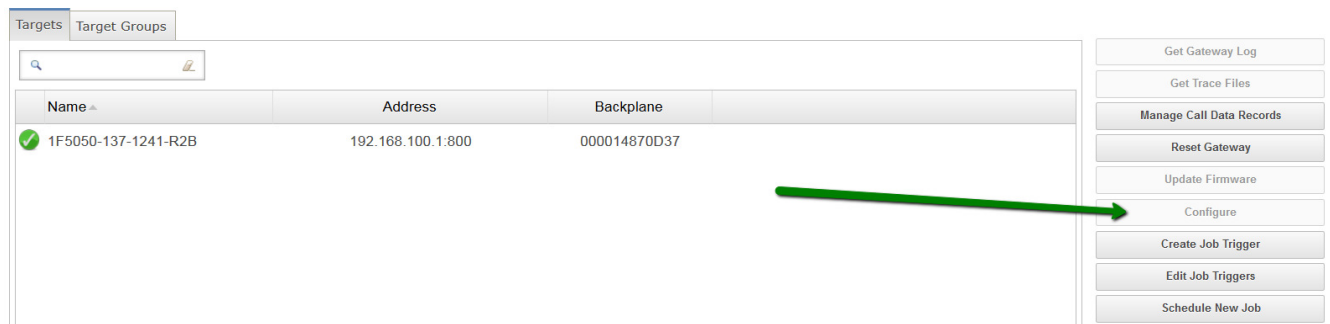
<code>„shownamescfg“</code>	displays the currently configured NAMES servers.
<code>„setnamesaddr &lt;IP&gt; [port] [ToS] [TLS]“</code>	sets the NAMES server to connect to.
<code>„setnamesaddr -d“</code>	deletes the NAMES server configured through the console.

Both the IP configuration and the NAMES server address are not written to the configuration file, but to a separate storage that persists through a factory reset. The configuration through the serial console should therefore only be necessary once, as long as the configured information does not change.

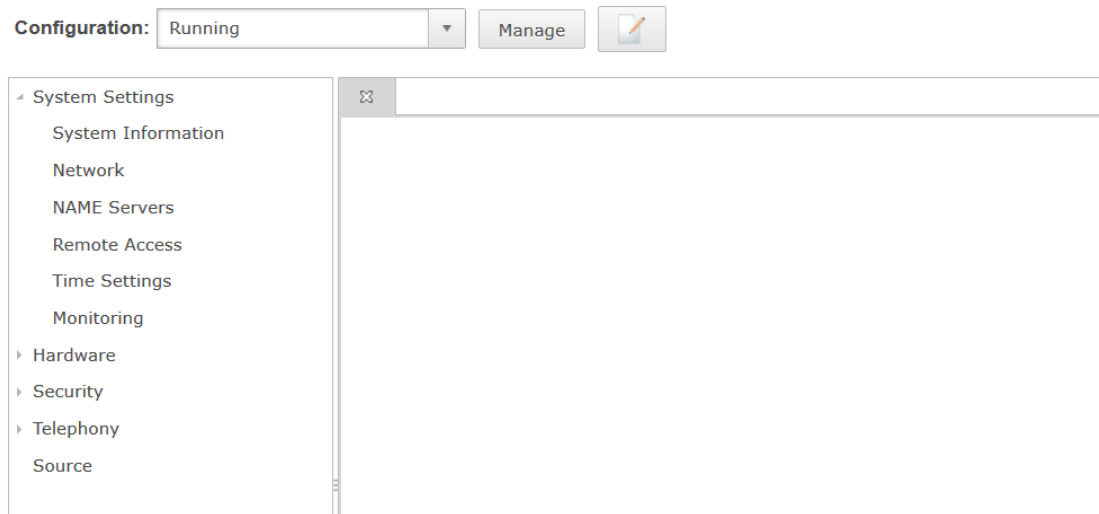
## 6.2 Configuring the system

To start configuring a system, select it from the list once it has connected to the NAMES server, then press the button marked „Configure“. The hardware components present in the system (chassis S8 and S21, modules and boards) are autodetected during startup if the system is in default and shown as part of the configuration. Older chassis that cannot be autodetected will be displayed as an S20 chassis. The chassis type may be changed without losing the already configured modules and boards, as long as the configured slot exists in the new chassis ([see chapter 6.2.2.1.1](#)).

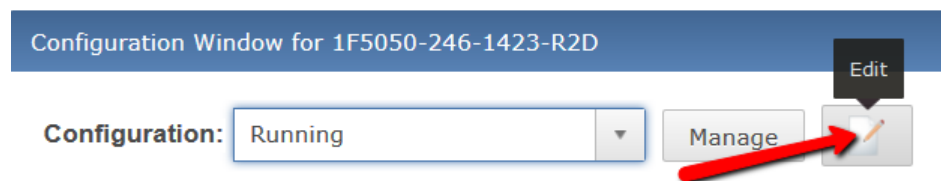
**Important: the CCU should always be inserted into slot 1 of the chassis!**



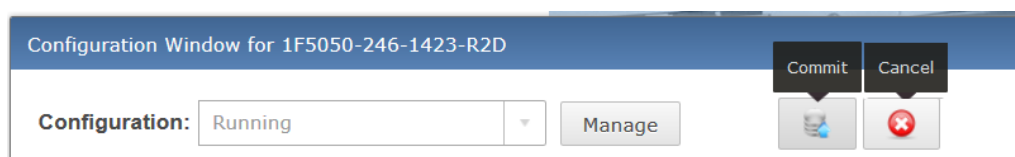
After clicking the „Configure“ button, the following window will open if the system is connected to NAMES (“online”):



Before any changes can be made to the configuration, it must be switched to edit mode by pressing the edit button. This will start an exclusive edit session. The user will be unable to switch to edit mode if another user is already editing the configuration.



After switching to edit mode, the edit button is replaced by the "Commit" and "Cancel" buttons.



The "Commit" button commits all changes made during the edit session to the edited configuration. Pressing the "Cancel" button on the other hand ends the edit session without storing any of the changes and reverts to the state before starting the edit session.

The configuration options available with the configuration plugin installed with NAMES 3.0 (configuration / plugin version 1.0) are described in the following sections. These options may differ when using a different configuration version and plugin; appropriate information will be contained in the documentation of the specific configuration plugin. The following sections are structured in correspondence with the configuration tree in the left panel of the configuration window.



## 6.2.1 System Settings

### 6.2.1.1 System Information

The "System Information" screen allows the user to configure several settings that are purely informational and do not influence the operation of the system. The following settings are available:

- Administrator: the email address of the administrator responsible for the system.
- System Name: a descriptive name for the system. This is not the same as the hostname.
- Description: any extra information about the system.
- Location: the physical location of the system.

A screenshot of the 'System Information' configuration screen. The title bar at the top says 'System Information' with a close button icon. Below the title bar, there are four input fields with labels to their left: 'Administrator:' with the value 'default@novatec.de', 'System Name:' with the value 'Default', 'Description:' with the value 'System is running in default mode.', and 'Location:' which is currently empty.

### 6.2.1.2 Network

The „Network“ panel allows configuration of basic networking settings.

#### 6.2.1.2.1 Mode

This basic setting determines whether the IP configuration is static (manually configured) or dynamic (configured by DHCP). When in dynamic mode, only the settings "Hostname", "Single Port" and "VLAN" are available, as the other settings are configured automatically at system boot.



Network

**Address**

Mode:

Hostname

☒ Single Port Output

**Interface System**

MTU

**IP Settings**

**Interface RTP**

**IP Settings**

**Default Gateway**

IPv4:

IPv6:

**DNS Servers**

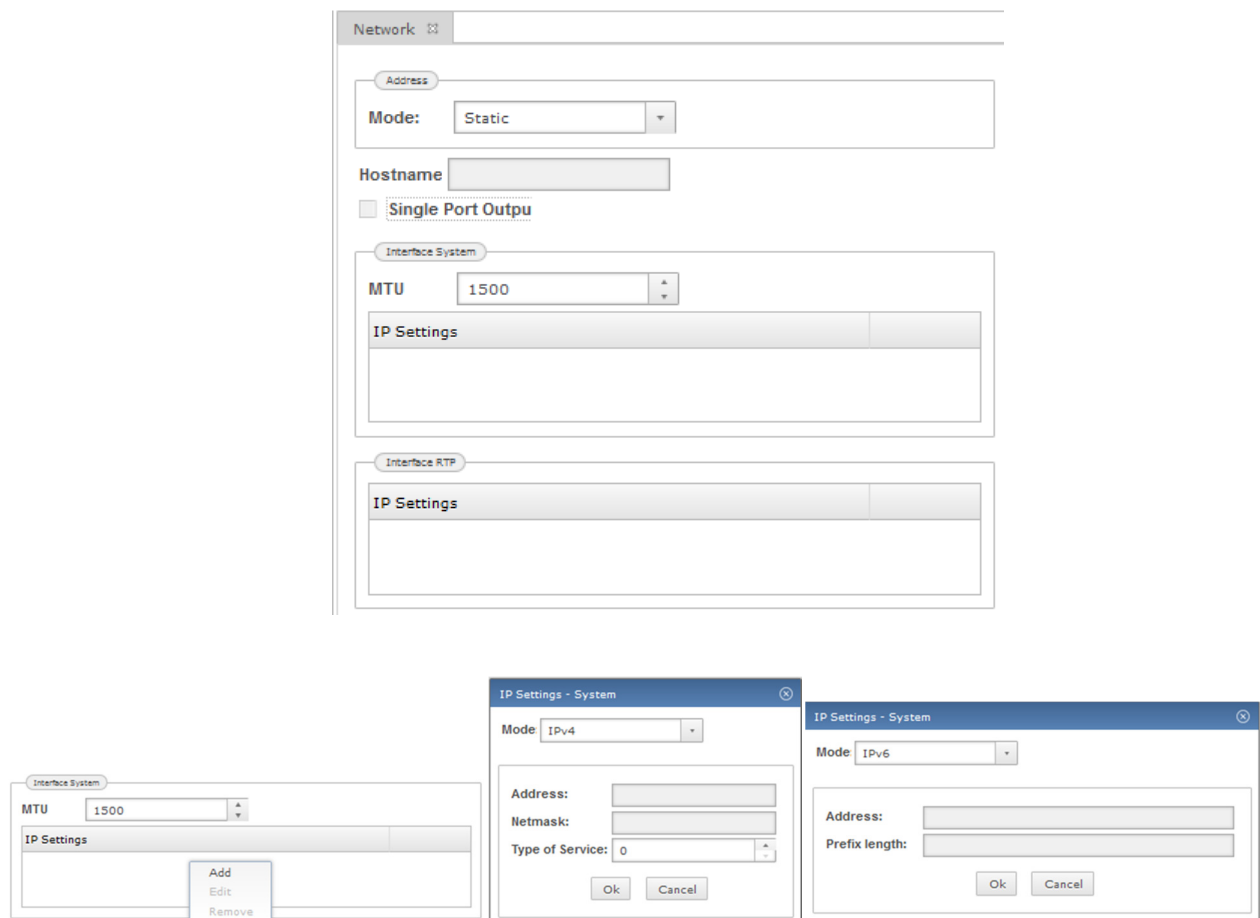
**DNS Server**

**VLAN**

☐ Use VLAN

ID  Priority

In static mode, all settings must be made manually. In particular, at least one IP address must be added to the "System" interface (SIP and management traffic), as well as to the "RTP" interface if RTP is to be used.



To add an IP address to an interface, right-click the table "IP Settings" and select "Add" from the context menu. You may choose either IPv4 or IPv6 from the "Mode" dropdown in the following dialogue, then specify the appropriate settings for the type of address.

#### 6.2.1.2.2 Hostname

The hostname should be unique in the DNS domain the system is a part of. It is provided with DHCP requests and, if the DHCP in use is configured to provide dynamic DNS, can then be resolved to the assigned IP address. For this reason, the hostname must be provided if the mode is "dynamic".

#### 6.2.1.2.3 Single Port

By default, traffic from the system interface (management and SIP traffic) is routed through a different physical port than traffic from the RTP interface. If this option is checked, all traffic will be routed through a single port (the "SIP" port in the image below).

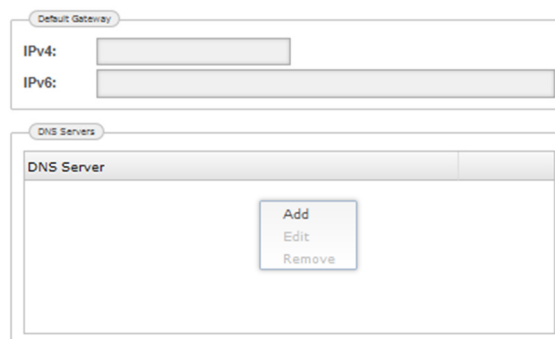


#### 6.2.1.2.4 MTU (Maximum Transfer Unit)

This setting specifies the maximum size of a single Ethernet frame. Typically, this is set to 1500, but some installations may require smaller numbers.

#### 6.2.1.2.5 Default Gateway

This setting specifies the IP address (IPv4 or IPv6) of the default gateway. This is the address of the gateway/router as seen from inside the LAN.

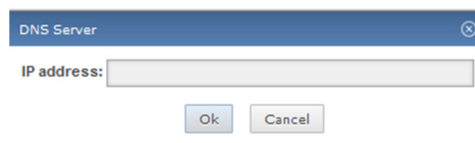


The image shows a configuration window with two sections. The top section, titled 'Default Gateway', contains two input fields: 'IPv4:' and 'IPv6:'. The bottom section, titled 'DNS Servers', contains a table with the header 'DNS Server'. To the right of the table is a context menu with three options: 'Add', 'Edit', and 'Remove'.

#### 6.2.1.2.6 DNS Servers

The DNS servers table lists the DNS servers that the system should use for resolving hostnames into IP addresses. At least **one** DNS server must be entered here.

To add or delete a DNS server entry, right-click the table to bring up the context menu.

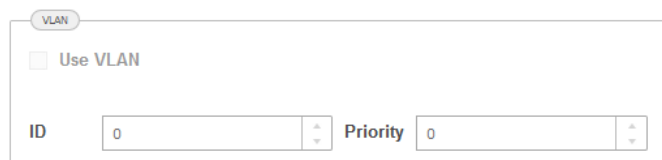


The image shows a dialog box titled 'DNS Server'. It contains a single input field labeled 'IP address:'. Below the input field are two buttons: 'Ok' and 'Cancel'.

#### 6.2.1.2.7 VLAN

To emit Ethernet frames with an IEEE 802.1Q VLAN tag, tick the "Use VLAN" checkbox and enter the values to be included in the tag:

- ID: the VLAN ID (VID) with which frames should be emitted.
- Priority (PCP): the Priority Code Point (PCP) for the frames emitted by the system.

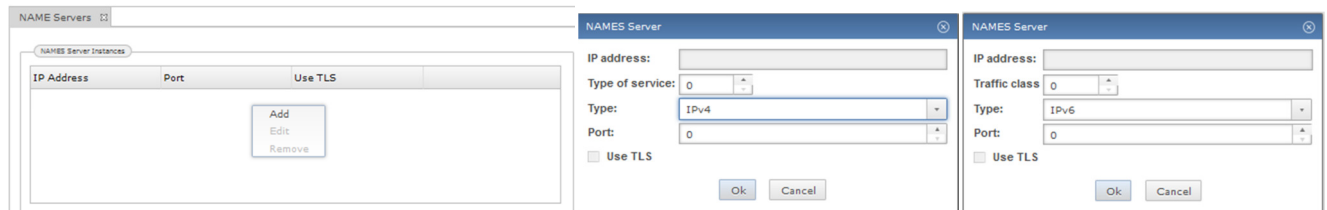


The image shows a configuration window titled 'VLAN'. It contains a checkbox labeled 'Use VLAN'. Below the checkbox are two input fields: 'ID' and 'Priority'. Both fields have a value of '0' and a small up/down arrow icon to their right.



### 6.2.1.3 NAMES Servers

This table allows you to specify one or more NAMES servers for the system to connect to, in addition to any servers retrieved from DHCP or configured via the serial console. If multiple NAMES servers are configured, the system will attempt to connect to them in the listed order; if the first server cannot be reached, a connection to the second server is attempted, and so forth. The system will only connect to one NAMES server at a time. The option to have multiple servers is available mainly for failover in case of failure of a NAMES server.



To add, edit or remove NAMES servers, right-click the table to bring up the context menu. When adding or editing a NAMES server, the following settings are available:

- IP address: the IP address of the NAMES server.
- Type of service/Traffic Class: a six-bit Differentiated Services Code Point (DSCP) for connections to this NAMES server.
- Type: whether the connection should be made via IPv4 or IPv6.
- Port: the port the NAMES server is configured to listen on.

#### 6.2.1.4 Time Settings

This section allows the configuration of how the system time should be set. There are multiple possible sources for the system to acquire the current time (NTP, NAMES or ISDN). One or more of these sources can be configured and arranged in the order of priority by dragging and dropping.

To add a time source, right-click the table and bring up the context menu. When adding an NTP time source, the IP address/hostname of the NTP server and the query frequency must be configured. When using NAMES as a time source, time is synchronized to the NAMES server time on every NAMES heartbeat (once per minute). When using ISDN as a time source, time is synchronized with the ISDN network on every outgoing call.

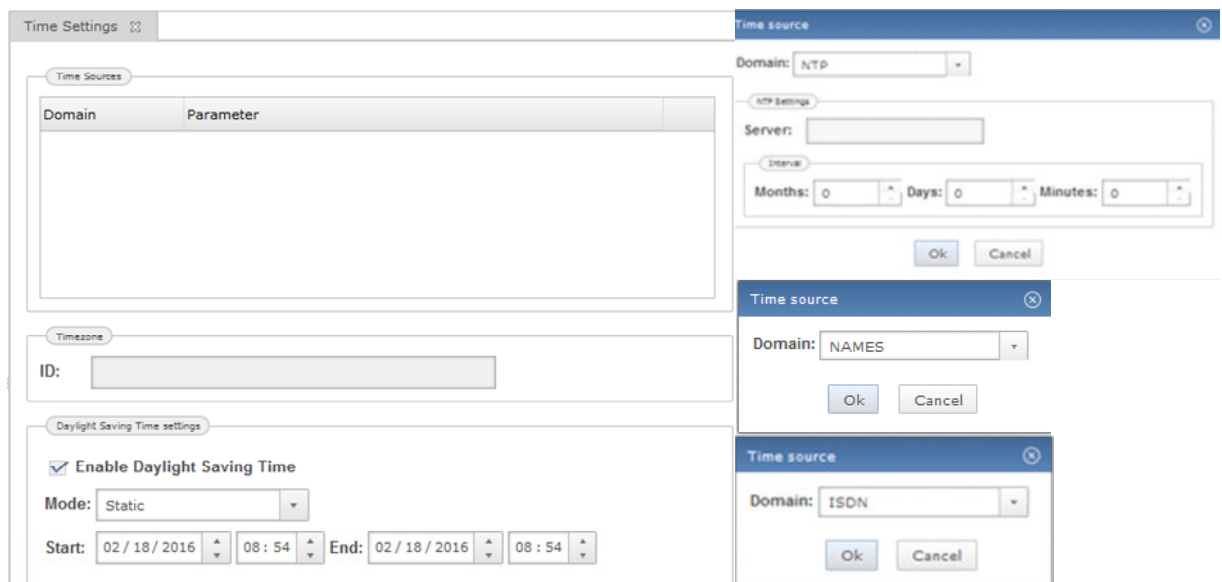
##### 6.2.1.4.1 Time zone

In order to calculate the correct local time from the UTC system time, a time zone must be provided. The available time zones are in the format "<Continent>/<City>", e.g. "Europe/Berlin", and the list of suggestions can be filtered by typing in several letters of the desired zone's name.

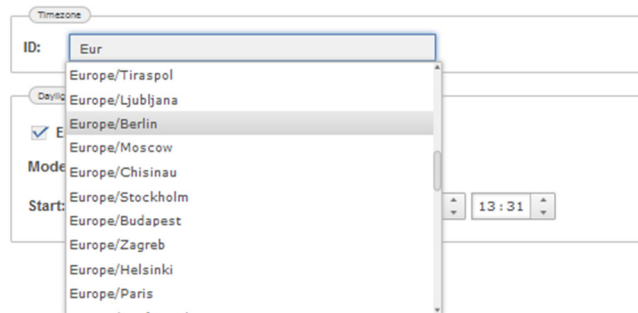
##### 6.2.1.4.2 Daylight Savings Time

For time zones which make use of Daylight Savings Time (DST), the appropriate adjustment of system local time offset may be enabled or disabled. If enabled, three modes are supported:

- Static: DST starts and ends at the manually configured date and time.
- NAMES: the DST start and end times are managed by NAMES and adjusted according to the information provided by the Java Runtime Environment.
- Automatic: available only for (most) European time zones, this setting allows the system to manage DST itself according to the schedule used by European countries.



The screenshot displays the 'Time Settings' window. It features three main sections: 'Time Sources' with a table for adding and managing time sources, 'Timezone' with an 'ID' field, and 'Daylight Saving Time settings' with a checkbox to 'Enable Daylight Saving Time', a 'Mode' dropdown (set to 'Static'), and 'Start' and 'End' date and time pickers. Overlaid on the right are three 'Time source' dialog boxes. The top dialog is for 'NTP' with fields for 'Server' and 'Interval' (Months, Days, Minutes). The middle dialog is for 'NAMES' with an 'Ok' button. The bottom dialog is for 'ISDN' with an 'Ok' button.



### 6.2.1.5 Monitoring

The Monitoring section allows the configuration of conditions and thresholds that will cause an alarm message to be sent to the NAMES server. Alarm messages may trigger jobs if configured that way (see section **Fehler! Verweisquelle konnte nicht gefunden werden.**), and are propagated as SNMP notifications if SNMP is properly configured in NAMES.

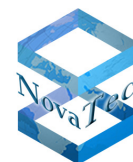
There are "parameterless alarms" which have either no parameters or no individual parameters (for ASR alarms), and there are alarms which need further configuration (thresholds).

To activate or deactivate a parameterless alarm, simply drag and drop the corresponding entry from the "inactive" table to the "active" table or vice versa. Multiple alarms may be moved at one time by holding Shift or Ctrl while selecting from the table.

#### 6.2.1.5.1 Parameterless alarms

The following parameterless alarms are currently supported:

- **Call data storage full**  
The system's storage area for CDRs is nearly full and should be emptied.
- **System ASR below threshold**  
The ASR (attempt successful rate) for the entire system has fallen below the defined threshold.
- **ISDN ASR below threshold**  
The ASR (attempt successful rate) for ISDN call legs has fallen below the defined threshold.
- **SIP ASR below threshold**  
The ASR (attempt successful rate) for SIP call legs has fallen below the defined threshold.
- **Layer 1 active**  
An ISDN interface's layer 1 has switched from inactive to active.
- **Layer 1 inactive**  
An ISDN interface's layer 1 has switched from active to inactive.
- **Layer 2 active**  
An ISDN interface's layer 2 has switched from inactive to active.
- **Layer 2 inactive**  
An ISDN interface's layer 2 has switched from active to inactive.
- **TLS certificate invalid in one week**  
The system's TLS certificate will become invalid in one week's time.
- **TLS has default time**  
The system time has not been properly set when attempting to verify TLS certificates.
- **TLS own chain invalid**  
The system's TLS certificate chain could not be validated.
- **Log storage full**  
The system's log storage area is full and should be emptied.
- **Trace storage full**  
The system's storage area for trace files is full and should be emptied.



- **System started**  
The system has successfully booted.
- **Trace fatal**  
A fatal error has occurred. This alarm is sent after the system has rebooted following the fatal error.
- **Trace warning**  
The system has registered a warning.
- **Trace error**  
The system has registered an error.
- **Invalid FW license**  
The system does not have a valid firmware license.
- **TLS unlicensed**  
The system does not have a valid TLS license/the TLS flag in the license is not set.
- **PSU redundancy failure**  
The system has lost PSU redundancy due to hardware failure or power loss. This alarm is only available with S8 and S21 chassis.
- **PSU redundancy restored**  
The system has regained PSU redundancy after a hardware failure or power loss. This notification is only available with S8 and S21 chassis.
- **RMCS connection lost**  
The system has lost its connection to the RMCS server.
- **RMCS connection attempt failed**  
The system's attempt to connect to an RMCS server failed.

#### 6.2.1.5.2 CPU usage Alarm

The CPU usage alarm is triggered by CPU load above the configured *alarm threshold* for a minimum time specified by the *alarm condition delay* – shorter spikes are ignored. Inversely, the alarm is cleared once the CPU load has dropped below the configured clear threshold for a minimum time specified by clear condition delay. Both the alarm and the clear are sent only if the corresponding checkbox is checked.

#### 6.2.1.5.3 Call Setup Time Alarm

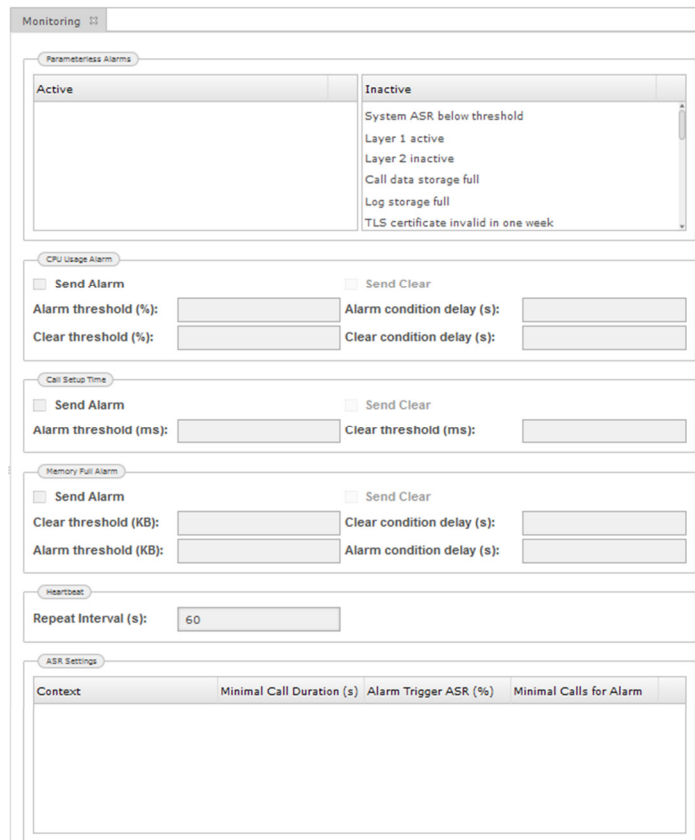
If the Call Setup Time (time to set up a call from the initial attempt to ringing or an error state) of a call exceeds the threshold specified, an alarm will be sent. The clear is sent once the Call Setup Time drops below the configured clear threshold again. Both the alarm and the clear are sent only if the corresponding checkbox is checked.

#### 6.2.1.5.4 Memory Full Alarm

The memory full alarm is triggered by free memory below the configured *alarm threshold* for a minimum time specified by the *alarm condition delay* – shorter spikes are ignored. Inversely, the alarm is cleared once the free memory has increased above the configured clear threshold for a minimum time specified by clear condition delay. Both the alarm and the clear are sent only if the corresponding checkbox is checked.

#### 6.2.1.5.5 Heartbeat

The system regularly generates a heartbeat signal that is sent to the NAMES server for liveness monitoring. The heartbeat interval in seconds can be configured.



