

Installation and Operation Manual Enhanced System Services, ESS

Contents

1 Introduction	1
1.1 Requirements	2
1.1.1 PC Requirements	2
1.1.2 Unite Modules Requirements	2
1.2 Additional Software Requirements	3
2 Installation	4
2.1 Description of LED indicators	4
2.2 Internal Inputs and Outputs	5
2.3 Error Relay	5
2.4 Licences	5
2.4.1 Unlicensed Mode	5
2.5 Sending E-mail	5
2.6 Printing Log Information	6
2.7 Additional Configuration in Unite Modules	7
2.7.1 Sending Status Log Messages to the ESS	7
2.7.2 Sending Activity Log Messages to the ESS	8
2.7.3 Sending Extended Activity Logs (optional)	8
2.7.4 Configuring the UNS	9
3 Remote Connection	10
4 ESS GUI	12
4.1 ESS Overview	12
4.2 Tab Descriptions	13
4.3 General Symbols in the GUI	14
5 Changing Language	15
5.1 Translation of the GUI	15
5.2 Set Language	16
5.3 Delete a Language	17
5.4 GUI Updates	17
5.5 Translation Mode	18
6 I/O Setup	19
6.1 Define Outputs	20
6.2 Define Inputs	20
7 Backup/Restore	21
7.1 Clear Databases	21
8 System Survey and Supervision	23
8.1 System Survey	23

8.2 Unite System Supervision	23
8.2.1 Adding a Module	24
8.2.2 Status Symbols	24
8.2.3 Changing the Supervision Settings	25
8.2.4 System Overview	26
8.2.5 Removing Modules from the Overview	27
8.3 Supervision of IP Equipment	27
8.3.1 Adding IP Equipment	28
8.3.2 Status Symbols	29
8.3.3 Changing Supervision Settings	29
8.3.4 Removing IP Equipment	30
8.4 Supervision of Auxiliary Equipment	30
8.4.1 Adding Auxiliary Equipment	30
8.4.2 Status Symbols	31
8.4.3 Changing Monitoring Settings	31
8.4.4 Removing Auxiliary Equipment	32
8.5 SNMP Traps	33
8.5.1 Management Information Base file	33
8.5.2 Information Received in Traps	34
8.5.3 Default SNMP Trap Action	35
8.5.4 Add/Change SNMP Trap Action	35
8.5.5 Removing SNMP Trap Action	37
8.6 Site Information	37
9 Fault Handling	38
9.1 Nomenclature	38
9.2 Active Faults	38
9.2.1 Module Fault List	39
9.3 ESS Fault Log File	40
9.3.1 Symbols used in the Fault Log	41
9.3.2 Block Repeated Faults	41
9.4 Trigger Conditions and Actions	41
9.4.1 Default Action	42
9.4.2 Add a Fault Action	42
9.4.3 Message Action	43
9.4.4 E-mail Action	43
9.4.5 SNMP Trap Action	44
9.4.6 Output Action	44
9.4.7 Error Relay Action	45
9.4.8 BusLogger Action	45
9.5 Summary Faults Actions	45

9.5.1 Activating Error Relay/Outputs	46
9.5.2 Sending Messages	47
9.6 Admin Log	48
9.6.1 Timeout	48
10 Message Routing.....	49
10.1 Message Routing Functions	50
10.1.1 Symbols Used in the Message Routing Function	51
10.2 Category Setup	52
10.2.1 Add a New Category	52
10.2.2 Default Category	53
10.2.3 Predefined Categories	53
10.3 Call IDs	54
10.3.1 Add a Call ID	54
10.3.2 Call ID Ranges	54
10.3.3 Search, View and Edit Call IDs	56
10.4 Add Multiple IDs	57
10.5 Delete Multiple IDs	57
10.6 Diversions	58
10.6.1 Individual Diversion Set Up	59
10.6.2 Diversion Chains	60
10.6.3 Adding Range Diversions	61
10.6.4 Search Diversions	62
10.7 Import/Export	62
11 Work Shifts	63
12 Group Handling.....	65
12.1 Group Handling Functions	65
12.1.1 Symbols Used in the Group Handling	66
12.2 Create a Multicast Group ID	67
12.2.1 Call ID Search	68
12.3 Create a Broadcast ID	68
12.4 Create a Group ID	69
12.5 View and Edit Groups	70
12.5.1 View and Edit Multicast Group ID	71
12.5.2 View and Edit Broadcast ID	71
12.5.3 View and Edit Group ID	72
13 Activity Logging	73
13.1 Log View	74
13.1.1 Symbols used in the Activity Log Viewer	74
13.1.2 Log information	74
13.1.3 View Activity Logs	74