The screenshot shows a 'Monitoring' window with several sections:

- Parameterless Alarms:** A list of alarms, categorized into 'Active' and 'Inactive'. The 'Inactive' list includes: System ASR below threshold, Layer 1 active, Layer 2 inactive, Call data storage full, Log storage full, and TLS certificate invalid in one week.
- CPU Usage Alarm:** Includes checkboxes for 'Send Alarm' and 'Send Clear', and input fields for 'Alarm threshold (%)', 'Clear threshold (%)', 'Alarm condition delay (s)', and 'Clear condition delay (s)'.
- Call Setup Time:** Includes checkboxes for 'Send Alarm' and 'Send Clear', and input fields for 'Alarm threshold (ms)' and 'Clear threshold (ms)'.
- Memory Full Alarm:** Includes checkboxes for 'Send Alarm' and 'Send Clear', and input fields for 'Clear threshold (KB)', 'Alarm threshold (KB)', 'Clear condition delay (s)', and 'Alarm condition delay (s)'.
- Heartbeat:** Includes a 'Repeat Interval (s)' input field set to 60.
- ASR Settings:** A table with columns: Context, Minimal Call Duration (s), Alarm Trigger ASR (%), and Minimal Calls for Alarm. The table is currently empty.

#### 6.2.1.5.6 ASR Settings

The ASR (Attempt Successful Rate) is the percentage of successful connection attempts compared to the total number of connection attempts. The ASR settings are used to determine the threshold for ASR alarms. The alarms themselves can be separately enabled or disabled for ISDN and SIP calls and overall calls, see section 6.2.1.5.1 oben.

- **Minimal call duration**

Calls that do not last at least the length specified here are always rated as being successful.

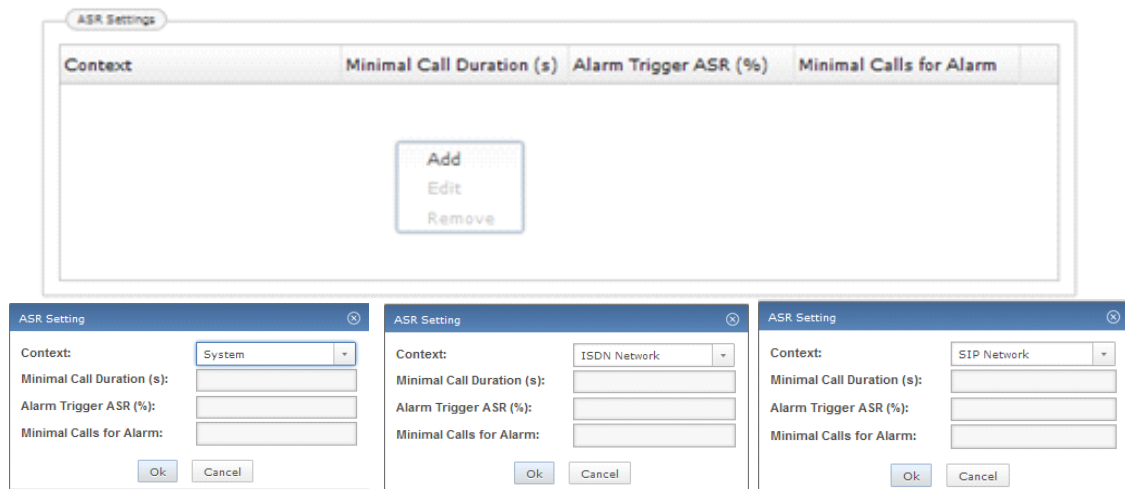
- **Alarm Trigger ASR**

If the ASR falls short of this limit, a call home is initiated. Values from 0 to 100 % are possible.

- **Minimal calls for Alarm**

This is a counter, which allows the system time to carry out the number of calls specified here, before the ASR is considered to be below the value set above. For example if this value is set to 1, then after a reset the first call that falls below the ASR will trigger the event ASR call home (if active).

Right-click into the free space in the window „ASR Settings“ and select „Add“. The appropriate windows for the ASR alarm settings appear.



The configured ASR alarms can be edited or removed. In you wish to change an ASR alarm, click on the corresponding alarm with the right mouse key and then press "Edit". After you have made your changes click the "Commit" button.

If you want to remove an ASR alarm, click onto the corresponding alarm with the right mouse key and then onto "Remove". After you have made your changes, press the "Commit" button.

## 6.2.2 Hardware

### 6.2.2.1 Chassis

In this section the hardware settings for a particular chassis and its components, interfaces, modules and their profiles can be made.

The following configuration is an example for the below explanations:

Click the menu „Chassis“. The following window pops up after restarting the target:

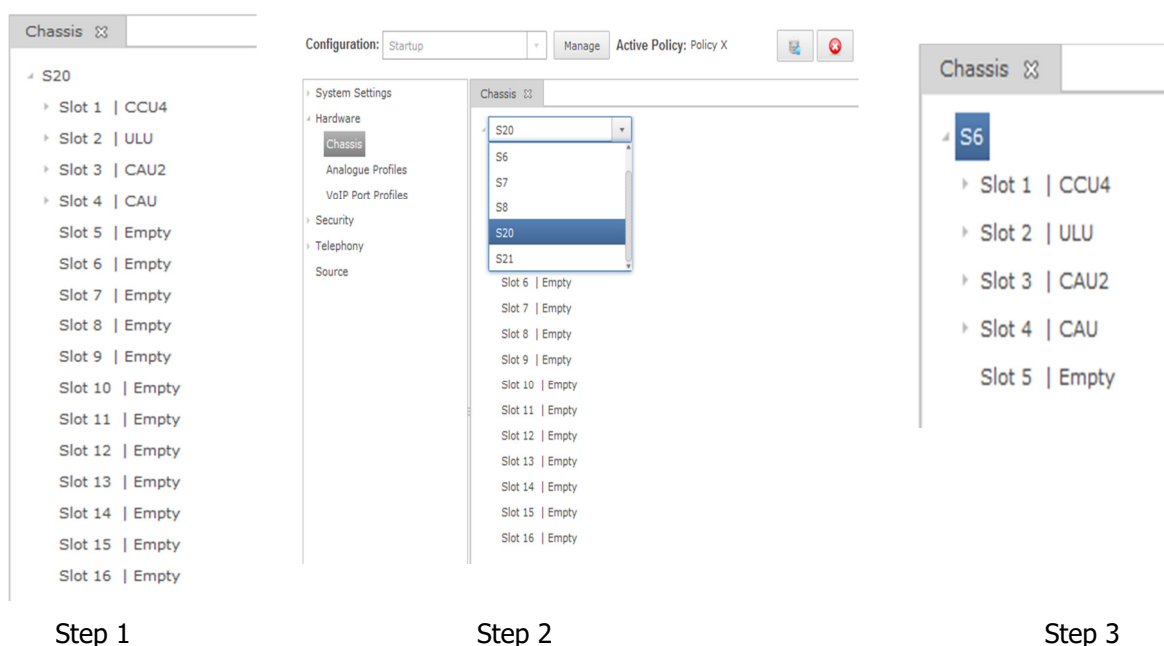


In the above window an S21 configuration with one CCU4 in slot1 and one PSU1 is shown. It is also possible to choose other chassis like S5+, S6, S7, S8 and S20. These chassis appear in the list, if you click onto S21 in the window. In the slots below "Slot1" other modules (e.g. CAU or ULU) can be configured.

### 6.2.2.1.1 Changing the chassis type

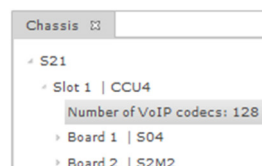
As mentioned in [chapter 6.2](#) , if an S5+, S6 or S7 is in use, this will be shown in the configuration of the unit after rebooting the target as an S20 chassis. To change the chassis type to the one currently in use, the following steps are necessary:

- Click onto "S20" in the window as shown below (Step 1), a dropdown menu will appear which contains all possible types of chassis to select from (Step 2).
- Select the type of chassis (S6). All slide cards and boards will remain as are available and detected during booting process (Step 3).



### 6.2.2.1.2 Slide in cards and daughter boards

Click onto slot 1 of the chassis showing CCU4 as available. A table with the available daughter boards S04, S2M2 and the amount of IP codecs is shown. You can also choose other daughter boards: ANA4, Uo4\_2B1Q or U04\_4B3T and Up04.



To view the interfaces and the settings of each daughter board, click onto the arrow on the left hand side of the corresponding board (here 1 or 2). Here a S04 on "Board 1" with four interfaces and on "Board 2" one S2M2 with two interfaces are available.

```

S21
├─ Slot 1 | CCU4
│   Number of VoIP codecs: 128
│   └─ Board 1 | S04
│       ISDN Interface 1 | Active | Master
│       ISDN Interface 2 | Active | Master
│       ISDN Interface 3 | Active | Master
│       ISDN Interface 4 | Active | Master
│   └─ Board 2 | S2M2
│       ISDN Interface 1 | Active | Master
│       ISDN Interface 2 | Active | Master

```

It is possible to modify the interface settings here. If you want to change the interface state from active to inactive mode, click onto the interface to be modified. A drop down window appears in which the desired mode can be selected.

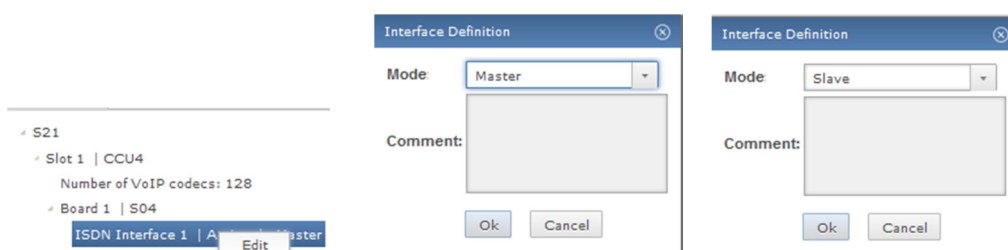
```

S21
├─ Slot 1 | CCU4
│   Number of VoIP codecs: 128
│   └─ Board 1 | S04
│       ISDN Interface 1 | Active | Master
│       ISDN Interface 2 | Active | Master
│       ISDN Interface 3 | Active | Master
│       ISDN Interface 4 | Active | Master
│   └─ Board 2 | S2M2
│       ISDN Interface 1 | Active | Master
│       ISDN Interface 2 | Active | Master

```

If you wish to change the interface mode from master to slave mode or vice versa, right click the interface you wish to adapt. Click onto edit in the pop up menu. The "Interface Definition" window appears. Select the appropriate mode and add a comment like changing reasons, names or location etc. into the comment section.

**Exceptions to this are U04 and Uko4 daughter boards. These boards can only be in master mode. In case an ULU slide-in card exists in one of the slots, all interfaces of this card can be configured in master or slave mode as bunch. You cannot single out interfaces.**



### 6.2.2.2 Analogue Profiles

In this section you will find a description of how to change the default configuration as provided by the system of every analogue interface if necessary.

ID	Max Hook Flash Duration	Call Charge PulseLength Type	Call Charge Pulse KHz	Caller ID	Country ID	Tone Detection
Default	310	100	N_16_K_HZ	ETSI	Germany	Fax Tone



If the given default configuration is useless for your application it can be changed like this: Click onto the appropriate „profile“ with the right key of the mouse. A menu with „Add, Edit and Remove“ is shown. Select „Edit“ and change the parameter as required by your application.

If you wish to create a new profile, proceed as follows:

Right-click into the analogue profiles list. A menu with „Add, Edit and Remove“ shows up. Select „Add“ and choose the relevant settings for the particular location or country.

Analogue Profiles						
ID	Max Hook Flash Duration	Call Charge PulseLength Type	Call Charge Pulse KHz	Caller ID	Country ID	Tone Detection
Default	310	100	N_16_K_HZ	ETSI	Germany	Fax Tone

Add  
Edit  
Remove

Analogue Profile

ID:

Default

Max Hook Flash Duration:

310

Call Charge PulseLength Type:

100

Call Charge Pulse KHz:

16kHz

Caller ID:

ETSI

Country ID:

Germany

Tone Detection:

Fax Tone

Ok

Cancel

Edit

Analogue Profile

ID:

Max Hook Flash Duration:

200

Call Charge PulseLength Type:

50

Call Charge Pulse KHz:

12kHz

Caller ID:

Off

Country ID:

Austria

Tone Detection:

Off

Ok

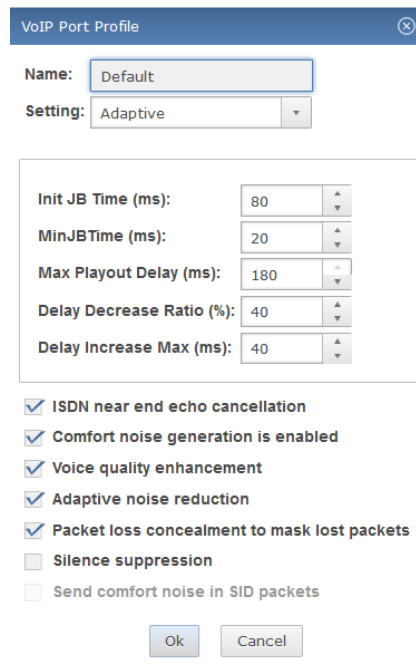
Cancel

Add

### 6.2.2.3 VoIP Port Profiles

In this chapter you will find a description of how to define the necessary SIP VoIP port profiles. The port profile determines the basic functionality of the corresponding port. The default port profile is shown in the picture below. This profile is applied to all associated SIP interfaces. These are the general settings for all associated SIP interfaces regardless of the negotiated codec type between the SIP partners. These settings can be modified or a completely new profile can be created.

VoIP Port Profiles								
Name	Init JB Time	MinJBTime (ms)	Max Playout Delay (ms)	Delay Decrease Ratio (%)	Delay Increase Max (ms)	Underrun (ms)	Overrun (ms)	ISDN near
Default	180	20	180	40	40			on



The VoIP port profile can be configured for two different modes:

- **Adaptive mode**

Adaptive dejittering mode is designed to automatically adjust the Jitter Buffer Delay based on network conditions. The goal is to minimize the time between packet reception and playout of its content on TDM, while keeping the jitter buffer large enough so that it can keep up with the current network jitter. To establish the size of the Jitter Buffer Delay, the Adaptive dejittering algorithm estimates the network delay as well as the network delay variations. It estimates these values based on packet reception. These estimations are made over time, so that sudden variations in packet flow do not trigger sudden variations in the delay, thus ensuring a smooth adaptation. Delay adjustments are made during silence periods: when decreasing the delay silence periods are shortened, while when increasing the delay, silence periods are stretched out. Note that while the delay may be modified, the PDV stays unchanged. This means that when the delay is reduced, it increases the amount of time by which a packet can be received in ahead of time. In turn, as the delay is increased, the amount of time allowed for packets received in advance is reduced.

Settings in JB mode: Adaptive

Init JB Time: 80 [ms]

Min. JB Time: 20 [ms]

Max. JB Time: 180 [ms]

- **Static mode**

Static Adjustment dejittering is characterized by a constant Jitter Buffer Delay. Whenever overruns or underruns occur, the associated packets are dropped and the Jitter Buffer Delay is readjusted based on user configuration. Using this mode in a network where there is no or little jitter, the delay between the time a packet is received and the time its content is played on TDM is constant and around the initial delay configured.

Settings in JB mode: Static

Init JB Time: 100 [ms]



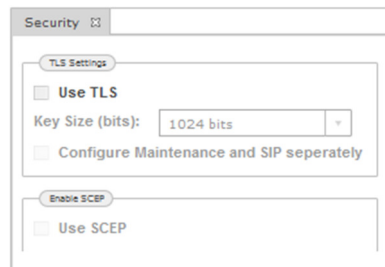
Max. JB Time: 180 [ms]

- ISDN near end echo cancellation  
Activates or deactivates the echo cancellation on the ISDN side of ISDN -> SIP connection leg
- Comfort Noise Generation is enabled  
During periods of transmit silence, when no packets are sent, the NMG has a choice of what to present to the listener. Muting the channel (playing absolutely nothing) gives the listener the unpleasant impression that the line has gone dead. CNG generates a local noise signal that it presents to the listener during silent periods.
- Voice quality enhancement  
The voice quality gets better.
- Adaptive noise reduction
- Packet loss concealment to mask lost packets  
Packet loss concealment (PLC) is a technology designed to minimize the practical effect of lost packets in digital communications. In particular, PLC is used in Voice over Internet Protocol (VoIP).
- Silence suppression  
Enables the codec to compress silence packets to minimize IP traffic. Please note, not all VoIP codecs support this option. For more information, please read the comments here.
- Send comfort noise in SID packets  
Comfort Noise (SCN) feature and the generation of Silence  
Insertion Descriptor (SID) packets during silence periods. This parameter is applicable only when SilenceSuppressionFlag is enabled
- Underrun  
In static jitter mode, average delay boundary, in milliseconds, at which the jitter buffer detects an overrun condition and re-adjusts itself to reduce communication delay.
- Overrun  
In static jitter mode, average delay boundary, in milliseconds, at which the jitter buffer detects an overrun condition and re-adjusts itself to reduce communication delay.

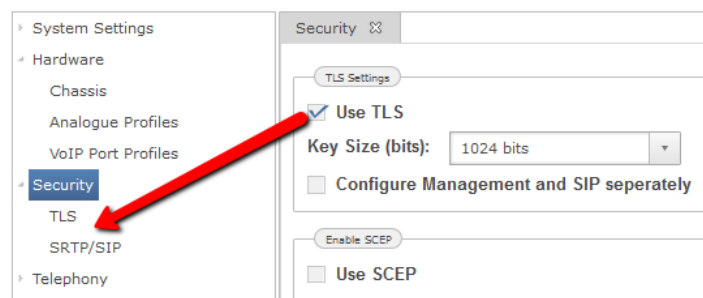
There is no special handling of the Jitter Buffer Delay when overruns or underruns occur. In contrast with the Static Adjustment mode that makes a complete re-adjustment of its delay, Adaptive dejittering mode keeps on performing the same adjustments in order to find the optimal delay for the current network conditions.

### 6.2.3 Security

This chapter explains the use of TLS and the associated settings as well as how to activate encryption for maintenance or SIP. Also signing via SCEP is described. You can define the size of keys in the window as shown below. The default setting is 2048 bits.



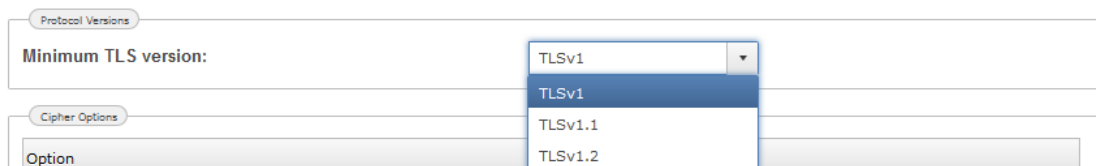
If you want to use TLS, the box „Use TLS“ has to be ticked. After the „Use TLS“ box is ticked, the key size can be changed and „Configure Maintenance and SIP separately“ as well as „Use SCEP“ can be selected. Also the sub-items “TLS” and “SRTP/SIP” appear under “Security”. In these sub-items you can configure the secured mode for SIP link and the link between the target and NAMES.

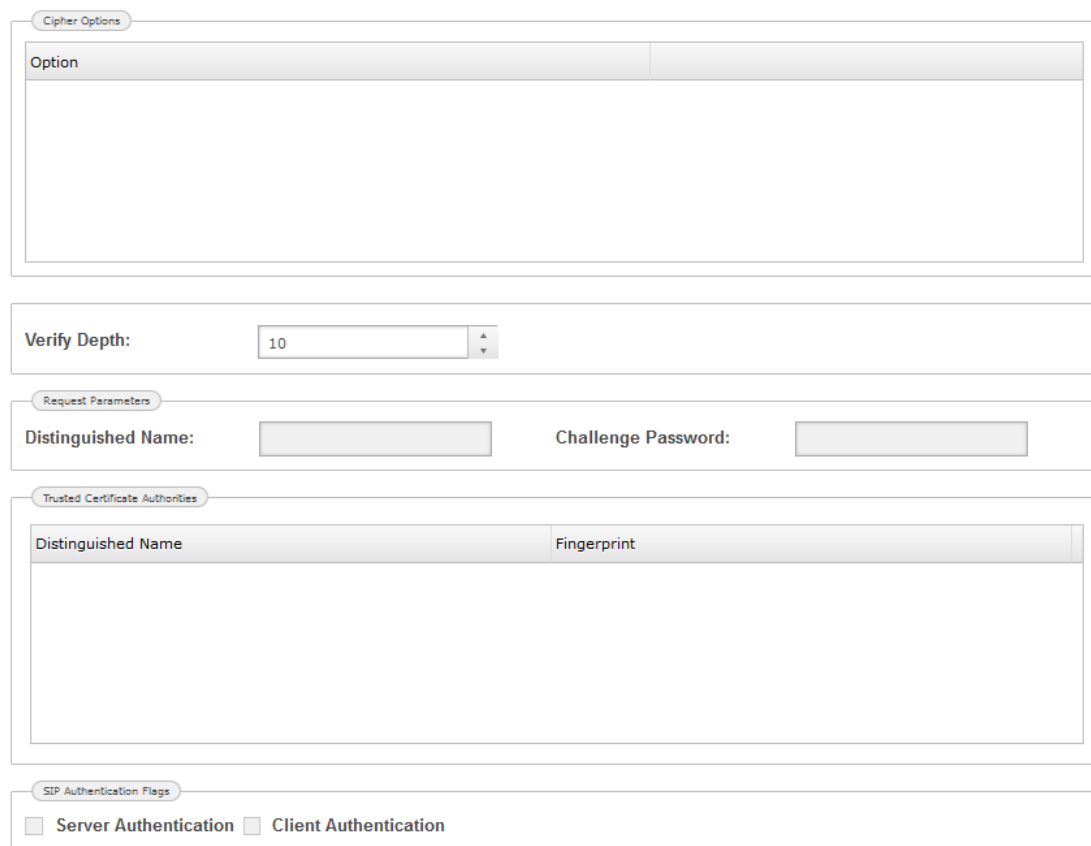


In order to set up the “TLS” adjustments, click onto the submenu “TLS”. The following drop down menu appears:

- Protocol version
- Minimum TLS version

The selected value for the TLS link has to be provided from the connected partner.





The screenshot displays the TLS configuration window with the following sections:

- Cipher Options:** A table with a header 'Option' and an empty body.
- Verify Depth:** A label 'Verify Depth:' followed by a text input field containing '10' and up/down arrow buttons.
- Request Parameters:** A section containing two text input fields: 'Distinguished Name:' and 'Challenge Password:'.
- Trusted Certificate Authorities:** A table with headers 'Distinguished Name' and 'Fingerprint' and an empty body.
- SIP Authentication Flags:** Two checkboxes labeled 'Server Authentication' and 'Client Authentication'.

The TLS submenu provides the following setting possibilities:

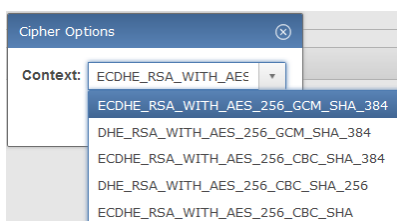
- **Cipher Options**

is a standard collection of cryptographic processes for encryption.

Right-click the section "Cipher Options" and select "Add or Add All". A drop down menu with a choice of possible processes appears. If more than one process is provided you can change the priority ranking as follows:

Select the required cipher option and drag it up or down with your mouse.

Cipher options cannot be edited or changed, only removed. To remove an option, click onto it with the right mouse key and onto "Remove" in the pop up menu.



- **Verify Depth**

With this option the depth of the verification of the certificate can be assigned.

Request Parameters

- **Distinguished Name:**

Here the content of the „Distinguished Name“ can be assigned to trigger a CSR request for later signing.

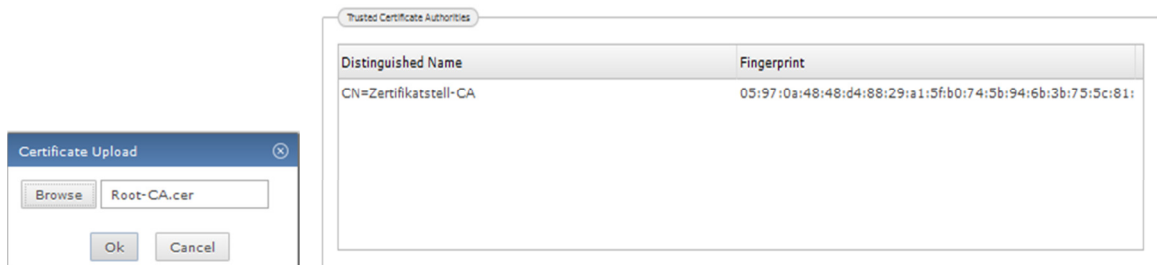
- Challenge Password:

If the optional „Challenge Password“ in the registry of the „Certificate Authority Server“ is activated, the two instances (MNT and SIP) of the NovaTec gateways will need an „One Time Password“. The „Challenge Password“ is a random string and can be transferred to NovaTec configuration by copy and paste.

- Trusted Certificate Authorities

CA certificates can be loaded into the trust list of the NovaTec gateways.

Right-click into the „Trusted Certificate Authorities“ window. Select „Add“ from the pop up menu. A new window opens. Press „browse“ and choose the required certificate, then press the „Ok“ button.

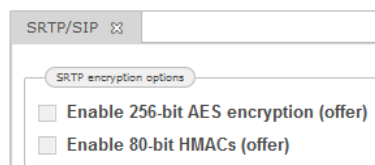


The content of certificates cannot be edited or changed, it can only be removed. To do so select the corresponding certificate right click it and select „Remove“ from the pop up menu.

- SIP Authentication Flags

To increase the security of a link, the identity of the TLS partner has to be verified. This can be done with the following flags.

- SRTP/SIP



- SRTP encryption options

If the sRTP mode (try to use or have to use) for SIP trunk has been activated ([see chapter 6.2.4.2.1.4](#)), the following additional encryption methods will be provided after one of the selection boxes in the section „SRTP encryption options“ has been ticked:

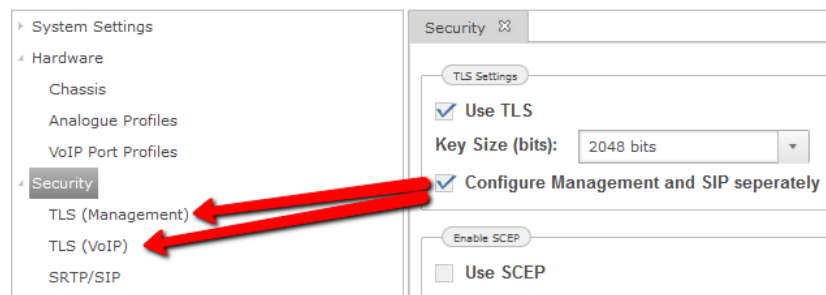
- |   |                         |
|---|-------------------------|
| <input type="checkbox"/> Enable 256-bit AES encryption (offer)            | AES_CM_128_HMAC_SHA1_32 |
| <input type="checkbox"/> Enable 80-bit HMACs (offer)                      |                         |
| <input checked="" type="checkbox"/> Enable 256-bit AES encryption (offer) | AES_CM_128_HMAC_SHA1_32 |
| <input type="checkbox"/> Enable 80-bit HMACs (offer)                      | AES_CM_256_HMAC_SHA1_32 |
| <input type="checkbox"/> Enable 256-bit AES encryption (offer)            | AES_CM_128_HMAC_SHA1_32 |
| <input checked="" type="checkbox"/> Enable 80-bit HMACs (offer)           | AES_CM_128_HMAC_SHA1_80 |
| <input checked="" type="checkbox"/> Enable 256-bit AES encryption (offer) | AES_CM_128_HMAC_SHA1_32 |
| <input checked="" type="checkbox"/> Enable 80-bit HMACs (offer)           |                         |

AES\_CM\_128\_HMAC\_SHA1\_80

AES\_CM\_256\_HMAC\_SHA1\_32

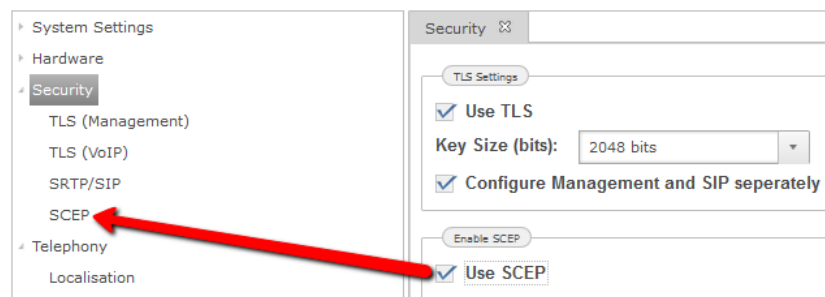
AES\_CM\_256\_HMAC\_SHA1\_80

If "Configure Management and SIP separately" has been ticked in addition to "Use TLS", a new sub menu appears under "Security". With these settings the TLS link between NAMES and the target as well as the secure SIP links of the targets can be configured separately.