13.1.4 Search	75
13.1.5 Print Search Result	77
13.1.6 View Related Activities	77
13.1.7 Print Related Activities	77
13.1.8 Continuous Log View	78
13.2 Filter Setup	78
13.2.1 Basic Filter Settings	79
13.2.2 Advanced Filter Settings	79
13.3 Printer Setup	81
13.3.1 Customized Printer Setup	82
13.3.2 Print Messages with Specified Priority	83
13.3.3 Discard/Print Activities for a Specific IP Address/Service	83
13.3.4 Print Activities based on Type	84
13.3.5 Discard Administration Events	84
13.4 Log Export Setup	85
13.4.1 Manual Export	86
13.4.2 Automatic Export	86
14 Users.....	89
14.1 Symbols	89
14.2 User Teams	89
14.2.1 Add User Team	90
14.2.2 Edit Messaging Rights	90
14.2.3 Edit Log View Rights	91
14.3 User Administration	91
14.3.1 Add Users	92
14.3.2 Add Additional Devices to Users	96
14.3.3 Additional User Call IDs	97
15 Clock Synchronisation.....	98
16 Document History	98
17 Related Documents	99
Appendix A: ESS and IT Security.....	100

1 Introduction

The Enhanced System Services (ESS) is a Unite module based on the ELISE hardware. The ESS main functionality is to act as a central unit in a Unite system. The main centralized services are:

- Number Planning and Message Routing
- System Supervision, logging and Fault Handling

This document describes the installation and configuration of the ESS.

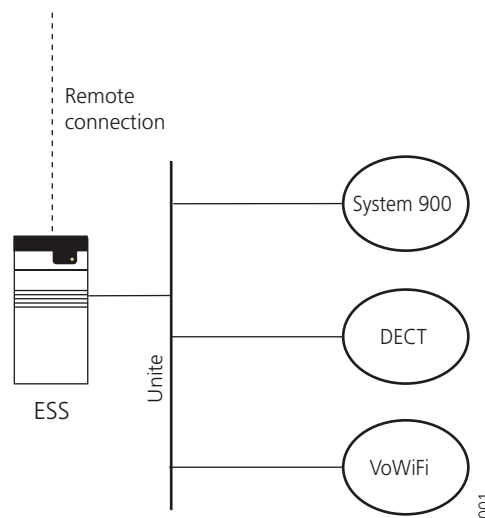


Figure 1. ESS connected to different carriers.

The ESS can be connected to different carriers such as System 900, DECT and VoWiFi Systems. All number planning, groups and individual users can be configured in one place. Messaging groups can be set up to send broadcast and/or multicast messages, if supported by the carrier system.

Access rights for messaging and activity log viewer can be set up. Call IDs are used for messaging in the Unite System and messages can be diverted to another Call ID depending on active work shift.

In the system overview, a summary of the system status is displayed. Unite modules and IP equipment can be supervised, and auxiliary equipment can be monitored via inputs. It is also possible to receive SNMP traps.

The ESS has a fault handling function where all active faults and fault logs are displayed. It is possible to configure and send; a message, an e-mail, an SNMP trap, or to activate an output when a fault is detected.

Another function in the ESS is to receive activity logs from the Unite system. Received activity logs can be displayed continuously and stored activity logs can be searched. Filters can be set up to minimize the internal database where the received activity logs are stored. The activity logs can be exported, and they can also be printed to a locally connected printer.

The ESS can also be used for remote connection to a customer site.

1.1 Requirements

1.1.1 PC Requirements

Microsoft Internet Explorer 6.0 or later.

JVM 1.5.0_06 (Java Runtime Environment Version 5.0)

1.1.2 Unite Modules Requirements

To be able to use the functionality of the ESS in a Unite system, the following versions of the Unite modules must be used:

Alarm Management Server (AMS)

Software version 5.20 or later.

Integrated Message Server (IMS)

Software version 2.60 or later.

MailGate

Software version 2.20 or later.

NetPage

Software version 3.60 or later.

Open Access Server (OAS)

Software version 3.60 or later.

Open Java Server (OJS)

Software version 2.20 or later.

Nurse Station Server (NSS)¹

Software version 3.00 or later.

Internetworking System Controller (ISC)¹

Software version 3.01 or later.

XGate

Software version 1.00 or later

¹.Message Routing, Number Planning and Activity Logging is not currently supported.

1.2 Additional Software Requirements

Radio Exchange DCT 1800 GAP

Software version R1E or later.

Support for Multicast and Broadcast Groups:

DCT 1800 GAP stand alone system with CPU2 - Software version R2A or later.

Central Unit System 900 S942C

Software version 6.10 or later.

teleCARE M Installation Program (TIP)

Software version 1.3 or later.

2 Installation

For mounting and connection of cables, see the *Installation Guide, ELISE2, TD 92232GB*.

If the ESS is to be used for remote management, a connection between the ESS and the Remote Management Client (RMC) is needed. For connection of cables, see *Installation and Operation Manual, Remote Management Client, TD 92256GB*.

2.1 Description of LED indicators

There are a number of LEDs on the ELISE hardware that indicate the status of the software, see [figure 2](#) on page 4. These status indications are software dependent and are described in this chapter. For information regarding indications by other LEDs, see the *Installation Guide, ELISE2, TD 92232GB*.

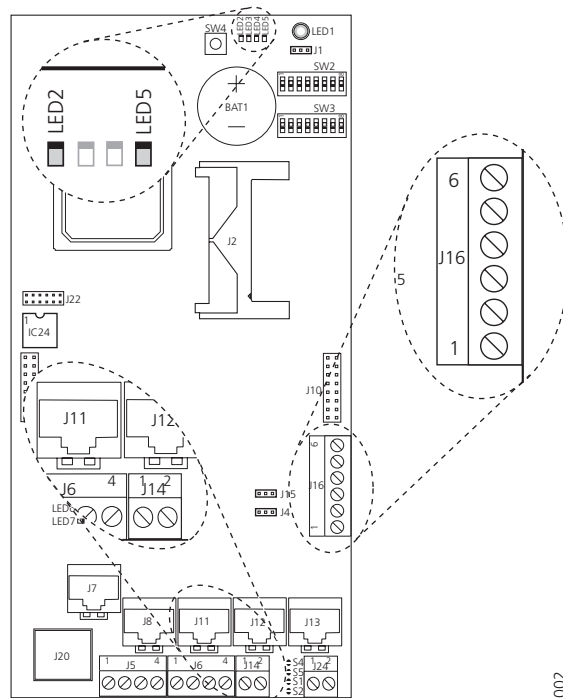


Figure 2. Location of the LEDs indicating the status of the ESS

LED #	LED Status	Indication
LED2	ON	Paging waiting in queue to A-bus.
	OFF	No pagings in queue.
LED5	ON	ESS applications are up and running.
	OFF	Problems when starting the applications. Check the log files on the ESS Administration web page for more information.

2.2 Internal Inputs and Outputs

The ESS has two open-collector outputs (J16, see [figure 2](#) above) that can be used by the Fault Handler in the ESS, see [9 Fault Handling](#) on page 38. The inputs on J16 are used for system supervision. For connections and a more detailed description of the outputs and inputs, see the *Installation Guide, ELISE2, TD 92232GB*.

2.3 Error Relay

The error relay output (J14 in [figure 2](#) above) can be used to indicate if the ESS is operating. When the ESS starts, the error relay operates. When the ESS is shutting down or rebooting, the error relay releases.

The error relay can also be released to indicate error (activated) and reset to normal operating mode by the Fault Handler, see [9 Fault Handling](#) on page 38.

Whether the error relay output opens or closes on actual relay status, depends on how the jumper J15 is set. For connections of the error relay and error relay output configuration, see the *Installation Guide, ELISE2, TD 92232GB*.

2.4 Licences

The ESS is delivered with the licences already programmed. For available licences, see *Data Sheet, Enhanced System Services, ESS, TD 92250GB*.

2.4.1 Unlicensed Mode

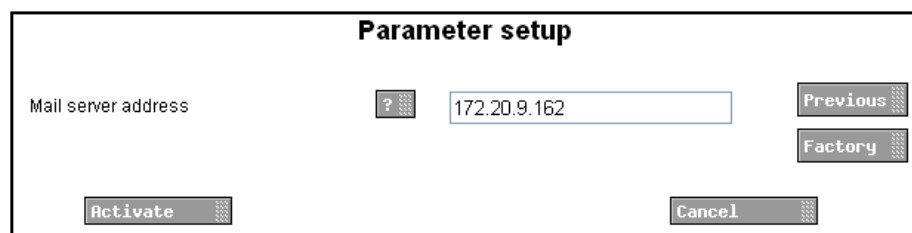
When needed, the ESS can be started in unlicensed mode. The ESS will have full functionality for 2 hours in unlicensed mode. After that, the ESS needs to be restarted, either physically or from the ESS Administration web page.

How to set the ESS in unlicensed mode is described in the *Installation Guide, ELISE2, TD 92232GB*.

2.5 Sending E-mail

A mail server address/host name has to be set up to be able to send E-mail from the Fault Handler and the Activity Logger.

- 1 Go to System Setup > Mail Server



114

Figure 3. Parameter setup for sending E-mail from the ESS.

- 2 In the Mail Server address field, enter the IP address/host name.
- 3 Click "Activate".

Note: The mail server must be set up to allow relaying to be able to send E-mails from the ESS.

2.6 Printing Log Information

To be able to print log information to a locally connected printer, the serial line printer must be connected to the ESS and the serial port of the ESS that is used for printing must be specified in the System Setup page. See *Data Sheet, Enhanced System Services, TD 92250GB* for supported printer.

Cable Connection between Serial Line Printer and the ESS

Use a straight data cable, article number "190255" or "190296" with RJ45 connector. Which cable to use depends on the length of the cable that is needed, see also *Data Sheet, Enhanced System Services, ESS, TD 92250GB*.

Attach the cable to the printer adapter and to a free RS232 connector on the ESS (there are three modular jacks for connection of RS232 communication on the ESS: J11 is serial port 1, J8 is serial port 2 and J7 is serial port 3). Then attach the printer adapter to the serial line printer.

Printer Settings in System Setup

- 1 Go to System Setup > Printer

Printer Settings

Serial port ? -- None -- Previous

Baud rate ? 19200 Factory

Parity ? None

Printed line length ? 80

Number of lines per page ? 55

[View advanced parameters](#)

Activate Cancel

130

Figure 4. Printer settings for the local connected printer.