The settings of the sub menu „TLS-Management“ and „TLS-SIP“ are identical to the settings of the sub menu „TLS“.

If an SCEP server is used to sign the certificates, the box „Use SCEP“ has to be ticked. The sub menu "SCEP" will appear under "Security" as soon as the box has been ticked.



Once „UseSCEP“ has been selected, following settings must be made:

Include the Microsoft Standard URL <http://FQDN/certsrv/mscep/mscep.dll> into the window "SCEP Server's URL". An extra DNS solution is required if you want to include the **Fully Qualified Domain Name** „FQDN“ server domain (caserver1.novanet.local), which provides the trustworthiness of the remote partner. A server IP address can also be included instead of "FQDN". The SCEP Protocol is based on „http“, therefore the default port number is always 80. Next step is to define the public key cryptography standard "PKCS#7" based algorithm for encryption and signature.

In accordance with the norms these are: DES, 3DES, Blowfish, md5 and sha1.

If a Microsoft Server is used as certificate authority for the enrollment with SCEP, two registration authority (RA) certificates for enrollment have to be imported from the Microsoft Server. The first is „usage: Digital Signature, Non Repudiation“, a signed RA Certificate (Enrollment Certificate), and the second „usage: Key Encipherment, Data Encipherment“ for encryption (Encipherment Certificate). Both must be exported from the

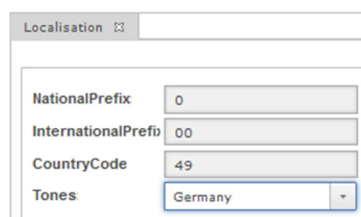
certification authority of the CA server in base64 format. With the selection of the buttons "Import enrollment certificate" and "Import encipherment certificate" these certificates can be transferred to the configuration of the targets.



## 6.2.4 Telephony

### 6.2.4.1 Localisation

The localisation options are used by various modules within the firmware and **must** correspond to the locale where the system is installed and operated from.



- **National prefix**  
The digit(s) that are required to be dialed for national numbers, for example in Germany "0" is the prefix that signifies a national number.
- **International prefix**  
The digit(s) that are required to be dialed for international numbers, for example in Germany "00" is the prefix that signifies an international number.
- **Country code**  
The digit(s) of the country, in which the NMG is installed. If the NMG is installed in Germany, the digits would be 49 (without the leading zero's). In the UK this would be 44.
- **Tones**  
The system can generate the required tones normally provided by the network provider (alerting etc.).

### 6.2.4.2 VoIP

#### 6.2.4.2.1 SIP

##### 6.2.4.2.1.1.1 SIP Codec Mapping

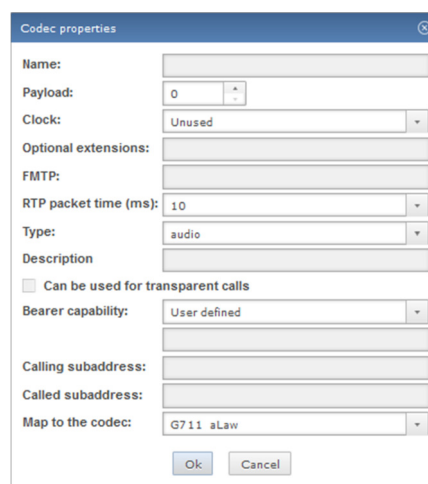


In this section, you can change the default behavior of the NovaTec system regarding the mapping of codecs. This is very useful when „exotic“ or manufacturer defined codecs are implemented by different systems, but could be used with the existing codecs installed on the NovaTec system using slightly different standard settings. Changing the settings, as shown here, can have a serious detrimental effect on the stability and functionality of the system!

SIP Codec Mappings ⓘ		
Description	Payload	Mapped to
aLaw64kbit/s	8	G711_aLaw
uLaw64kbit/s	0	G711_aLaw
CISCO X-CCD	125	G711_aLaw
G729_AB 8kbit/s MOS 3,6	18	G729_AB
G726 40kbit/s MOS 4,0	114	G_726_40
G.722.1 32kbit/s MOS 4,3	127	G_722_1_32
G722 64kbit/s MOS 4,4	9	G_722_64
iLBC 13,3 - 15,2kbit/s MOS 4	97	iLBC

Dependent on the codec set which is currently active, the display may differ slightly from what is seen on a normal system. The standard codecs are automatically „mapped“ to the codec (i.e. themselves). User defined codecs can be here, and then mapped to a codec that is installed on the system.

The priority of the selected codecs can be changed as follows: Click on the selected codec and drag it up or down in the priority list with the mouse.



The dialog box shows the following fields:

- Name: (text input)
- Payload: 0 (spin box)
- Clock: Unused (dropdown)
- Optional extensions: (text input)
- FMTP: (text input)
- RTP packet time (ms): 10 (spin box)
- Type: audio (dropdown)
- Description: (text input)
- ☐ Can be used for transparent calls
- Bearer capability: User defined (dropdown)
- Calling subaddress: (text input)
- Called subaddress: (text input)
- Map to the codec: G711 aLaw (dropdown)
- Ok and Cancel buttons

above system.  
correct created NovaTec  
follows:  
priority list

To create a new codec:

Right-click into the window „SIP Codec Mappings“ and select „Add“ from the pop up menu. Then edit the required parameter:

- Name  
The name of the codec which is going to be used.
- Payload  
The numerical RTP payload type.
- Clock  
The clock settings for this codec. It is recommended not to change this value.
- FMTP  
The FMTP setting for this codec. This value indicates which named events a codec can handle. For more information please read the Session Description Protocol (RFC 2327 [7]) It is recommended not to change this value.
- RTP packet time (ms)



This value defines the length of time (Packet time) in milliseconds represented by the media in a packet. It is recommended not to change this value.

- Type

The type of this codec. This is an internal value used by the NMG system to identify the codec type. Possible values are: audio, DTMF, fax and video. It is recommended not to change this value. Standard is audio.

- Description

The informational description for this codec. This value is used internally for informational purposes only. It must not be left empty.

- Can be used for transparent calls

When activated, this allows the NMG to use this codec for transparent (data or fax) calls. It is recommended that at least one codec has this flag set.

The following fields are inserted into the codec properties verbatim. If you have not been asked to enter anything here, or are not sure, DO NOT CHANGE ANY OF THESE SETTINGS!

- Bearer capability

The bearer capability of this codec.

- Calling sub address

The SubSrc property of this codec.

- Called sub address

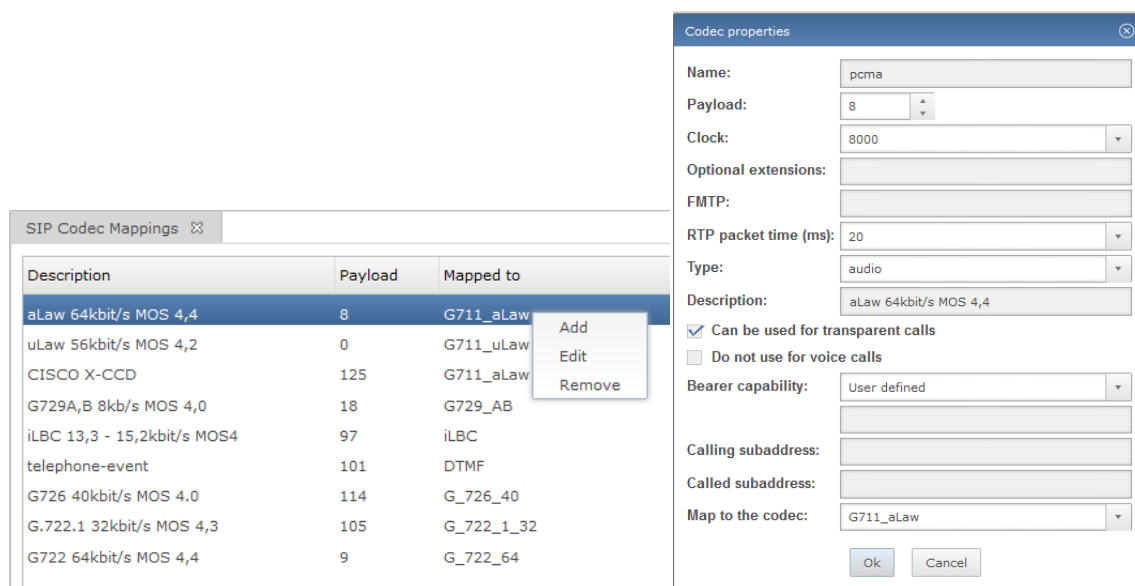
The SubDst property of this codec.

- Map to the codec...

This codec is currently mapped to the codec displayed in the combo box (if any).

To change or edit a codec:

Right-click the codec which has to be changed in the list under "Sip Codec Mappings". A pop up menu appears. Select "Edit" and then make the required changes.



The screenshot shows the 'SIP Codec Mappings' window with a table of codecs. A right-click context menu is open over the first row, showing 'Add', 'Edit', and 'Remove' options. The 'Edit' option is selected. To the right, the 'Codec properties' dialog is shown, displaying fields for Name, Payload, Clock, Optional extensions, FMTP, RTP packet time, Type, Description, and checkboxes for 'Can be used for transparent calls' and 'Do not use for voice calls'. It also includes fields for Bearer capability, Calling subaddress, Called subaddress, and a 'Map to the codec' dropdown.

Description	Payload	Mapped to
aLaw 64kbit/s MOS 4,4	8	G711_aLaw
uLaw 56kbit/s MOS 4,2	0	G711_uLaw
CISCO X-CCD	125	G711_aLaw
G729A,B 8kb/s MOS 4,0	18	G729_AB
iLBC 13,3 - 15,2kbit/s MOS4	97	iLBC
telephone-event	101	DTMF
G726 40kbit/s MOS 4,0	114	G_726_40
G.722.1 32kbit/s MOS 4,3	105	G_722_1_32
G722 64kbit/s MOS 4,4	9	G_722_64

To remove a codec proceed as follows:

Right-click the codec which has to be removed in the list under "Sip Codec Mappings". A pop up menu appears. Select "Remove".



#### 6.2.4.2.1.2 Global SIP Options

In this chapter you will find a description on how to set the global options for the SIP applications of the targets:

##### General settings

A screenshot of the 'General settings' form. It has a tab labeled 'General settings'. Inside the form, there are three input fields: 'Session owner:' with a text box containing 'Sess\_Owner', 'Session name:' with a text box containing 'Sess\_Name', and 'Anonymous name:' with a text box containing 'Ano\_Name'.

- Session owner  
The session owner of the SIP session. This value is used between systems for administration purposes. Please note that this value should not contain any spaces.
- Session name  
The session name. This value is for informational purposes only.
- Anonymous name  
Standard name to identify the system under CLIR conditions.

- Feature options

A screenshot of the 'Feature options' form. It has a tab labeled 'Feature options'. Inside the form, there are six checkboxes arranged in two columns. The first column contains: 'Register as Cisco device at UCM' (unchecked), 'Support IETF drafts' (checked), and 'Support proprietary SIP plus' (checked). The second column contains: 'Activate SIP bridging' (unchecked), 'Support PRACK' (checked), and 'Support 484 incomplete number' (unchecked).

##### If ticked

- Register as Cisco device at UCM  
If the target needs to register as a line / phone.
  - Support IETF drafts  
Should preliminary IETF extensions (which are standard de facto) be supported.
  - Support proprietary SIP plus  
Support the incomplete number processing. This option is currently not recommended.
  - Activate SIP bridging  
The signaling runs via the CCU, the RTP stream between SIP trunks or SIP subscribers.
  - Support PRACK  
Support extensions (100rels) to SIP.
  - Support 484 incomplete number  
Support the incomplete number processing. This option is currently not recommended.
- SDP options



SDP options

<input checked="" type="checkbox"/> Negotiate telephone events 32 to 35 ANS and ANSAM	<input type="checkbox"/> Do not detect DTMF payload type change
<input type="checkbox"/> Do not repeat SDP after early media	<input type="checkbox"/> Do not detect obsolete voice codecs

If ticked

- Negotiate telephone events 32 to 35 ANS and ANSAM

If the flag is disabled, the gateway will enable telephone events per default (tone detection and generation in RTP/SRTP) for ANS and ANSAM tones even if the SIP counterpart does not signal support for it during SIP SDP/codec negotiation. If the flag is enabled, the ANS and ANSAM telephone events will only be activated if the SIP counterpart does signal support for it.

- Do not repeat SDP after early media

Some remote systems (i.e. the third party software) may 'loose' the signaled RTP parameters, that were provided with the 'early media' (18x), while processing the connect response (200). This flag allows resending SDP with the 200 (connect) response. It is recommended to set this option.

- Do not detect DTMF payload type change

Automatically detect any changes in the poorly specified DTMF payload type, during session communication.

- Do not detect obsolete voice codecs

This option allows to avoid a codec agreement only upon the payload type number. If the parameter is set, the codec names will be compared (case insensitive) as well. Some third party software uses old payload type numbers for some archaic codecs.

- RTP settings

RTP settings

IP port start:	30000	IP port stop:	30254
<input type="checkbox"/> Disable codec filtering			

- IP port start/IP port stop

Defines the range of the port numbers to be used for VoIP.

**Attention:** The Port range should not be smaller than the number of the selected Codecs.

- Disable codec filtering

With this box the codec filter can be switched on or off.

In case the filter has not been disabled, the Codec will be negotiated between the VoIP partners.

- Session timers RFC4028

Session Timers RFC4028

<input checked="" type="checkbox"/> Support timer	
Min session expire (s): 1800	Session expire (s): 28800

If ticked

- Support timer

Try to arbitrate the session renewal using the „timer“ utility/extension to SIP.



While having this ('keep alive') extension active, the session must be renewed automatically from either a server, or a client.

The other fixed session expire timeouts ('Expire time for active calls') will not be applied in this case.

- Min session expire (s)

A value that will be used during arbitration of the „timer“ utility/extension to SIP. Please refer to RFC for this parameter. The standard value is recommended.

- Session expire (s)

A value that will be used during arbitration of the „timer“ utility/extension to SIP. Please refer to RFC for this parameter. The standard value is recommended.

- Refer method RFC3515

REFER method RFC3515

☐ Ignore external REFER Cctr ☐ Obey external blind call transfer  
☒ Execute call transfer with REFER method

If ticked

- Ignore external REFER Cctr

Explicitly ignore an external 'consultative' call transfer (CCTR) with REFER, as the provided destination numbers or the call transfer itself via SIP might be unwished.

- Execute call transfer with REFER method

If this flag is disabled, the gateway will perform a call transfer by internally through-connecting the two parties. After the call transfer the new resulting call will still use the gateway/resources in the gateway.

If the flag is enabled, the gateway will send a SIP REFER message on call transfer to instruct the SIP counterpart (e.g. a Cisco UCM) to perform the call transfer in the network. After the call transfer the new resulting call bypasses the gateway completely and all previously occupied resources are freed immediately after the transfer (channels, codecs/DSP resources and memory).

- Obey external blind call transfer

Explicitly enable an externally provided 'blind' call transfer (BCTR) with REFER, as the provided destination numbers or the call transfer itself via SIP might be unwanted.

- Symmetric response routing RFC3581

Symmetric response routing RFC3581

☐ Use R port ☐ Support received

If ticked

- Use R port

'rport' is a diagnostic parameter used in SIP transport lines („Via:“ header). Please refer to RFC about details. The response to 'rport' provides the own IP send port values as seen from the remote side. It



allows to diagnose some transport related issues (like NAT). The option is irrelevant except for the system managers in certain trouble shooting scenarios.

- Support received

'Received' is a diagnostic parameter used in SIP transport lines („Via:” header). Please refer to RFC about details. The IP address values will be returned with 'Received' to the requester. It allows to diagnose some transport related issues (like NAT). The option is irrelevant except for the system managers in certain trouble shooting scenarios.

- Global addressing options

A screenshot of a web form titled 'Global addressing options'. It contains a sub-section 'External gateway IP' with four input fields: 'IPv4 address:', 'IPv6 address:', 'External name:', and 'VPN mask:'. Below these fields are five checkboxes: 'Use local name', 'Insert plus for international numbers', 'Accept deregistered destination if address known', 'Allow change of invalid SIP addresses', and 'No IP address verification'. The checkbox 'Replace local numbers with available outbound maps' is checked.

If ticked

- IPv4 address

The external IPv4-Address of the firewall/router. This is the address of the gateway seen from outside of the internet.

- IPv6 address

The external IPv6-Address of the firewall/router. This is the address of the gateway seen from outside of the internet.

- External name

The external domain name.

- VPN mask

The IP-Address of this system used in a „Virtual Private Network”.

- Use local name

Use the domain name (respectively alias name if supplied), to identify itself. If not supplied, use the system IP address.

- Insert plus for international numbers

Insert automatically the '+' for international numbers.

- Accept deregistered destination if address known

Route to deregistered destination addresses if the address is statically assigned.

- Allow change of invalid SIP address

NMG software follows a very tight security policy. The SIP packets are verified, whether they are tempered, faked or malformed. Especially the IP addresses are verified against the registration (account)



data. Some third party software provides, for example LAN IP addresses in public transport lines. SIP requests from such counterparts will be discarded. This parameter allows to 'switch on' a 'softer' policy. In this case the option 'Correct faulty format' may be applied individually to the entries in the 'user mappings'.

- No IP address verification
- Replace local numbers with available outbound maps

The 'local mappings', which result in a registration on external servers, will be always inserted to the 'reverse local map'. The 'reverse local map' creates a reference between the local subscriber number and his identity at the external server (registrar). The flag forces creating the reverse references to all local subscriber numbers, so that the externally presented name or number will result from the reverse map.

- Routing options

Routing options

☐ Allow direct SIP routing

- Allow direct SIP routing

If ticked, it allows the direct routing of SIP to SIP calls without passing through the Layer 3 administration modules (not recommended).

- Performance options

Performance options

☐ Establish TLS connection queue

If ticked

- Establish TLS connection queue

To avoid system overload if too many TLS linkups are expected at the same time after system restart, this queue can be activated.

- Security options

Security options

☐ Do not ignore unauthorized sites ☐ Do not use authorization

- Do not ignore unauthorized sites

Authorization is enabled by default and unauthorized sites are ignored to prevent / minimize the risk of DoS attacks. Checking this option is not recommended, a site which has no authorization to use this NMG, would then receive a reply stating.

- Do not use authorization

Account and password are not verified when logging in.



- Signaling options

Signalling options

☐ Use to header uri instead of request URI
 ☐ Add no optional at host ip to the call ID

☐ Ignore always every received contact field
 ☐ Use Received Contact Only With At

- Use to header uri instead of request URI

If checked, the „To:“ header field is used instead of the INVITE request URI in the SIP protocol.

- Ignore always every received contact field

The address in the field “contact” of the received SIP session will not be included into the URI of the following SIP sessions.

- Add no optional at host ip to the call ID

Adds the call ID to the end of an outgoing SIP session.

@IP-Adresse: bilioew-gnv-uyefybqbrutfgi@192.169.40.162

Without: bilioew-gnv-uyefybqbrutfgi

- Use Received Contact Only With At

Similar to „Ignore always every received contact field“.

If there is no IP address or hostname provided in the received contact field, the content will not be included as URI in the following SIP sessions.

- ISDN GW options

ISDN GW options

Send progress

None

- Send progress

The progress indication will be sent (in the ISDN leg).

Indication type

Destination is non ISDN

The terminal is not ISDN equipment.

Call is not „End to End“

This option indicates that the call is passing through a non ISDN network.

### 6.2.4.2.1.3 SIP Timeout Options

Here the various timeout options are set for the SIP application running on the System. These timeouts are set to standard values, which by default should work with the various environments that the NMG could be used in.

- Call setup timeout (s)

SIP Timeout Options

Call setup timeout (s):

102

Repeat interval (ms):

500

Maximal number of repeats:

0

Ping time (s, 0 = disabled):

0

Disconnect wait (s):

10

Expire time for active calls (s):

28800

System session timeout (s) MUST > Expire time:

86400

Time limit to cache DNS resolutions (s):

86400

Maximum number of retries to resolve an address (s):

0

Backoff time for unresolved name:

0

DNS request timeout:

0

URI SIP resolution timeout:

0

Registration Expire Time:

0

Public registration expire time:

300

Proxy link expire time:

180

Inter digit timer delay (s):

0

Fake alerting timer delay (s):

7

Wait for alert timer delay (s):

0

Wait for connect timer delay (s):

0

Wait for release timer delay (s):

0

Wait for release complete timer delay (s):

0

Disconnect tone duration (s):

0



- The Call setup timeout for outgoing SIP calls.
- Repeat interval (ms)  
The interval between Call setup attempts to the ISDN network.
- Maximal number of repeats  
The maximal number of attempts to route / contact the ISDN network (call setup).
- Ping time  
Time between each „ping“ sent to ensure that the session is still valid (0 = disabled).
- Disconnect wait (s)  
The time that the system will wait before automatically disconnecting any calls that may not have been cleared correctly.
- Expire time for active calls (s)  
The maximal time that a SIP call may be active (prevents unnecessary IP traffic and use in the case of SIP errors during the disconnect stage).
- System session timeout (s) Must > Expire time  
The maximal time that a single session may be active for. This time MUST BE larger than the Expire time for active calls.
- Time limit to cache DNS resolutions (s)  
The time limit that is used before any DNS cache entries are cleared (cache flushing).
- Maximum number of retries to resolve an address (s)  
The maximal number of attempts to resolve an address to it's ISDN counterpart.
- Back off for unresolved name  
The time span between unsuccessful attempts to resolve an address/name.
- DNS request timeout  
The timeout for DNS requests.
- URI SIP resolution timeout  
The timeout before unsuccessfully SIP resolution actions are accounted as failed.
- Registration Expire Time  
The expire time which this NMG uses to register at an external system.
- Public registration expire time  
The expire time which this NMG uses to register at a public external system.
- Proxy link expire time  
The time interval used internally by the NMG, to keep temporary information. Please leave this value unchanged, unless the NovaTec support team recommends using another value.
- Inter digit timer delay (s)  
Automatically clear the call, after the number of seconds entered here, once the called party has hung up.
- Fake alerting timer delay (s)  
The NMG will „fake“ the alerting signal, when the network / user has not responded to the call setup within the time here. The tone type is set here.

- Wait for alert timer delay (s)  
The maximal waiting time for the ALERT signal before aborting the call.
- Wait for connect timer delay (s)  
The maximal waiting time for the CONNECT signal before aborting the call.
- Wait for release timer delay (s)  
The maximal waiting time for the RELEASE signal, before carrying out normal call clearing.
- Wait for release complete timer delay (s)  
The maximal waiting time for the RELEASE COMPLETE signal, before carrying out normal call clearing.
- Disconnect tone duration (s)  
Automatically clear the call, after the number of seconds entered here, once the called party has hung up.

#### 6.2.4.2.1.4 Trunks

This chapter explains the special settings for a configuration of an SIP trunk to a Cisco CUCM.

Any other partner but CUCM does not need these special settings.

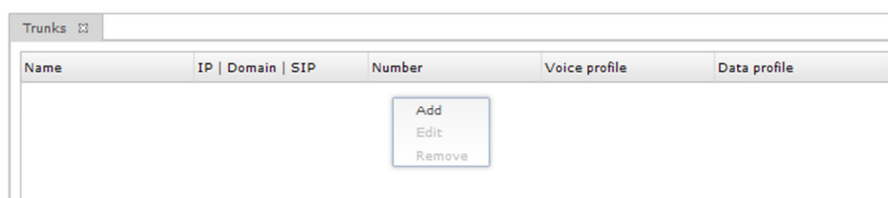
Click on trunk. The following window appears:



Name	IP   Domain   SIP	Number	Voice profile	Data profile
------	-------------------	--------	---------------	--------------

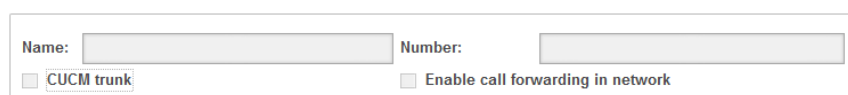
To create trunk(s) right-click into the section „Trunks“ and select “ADD” from the pop up menu. Enter the exact parameter of the trunk.

Each entry or trunk can be edited (Edit) or removed (Remove) with a click onto corresponding trunk with the right mouse button.



Name	IP   Domain   SIP	Number	Voice profile	Data profile
------	-------------------	--------	---------------	--------------

The window SIP trunk appears:



Name:  Number:

☐ CUCM trunk ☐ Enable call forwarding in network

- Name  
Edit any name for the trunk like publisher or subscriber etc.
- Number

Head number of the trunk line

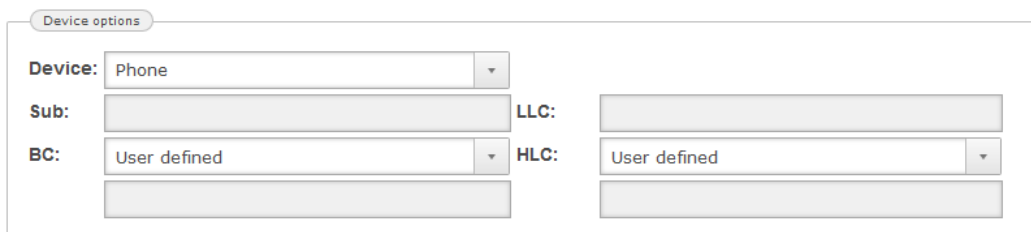
- CUCM trunk

This option does not need to be activated, if the option „Ping of the SIP Trunks within the CUCM configuration“ has been activated.

- Enable call forwarding in network

Call forwarding will be done on the remote end when enabled.

- Device options



The 'Device options' form contains the following fields:

- Device:** A dropdown menu with 'Phone' selected.
- Sub:** An empty text input field.
- BC:** A dropdown menu with 'User defined' selected.
- LLC:** An empty text input field.
- HLC:** A dropdown menu with 'User defined' selected.

- Device

Select the device for this user. Valid devices are phone, facsimile, modem or combined device.

- Sub

Enter here the sub address information element.

- BC

Select here the bearer capability of this user.