- 2 Select serial port that the printer is connected to.
- 3 Select baud rate from the drop-down list. The baud rate is determined by the connected printer. For the recommended printer, set the baud rate to "19200".
- 4 Select parity from the drop-down list. The parity has to comply with the connected printer. For the recommended printer, set the parity to "None".

It is also possible to set the printed line length, by default it is set to 80 lines. Minimum value is 1 and maximum value is 1000.

In the *View advanced parameters*, control switches for formatting can be turned On or Off and other formatting parameters can be defined, for example changing text lines to be truncated if it exceeds the line length.

Printer Status

Status from the printer is sent as a Status Log, for example if the printer has run out of paper or the connection is down.

2.7 Additional Configuration in Unite Modules

To use the Fault Handling function and the UNS (Unite Name Server) in the ESS, other ELISE modules must be configured to send their status log messages and UNS requests to the ESS. To use the Activity Log functions in the ESS, all activity log messages from the modules connected to Unite must be sent to the ESS. This is done in the System Setup for each module.

For surveyed modules, a link to the administration pages is available from the ESS GUI. It is found in the module's setup page in System Overview > Unite Modules. See [8.1 System Survey](#) on page 23, [8.2 Unite System Supervision](#) on page 23, and [figure 27](#) on page 26 where the link is located.

The administration web page can also be reached from the direct link `http://xxx.xxx.xxx.xxx/admin`, where `xxx.xxx.xxx.xxx` is the IP address of the module that needs to be configured.

2.7.1 Sending Status Log Messages to the ESS

To use the Fault Handling function in the ESS, all status log messages from the modules connected to Unite must be sent to the ESS. This configuration is done for each module.

- 1 Go to System Setup > Logging > Status Log

The screenshot shows a configuration window titled "Module status log distribution". It features a "Destinations" field on the left and a "Status Log" section in the center. The "Status Log" section contains a list of text boxes, with the first one containing the text "172.20.9.140/FaultHandler". To the right of the list are "Previous" and "Factory" buttons. At the bottom of the window are "Activate" and "Cancel" buttons. A small "016" is visible in the bottom right corner of the window frame.

Figure 5. Module Status log distribution

- 2 In the Destinations field, enter the IP address of the ESS and the service FaultHandler on the format `xxx.xxx.xxx.xxx/FaultHandler`, see [figure 5](#) above.
- 3 Click "Activate". The module now sends all status log messages to the Fault Handler in the ESS.

A fault can be written multiple times to the ESS Status Log when the A-bus is connected to several Unite modules. To avoid this, do as follows:

- 4 Go to the administration web page for the module that should not send A-bus status messages. In the left menu in the 900 Interface part, select "System 900".
- 5 Select "No" in the drop-down list for Send module status from A-bus to UNITE?
- 6 Click "Activate". The module will from now on not send module status messages that are received from the A-bus.

2.7.2 Sending Activity Log Messages to the ESS

To use the Activity Log functions in the ESS, all activity log messages from the modules connected to Unite must be sent to the ESS. This configuration is done for each module in the Module activity log distribution.

- 1 Go to System Setup > Logging > System Activity Log

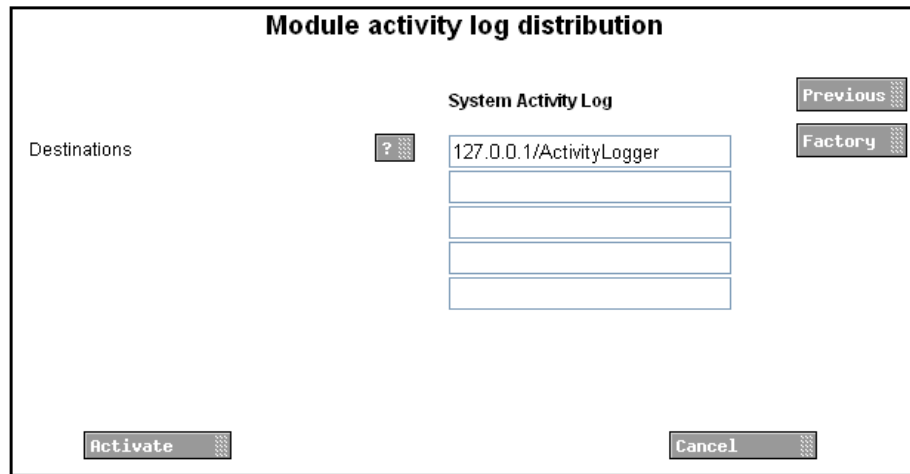


Figure 6. Module activity log distribution

- 2 In the Destinations field, enter the IP address of the ESS and the service ActivityLogger on the format xxx.xxx.xxx.xxx/ActivityLogger, see figure 6 above.
- 3 Click "Activate". The module will from now on send all activity log messages to the Activity Logger in the ESS.

2.7.3 Sending Extended Activity Logs (optional)

There is also an advanced setting page for extended activity logs: System Setup > Logging > View advanced parameters > Extended Activity Log.



Figure 7. Parameter setup to send extended activity logs.

Every Unite module in a system can be configured to make an extended activity log for all activities that passes the modules. The extended activity logs are not stored in the ESS, it is only for immediate use in the on-line view (page 78), and for quick information when tracing activity logs during troubleshooting. See also Function Description, Activity Logging in Unite, TD 92341GB, for more information. The function is disabled as default.

- 1 Select Enabled from the drop-down list.
- 2 Click "Activate".

2.7.4 Configuring the UNS

Each module may use the local UNS or forward all number plan requests to the central number plan in the ESS. If the module is configured to forward all requests to a central number plan, the local number plan is not used.

- 1 Go to System Setup > UNS > Setup.

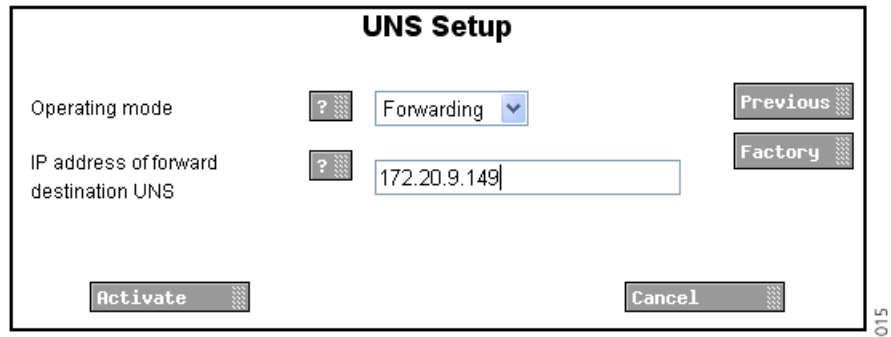


Figure 8. The UNS setup page in a Unite module.

- 2 Select "Forwarding" in the Operating mode drop-down list and enter the ESS IP address.
- 3 Click "Activate". The module now uses the ESS number plan.

3 Remote Connection

Through the ESS, it is possible to establish a remote connection to a customer site. This makes it possible to configure and maintain sites, independent of distance.

The remote management connection is established via the Remote Management Client (RMC), which is a Windows based tool. For installation and configuration of the RMC, see *Installation and Operation Manual, Remote Management Client, TD 92256GB*.

To be able to connect remotely, the remote management server in the ESS has to be configured.

- 1 Open the ESS administration web page and select "Remote Management" in the left menu. The *Remote Management Server* configuration page is opened

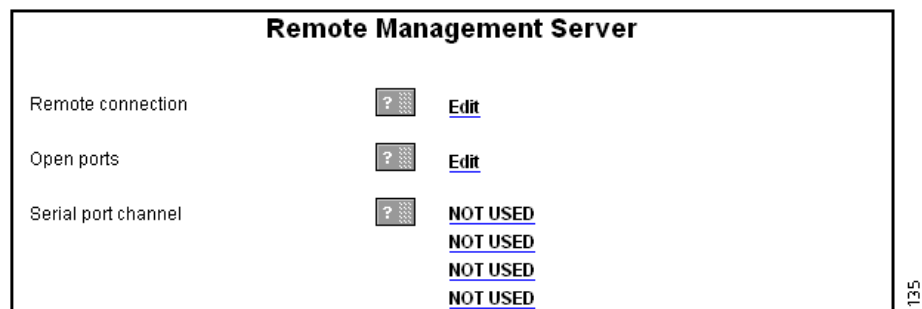


Figure 9. Parameters for Remote Management Server.

- 2 Click "Edit" for *Remote Connection*, to set up the connection parameters.

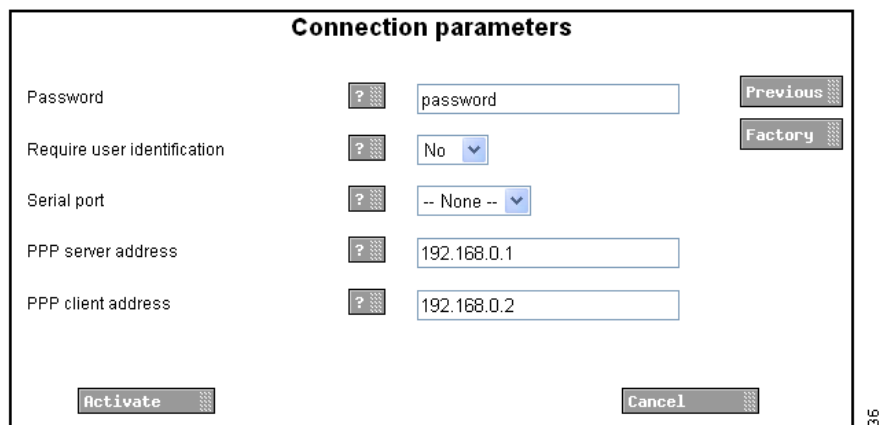


Figure 10. Remote connection parameters.

- 3 Set up the connection parameters and click "Activate".