- LLC

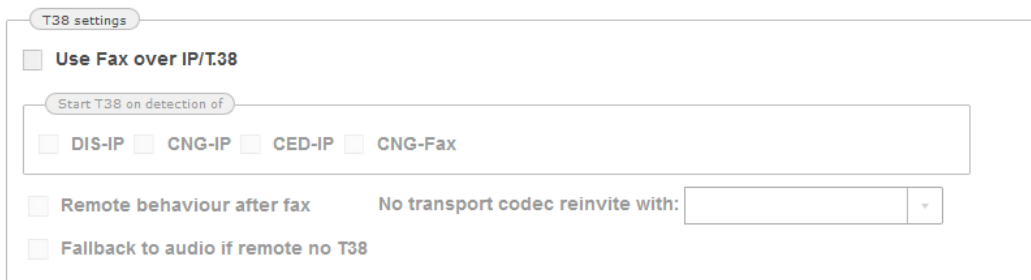
Enter here the low layer compatibility information element.

- HLC

Select here the high layer compatibility of this user.

- T38 Settings

**This function will be implemented in a higher / later version of NAMES.**

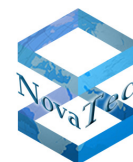


The 'T38 settings' form contains the following fields:

- ☐ **Use Fax over IP/T.38**
- Start T38 on detection of** (dropdown menu):
  - ☐ DIS-IP
  - ☐ CNG-IP
  - ☐ CED-IP
  - ☐ CNG-Fax
- ☐ **Remote behaviour after fax**      **No transport codec reinvoke with:** (dropdown menu)
- ☐ **Fallback to audio if remote no T38**

- Use Fax over IP/T.38

Check this option to enable or disable the T.38 functionality.



It is recommended to prioritize the transparent voice codecs (for example: pcm-aLaw, pcm-uLaw,...) higher than non-transparent voice codecs to increase the likelihood to send a fax to non T.38 enabled devices.

- DIS-IP  
Digital Identification Signal (over IP)
- CNG-IP  
Calling tone (over IP)
- CED-IP  
Called Terminal Identification (over IP)
- CNG-Fax  
Calling Tone (from own facsimile)
- Remote behavior after fax

If this option is disabled, the system closes the connection after completion of fax-transfer.

By activation of this option, the system depends on the remote side behaviour, i.e. the remote side decides to close or not to close the connection.

- Fallback to audio if remote no T38  
If the remote side does not support T.38, normally the T.38 connection would be closed.  
After activation of this flag, if the remote side does not support T.38, the system tries to „fall-back“ to audio, i.e. the system tries to use a transparent codec (negotiated at the first session establishment) to establish a T.38 connection.
- No transport codec reinvite with  
If at the initial session establishment no transparent codec was negotiated and the system tries to send a facsimile, you can choose to re-invite with a new negotiated transparent-codec or direct with the T.38 protocol.

- Address settings

A screenshot of the 'Address settings' dialog box. It contains a 'URI:' label followed by a text input field. Below it is an 'IP service:' label followed by a dropdown menu currently showing 'UDP'. At the bottom, there are three checkboxes: 'Correct faulty format', 'Public access', and 'Can redirect in LAN', all of which are currently unchecked.

URI

- The URI, user name or IP address.
- IP service  
There are three protocols to choose from, depending on the type of service required. The three protocols are: UDP, TCP and TLS.
- Correct faulty format  
If this option is checked, then faulty/incomplete IP addresses will be accepted.
- Public access  
If this option is checked, public access is allowed
- Can redirect in LAN  
If this option is checked, a direct connection within a LAN is preferred (answer with 305/reflection if both SIP devices flagged and in LAN).



- Codec negotiation settings

A screenshot of the 'Codec negotiation settings' window. It has a title bar with the text 'Codec negotiation settings'. Inside, there are two labels: 'Pref. voice codec:' and 'Pref. data codec:'. Each label is followed by a dropdown menu. Both dropdown menus currently show 'Any (negotiate)' as the selected option.

- Pref. Voice codec/ Pref. data codec

The preferred voice and data codecs to be used for this user. These options can be used to „force“ a specific user to use specific codecs contrary to the standard codec negotiation settings.

- Account settings

A screenshot of the 'Account settings' window. It has a title bar with the text 'Account settings'. Inside, there are four settings: 'SRTP mode:' with a dropdown menu showing 'Do not use'; 'RTP timeout:' with a numeric input field showing '0' and up/down arrows; 'VoIP port profile voice:' with a dropdown menu; and 'VoIP port profile data:' with a dropdown menu.

- SRTP mode

Here, the encryption mode can be set. Possible values are:

- Do not use

Encryption should not be used for this user.

- Try to use

Encryption should be used for this user as default, however if no encryption capability is available (either on this system, or the called party) the call will be made anyway.

- Must use

Encryption must be used by this user. If no encryption capability is available (either on this system, or the called party) the call will not be completed.

- VoIP port profile voice/ VoIP port profile data

In this section, the profiles that may have been created in VoIP port profiles, are assigned to the available SIP interfaces and define the default behaviour of these interfaces. If you have not created any port profiles, the standard port profile is automatically assigned to the available interfaces. If you delete a profile, which was previously assigned to an interface, the standard profile is automatically re-assigned to the interface(s).

- RTP timeout

The time (in milli seconds) to be used for the SIP packet time encoding.

A screenshot of a settings section. It contains a label 'Minimal number of digits:' followed by a text input field. To the right of this is a checkbox labeled 'Disable early media for voice'. Below the first label is another checkbox labeled 'Disable early media for data'.

- Minimal number of digits

Here the minimal number of digits is set. This number represents the minimal number of digits that will be cached, before the number is considered to be complete, and the Call setup will be carried out.

- Disable early media for data

If this option is checked, then the EARLY MEDIA event is sent for data calls. This of course incurs traffic over the RTP stream, which in some cases may not be desirable. If this is the case, the EARLY MEDIA event can be de-activated (checking the option).

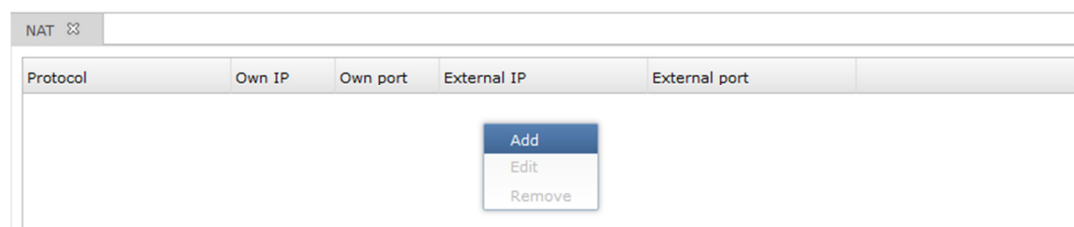
- Disable early media for voice

If this option is not checked, then the EARLY MEDIA event is sent for voice calls. This of course incurs traffic over the RTP stream, which in some cases may not be desirable. If this is the case, the EARLY MEDIA event can be de-activated (checking the option). The standard setting is activated.

#### 6.2.4.2.2 NAT

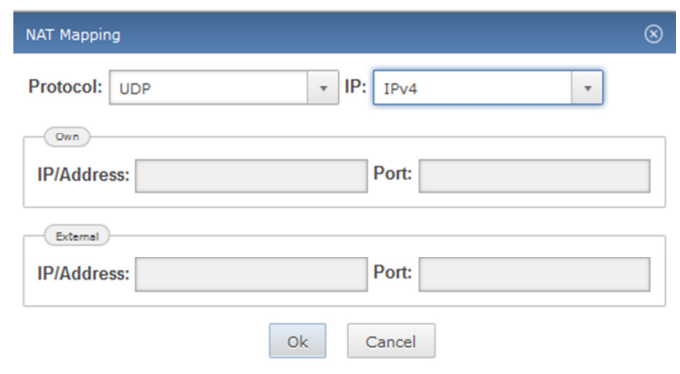
The System NAT mapping is the configuration page to set up the NMG system when working behind a firewall/router and a connection is required to the internet. Most notably for the NIP, VSMSC, and SIM server-SIM client applications. Various modules / applications use these settings. It is advisable to make changes here with the help of the Network Administrator to avoid any problems.

Click on „NAT“. The following window appears:



To create a NAT mapping, right-click into the NAT window. The Following window appears: NAT Mapping

- Protocol  
The protocol can be set to UDP or TCP.
- IP  
The RTP-IP address can be found on CCU.
- Own IP/Address  
The IP address can be found on the CCU.
- Port  
The internal port has to be mapped.



- External IP/Address  
This is where the IP address of the firewall would be entered. If this box is left blank (or filled with zero's), the standard IP address or the domain name will be used (if entered).
- Port  
The port that is to be mapped to. This must be set, so that any request / connections to the firewall on this port are forwarded to the IP address port as set in the second column. As mentioned previously, these settings should be made with the help of the Network Administrator.

#### 6.2.4.2.3 STUN

STUN enables a device to find out its public IP address and the type of NAT service its sitting behind.

STUN operates on TCP and UDP port 3478. STUN and NAT have not been defined for IPv6, because none of them is necessary in IPv6 network.



- STUN

- Mode

Three settings are available: Off, Server and Client.

**STUN Client:** A STUN client (also just referred to as a client) is an entity that generates STUN requests. A STUN client can execute on an end system, such as a user's PC, or can run in a network element, such as a conferencing server.

**STUN Server:** A STUN Server (also just referred to as a server) is an entity that receives STUN requests, and sends STUN responses. STUN servers are generally attached to the public Internet.

- Own port

The port on which the service will be sending on.

- Remote server IP

The IP address of the remote machine / service that this service is to connect to. This value is only applicable if this service is a **client**.

- Remote server name

The (domain) name of the remote machine / service that this service is to connect to. This value is only applicable if this service is a **client**.

- Remote port

The port on which the service will be receiving on, for example 3478 for STUN.

## 6.2.4.3 ISDN

### 6.2.4.3.1 Trunks

This section explains how to provide an ISDN trunk to a second party PABX, PSTN line or gateway. The ISDN Trunk can be created in master or slave mode.

Click on „Trunk“. The following window appears:

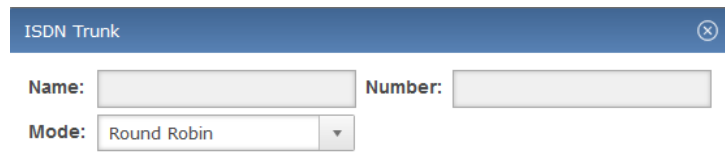
Name	Mode	Number	Interfaces
------	------	--------	------------

To create an ISDN trunk right-click in the section „Trunk“ and then onto “Add” in the pop up menu. In the window opening up you can remove, edit or fill in the required parameter of the trunk system.

Name	Mode	Number	Interfaces
<div> Add  Edit  Remove </div>			

The window “ISDN Trunk” appears:





The 'ISDN Trunk' window contains three fields: 'Name' (text input), 'Number' (text input), and 'Mode' (dropdown menu currently showing 'Round Robin').

- ISDN Trunk

- Name

Any name can be used for the trunk.

- Mode

Round-robin

For each call that comes to this trunk, the next interface will be used for that call. For example, there are four interfaces assigned to this trunk, 1, 2, 3 and 4. The last call that came to this trunk was sent to interface 2, therefore, the next call will be sent to interface 3, the next to interface 4 ....

This mode of operation ensures that all interfaces within a trunk are evenly used.

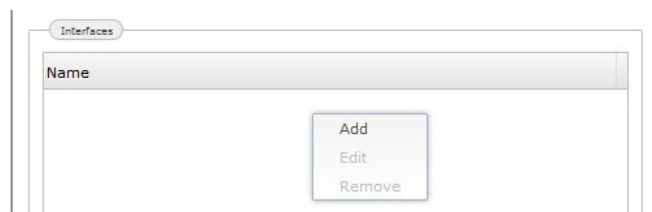
Sequential

In this mode of operation, each interface in the trunk is used in order, i.e. if of the four interfaces assigned to this trunk, interface 1 is in use, then the next call will be sent to interface 2, if in the meantime the call using interface 1 has been completed, and another call comes in on this trunk, then it will use interface 1, as it is free.

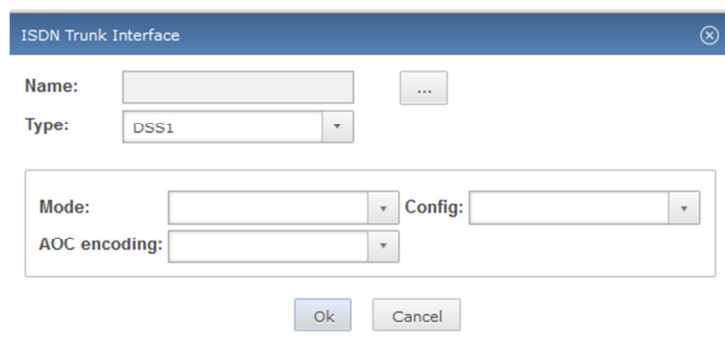
- Number

Head number of the trunks

The next step is to setup the interfaces of the trunk: Right-click into the section "Interfaces" and select "Add" from the pop up menu to edit the local parameter. All entries regarding the trunk can be changed by selecting "Edit" or deleted by selecting "Remove" instead of "Add".

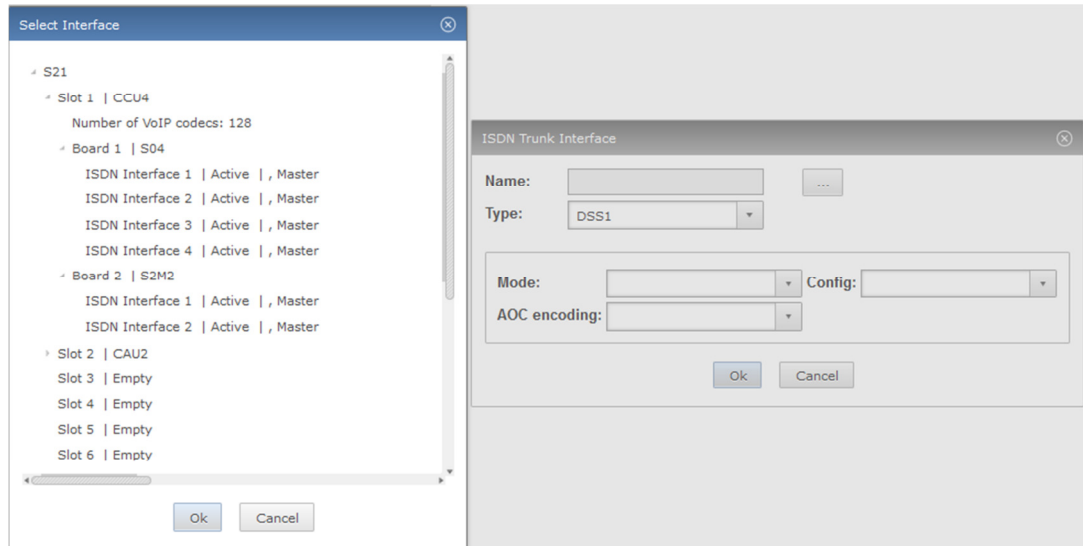


After selecting "Add", the following window appears:

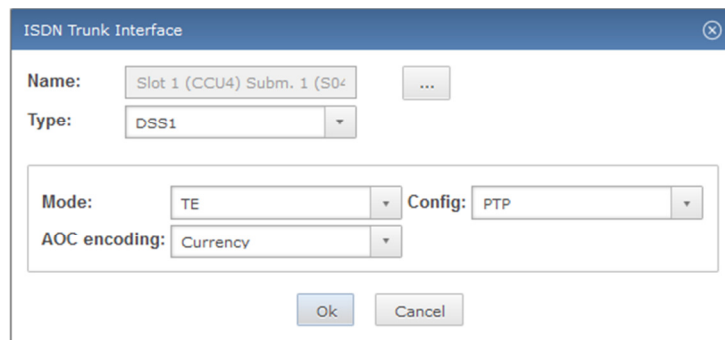


The 'ISDN Trunk Interface' window contains several fields: 'Name' (text input with a browse button '...'), 'Type' (dropdown menu showing 'DSS1'), 'Mode' (dropdown menu), 'Config' (dropdown menu), and 'AOC encoding' (dropdown menu). At the bottom are 'Ok' and 'Cancel' buttons.

Press „...” and choose the available interfaces in the opening window to assign them to the corresponding trunk:



After choosing the required interface press button “Ok”.



The selected interface appears in the box „Name”. Further settings are necessary:

- Type  
DSS1  
QSIG
- Mode  
TE  
NT
- Config  
PTP -> Point to point connection with TEI=0 (for example PABX Trunks)  
PTMP -> Point to multi point connection (up to 50 MSNs possible)
- AOC encoding
  - Currency  
If AOC information needs to be generated by the target, it will be sent as currency.
  - Units  
If AOC information needs to be generated by the target, it will be sent as units.

Outgoing calls can be distributed between the interfaces of a trunk by the system in a given sequence. The sequence can be changed by dragging the appropriate interface up or down within the list of interfaces.

#### 6.2.4.4 Call Routing

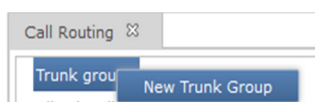
This chapter describes how to create trunk groups, subscriber groups and line groups and the setup of routings between them.

The first step is to create the trunk group:

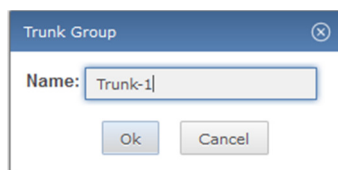
##### 6.2.4.4.1 Trunk groups

###### 6.2.4.4.1.1 New Trunk Group

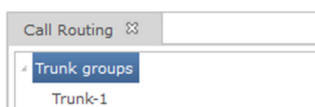
Click on call routing and the following window will appear. Right-click onto "Trunk Group" and then onto "New Trunk Group" in the pop up menu.



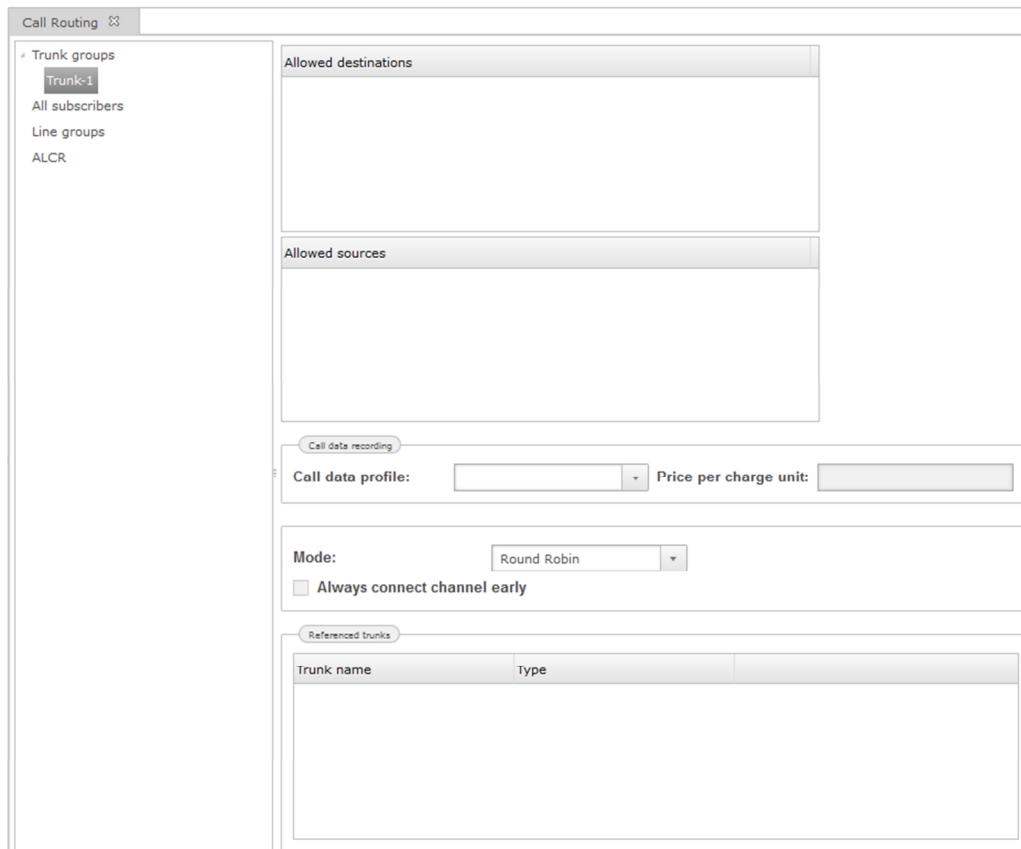
The following window appears:



Enter a name for the trunk group (here Trunk-1). Click on Ok. The following window appears:



In the new window the new trunk group (here Trunk-1) is now visible. For further settings simply click onto Trunk-1 and following window appears:



- The box „Allowed destination“:  
Is for all destinations like subscribers of the system itself.
- The box “Allowed sources”:  
Is for all outer destinations.
- Section Call data recording
  - Call data profile  
Is a selection of the profiles which have been created as call data profiles before ([See chapter 6.2.4.8](#)).
  - Price per charge unit  
The unit cost of the trunk line in the local currency can be entered here. It is advisable to enter the value of 0.01 here for internally generated unit charges. This value must also be entered on the subscriber's terminal equipment. For externally generated unit charges, enter the trunk line standard price i.e the price per unit of the provider.
- Mode
  - Round Robin  
For each call that comes to this trunk group, the next interface will be used for that call. For example, there are four interfaces assigned to this trunk group, 1, 2, 3 and 4. The last call that came to this trunk group was sent to interface 2, therefore, the next call will be sent to interface 3, the next to interface 4 ....  
This mode of operation ensures that all interfaces within a trunk group are evenly used.
  - Sequential



In this mode of operation, each interface in the trunk group is used in order, i.e. if of the four interfaces assigned to this trunk group, interface 1 is in use, the next call will be sent to interface 2, if in the meantime the call using interface 1 has been completed and another call comes in on this trunk group, it will use interface 1, as it is free.

This method is not recommended for use in trunk groups that have GSM interfaces assigned to it, as the SIMs used by the interfaces will not be evenly used.

- Always connect channel early

If this option is activated, the NovaTec gateway will always connect the b-channel through when the call is alerting even if the called PBX does not signal/indicate the presence of a ring back tone. This is the default setting and matches the behaviour of previous firmware versions.

If the option is deactivated, the NovaTec gateway will play its own ring back tone when the call is alerting and the PBX does not signal/indicate the presence of a ring back tone.

- Referenced trunks

All trunk groups listed here (SIP or ISDN) will receive the same sequence mode as selected under top down menu of mode. The sequence can be changed by select and pull function with a click onto the trunk group.

- Number Modification

Number modifications are optional and can be created to modify or change the parameters like calling number of a call session. Also during routing of a call the prefix of a calling number can be removed or the configured head number of the trunk inserted. Generally for major number masquerading, the number modification can be used.

A number modification entry contains two parts: One part is called "Match" and the second is called "Action". The "Action" part determines, what and how is changed (for example: Add a prefix to the calling number or cut off a part of the caller number). The "Match" part determines under which circumstances the corresponding action is executed. For example: Under all circumstances or only for inbound calls or if the caller number has got a certain TON (Type of number).

Right-click into the window and select "Add" from the pop up menu. The following window appears:

A screenshot of a software window titled "Number modifications". It contains two columns: "Match" and "Action". Below these columns is a large empty rectangular area. A context menu is open over this area, showing three options: "Add", "Edit", and "Remove".

- Match

- Always (If checked)
- Direction (defines in which direction the "Action" is executed - "inbound" or "outbound" calls )
- Both  
(defines, that the "Action" is executed in both directions - "inbound" and "outbound" calls)
  - Incoming  
Execute the "Action" only for inbound calls.
  - Outgoing  
Execute the "Action" only for outbound calls.

- Calling number

Execute the "Action" only when the caller number is identical to the included prefix in the match list. In case there is no entry in the match list, the "Action" will be executed regardless of the caller number.

- **Called number**  
Execute the "Action" only when the calling number is identical to the included prefix in the match list. In case there is no entry in the match list, the "Action" will be executed regardless of the calling number.
- **Calling TON**  
Execute the "Action" only when the TON (Type of number) of the caller number is identical to the included TON in the match list. If there is no entry in the match list, the "Action" will be executed regardless of the TON of the caller number.
- **Called TON**  
Execute the "Action" only if the TON (Type Of Number) of the calling number is identical to the included prefix in the match list. In case there is no entry in the match list, the "Action" will be executed regardless of the TON of the calling number.

All corresponding sectors under "Match" will be operated as an "AND Operation", if more than one sector has been filled out. If for example a value has been edited under direction and calling number the call route and the calling number must be equal to the included values to execute the appropriate "Action".

Match

☐ Always

Direction:

Calling number:

Called number:

Calling TON:

Called TON:

Action

Calling number

Set TON:

Set NPI:

AddPrefix:

DelPrefix:

AddSuffix:

DelSuffix:

Insert

At position:

Digits:

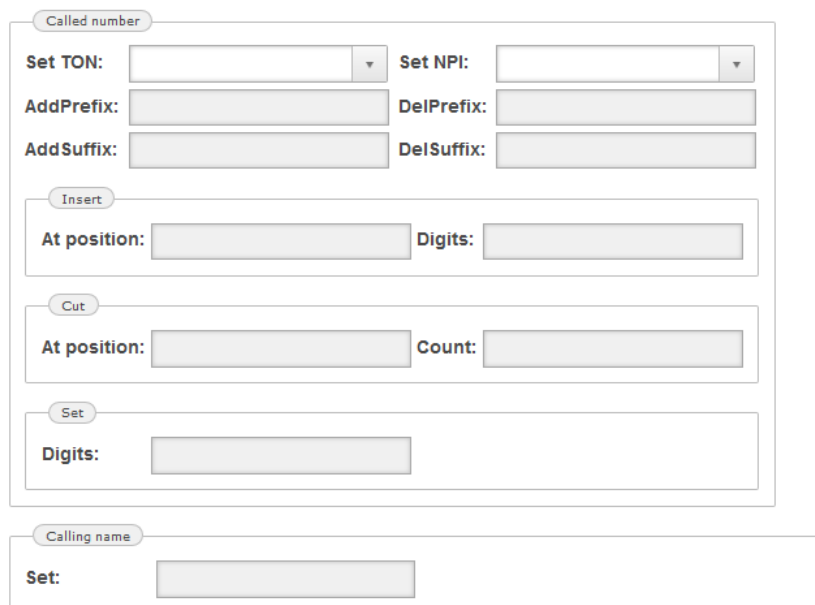
Cut

At position:

Count:

Set

Digits:



- Action (what is to be executed?)
  - Calling Number
 

All entries in these boxes of the group will change the calling number:

    - Set TON: Change the type of number to the entered value!
    - Set NPI: Change the numbering plan identification NPI like ISDN, data etc. to the entered value!
    - AddPrefix: Insert the following digits at the beginning of the number.
    - DelPrefix: Delete the following digits from the beginning of the number (only at match).
    - AddSuffix: Insert the following digits at the end of the number.
    - DelSuffix: Delete the following digits from the end of the number.
    - Insert: Insert the following digits at the given position in the string of the number.
    - Cut: Delete the following number of digits from the given position in the string of the number.
    - Set: Exchange the whole number against the one following.
  - Called Number
 

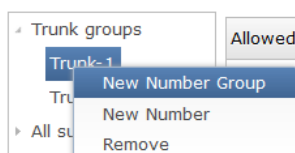
All entries into the boxes of this group will change the called number. The boxes for these settings are the same as for the calling number.
  - Calling Name
 

Change the calling name.

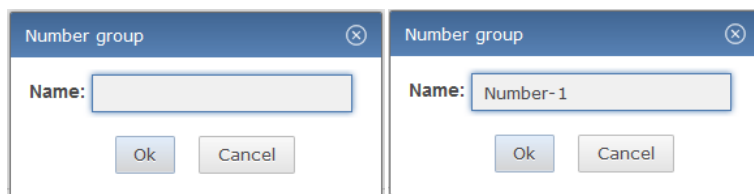
    - Set: Set the calling name to the entered value.