- Click "Edit" for *Open Ports*, to open any additional ports that are needed for configuration tools. To be able to configure ports, section 8 on switch number 3 has to be set to ON.

Port

Switch nr 8 must be set to be able to change parameters

Open ports

10101

12345

Previous

Factory

Activate

Cancel

137

Figure 11. Open Ports for remote access.

For WinBK, CSM and TIP port 10101 has to be open. To be able to use the Activity Log Viewer over a remote connection, port 10130 has to be open.

- Click one of the "NOT USED" links for *Serial port channel*, to set up a new channel.

Serial port channel

Name

IP address

Remote Serial port

Baud rate

Parity

Notes

Previous

Factory

Activate

Cancel

138

Figure 12. parameters for serial port channel.

One serial port channel for each tool, for example WinBK for System 900 configuration, has to be set up. Web based configuration tools do not require serial port channels.

- Set up the channel and click "Activate".
- The configuration of the remote management server is described in detail in *Function Description, Remote Management, TD 92257GB*.

4 ESS GUI

To open the ESS GUI, enter the ESS IP address in the web browser address field.

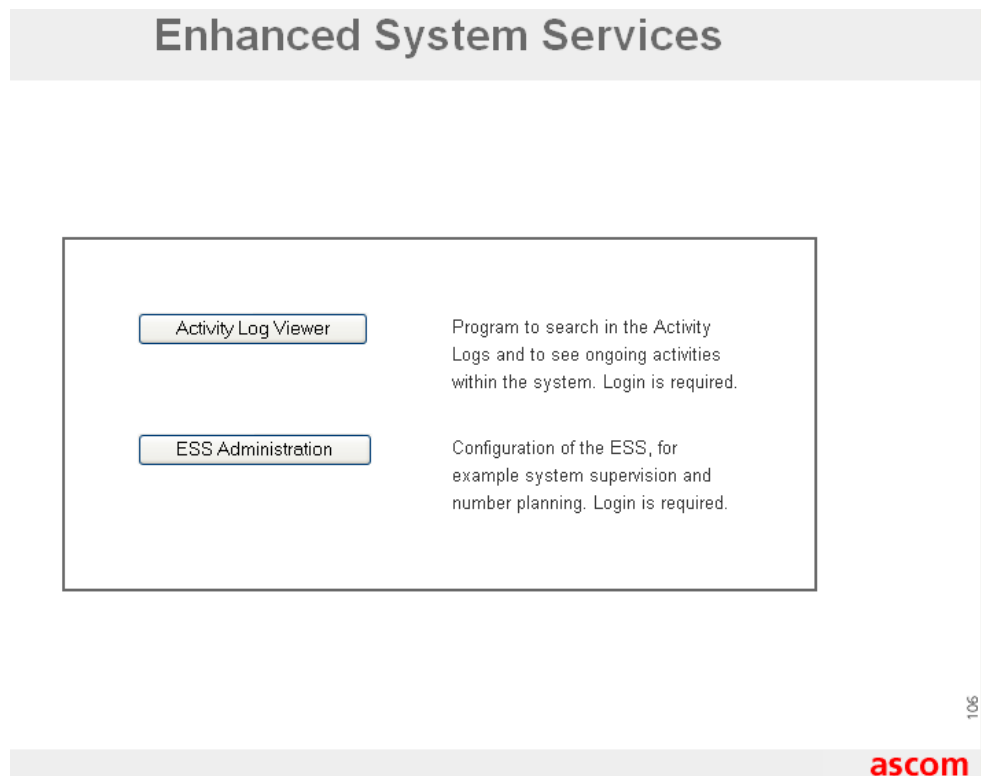


Figure 13. The start page of the ESS.

- The "Activity Log Viewer" button is a direct link to the *Activity Log Viewer*, see also [13 Activity Logging](#) on page 73.
To enter the page, user ID and password are required. The users are, admin, sysadmin or a user configured in the ESS. The user, configured in the ESS, log in with its own user ID and password that is set up by the administrator.
- The "ESS Administration" button opens the ESS home page.
To enter the page user ID and password are required.
The users "user", "admin" and "sysadmin" can be used to configure the ESS. The users "admin" and "sysadmin" have full access while "user" only has permission to the functions; *Group Handling*, and *Message Routing* except *Category Setup*. For more information about users and passwords, see *Installation Guide, ELISE2, TD 92232GB*.

4.1 ESS Overview

- Click the "ESS Administration" button to open the ESS home page.

The following page is opened when the correct password is entered.