#### 6.2.4.4.1.1.1 New Number Group

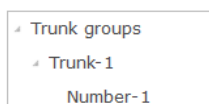
For the new created trunk group (here Trunk-1) a new number group and/or new number can be set. First a number group must be created: Right-click on "Trunk-1" and select "New Number Group" from the menu. In the following the settings for a new number are explained:



The following window appears:

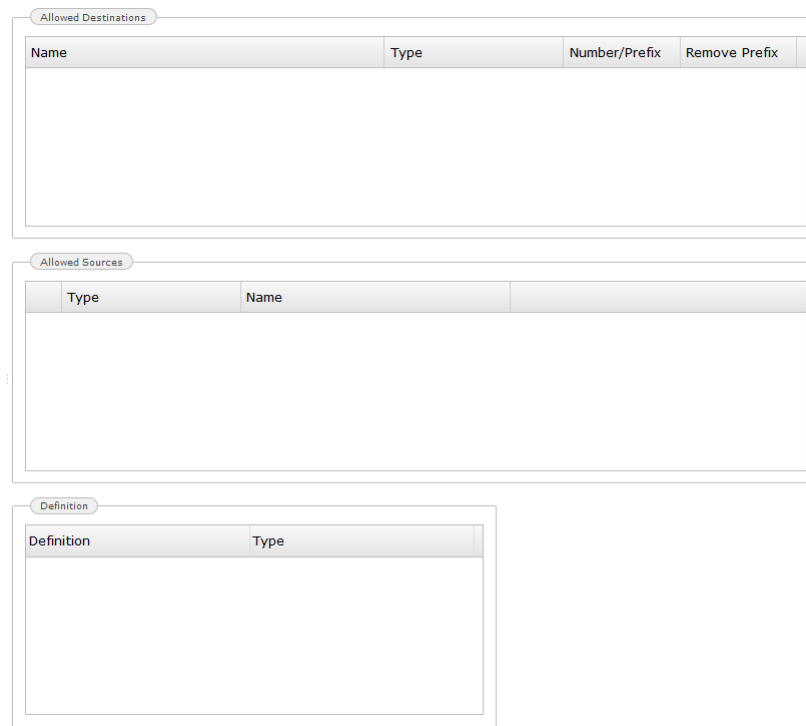


The number group can be named in the correlating window „Number group“. After clicking onto Ok, this given name appears under Trunk-1 (see following picture, here Number-1). In this number group single numbers or number ranges can be entered. For example the subscriber can setup an outbound call on Trunk-1 with this number group.



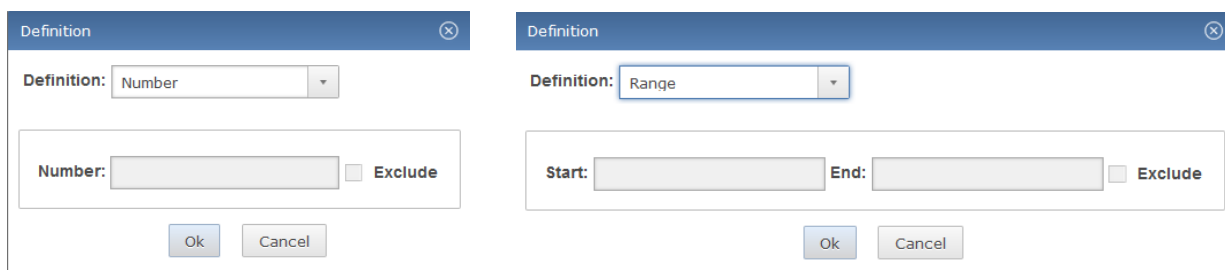


Click onto Number-1. The following window appears:



The image shows three stacked windows. The top window is titled 'Allowed Destinations' and contains a table with columns: Name, Type, Number/Prefix, and Remove Prefix. The middle window is titled 'Allowed Sources' and contains a table with columns: Type and Name. The bottom window is titled 'Definition' and contains a table with columns: Definition and Type.

To enter a single number or a range of numbers right-click under "Definition" and then select "Add" in the pop up menu. The following window appears:



The image shows two 'Definition' windows side-by-side. The left window has 'Definition' set to 'Number' and a text input field for 'Number' with an 'Exclude' checkbox. The right window has 'Definition' set to 'Range' and text input fields for 'Start' and 'End' with an 'Exclude' checkbox. Both windows have 'Ok' and 'Cancel' buttons at the bottom.

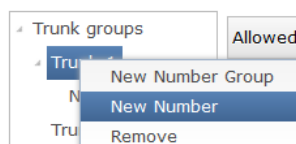
- **Definition**  
Is a drop down menu to adjust whether you are defining a number or a range of numbers.
  - **Number**  
After selecting "Number" only one prefix should be included to assign a trunk.
  - **Range**  
If „Range" is selected, a range of numbers (for example Start:0 and End: 9) can be defined to assign a trunk.
- **Exclude**  
If this box is ticked, the corresponding number or range of numbers is blocked and cannot assign this trunk.

It is also possible that two number ranges overlap. For example one range can start with the digit "3" and end on "9", whilst the range from "31" to "32" within the above mentioned range is blocked.

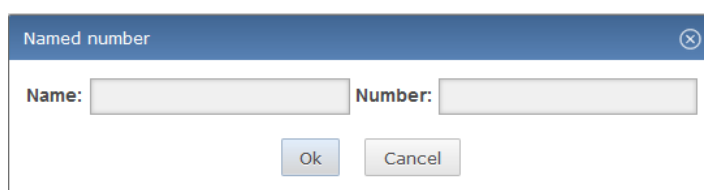
Definition	
Definition	Type
21	Number
0 - 1	Range
22 - 29	Range
3 - 9	Range
31 - 32, barred	Range
20, barred	Number

#### 6.2.4.4.1.1.2 New Number

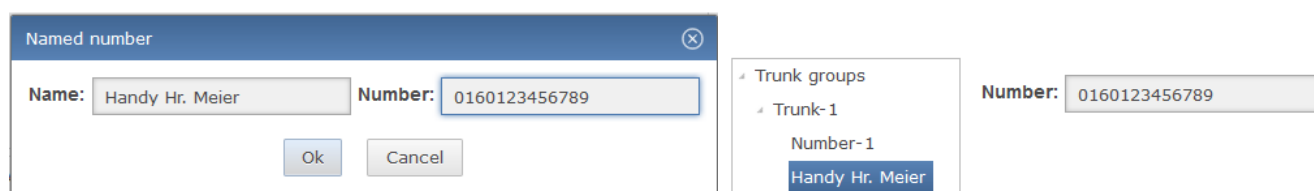
To create a new number, right-click TRUNK-1 and select "New Number":



The following window appears:




The name of the owner of the number should be entered under „NAME“ and the corresponding number under „Number“ (see below picture) and confirmed with Ok. The owner name will appear under Trunk-1/ Number-1.



The named number can also be used for routing (subscriber, line group, trunk group and call data profile). All settings under trunk groups can be changed, edited or removed.

#### 6.2.4.4.2 All subscribers

All settings of every subscriber are gathered under all subscribers. Here one or more subscribers can be combined to a subscriber group and all subscriber groups are subordinated to the item "All subscribers". Settings made under "All subscribers" are inherited by all subscriber groups. Settings made within a subscriber group are inherited by all subscribers of that group. Here also permissions can be granted. Simply click the permissions you want to grant to do so. A green tick  appears. In order to withdraw permission you only need to click it anew. Permissions granted here are valid for subscriber groups and subscriber.

Allowed Destinations

Name	Type	Number/Prefix	Remove Prefix

Allowed Sources

Type	Name

Permissions

<input type="checkbox"/> Short Code Dialing	<input type="checkbox"/> Call Forwarding	<input type="checkbox"/> Hold	<input type="checkbox"/> Explicit call transfer
<input type="checkbox"/> Call take over	<input type="checkbox"/> Advice of charge	<input type="checkbox"/> Three party	<input type="checkbox"/> MLPP

Permissions

<input checked="" type="checkbox"/> Short Code Dialing	<input checked="" type="checkbox"/> Call Forwarding	<input checked="" type="checkbox"/> Hold	<input checked="" type="checkbox"/> Explicit call transfer
<input checked="" type="checkbox"/> Call take over	<input checked="" type="checkbox"/> Advice of charge	<input checked="" type="checkbox"/> Three party	<input checked="" type="checkbox"/> MLPP

- Call data recording

Call data recording

Call data profile:

Price per charge unit:

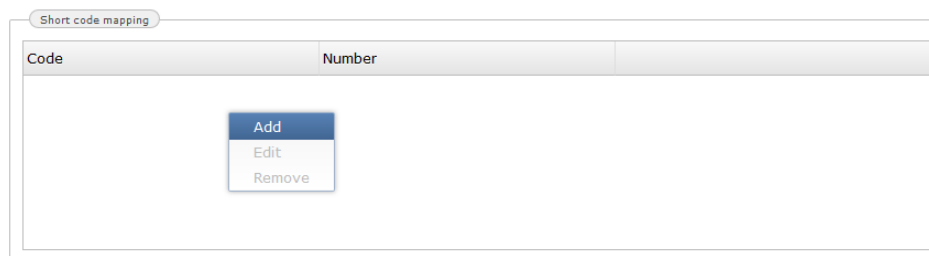
- Call data profile

If call data of all subscriber groups and of all subscribers within the groups needs to be stored, you need to select a profile previously created within the call data profiles ([see chapter 6.2.4.8](#)). The selected profile is then valid for all subscriber groups and subscribers.

- Price per charge unit

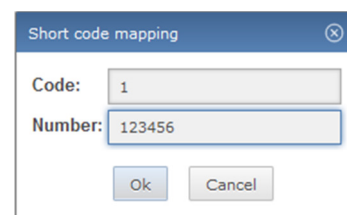
If a profile has been selected, you have the possibility to enter the charge per unit here. The entered value is then valid for all subscriber groups and subscribers. If no call data profile is selected this box remains grey.

- Short code mapping



The 'Short code mapping' window contains a table with two columns: 'Code' and 'Number'. Below the table is a context menu with three options: 'Add', 'Edit', and 'Remove'.

- Short code dialing  
Enter the short code dialing number here.
- Number  
Enter the destination telephone number here.



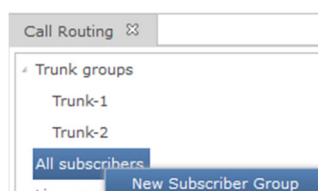
The 'Short code mapping' dialog box has two input fields: 'Code' with the value '1' and 'Number' with the value '123456'. At the bottom are 'Ok' and 'Cancel' buttons.

- Number modifications  
For more details please see [chapter 6.2.4.4.1.1](#).

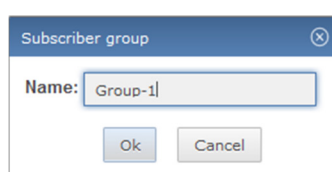
#### 6.2.4.4.2.1 Subscriber group

A subscriber group can be created as follows:

Right-click on „All subscribers“ and select „New Subscriber Group“:



The following window appears:



The 'Subscriber group' dialog box has a 'Name:' label and a text input field containing 'Group-1'. At the bottom are 'Ok' and 'Cancel' buttons.

Enter a name for the subscriber group and press Ok. A second window appears:

In this window the created group is shown as sub item of „All subscribers“.

Trunk groups
SIP-CM
All subscribers
Group-1
Line groups
ALCR

Allowed Destinations

Name	Type	Number/Prefix	Remove Prefix
------	------	---------------	---------------

Allowed Sources

Type	Name
------	------

Permissions

Short Code Dialing

Call Forwarding

Hold

Explicit call transfer




Call take over

Advice of charge

Three party

MLPP

- Permissions

The green arrow pointing downwards  in the section permission means, that all the settings in the upper instances within the configuration have been adopted. A green tick  in the permission box means, that the setting is only active here. A white cross on red  tells you, that the corresponding permission is deactivated.

- Call data recording

Call data recording

Call data profile:
Price per charge unit:

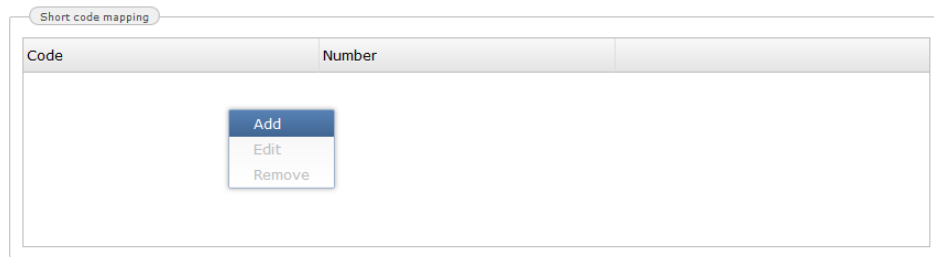
- Call data profile

If call data of the subscriber group or of the subscribers within the group needs to be saved, a profile previously created in the call data profiles ([see chapter 6.2.4.8](#)) is selected. The selected profile is then valid for the subscriber group and for all subscribers within. Values from higher instances are replaced.

- Price per charge unit

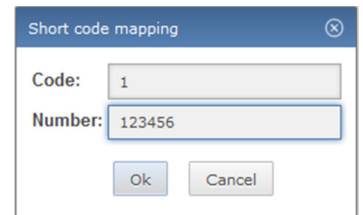
If a profile has been selected you have the possibility to enter a price per charge unit here. The entered value is valid for the subscriber group and the subscribers. Values from higher instances are replaced.

- Short code mapping



Code	Number
<div> Add  Edit  Remove </div>	

- Short code dialing  
Enter the short code dialing number here.
- Number  
Enter the destination telephone number here.



Short code mapping

Code: 1

Number: 123456

Ok Cancel

If values are entered these are valid for the subscriber group and the subscribers. Values from higher instances are replaced.

- Number modifications  
Is described more detailed under trunk groups ([see chapter 6.2.4.4.1.1](#))

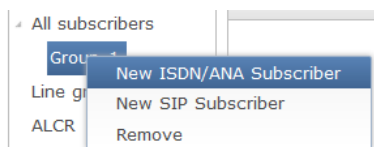
If values are entered these are valid for subscriber group and subscribers. Values from higher instances are replaced.

#### 6.2.4.4.2.1.1 Creating a Subscriber

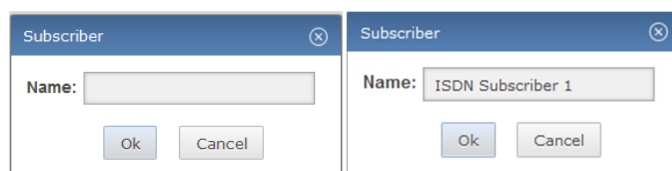
You can now set up an ISDN/ANA or SIP subscriber under subscriber group 1. First we will describe how to set up an ISDN/ANA subscriber. How to set up a SIP subscriber is described afterwards.

Please proceed as follows:

Right-click onto „Group-1“ and then select „New ISDN/ANA Subscriber“ from the menu.

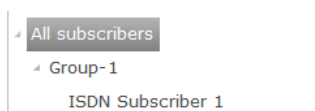


The following window appears:

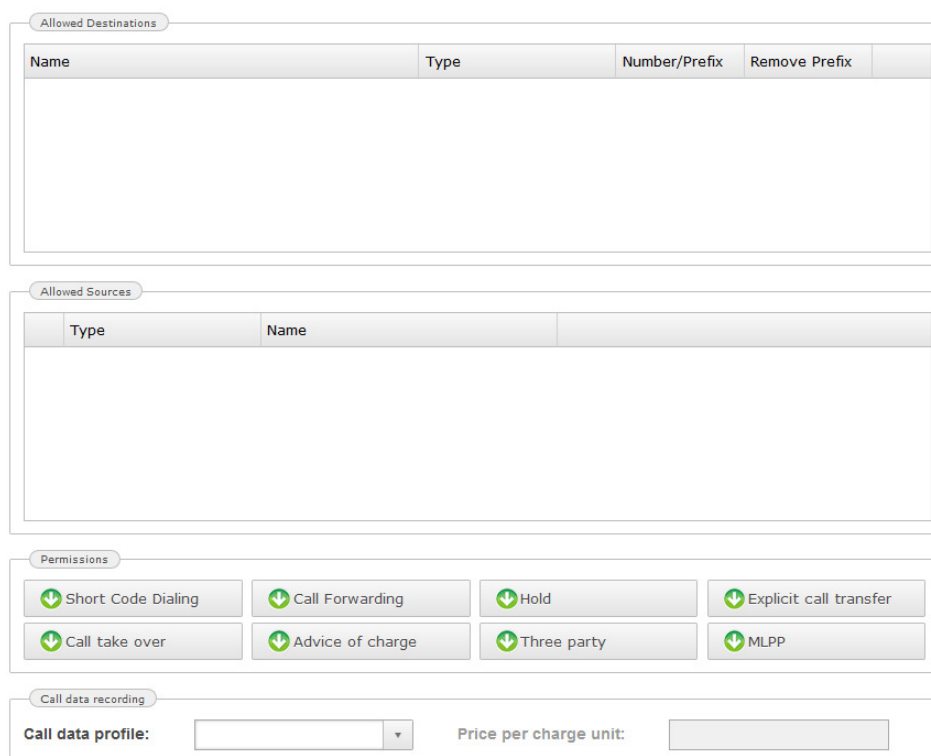


Two Subscriber dialog boxes are shown. The first has an empty Name field. The second has the Name field filled with "ISDN Subscriber 1". Both have Ok and Cancel buttons.

Please enter a name for the subscriber here. After pressing button "Ok" a further window will appear.






The created subscriber is then listed under „Group-1“. When setting up an ISDN or analogue subscriber there is no difference apart of the interface type. In order to make further adjustments to the subscriber settings, click onto the created subscriber. The following window opens:



The screenshot shows a configuration window with four main sections:

- Allowed Destinations:** A table with columns: Name, Type, Number/Prefix, Remove Prefix.
- Allowed Sources:** A table with columns: Type, Name.
- Permissions:** A grid of buttons for various call features: Short Code Dialing, Call Forwarding, Hold, Explicit call transfer, Call take over, Advice of charge, Three party, and MLPP. Each button has a green arrow icon.
- Call data recording:** Includes a dropdown for "Call data profile:" and a text input for "Price per charge unit:".

- Permissions

The green arrow pointing downwards  in the section permission means, that all the settings in the upper instances within the configuration have been adopted. A green tick  in the permission box means, that the setting is only active here. A white cross on red  tells you, that the corresponding permission is deactivated.

- Call data recording
  - Call data profile

If you wish to save call data for the subscriber you need to select a profile created in call data profiles previously ([see chapter 6.2.4.8](#)).

- Price per charge unit

If a profile has been selected, you have the possibility to enter the price per charge unit here. The entered value is then valid for all subscriber groups and subscriber. Values from a higher instance are replaced.

Short code mapping

Code	Number
------	--------

Number modifications

Match	Action
-------	--------

#### Short code mapping

- Short code dialling  
Enter the short code dialling number here.
- Number  
Enter the destination telephone number here.

If values are entered these are valid for the corresponding subscriber group and subscriber. Values from higher instances are replaced.

- Number modifications  
For more details please ([see chapter 6.2.4.4.1.1](#))

If values are entered these are valid for the corresponding subscriber group and subscriber. Values from higher configurational instances are replaced.

Following definitions can be made in the next window:

Number:	<input type="text" value="6789123"/>	Description:	<input type="text"/>
Interface:	<input type="text" value="Slot 1 (CCU4) Subm. 1 (S0)"/> ...	Call take over group:	<input type="text"/>


- Number  
Enter the subscriber number.
- Description  
You can enter a (unambiguous) description of the subscriber (name, department, etc.) in this row.
- Interface  
Select a dedicated interface for the subscriber with the  button.



- Call take over group

Select the call take over group of subscribers. The appropriate group must have been created in the call take over groups ([see chapter 6.2.4.5](#)).

- Device options



The 'Device options' form contains the following fields:

- Device:** A dropdown menu with 'Phone' selected.
- Sub:** A text input field.
- LLC:** A text input field.
- BC:** A dropdown menu with 'User defined' selected.
- HLC:** A dropdown menu with 'User defined' selected.
- AOC encoding:** A dropdown menu with 'Currency' selected.

- Device

Select the type of device connected to the chosen interface above. Available choices are phone, facsimile, modem or a combined device.

- Sub

The additional addressing possibility may be used as additional terminals after the ISDN subscribers interface to be addressed, such as the activation of an amplifier for an announcement or to start a computer program.

The maximum length of sub addresses is 42 digits.

- LLC

Enter here the individual low layer compatibility IE. The maximum length of the low layer compatibility IE is 22 digits.

- BC

Defines the mandatory bearer capability for this subscriber. You can choose between pre-defined profiles or, if you wish, use the user defined profile to declare an individual bearer capability. The maximum length of the bearer capability IE is 22 numbers.

- HLC

Define here the services used by the subscriber. You can choose between pre-defined profiles or, if you wish, use the user defined profile to declare an individual high layer compatibility IE. The maximum length of the high layer compatibility IE is 6 digits.

- AOC encoding

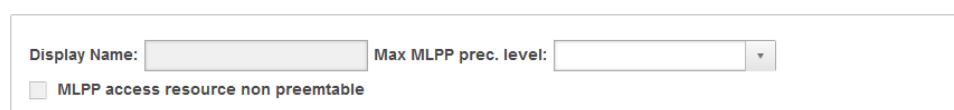
- Currency

If AOC information is to be generated by the target, it will be sent as currency.

- Units

If AOC information is to be generated by the target, then it will be sent as units.

Following definitions can be made in the next window:



The next window contains the following fields:

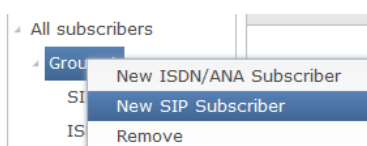
- Display Name:** A text input field.
- Max MLPP prec. level:** A dropdown menu.
- ☐ **MLPP access resource non preemptable**

- **Display Name**  
The subscriber name can be included here. This name will be shown if Q.SIG or SIP protocol is used. If the DSS1-protocol is used, this name will be sent to the display IE. Depending on the ISDN telephone used, this name is shown in the display of the telephone set.
- **Max MLPP prec. level**  
This box determines the priority of the subscriber.
- **MLPP access resource non preemptable**  
If this is selected, this subscriber is not allowed to interrupt the connection. If not checked, pre-emption is always allowed.

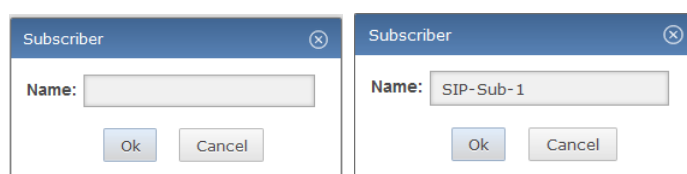
All settings of ISDN/ANA subscribers can be edited or removed.

#### 6.2.4.4.2.1.2 Creating a SIP Subscriber

Click on "Group-1" in the window shown below. The next appearing window allows the selection of a new SIP subscriber by click.



The following window appears:






Enter a subscriber name (here SIP-Sub-1) and confirm with Ok.



The given name appears under "Group-1" in the „All subscribers" tree.

For further settings of the SIP subscriber, just click onto the subscriber (here SIP-Sub-1). The following window appears:

- Permissions

The green arrow pointing downwards  in the section permission means, that all the settings in the upper instances within the configuration have been adopted. A green tick  in the permission box means, that the setting is only active here. A white cross on red  tells you, that the corresponding permission is deactivated.

- Call data recording
  - Call data profile
    - If you wish to save call data for the subscriber you need to select a profile created in call data profiles previously ([see chapter 6.2.4.8](#)). The selected profile is then valid for the subscriber. Values from higher instances are replaced.
  - Price per charge unit

If a profile has been selected you have here the possibility to enter the price per charge unit. The entered value is then values for all subscriber groups and subscribers. Values from higher instances are replaced.

Short code mapping

Code	Number
------	--------

Number modifications

Match	Action
-------	--------

#### Short code mapping

- Short code dialling  
Enter the short code dialling number here.
- Number  
Enter the destination telephone number here.

If values are entered these are valid for the subscriber group and the subscriber. Values from higher instances are replaced.

- Number modifications  
Is described in detail under "Trunk groups" ([see chapter 6.2.4.4.1.1](#))

If values are entered these are valid for the subscriber group and the subscriber. Values from higher instances are replaced.

The next window enables you to make the following settings:

Number:	<input type="text"/>	Description:	<input type="text"/>
Call take over group:	<input type="text"/>	Display Name:	<input type="text"/>
Max MLPP prec. level:	<input type="text"/>	<input type="checkbox"/> MLPP access resource non preemptable	

- Number  
Entry of the participant's number
- Description  
You can enter a (unambiguous) description of the subscriber (name, department, etc.) in this row.
- Call take over group

Selection of the call take over group for the subscriber. The group has to be set up previously in call take over groups ([see chapter 6.2.4.5](#)).

- Display Name

The name of the subscriber can be included here. This name will be shown if the Q.SIG or SIP protocol is used. If the DSS1-protocol is used, this name will be sent to the display IE. Depending on the used ISDN telephone, this name will be shown in the display of the telephone set.

- Max MLPP prec. level

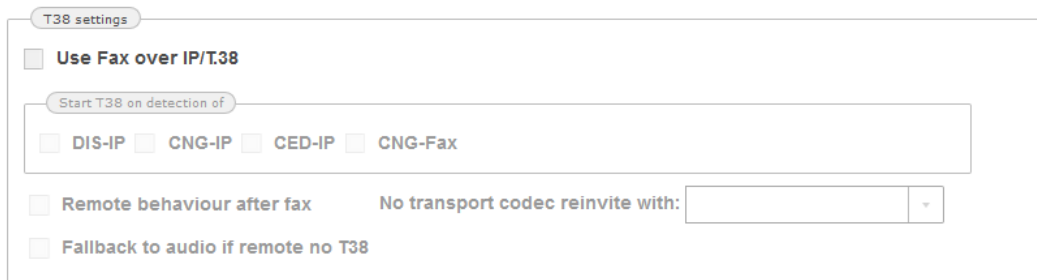
This field selects the priority of the subscriber.

- MLPP access resource non preemptable

If this is selected, the subscriber is not allowed to interrupt the connection. If not checked, preemption is always allowed.

- T38 settings

**This part will be implemented in a later version.**



- Use Fax over IP/T.38

Check this option to enable or disable the T.38 functionality.

It is recommended to prioritize the transparent voice codecs higher (for example: pcm-aLaw, pcm-uLaw,...) than non-transparent voice codecs to increase the likelihood to send a fax to non T.38-enabled devices.

- DIS-IP

Digital Identification Signal (over IP)

- CNG-IP

Calling tone (over IP)

- CED-IP

Called Terminal Identification (over IP)

- CNG-Fax

Calling Tone (from own facsimile)

- Remote behavior after fax

If this option is disabled, the system closes the connection after completion of fax-transfer.

By activation of this option, the system depends on the remote side behaviour, i.e. the remote side decides to close or not to close the connection.

- Fallback to audio if remote no T38

If the remote side does not support T.38, normally the T.38 connection would be closed.



After activation of this flag, if the remote side does not support T.38, the system tries to „fall-back“ to audio, i.e. the system tries to use a transparent codec (negotiated at the first session establishment) to establish a T.38 connection.