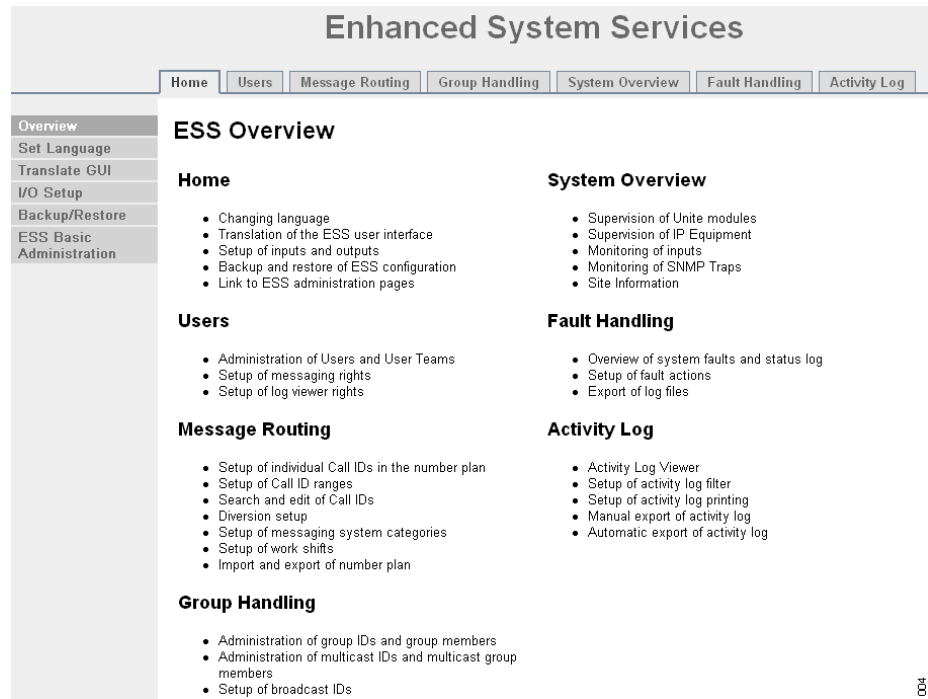


Figure 14. The ESS home page.

4.2 Tab Descriptions

The functionality behind each tab in the ESS is described below.

ESS Home

This page shows an overview of the ESS functions. It is possible to change the language and add translations. Inputs used by the System Supervisor and outputs used by the Fault Handler are set up here. The settings made in the ESS GUI can be backed up and restored. A link to the basic administration pages of the ESS is also available.

Users

On this page users and User Teams are administrated. Access rights are given to the User Teams, for messaging rights and log view rights.

Message Routing

On this page Call IDs are added to the number plan and available categories and diversion conditions are set up. It is possible to search in the number plan and for diversion conditions. It is also possible to set up work shifts for the system.

Group Handling

In Group Handling, messaging groups are created and managed.

System Overview

The System Overview gives a summary of the system status. Supervision of modules are set up on this page. It is also possible to set up supervision of IP equipment, to monitor auxiliary equipment via inputs and to set up triggers for received SNMP traps.

Fault Handling

In Fault Handling, it is possible to configure actions triggered by a fault. All active faults and fault logs are shown in a list.

Activity Log

In the Activity Log pages, you can set up filters and administrate the export of activity logs. In the Activity Log Viewer, the most recent activities can be displayed and stored system activity logs can be searched. There is also a Printer Setup page where printing of the log information can be enabled. It is possible to customize which log information that should be printed.

4.3 General Symbols in the GUI

The following symbols are generally used in the GUI:



Symbol	Description
	Delete
	Add web page to favorites

Figure 15. Symbols generally used in the GUI

To add a page to Favorites, click the "Add to favorites" symbol on each page (the symbol shown above). The general "Add web page to favorites" symbol available in the browser only creates a link to the first page of the ESS and not to any of the other pages.

5 Changing Language

The default language in the ESS GUI is English. The text that appear in the GUI are stored in a database. Several languages can be stored in the database, but it is not possible to edit or remove the default language.

5.1 Translation of the GUI

To translate the GUI, go to the *Translate GUI* page found in the left menu on the ESS *Home* page.

Translation

Existing languages:

[english](#)

Each language can be exported as an XML file. To create a new language or update an existing, click a language link above to download the file. If a new language should be created, change the language indication in the "language" tag. Translate/Update the text within "translation" and "helptext" tags and save the file. Import the XML file.

Import language file:

Enable translation mode:

In "Translation mode" all text will be exchanged with the identification in the language file. This can be used to identify where a text is displayed in the GUI.

005

Figure 16. The Language page.

The file that needs to be translated is an XML file generated from the ESS. To save the file for translation or editing purposes, click the language link in the window and save the file. The file can be saved in any name during the translation.

In the language file, there are numerous tags but only two tags and one attribute needs to be translated:

- <language id="English">
the "id" attribute is the text that appears in the drop-down list
- <translation>
text displayed in menus, on buttons, tabs etc.
- <helptext>
on-line help text

Below is an example of a language file (just showing two buttons with helptext, for simplicity).

```
<?xml version="1.0" encoding="UTF-8" ?>
- <translations>
- <language id="english" type="complete">
- <app id="ESS">
- <text id="MENU_ESS">
  <translation>Home</translation>
  <helptext>Access to ESS Logs and settings</helptext>
</text>
- <text id="MENU_ESS_M_ADMIN">
  <translation>Basic settings</translation>
  <helptext>Help text for Basic settings</helptext>
</text>
</app>
</language>
</translations>
```

906

Figure 17. An example of a translation file

When the file is translated, it must be imported to the database. Click "Browse" to locate the translated file and click the "Import" button.