- No transport codec re-invite with

If at the initial session establishment no transparent codec was negotiated and the system tries to send a facsimile, you can choose to re-invite with a new negotiated transparent-codec or directly with the T.38 protocol.

- Address settings

A screenshot of the 'Address settings' form. It includes a 'URI:' label followed by a text input field. Below that is an 'IP service:' label followed by a dropdown menu currently showing 'UDP'. At the bottom, there are three checkboxes: 'Correct faulty format', 'Public access', and 'Can redirect in LAN', all of which are currently unchecked.

- URI

The URI, user name or IP address.

- IP service

There are three protocols to choose from, dependant of the type of service required. The three protocols are: UDP, TCP and TLS.

- Correct faulty format

If this option is checked, faulty/incomplete IP addresses will be accepted.

- Public access

If this option is checked, public access is allowed

- Can redirect in LAN

If this option is checked, prefer a direct connection within a LAN (answer with 305/reflection if both SIP devices flagged and in LAN).

- Codec negotiation settings

A screenshot of the 'Codec negotiation settings' form. It contains two labels: 'Pref. voice codec:' and 'Pref. data codec:'. Each label is followed by a dropdown menu, both of which are currently set to 'Any (negotiate)'.

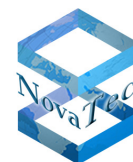
- Pref. Voice codec/ Pref. data codec

The preferred voice and data codecs to be used for this user. These options can be used to „force“ a specific user to use specific codecs contrary to the standard codec negotiation settings.

- Account settings

A screenshot of the 'Account settings' form. It includes an 'Account:' label with a text input field, and a 'Password:' label with a text input field. Below these are 'SRTP mode:' with a dropdown set to 'Do not use', and 'VoIP port profile voice:' with a dropdown. To the right of these are 'RTP timeout:' with a numeric input set to '0', and 'VoIP port profile data:' with a dropdown. At the bottom, there are four checkboxes: 'Simplified digest', 'Basic authorisation', 'Disable early media for voice', and 'Disable early media for data', all of which are currently unchecked.

- Account



- The account or user name.
- Password  
The password for the account.
- SRTP mode  
Here, the encryption mode can be set. Possible values are:
  - Do not use  
Encryption should not be used for this user.
  - Try to use  
Encryption should be used for this user as default, however if no encryption capability is available (either on this system, or the called party) the call should be made anyway.
  - Must use  
Encryption must be used by this user. If no encryption capability is available (either on this system, or the called party) the call will not be completed.
- RTP timeout  
The time (in milli seconds) used for the SIP packet time encoding.
- VoIP port profile voice/ VoIP port profile data  
In this section, the profiles that may have been created in VoIP port profiles, are assigned to the available SIP interfaces and define the default behaviour of the interfaces. If you have not created any port profiles, the standard port profile is automatically assigned to the available interfaces. If you delete a profile that was previously assigned to an interface, the standard profile is automatically re-assigned to the interface(s).
- Simplified digest  
If this option is checked, simplified digest will be used during the authorisation process.
- Basic authorization  
If this option is checked, basic authorisation will be used.
- Disable early media for data  
If this option is checked, the EARLY MEDIA event is sent for data calls. This of course incurs traffic over the RTP stream, which in some cases may not be desirable. If this is the case, the EARLY MEDIA event can be de-activated (checking the option).
- Disable early media for voice  
If this option is not checked, the EARLY MEDIA event is sent for voice calls. This of course incurs traffic over the RTP stream, which in some cases may not be desirable. If this is the case, the EARLY MEDIA event can be de-activated (checking the option). The standard setting is activated.

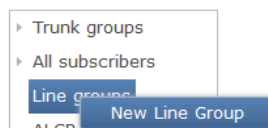
#### **6.2.4.4.3 Line groups**

A line group enables you to unite individual subscribers into a group under one phone number.

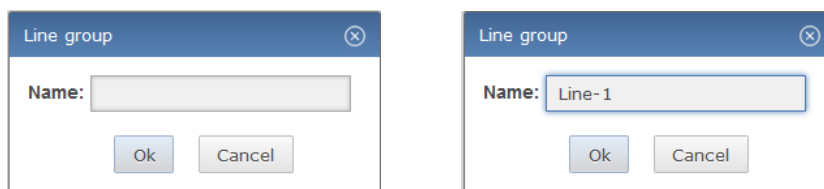
##### **6.2.4.4.3.1 New Line Group**

In this step a line group is set up. Please proceed as follows:

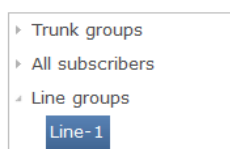
Right-click onto „Line group“ and select „New Line Group“.



The following window appears:



Enter a name for the line group and confirm by pressing „Ok“.



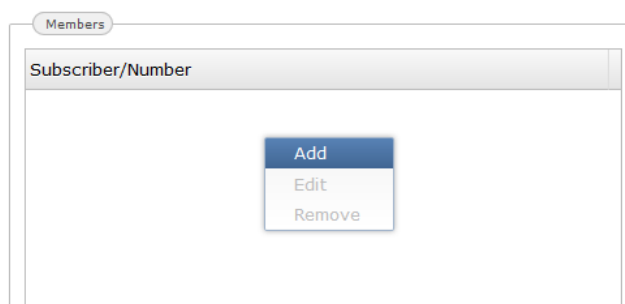
The line group is shown as sub item of „Line groups“. To adjust the settings of the newly created line group click onto the line group. The following window opens.

Number:	<input type="text"/>	Alert time:	<input type="text" value="1"/>
Type of call:	<input type="text"/>	Number presentation:	<input type="text"/>

The following boxes have to be filled in:

- Number  
If you define a line group, the subscriber telephone numbers that relate to this line group must be entered under the respective dialing tree in the telephone number plan.
- Alert time  
Maximum duration of ringing in seconds. A maximum of 119 seconds can be entered. This is because ISDN connections are automatically broken-off after a maximum of 2 minutes (120 seconds).
- Type of call  
The following ringing sequence adjustments are possible.
  - Parallel  
All telephones ring at the same time
  - Sequential  
All telephones ring in order, one after another
  - Round-Robin  
The telephone that comes after the last one that rang, is the next that will ring
- Number presentation  
This is where you select which telephone number will be displayed on the call recipient's telephone.
- Members





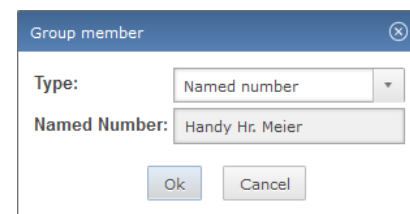
To add subscribers/numbers to the group, right-click into the window below "Subscriber/Number" and select "Add".

The following window opens:

You have the following choices here:

- Named number

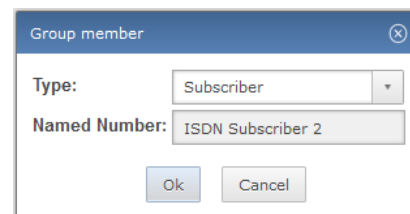
Here you enter the name of the „New Number“ under „Trunk groups“-> „Trunk-1“ in the box „Named Number“.



or the selection of

- Subscriber

Here you enter the name of the subscriber created under „All Subscribers“->„Group-1“->„New ISDN/ANA Subscriber“ or „New SIP Subscribe“.



**All settings in the line groups can be edited or deleted.**

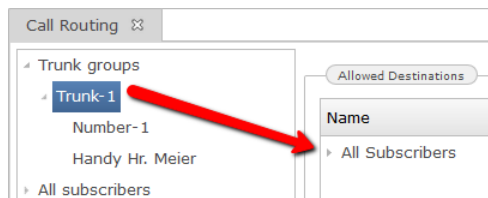
#### 6.2.4.4.4 Adjusting the routing

In this chapter we will adjust the availability of the created trunk groups, subscriber groups, number groups and line groups. These settings are made in the "Allowed destinations" and "Allowed sources" of the trunk group, "All subscribers", the subscriber group and the subscribers. This is done as follows:

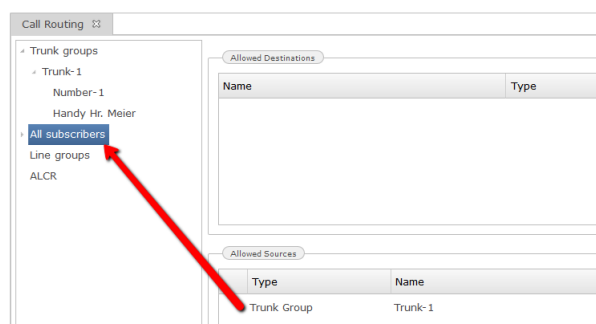
Mark „Trunk-1“ under „Trunk groups“.

Drag „All subscribers“ into the box „Allowed destinations“. It is now secured, that "Trunk-1" can reach all subscribers.

„Trunk-1“ is automatically added to the „Allowed sources“ of „All subscribers“. It is now secured, that all subscribers are available for "Trunk-1".



Picture 1

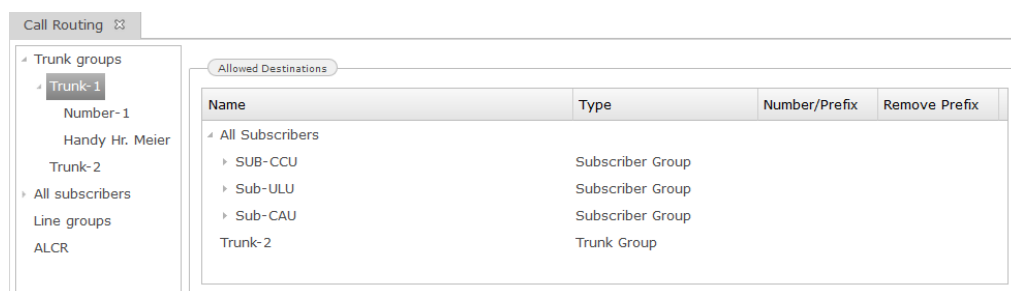


Picture 2

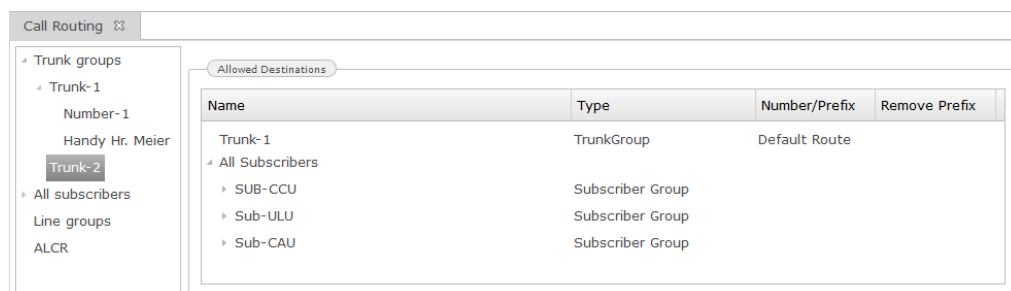
Picture 1: direct connection from „Trunk-1“ to „All subscribers“.

Picture 2: Connection from „All subscribers“ to „Trunk-1“.

In the following pictures further possible settings are shown.



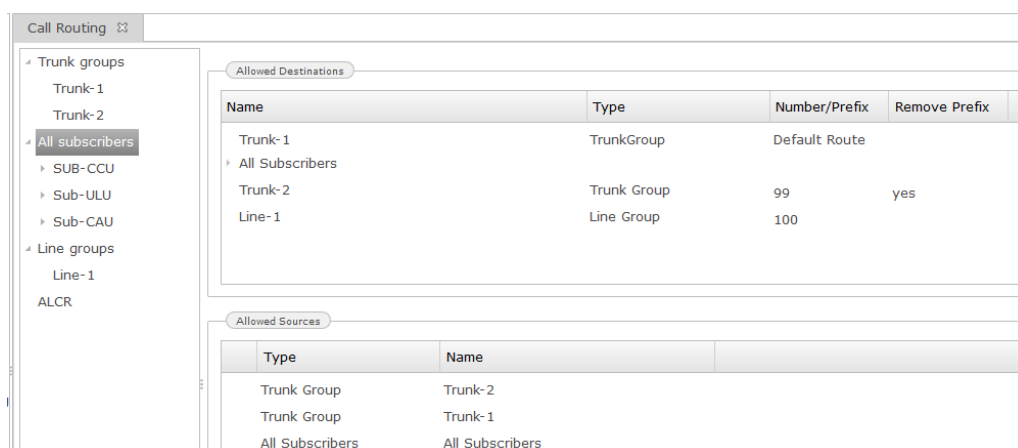
Picture 3



Picture 4

Picture 3: Connections from „Tunk-1“ to „All subscribers“, „Trunk-2“ and line group („Line-1“). The line group („Line-1“) can only be called.

Picture 4: Outgoing connections from „Trunk-2“ to „All subscribers“ and incoming connections to „Trunk-2“ from „Trunk-1“ and „All subscribers“.



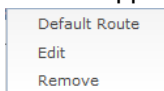
Picture 5

Picture 5: Outgoing connections from „All subscribers“ to „Trunk-1“ (as default route), „All subscribers“, „Trunk-2“ (with prefix: 99) and line group („Line-1“), as well as incoming connections from „Trunk-1“, „Trunk-2“ and „All subscribers“.

The settings of „Default route“ and „Prefix“ of the trunk as well as the number of the line group are made as follows:

- Default route

Click onto all subscribers. „Trunk-1“ appears in the box „Allowed destinations“. Right-click onto „Trunk-1“

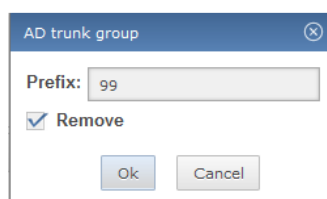


and select „Default Route“.

„Trunk-1“ is now marked as default route. All calls to targets not included in the „Allowed destinations“ are sent via this default route.

- Prefix

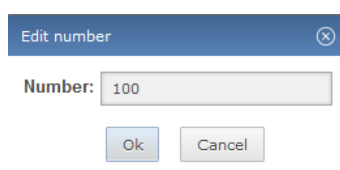
Click onto „Allowed destinations“. „Trunk-2“ is shown. Right-click „Trunk-2“ and select „Edit“. The following window appears:



Enter a number into the box „Prefix“. This number is now set as prefix for this trunk. If the box „Remove“ is ticked, the prefix is deleted.

The settings of the number for „Line group (Line-1)“ are made as follows:

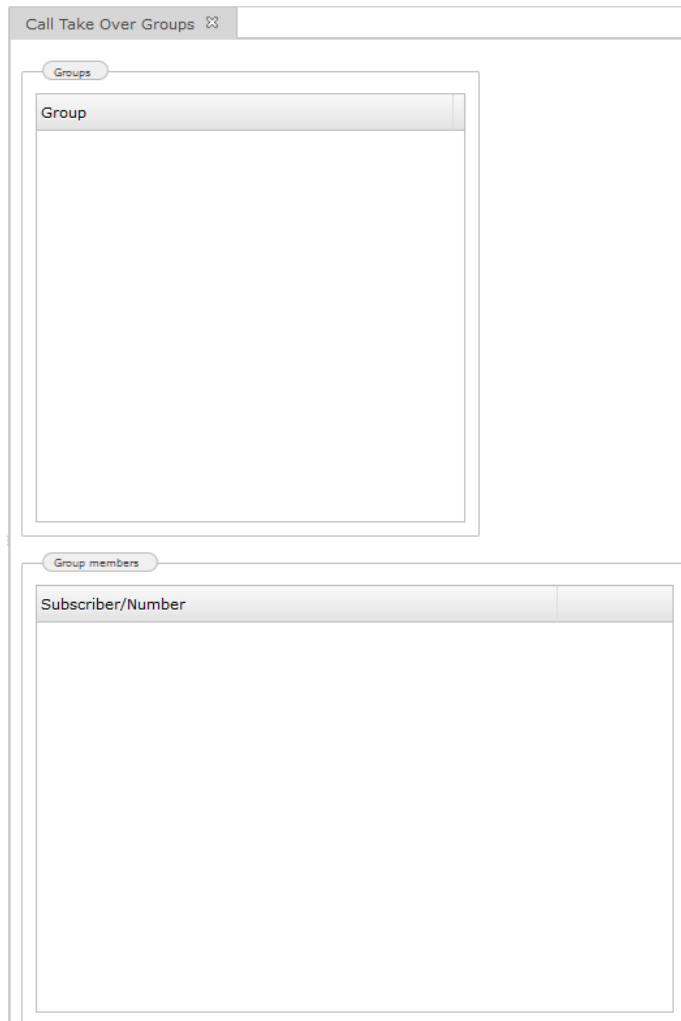
Click „All subscribers“ and „line group (Line-1)“ will appear in the box „Allowed destination“. Right-click „Line group (Line-1)“ and select „Edit“. Enter a number in the box, under which this line group can then be reached.



#### 6.2.4.5 Call Take Over Groups

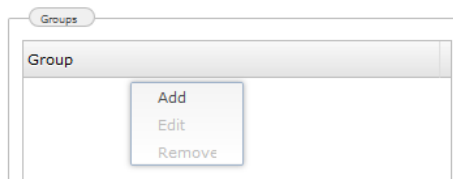
To create a call take over group click onto „Call Take Over Group“ and the following window will open:

In this window you have the possibility to adjust the group under „Groups“ and the „Subscriber/Number“, belonging to the group, under „Group members“.



- Group

In order to set up the group right-click into the window below „Group“ and select „Add“.





The following window appears:

A small dialog box titled 'New group' with a close button (X) in the top right corner. It contains a text input field labeled 'Group name:' and two buttons at the bottom: 'Ok' and 'Cancel'.

Enter a name for the group in the box „Group name“. Confirm with „Ok“.

The 'New group' dialog box with the 'Group name:' field now containing the text 'CTO-1'. The 'Ok' and 'Cancel' buttons remain at the bottom.

The newly created group is now shown under "Group".

A window titled 'Groups' showing a list of groups. The list has a header 'Group' and one entry, 'CTO-1'.

This Group „CTO-1“ is then added to the corresponding subscribers under „All subscriber“ -> „Group-1“.

In the next step the subscribers / numbers, which belong to this group, are set up.  
Click onto „Subscriber/Number“ and then right-click into the window. Select „Add“.

A window titled 'Group members' with a sub-header 'Subscriber/Number'. It contains a large empty area for a list. A context menu is open over this area, showing three options: 'Add' (highlighted in blue), 'Edit', and 'Remove'.

The following window opens:

Under type you can choose between:

- Subscriber  
Here the subscriber created under „All subscribers“ -> „Group-1“-> "New ISDN/ANA Subscriber" or "New SIP Subscriber" is entered.

A dialog box titled 'Group member' with a close button (X) in the top right corner. It has two fields: 'Type:' with a dropdown menu showing 'Subscriber', and 'Subscriber:' with an empty text input field. 'Ok' and 'Cancel' buttons are at the bottom.A dialog box titled 'Group member' with a close button (X) in the top right corner. It has two fields: 'Type:' with a dropdown menu showing 'Named number', and 'Named Number:' with an empty text input field. 'Ok' and 'Cancel' buttons are at the bottom.

or

- Named number  
In this case the "Named Number" from "Trunk groups" -> "Trunk-1" -> "New Number" is entered.

The created subscribers / numbers are then shown under „Group members“.

**All settings in the call take over groups can be edited and deleted.**

#### 6.2.4.6 Dialling Codes

Under this point the specific dialling codes for the supplementary services can be configured.

Dialling Codes ☒			
Supplementary Services			
Clear Held Call:	R0	Activate Fwd. Busy Prefix:	*67*
Clear Active Call:	R1	Activate Fwd. Busy Postfix:	#
Hold:	R	Deactivate Fixed Fwd:	#21#
Alternation between Lines:	R2	Deactivate Fwd. No Reply:	#61#
Activate Fixed Call Fwd. Prefix:	*21*	Deactivate Fwd. Busy:	#67#
Activate Fixed Call Fwd. Postfix:	#	Call Pick Up:	*14*
Activate Fwd. No Reply Prefix:	*61*	Short code dial:	*#
Activate Fwd. No Reply Postfix:	#	Activate MLPP Prefix:	*35*
Three Party - START:	R3	Activate MLPP Postfix:	*
Three Party - STOP:	R3	CLIR:	*31#
Transfer:	R4	Fax:	*32#
MCID:	R*84	activate_cw:	*43#
deactivate_cw:	#43#		

On analogue subscriber lines all the dialling codes listed above are available. The 'R' represents the flash on analogue lines.

On ISDN subscriber lines only the following dialling codes can be used:

- Activate MLPP Prefix/Postfix
- Call Pick Up
- Abb. Dial

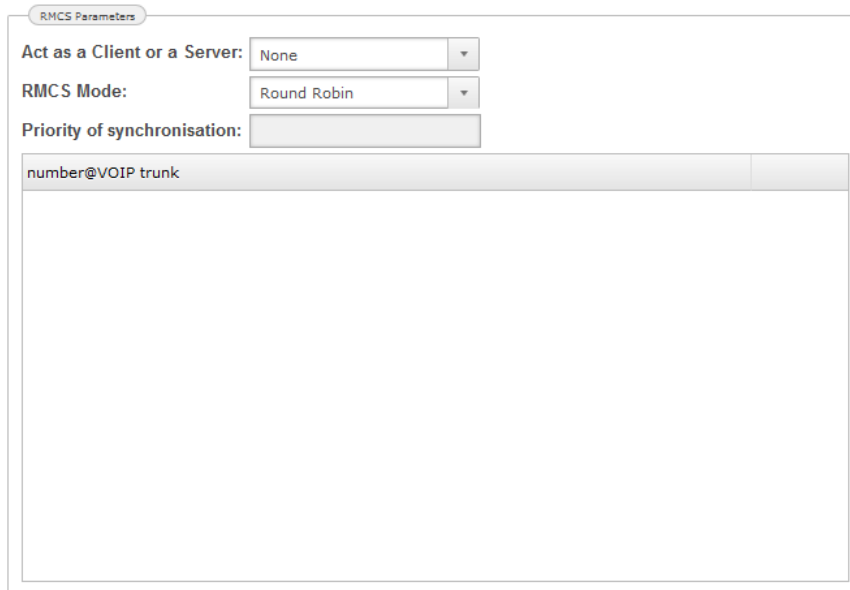
All other supplementary services on ISDN phones can be controlled over the phones soft keys/menu only. Please check the user manual of your phone for further instructions.

All entered dialling codes must be unique.

### 6.2.4.7 Synchronisation

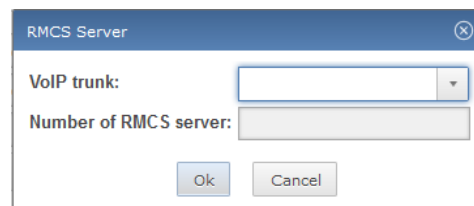
The synchronisation of the systems can be effected via RMCS server or ISDN trunks. How it takes place is defined in the synchronisation priority.

Synchronisation via a RMCS server is set as follows:



The image shows a configuration window titled "RMCS Parameters". It contains three dropdown menus: "Act as a Client or a Server:" set to "None", "RMCS Mode:" set to "Round Robin", and "Priority of synchronisation:". Below these is a large text area with the text "number@VOIP trunk" entered in the top line.

- **Act as a Client or a Server**  
Shows, if the system works as a client or as a server. The „Client“ need to be selected here.
- **RMCS Mode**  
Shows, if the RMCS-Server is selected as a clock source by the client with the sequential or round robin method. Both methods are possible. With the sequential method, the first server of the list will be selected and the next server will only be selected, if the RMCS call to the first server is not successful. With round robin method, on next try, the next server in the list will be selected until the end of the list has been reached. Then it restarts from the beginning of the list.
- **Priority of synchronization**  
This field offers a list of priorities to be selected for the RTP synchronization method within the NovaTec gateway. This selection will also be shown in the „Interface Sync Priority“, together with all other synchronization sources.
- **number@VOIP trunk**  
In this field the subscriber number of the RMCS server is entered. The number should also be entered in the CUCM. In order to set up this subscriber number please proceed as follows:  
Click into the window and then right-click. Select „Add“ and the following window appears:



The image shows a small configuration window titled "RMCS Server". It contains two fields: "VoIP trunk:" with a dropdown menu and "Number of RMCS server:" with a text input field. At the bottom are "Ok" and "Cancel" buttons.

The trunk created under "Telephony" -> "SIP" -> "Trunks" can be selected in the top down menu "VoIP Trunk".

Number of RMCS server:

Enter the calling number of the RMCS Server.

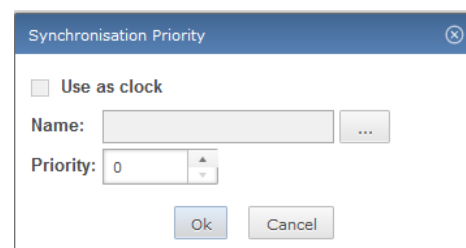
For synchronisation via an ISDN interface proceed as follows:

Click into the window „Set Synchronisation Priority for Interfaces“ right-click and select „Add“.



The following window opens

- Use as clock  
If checked, the entered source is used as clock.
- Name  
Via [...] the interface for the synchronisation is selected. The interface should be in slave mode.
- Priority  
Entries for the priority level ranging from 0 to 99 are possible.



Both synchronisation types can be activated at the same time (RMCS and interface), but it is necessary to differentiate with help of the priority. The lowest value has the highest priority. The priorities should be set as follows:

PRI highest priority

BRI

RMCS

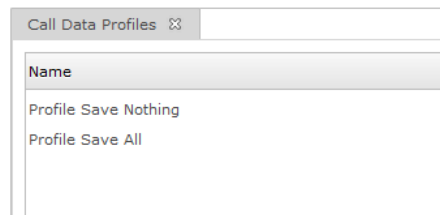
**All settings can be edited and deleted.**

#### 6.2.4.8 Call Data Profiles

Under call data profiles you will find the settings for storage of call data within the system.

If you click onto "Call Data Profiles", two preinstalled profiles are shown.



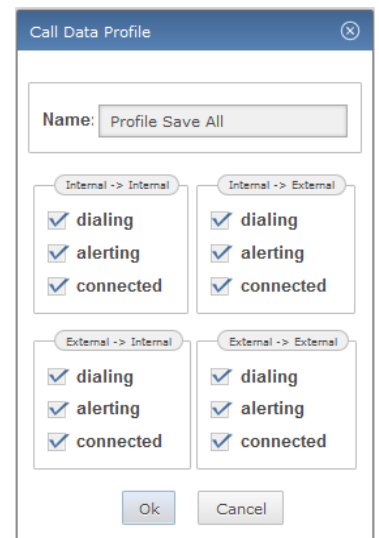


These profiles can be used by editing them. To do so, right-click onto a profile and select "edit" from the pop up menu.

The following window appears:

You can enter a new profile name in the box „Name“ and activate or deactivate the various options.

- Internal -> Internal  
Stores the connections between the subscribers of a system.
- Internal -> External  
Stores the connections from subscriber to trunk.
- External -> Internal  
Stores the connections from trunk to subscriber.
- External -> External  
Stores the connections from one trunk to another trunk.
- Dialling  
The data is saved even if the connection has not passed dialling state.
- Alerting  
The data is saved if the connection is in calling state.
- Connected  
The data is stored if the connection has been established.



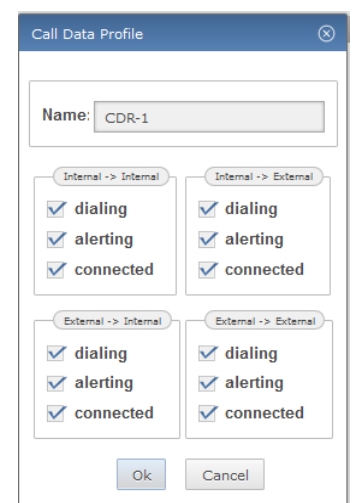
You can also create new profiles. If you wish to do so, please proceed as follows:

Click into the window "Call Data Profiles" with the right mouse button and select "Add" from the pop up menu.

The following window appears:

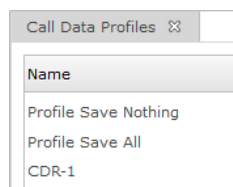
Enter a profile name in the box „Name“ and activate or deactivate the various options.

- Internal -> Internal  
Stores the connections between the subscribers of a system.
- Internal -> External  
Stores the connections from subscriber to trunk.
- External -> Internal  
Stores the connections from trunk to subscriber.
- External -> External  
Stores the connections from one trunk to another trunk.
- Dialling  
The data is saved even if the connection has not passed dialling state.
- Alerting  
The data is saved if the connection is in calling state.
- Connected



The data is stored if the connection has been established.

Confirm with "Ok". The new profile is now shown in the list of call data profiles.

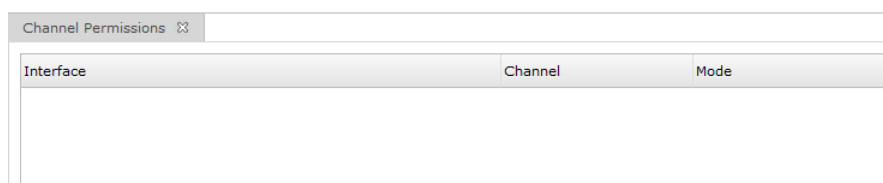


**All settings within the call data profiles can be changed or removed.**

#### 6.2.4.9 Channel Permissions

In the window „Channel Permissions“ you can block the B-channels of the interfaces in different modes.

This works as follows:



Right-click into the window „Channel Permissions“ and select „ADD“.

The following window appears:

- Interface

Choose the corresponding interface via .

- Channel

Here you can choose the channel to be blocked.

- Mode

- Incoming

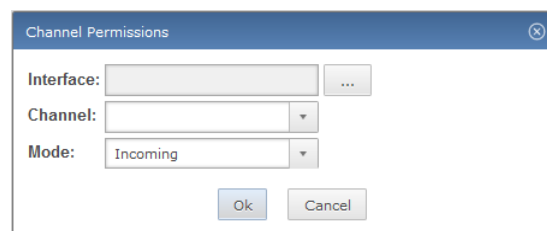
The B-channel is only available for incoming calls.

- Going

The B-channel is only available for going calls.

- Blocked

The B-channel is not available at all and is completely blocked in both directions.

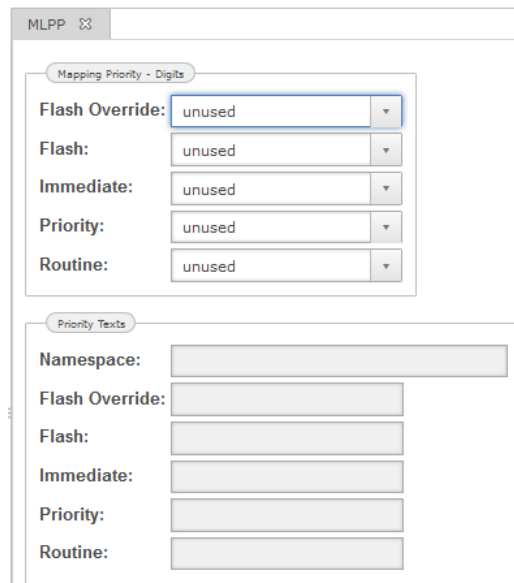


**Settings in the „Channel Permissions“ can be edited or deleted.**

#### 6.2.4.10 MLPP

Multi Level Precedence and Preemption

MLPP is a priority controlled access method. This feature originates in the military communication technology in an interconnection with Cisco Unified Communication Manager. The access of a subscriber to a network resource can be interrupted only by a subscriber with a higher priority.



#### Mapping Priority – Digits

On incoming calls from ISDN or analogue lines the user needs to specify the required priority level by dialling a certain digit (after the MLPP dialling code, also see the dialling codes section). At this point the user can specify which digit is mapped to which priority.

Flash Override --> highest Priority: select the digit representing Flash override priority.

Flash: select the digit representing 'Flash' priority.

Immediate: select the digit representing 'Immediate' priority.

Priority: select the digit representing 'Priority' priority.

Routine --> lowest Priority: select the digit representing 'Routine' priority.

If 'unused' is selected for any of the boxes, the corresponding priority level is not selectable for calls initiated by ISDN or analogue subscribers.

#### Resource-Priority-Namespace

Entries can be change with the button „Edit“. In the field „Resource-Priority-Namespace“ enter the same name as used in the CUCM.

#### 6.2.4.11 ALCR

The "Advanced Least Cost Router (ALCR)" is a feature to enable an automatic selection of the least priced provider for a certain destination.



- Telephony
  - Localisation
  - VoIP
  - ISDN
    - Call Routing
    - Call Take Over Groups
    - Dialing Codes
    - Synchronisation
    - Call Data Profiles
    - Channel Permissions
    - MLPP
  - Advanced Least Cost Routing
    - Global Options
    - Bank Holidays
    - Premium Rate Numbers
    - Network Service Providers

The following settings are possible:

- Global Options
- Bank holidays
- Premium Rate Numbers
- Network Service Provider

#### 6.2.4.12 Global Options

A screenshot of a software window titled 'Global Options'. It contains three input fields: 'Typical call duration (s):', 'Currency:', and a checkbox labeled 'Standard charge generation' followed by a dropdown menu.

- **Typical call duration**

Enter the average duration of your telephone calls in seconds here. The cost basis of individual network providers varies from charging for exact seconds of use to blocks of 60 seconds or above (1/1, 60/60, 240/240). The ALCR module calculates the most cost-effective provider based on the time span you have entered here.

- **Currency**

This text is inserted into the various currency options within the ALCR module and it's settings.

- **Standard charge generation**

The ALCR offers the opportunity to display the charges of an alternative network service provider on your ISDN terminal equipment, regardless of whether a cheaper provider is being used or not. This can be advantageous for the commercial use of telephone connections (e. g. pay phones). To use this function, tick the box "Standard charge generation" and select the desired service network provider.

#### 6.2.4.13 Bank holidays

Bank holidays can generally be differentiated into two types:

- **Fixed bank holidays**

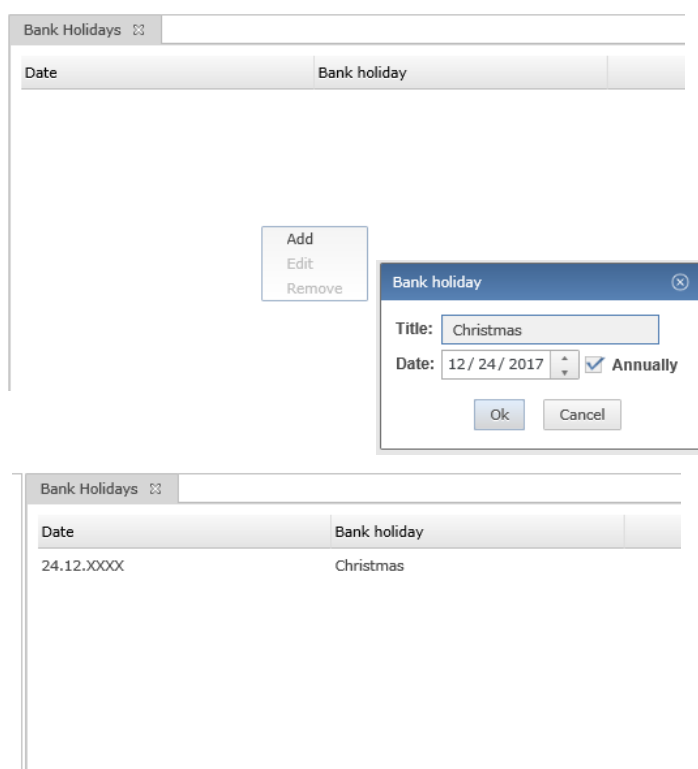
These bank holidays occur on the same date every year (e.g. Christmas). They are marked with a red letter symbol in front of the date. Only the day and month are displayed.

- **Variable bank holidays**

These bank holidays occur each year on a different date (e.g. Easter). They are marked with a blue letter symbol in front of the date. In addition, the date includes the year.

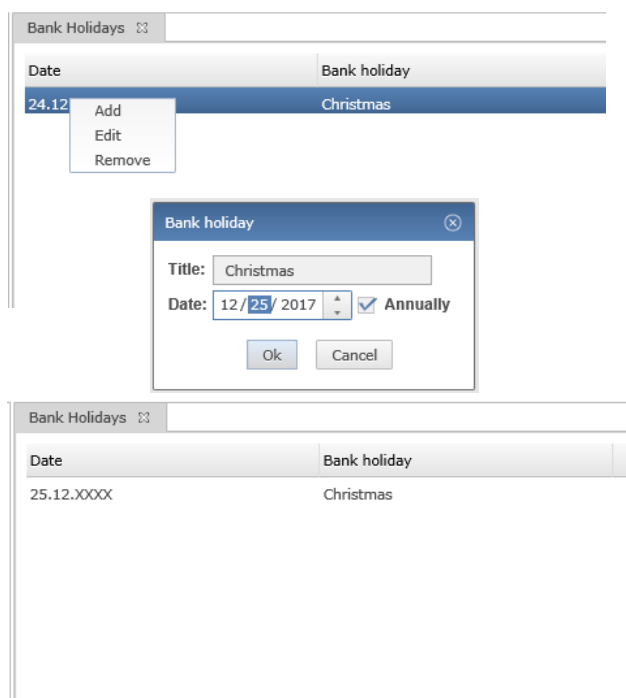
If you wish to add a bank holiday, proceed as follows:

Right-click into the window „Bank Holidays“. A menu with the options „Add“, „Edit“ and „Remove“ appears. Select „Add“ and enter the relevant holiday.

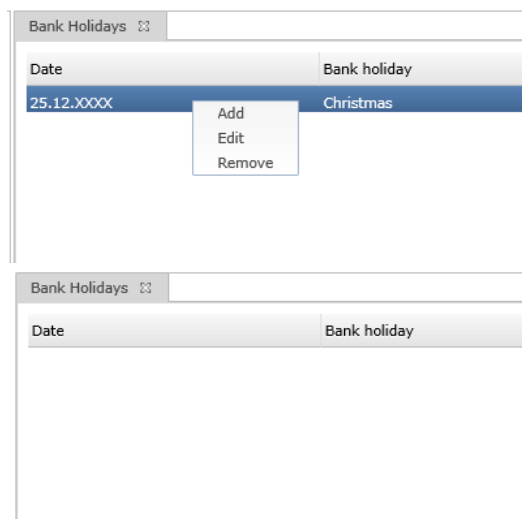


If you need to edit a bank holiday, please take the following steps:

Right-click onto the bank holiday in the list. A menu with the options „Add“, „Edit“ and „Remove“ appears. Select „Edit“ and make the necessary changes. Confirm with O.K.



If you need to delete a bank holiday, please take the following steps:  
Right-click onto the bank holiday in the list. A menu with the options "Add", "Edit" and "Remove" appears.  
Select "Remove".



#### 6.2.4.14 Premium Rate Numbers

Here you can set up premium rate services and call barring that will apply to all network service providers.

- **Call barred**

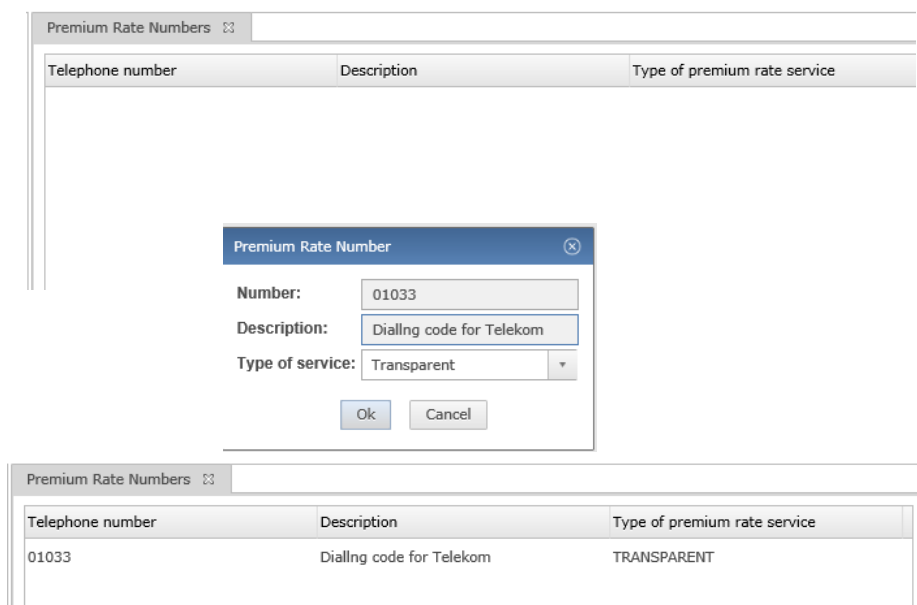
Access to any telephone number with this dialing code is blocked for all network service providers.

- **Cut-String:**

This dialling code will be deleted from the beginning of numbers being dialled. This prevents the user selecting an expensive network service provider. The ALCR cuts off this manually selected dialling code and replaces it using the cheapest network service provider found in the database

- **Transparent**

The selected telephone number will be routed without any modification. This means, that Least Cost Routing will not apply to this telephone number.



The screenshot shows the 'Premium Rate Numbers' window with a table containing three columns: 'Telephone number', 'Description', and 'Type of premium rate service'. A dialog box titled 'Premium Rate Number' is open, showing the following fields:

- Number: 01033
- Description: Dialling code for Telekom
- Type of service: Transparent

Buttons for 'Ok' and 'Cancel' are at the bottom of the dialog box.

Telephone number	Description	Type of premium rate service
01033	Dialling code for Telekom	TRANSPARENT

#### 6.2.4.15 Network Service Provider

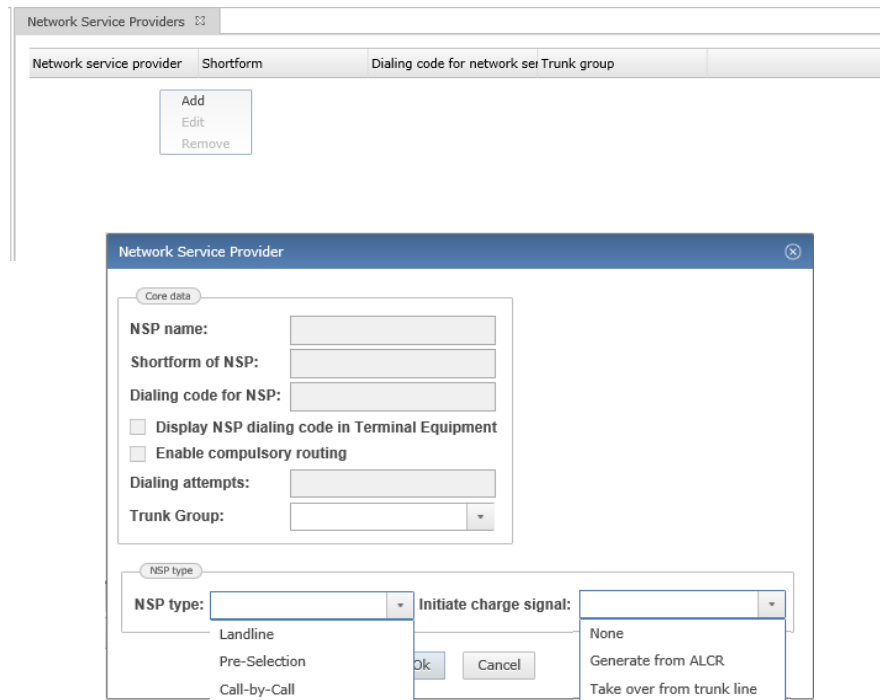
Before it is possible to select the most favourable provider and his best rates, several parameters have to be entered. It is possible to select the most favourable provider and connection after the following information has been entered:

Following settings have to be made in the provider window:

- Network Service Provider
- Regional charge categories
- Time charge categories
- Assign telephone numbers
- Call barring

##### 6.2.4.15.1 Network Service Provider

Right-click into the window. A menu with "Add", "Edit" and "Remove" opens. Select "Add" and enter the relevant parameter.



The screenshot shows the 'Network Service Providers' management interface. At the top, there is a table with columns: 'Network service provider', 'Shortform', and 'Dialing code for network sei Trunk group'. Below the table are 'Add', 'Edit', and 'Remove' buttons. A modal dialog titled 'Network Service Provider' is open, showing configuration options. The 'Core data' section includes fields for 'NSP name', 'Shortform of NSP', and 'Dialing code for NSP', along with checkboxes for 'Display NSP dialing code in Terminal Equipment' and 'Enable compulsory routing', and a 'Dialing attempts' field. The 'Trunk Group' is a dropdown menu. The 'NSP type' section has a dropdown menu with options: 'Landline', 'Pre-Selection', and 'Call-by-Call'. The 'Initiate charge signal' dropdown menu is open, showing options: 'None', 'Generate from ALCR', and 'Take over from trunk line'. 'Ok' and 'Cancel' buttons are at the bottom of the dialog.

Network service provider (NSP) is accessible

- **NSP name**  
Enter an explanatory name for the NSP
- **Shortform of NSP:**  
Enter a short form of the above entered name for the NSP
- **Dialing code for NSP**  
Enter the dialing code for the NSP (e.g. 01033). The number will automatically be transferred to the telephone number directory
- **Display NSP dialing code in Terminal Equipment:**  
If this option is activated, the provider selected by the ALCR will be displayed on any terminals connected to the system
- **Enable compulsory routing**  
This setting forces routing via a selected provider
- **Dialling attempts**  
Determines the number of dialling attempts the ALCR will undertake if all lines available with this network service provider are busy. This does not mean that the telephone number you are attempting to reach is engaged. If these dialling attempts are unsuccessful, the ALCR will automatically try the next most cost-effective provider. Please bear in mind that a connection will be slower under these circumstances as each dialling attempt takes time.
- **Trunk group**  
Assigns the NSP to a predefined Trunk group
- **NSP type**  
This option defines the NSP type. Possible settings are:
  - **Landline**  
The network service provider to be entered is also your telecommunications company. It is therefore not necessary to pre-dial any network service provider dialling code. It is possible to enter more than



one network service provider of this type, but only one provider can be set to network service provider (NSP).

- **Pre-selection**

All outgoing long distance telephone calls are being routed via this provider. It is possible to enter more than one network service providers of this type, but only one provider can be set to network service provider (NSP).

- **Call-by-Call**

In this case, access is provided by dialling the code for the network service provider before the telephone number of the recipient of the call.

- **Initiate charge signal**

This option defines how the accrued connection costs will be transmitted to your PABX system

- **None**

If you do not require the charging signal, choose this option

- **Take over from trunk line**

If your network service provider provides the charge information, choose this option

- **Generate from ALCR**

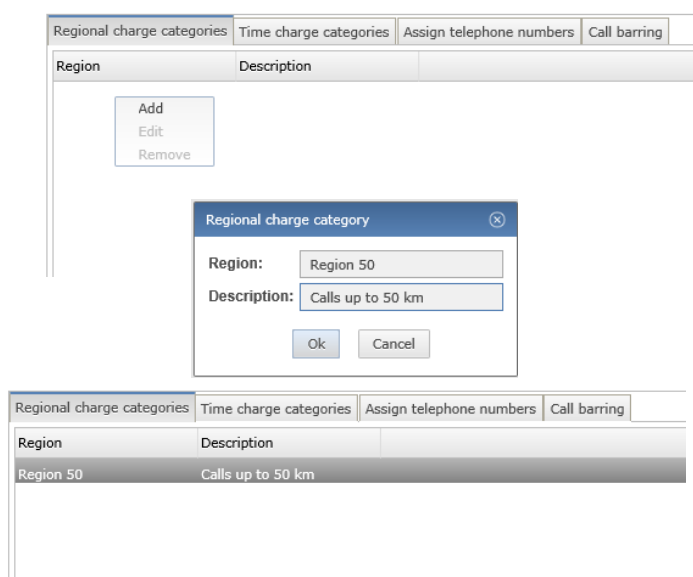
If the charge information is not available, the ALCR is able to generate this information from the data that has been entered.

#### 6.2.4.15.2 Regional charge categories

In the Regional charge categories window you can enter the charge categories of every network service provider.

To set up a new regional charge category, proceed as follows:

Right-click into column „Region“ and select „Add“ from the pop up menu. Enter the required region and description and confirm with “Ok”.



The screenshot shows the 'Regional charge categories' window with four tabs: 'Regional charge categories', 'Time charge categories', 'Assign telephone numbers', and 'Call barring'. The 'Regional charge categories' tab is active, displaying a table with two columns: 'Region' and 'Description'. A context menu is open over the 'Region' column, showing 'Add', 'Edit', and 'Remove' options. A dialog box titled 'Regional charge category' is open, with 'Region' set to 'Region 50' and 'Description' set to 'Calls up to 50 km'. The 'Ok' button is highlighted.

Region	Description
Region 50	Calls up to 50 km

- **Region**  
The „official“ name of the region (for example Region 50)
- **Description**  
Enter a description of the region (for example 50 km )

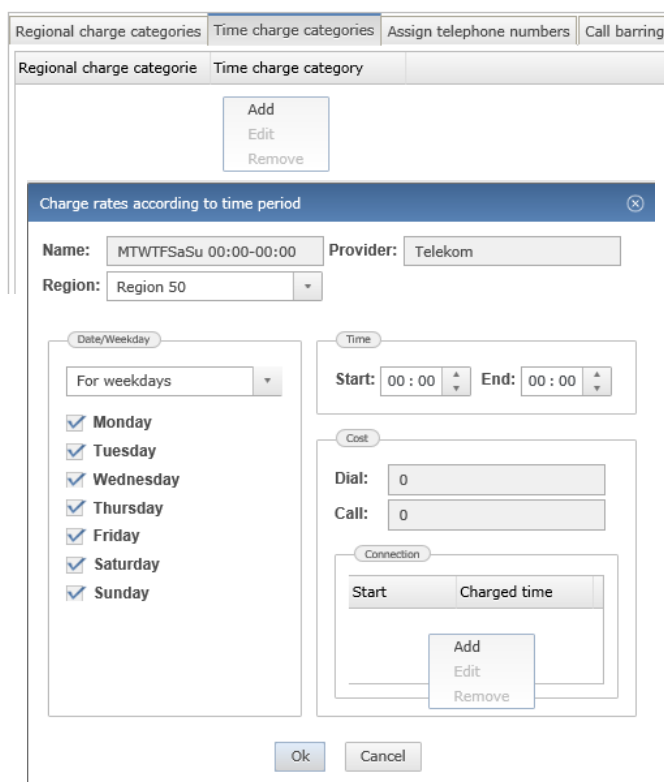
### 6.2.4.15.3 Time charge categories

In the regional charge categories and time charge categories window every charge will be assigned to its valid time zone. All currently entered charges are listed alphabetically in the window of the appropriate network service provider.

To define the time zones and tariffs, follow the steps below:

Click on the „Time charge categories“ and then onto „Add“ with the right key of the mouse.

Enter the relevant tariffs and choose the appropriate time zones and confirm with “Ok”.



- **Name**  
Enter the name of the time charge category. This row is provided purely as a comment row for your assistance and will be displayed in the column “Time charge category”. We would advise you to use a standard method of description (e.g. Mon-Sun 00–00 Hr) as this will help subsequent sorting. However, entering a time charge category name is not necessary. If no name has been entered, the application automatically processes a time charge category name from the entered charge times
- **Provider**  
The short form name of the provider to whom this category is assigned to. This field is not editable
- **Region**

All regions that have been entered in this providers "Regional charge category" will appear here. Please select the region that is applicable.

- **Date/Weekday**

Allocate the day on which the charge is valid. If nothing is entered the charge will be valid on all days.

- **Time**

Enter the time at which the charge is valid. In case of a single charge level for a full day enter 00:00 for both begin and end. The time information must always be entered with a colon, (e.g. 00:00, 23:00 etc.)

- **Cost**

The Cost field offers different charging possibilities

- **Dial**

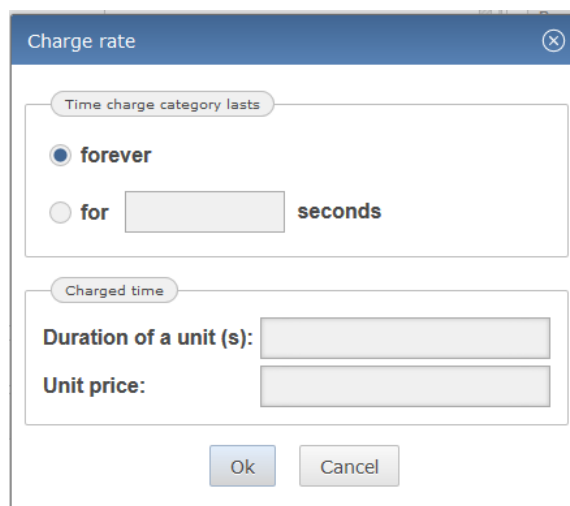
In cases where the network service provider charges a fixed amount for dialling, enter this charge here

- **Call**

In cases where a fee is charged for a connection even when the called subscriber did not answer, please enter this charge here

- **Connection**

The actual connection costs should be entered here. To edit or create a connection rate click the corresponding button "Add" and the following dialog will appear



The dialog box titled "Charge rate" contains two sections. The first section, "Time charge category lasts", has two radio buttons: "forever" (selected) and "for" (with a text input field and the word "seconds"). The second section, "Charged time", has two text input fields labeled "Duration of a unit (s):" and "Unit price:". At the bottom are "Ok" and "Cancel" buttons.

Now select the start of the conversation option and enter the call duration and the unit price. Then click on Ok. The entry will now be transferred to the list. If the provider changes the charge level after the telephone conversation has been running for a specific length of time, this can also be entered. To proceed, click once again onto "Add" and select the option "Seconds after conversation starts". Enter the call duration after which the charge level changes. Enter the changed charge level as before and confirm with "Ok".

Regional charge categories	Time charge categories	Assign telephone numbers	Call barring
Regional charge categorie	Time charge category		
Region 50	MTWTFSSaSu 00:00-00:00		

#### 6.2.4.15.4 Assign telephone numbers

In this window all numbers will be assigned to specific charge zones of individual network service providers. This means that the same dialling codes can be assigned to network service provider 'A' as a regional zone code and to network service provider 'B' as a long distance zone code. For this reason each dialling code has to be assigned separately to each network service provider.



Regional charge categories	Time charge categories	Assign telephone numbers	Call barring
----------------------------	------------------------	--------------------------	--------------

Regional charge categorie	Telephone number
<div>Individual assignment</div> <div>Remove</div>	

**Assign Telephone Numbers**

Telephone number: 04

Region: Region 50

Ok Cancel

Regional charge categories	Time charge categories	Assign telephone numbers	Call barring
----------------------------	------------------------	--------------------------	--------------

Regional charge categorie	Telephone number
Region 50	04

- **Telephone number**  
List of telephone numbers that may be assigned a regional charge category
- **Regional charge category**  
Available regional charge categories that may be assigned to a telephone number

#### 6.2.4.15.5 Call barring

In the "Call Barring" window you can block individual dialling codes for each network service provider on a provider by provider basis.

Regional charge categories	Time charge categories	Assign telephone numbers	Call barring
----------------------------	------------------------	--------------------------	--------------

Telephone number
<div>Individual assignment</div> <div>Remove</div>

**Assign call barring number**

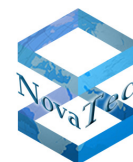
Number: 0700

Ok Cancel

Regional charge categories	Time charge categories	Assign telephone numbers	Call barring
----------------------------	------------------------	--------------------------	--------------

Telephone number
0700

Entering a new barred number:



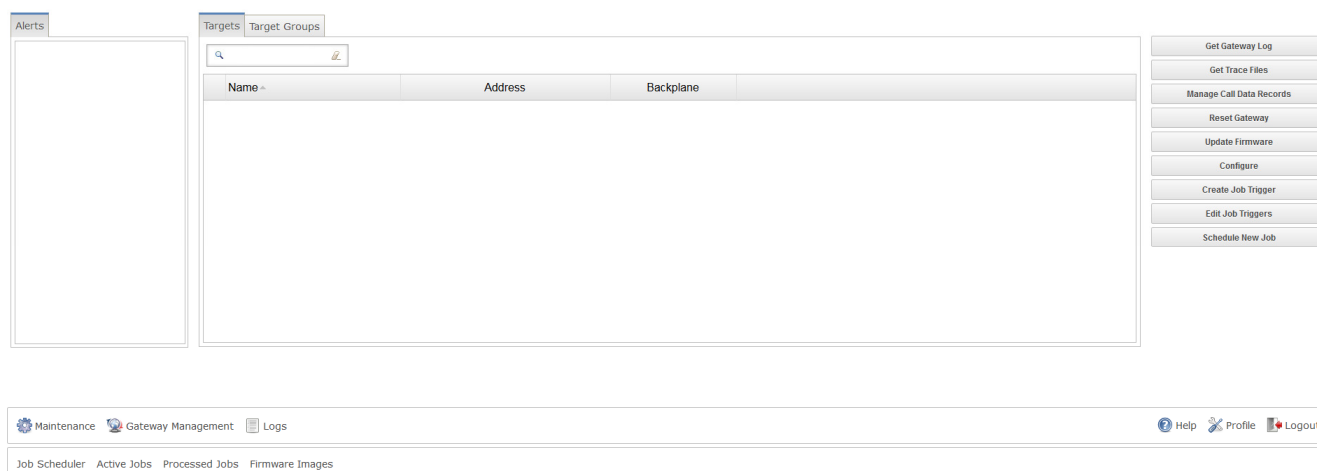
Select the network service provider, then click onto "Individual assignment".

Enter the numbers to be blocked and confirm with "OK".

## 6.3 Targets

In NAMES, the word „target“ signifies a NovaTec device which has been added to the database and is to be administered through the application. It can be a target for the „jobs“ that NAMES can perform.

The main application element in NAMES is the target list, which is always displayed centrally in the main window. After NAMES has been installed, the target list is empty and has to be populated by the user:



The target list allows you to view, select, create, edit and remove targets.

### 6.3.1 Editing a target

To edit a target, right-click the target entry in the list and select „Edit“ from the context menu. The „Edit Target“ dialogue is identical to the „Create Target“ dialogue, except for the checkbox next to the „Password“ field. This checkbox specifies whether the password should be changed; if unchecked, no change will be made to the password. To clear the current password, tick the checkbox and leave the password field empty.

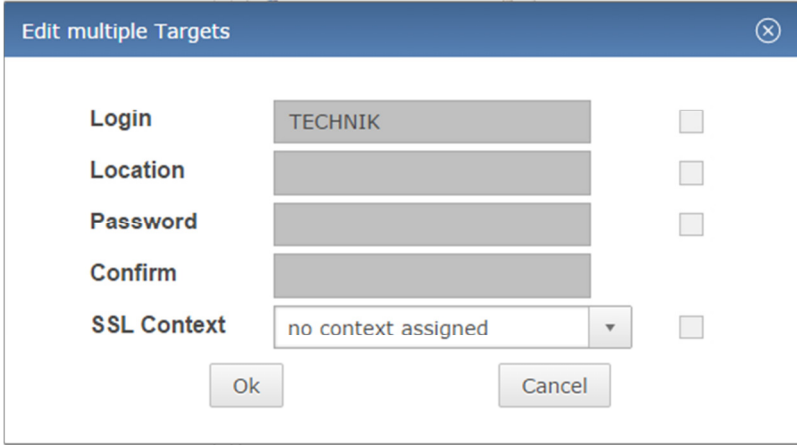
### 6.3.2 Removing a target

To remove a target, right-click the entry in the list and select „Delete“ from the context menu. It may not be possible to remove a target, for example if running or waiting jobs still exist. A confirmation dialogue will be shown before the target is deleted.

### 6.3.3 Multiple target actions

Both the „Edit“ and „Delete“ actions may be applied to multiple targets at a time. Simply select multiple targets from the list by holding the **Ctrl** button on your keyboard to select individual targets or the **Shift** button to select a range. Right-click the selection and select „Delete“ or „MultiEdit“ from the context menu.

The „Edit multiple targets“ dialogue differs from the „Edit Target“ dialogue, as it only contains items that can be set for multiple targets at the same time: login name, location, password and SSL context.



The "Edit multiple Targets" dialog box contains the following fields and checkboxes:

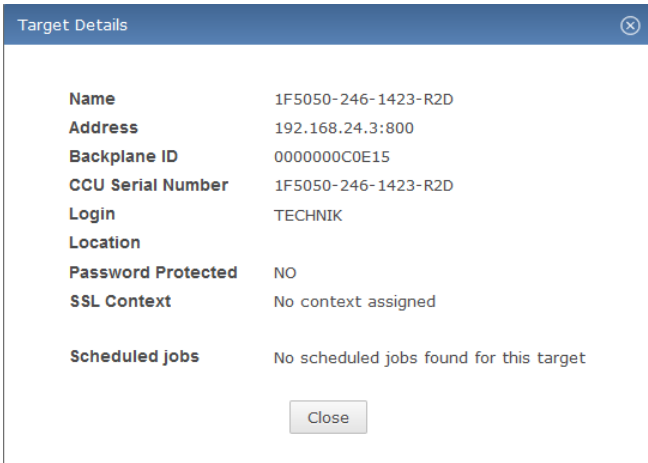
Field	Value	Checkbox
Login	TECHNIK	<input type="checkbox"/>
Location		<input type="checkbox"/>
Password		<input type="checkbox"/>
Confirm		<input type="checkbox"/>
SSL Context	no context assigned	<input type="checkbox"/>

Buttons: Ok, Cancel

As with the password in the regular „Edit Target“ dialogue, the checkbox corresponding to a field in the „Edit multiple targets“ dialogue must be ticked if changes are to be made. For example, to clear the „Location“ value on all selected targets, tick the checkbox next to the „Location“ field and leave the input box empty.

### 6.3.4 Target details

To show the „Target Details“ dialogue for a target, double-click its entry in the list. In addition to information that can be configured in the „Target Edit“ dialogue, this window also displays whether a password is configured for this device (but not the actual password – that is never sent to the web client), which configuration was last transmitted to the device and whether any jobs are currently scheduled for the target:



The "Target Details" dialog box displays the following information:

Name	1F5050-246-1423-R2D
Address	192.168.24.3:800
Backplane ID	000000C0E15
CCU Serial Number	1F5050-246-1423-R2D
Login	TECHNIK
Location	
Password Protected	NO
SSL Context	No context assigned
Scheduled jobs	No scheduled jobs found for this target

Button: Close

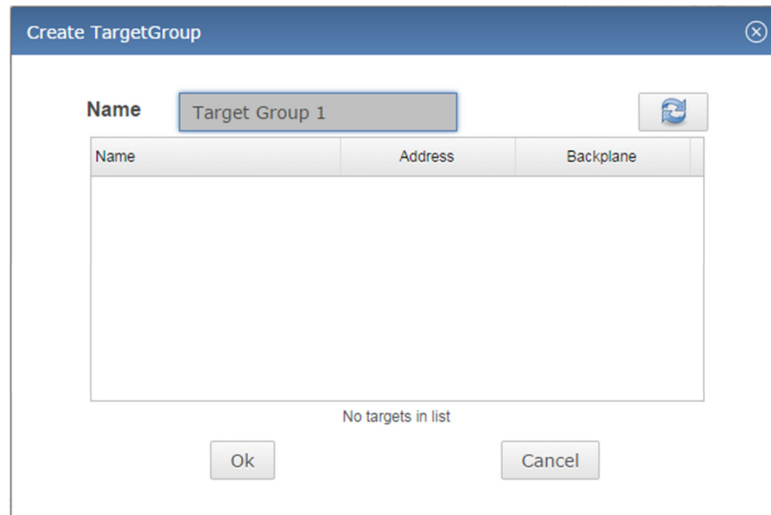
This dialogue does not have any edit functions and is for informational purposes only.

## 6.4 Target groups

Targets can be collected in target groups. This makes tasks such as creating a job for an entire group of targets much easier. Target groups are administered through the „Target Groups“ tab of the main UI window, which will switch the target list to a target group list.

### 6.4.1 Creating a target group

To create a target group, right-click in the target group list and select „Create” from the context menu. The „Create TargetGroup” dialogue is displayed:



The dialog box titled "Create TargetGroup" has a close button in the top right corner. It contains a "Name" label and a text input field with the value "Target Group 1". To the right of the input field is a small icon of a document with a plus sign. Below the input field is a table with three columns: "Name", "Address", and "Backplane". The table is currently empty, and the text "No targets in list" is displayed below it. At the bottom of the dialog are "Ok" and "Cancel" buttons.

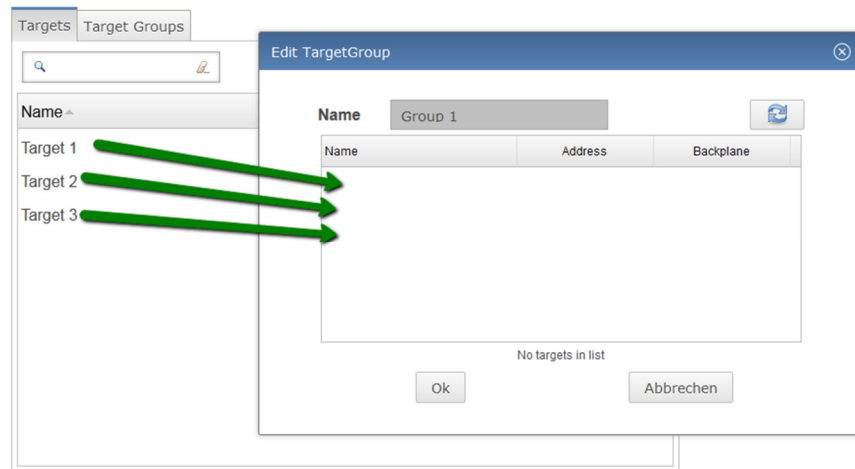
You have to enter a name for the target group. You may add targets to the group (see section 6.4.2) now, or leave it empty and add them later. Click „OK” to finish creating the group.

### 6.4.2 Editing a target group

Editing a target group allows you to change the group name or which targets are group members. To edit a target group, right-click the target group in the list and select „Edit” from the context menu. The „Edit TargetGroup” dialogue is displayed, which is identical to the „Create TargetGroup” dialogue.

#### 6.4.2.1 Adding Targets

To add targets to a target group, switch back to the „Targets” tab of the main window with the „Edit TargetGroup” window still open. Select the targets you wish to include from the target list and drag them over to the list in the „Edit TargetGroup” dialogue:



### 6.4.2.2 Removing targets

To remove a target from a target group, right-click it in the list of the „Edit TargetGroup“ dialogue and select „Remove from Group“ from the context menu.

### 6.4.3 Removing a target group

In order to remove a target group, right-click it in the list and select „Delete“ from the context menu.

## 6.5 Jobs

In NAMES any changes made to a target are achieved through a „job“. Several different types of jobs exist, allowing a number of different administrative and maintenance tasks to be carried out. Jobs may be created by a user – explicitly by using the „Schedule New Job“ function, or implicitly by using other functions from the action bar – or in response to a CallHome event (if a corresponding trigger is configured), and may be executed immediately or scheduled for a specific time.

A limited number of jobs can be run at the same time; the maximum number of simultaneous jobs is configured in the NAMES settings (see section 5.3.1) and may be any number in the range of 1 to 10. If all slots are occupied with running jobs, other jobs that are scheduled to run at this time will be added to a waiting queue and executed as slots become available.

### 6.5.1 Job types

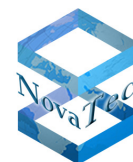
#### 6.5.1.1 Upload Firmware

This job type facilitates a firmware update. Firmware has to be uploaded to NAMES (see section 5.9.1) first, which may require additional privileges. After that, firmware upload jobs may be created, which will upload the firmware to the target. The device will then write the new firmware to its flash and automatically restart once all phone connections have been terminated.

#### 6.5.1.2 Reset

This job type sends a reset signal to the device, which will then restart. The device will be unavailable for both phone and maintenance connections whilst restarting. The length of the restart period depends on the device in use.





### 6.5.1.3 Download Trace Files

This job type downloads all current trace files (error diagnostic information) from the device to NAMES. These trace files are stored in the database and may be downloaded from NAMES for analysis at a later point. Default behaviour is to delete the files on the target after download, but this can be disabled.

### 6.5.1.4 Download Log File

This job type retrieves the current content of the target device's log and adds it to the database. Log information may later be downloaded from NAMES for analysis by specifying a time range from which logs are to be downloaded. Default behaviour is to clear the targets log after download, but this can be disabled.

### 6.5.1.5 Download CDRs

This job type retrieves CDRs (Call Data Records) from the target device and saves them in the database. The CDRs may be downloaded from NAMES for analysis later, for a single device or consolidated through target groups.

### 6.5.1.6 Sign Certificate

This job type retrieves Certificate Signing Requests (CSRs) from the target device and issues corresponding certificates using the internal Certificate Authority (CA). The certificates are then uploaded to the device and the device is restarted to activate the TLS configuration. For this job type to work, the internal CA has to be correctly configured (see section 5.7) and the device has to be configured with TLS active and at least one of the communication channels (Maintenance and SIP) has to be configured to generate a CSR.

## 6.5.2 Job states

All jobs are in one of a number of states. The possible states and their meanings are as follows:

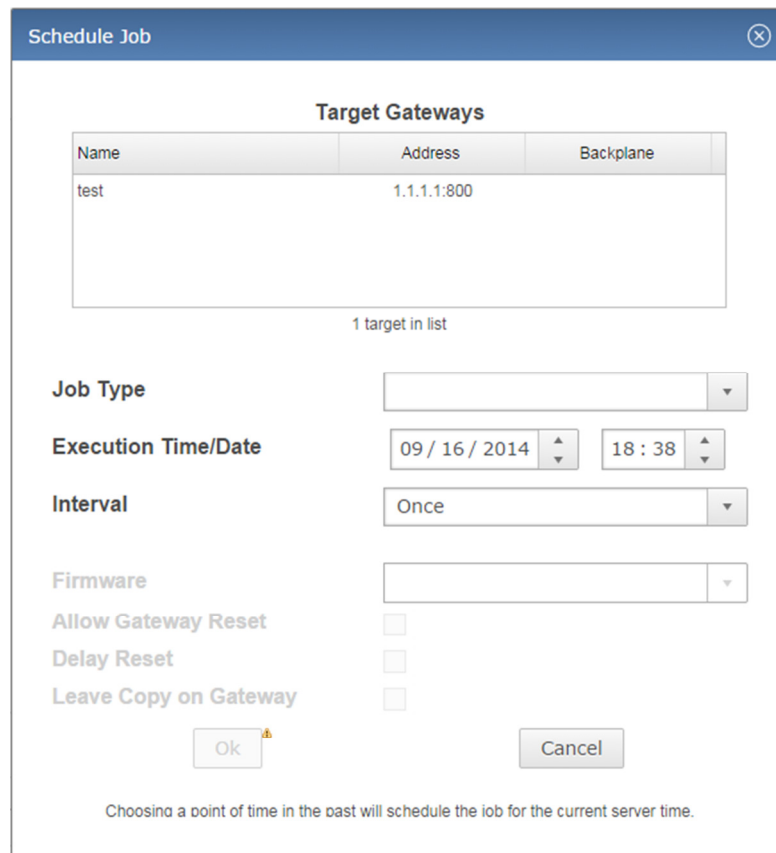
- **Pending:** these jobs have been scheduled for a point of time in the future.
- **Waiting:** these jobs are due to run, but are waiting for slots to become available.
- **Running:** these jobs are currently being run.
- **Done:** these jobs were completed successfully.
- **Failed:** these jobs encountered an error and could not be completed.
- **Obsolete:** these jobs should have been run during NAMES downtime and have been marked obsolete. They may be reactivated from the „Obsolete Jobs“ window.

## 6.5.3 Creating a job

Jobs can be created through various means. They may be created automatically in response to events that have occurred on a target device (see section 6.6), created in response to configuration changes through the „Reconfiguration API“, triggered through „refresh“ buttons in several UI windows and finally scheduled through the „Schedule Job“ dialogue.

This section will address the express scheduling of jobs through the „Schedule Job“ dialogue; other ways of creating a job will be addressed at the appropriate point in the manual.

The „Schedule Job“ dialogue allows all job types, except for „Upload Configuration“, to be scheduled. To open the dialogue, select the target, targets or target group you wish to schedule jobs for and then click the „Schedule New Job“ button in the action bar on the right:



Name	Address	Backplane
test	1.1.1.1:800	

1 target in list

Job Type: [dropdown]

Execution Time/Date: [09 / 16 / 2014] [18 : 38]

Interval: [Once]

Firmware: [dropdown]

Allow Gateway Reset: ☐

Delay Reset: ☐

Leave Copy on Gateway: ☐

Ok Cancel

Choosing a point of time in the past will schedule the job for the current server time.

The target list at the top shows the selected targets and may be further edited by dragging targets from the main window into the list or right-clicking targets and selecting remove.

Select a job type from the drop down menu and select the time you wish the job to be scheduled for. If you select the current time or a time in the past, the job will run immediately. If you wish the job to be repeated periodically, select the appropriate interval from the „Interval“ drop down menu.

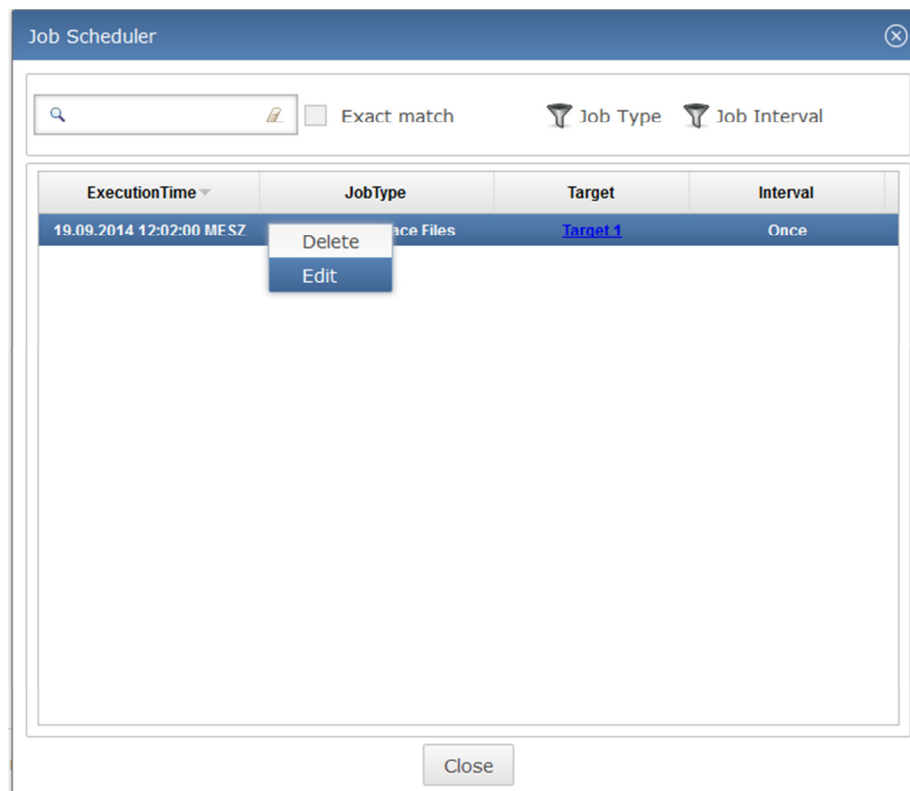
The remaining options depend on the job type you have selected:

- **Firmware:** for an Upload Firmware job, select the firmware you wish to upload to the target.
- **Delay Reset:** for a Reset job, select whether the reset should be delayed until all phone connections have been terminated.
- **Leave Copy on Gateway:** for all download jobs, select whether the job should leave a copy of the data on the target or remove it. Warning: Using this option with log downloads will cause duplicate log entries in the NAMES database if the device log is not otherwise cleared, as NAMES cannot reliably detect duplicate log entries at the moment.

After selecting the options you wish to use, click “OK” to schedule the job.

#### 6.5.4 Viewing and modifying scheduled jobs

Once a job has been scheduled and is in pending state, it will appear in the „Job Scheduler“ window, which can be reached through the „Gateway Management“ menu and by default through the quick bar:



Jobs can be deleted or edited by right-clicking on their entry and selecting „Delete“ or „Edit“ from the context menu as long as they are in the pending state. Once their execution time has arrived and they progress to waiting or running, they can no longer be deleted or edited.

Job types cannot be changed after creation, as this is viewed as an entirely different job. If you wish to do this, simply delete the job and recreate it with the required type.

### 6.5.5 Active jobs

The currently running jobs may be viewed by opening the „Active Jobs“ window, reachable from the „Gateway Management“ menu or through the quick bar. The current job activity state (connecting, uploading, downloading, working...) is displayed. If the job is uploading data to the target, a progress bar for the upload is also displayed.

### 6.5.6 Completed and failed jobs

Completed and failed jobs can be viewed in the „Processed Jobs“ window. In addition, a message will be displayed in the notification area to the left of the target list whenever a job fails.

Double-clicking a job in the notification area or the list in the „Processed Jobs“ window will open a window showing information about the job, including a failure message that indicates why the job could not be completed.

Jobs may be deleted by right-clicking them in the „Processed Jobs“ window and selecting „Delete“ from the context menu.



## 6.6 Job Trigger

Job Trigger may be used to automate certain maintenance tasks. The jobs are automatically created and queued by NAMES when a specific event occurs. The association of an event with a job template is referred to as a „Job Trigger“ in NAMES.

The following event types may be used to trigger a job:

- **CDR full:** target system storage for CDRs has reached 50% fill level.
- **Trace full:** the maximum amount of trace files have been stored on the target system.
- **Log full:** target system storage for logs has reached 100% fill level.
- **Systemstart normal:** the target system has finished booting.
- **TLS has default time:** TLS is configured, but system time is not set.
- **Free RAM threshold:** the amount of free RAM has fallen below the configured threshold.

Any of these events may be used to trigger any of the following jobs, although the default job type for each event is usually the only useful combination:

- Download CDR's
- Download trace files
- Download log file
- Reset
- Sign certificates

### 6.6.1 Creating a Job trigger

Job triggers may be created either for a single target or for a target group. Creating a Job trigger for a target group will result in creation of Job triggers for each of the targets in the group. Select the target or target group you wish to create a trigger for from the target or target group list, then click the „Create Job Trigger“ button in the action bar. The „Create Job Trigger“ dialogue is displayed:

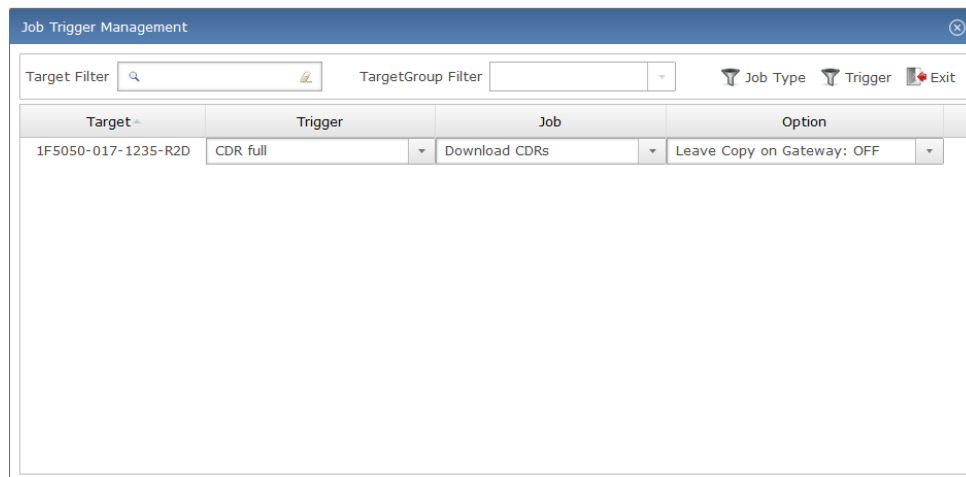
A screenshot of the 'Create Job Trigger' dialog box. The dialog has a blue title bar with the text 'Create Job Trigger' and a close button. Inside, there are two dropdown menus: 'Trigger' with 'CDR full' selected and 'Job Type' with 'Download CDRs' selected. Below these are five checkboxes: 'Disable TLS' (unchecked), 'Leave Copy on Gateway' (unchecked), 'Reset if necessary' (checked), and 'Immediate reset (don't wait for calls)' (unchecked). At the bottom are 'Ok' and 'Cancel' buttons.

Trigger	CDR full
Job Type	Download CDRs
Disable TLS	<input type="checkbox"/>
Leave Copy on Gateway	<input type="checkbox"/>
Reset if necessary	<input checked="" type="checkbox"/>
Immediate reset (don't wait for calls)	<input type="checkbox"/>

Start by selecting the event type you wish to trigger the job from the „Trigger“ combo box. When selecting an event type, the default corresponding job type is automatically selected for you. If you wish a different job type to be triggered, change the selection in the „Job Type“ combo box. Finally, configure the job parameters that are available for the selected job type, and click „OK“.

## 6.6.2 Edit Job triggers

To edit Job triggers, select the target or target group you wish to edit Job settings for from the target or target group list and then click the „Edit Job Triggers“ button in the action bar to the right. The „Job Trigger Management“ window is displayed:



To edit a single entry, select the appropriate settings through the combo boxes.

To remove a trigger, right-click the trigger and select „Delete“ from the context menu.

The window also offers a „MultiEdit“ function which may be used to alter settings for multiple CallHome triggers at once. This is most useful when editing triggers for a target group. To use this function, select multiple CallHome triggers by holding the **Ctrl** button to add individual entries to your selection or the **Shift** button to add a range of entries to your selection. Right-click the selection and select „MultiEdit“ from the context menu. The „MultiEdit CallHome Triggers“ dialogue is displayed, which is functionally identical to the „Create CallHome Trigger“ dialogue.

## 6.7 User settings

User settings are available through the „Profile“ menu. They allow users to change their password, to select an icon theme that is more appropriate for users suffering from red-green colour blindness or to configure the tool bar located at the bottom of the UI. Currently, icon and tool bar settings are not saved between sessions.

To change the user password, select „My Settings“ from the „Profile“ menu, then enter a new password into the „Password“ input box and confirm it by entering the same password again into the „Confirm“ box. Ensure that the checkbox to the right of the „Password“ input box is ticked and then click „OK“.

The new password must conform to basic password safety rules: it must contain at least five characters, of which at least one must be a lower case letter, one an upper case letter and one a number. If either of these rules are not observed or the password does not match its confirmation, a validation error will be shown and form submission will not be allowed (the „OK“ button is disabled).