The name of the translated language (the language "id" attribute) will appear as a link in the *Existing Language* list and can be downloaded for editing purposes.

The ESS GUI only supports the Latin-1 character set.

5.2 Set Language

The translated language (the language "id" attribute) is shown in the language drop-down list in the *Set Language* page. To choose language, select the language in the drop-down list and click "Change Language". To change language for this session only, i.e. temporarily, click "Apply".

5.3 Delete a Language

A language file can be deleted from the ESS by clicking the "Delete" symbol. It is not possible to remove the default language.

Translation

Existing languages:

[Svenska](#) 
[English](#)

Each language can be exported as an XML file. To create a new language or update an existing, click a language link above to download the file. If a new language should be created, change the language indication in the "language" tag. Translate/Update the text within "translation" and "helptext" tags and save the file. Import the XML file.

Import language file:

Enable translation mode:

In "Translation mode" all text will be exchanged with the identification in the language file. This can be used to identify where a text is displayed in the GUI.

060

Figure 18. A language file to be deleted.

5.4 GUI Updates

When a new version of the ESS is released, there might be changes in the GUI that need to be translated.

- 1 Import your old translated file to the new ESS software version. New text and buttons in the GUI are shown in English.
- 2 Click the language file link and save it.
- 3 Open the file and all tags that are not translated are marked with the comment:
<!-- The text identifier below couldn't be translated -->
- 4 Translate the new text and import the translated file again.

5.5 Translation Mode

All texts, buttons, menus etc. are identified with labels (for example MENU_ESS). With the translation mode function, it is possible to view the label for each button, menu etc. This can be helpful when translating the language file.

Mark the "Enable translation mode" check-box in the *Translate* page, see [figure 16](#) on page 15. Click "Apply" and all the labels on the pages are shown, see example below.

TEXT_TRANSLATION_TITLE

TEXT_TRANSLATION_LANGUAGE_TEXT

[English](#)

TEXT_TRANSLATION_EXPORT_TEXT

TEXT_IMPORT_LANGUAGE

TEXT_TRANSLATION_CHECKBOX_CAPTION

OPTION_DESIGN_MODE

TEXT_TRANSLATION_SAVE_TEXT

007

Figure 19. Design mode of the Translation page.

Clear the "OPTION_DESIGN_MODE" box and click "BUTTON_SAVE" to return to standard view.

6 I/O Setup

In the I/O Setup page, inputs and outputs are defined. The initial state for the output can be, low or high. The inputs can be selected to be activated on opening or on closing.

I/O Setup

Outputs

ID	Output Name	Module Address	Output	Inactive/Initial State	
1	Internal Output 1	Internal	1	High (open-collector) ▼	Reset
2	Internal Output 2	Internal	2	High (open-collector) ▼	Reset
5	OM2	6	2	High ▼	Reset ✖
6	OM1	4	1	Low ▼	Reset ✖

Define new output

Inputs

ID	Input Name	Module Address	Input	Activation	Activation Time	Last known status
1	Internal Input 1	Internal	1	On Opening ▼		
2	Internal Input 2	Internal	2	On Opening ▼		

Define new input

Save Cancel 035

Figure 20. I/O Setup page.

For the outputs, the state is set to the opposite of the initial state when activated. For example, if output 2 is set to low in initial state, the output will automatically be set to high when activated.

In addition to the internal outputs, outputs on an Output Module connected to the ESS A-bus can be used.

Inputs on an Alarm Module connected to the ESS A-bus can also be used.

Every time a new output or input is defined an automatic ID is created. The ID is a running number which can manually be changed into another number or a text if wanted. When an output or input has been deleted, the ESS will not remember that the previous ID number is free to be used again. The numbering will just continue on the number after the last created one. See [figure 21](#) on page 20.

6.1 Define Outputs

- 1 Click "Define new output".

Outputs

ID	Output Name	Module Address	Output	Inactive/Initial State	
1	Internal Output 1	Internal	1	High (open-collector)	Reset
2	Internal Output 2	Internal	2	High (open-collector)	Reset
5	OM2	6	2	High	Reset ✖
6	OM1	4	1	Low	Save ✖

104

Figure 21. Define new outputs.

- 2 Enter *Output Name*, *A-bus Module Address* and *Output* number.
- 3 Select *Initial State*.
- 4 Click "Save".

6.2 Define Inputs

- 1 Click "Define new input".

Inputs

ID	Input Name	Module Address	Input	Activation	Activation Time	Last known status
1	Internal Input 1	Internal	1	On Opening		
2	Internal Input 2	Internal	2	On Opening		
4	OM2	6	2	On Closing		

Save Cancel 105

Figure 22. Define new inputs.

- 2 Enter *Input Name*, *A-bus Module Address* and *Input* number.
- 3 Select *Activation* condition.
- 4 Enter *Activation Time*. By default there is a notification indicating that the activation will be sent immediately. If you enter activation time, the input has to be active for the set time before a notification is sent.
- 5 Click "Save".

7 Backup/Restore

In the ESS *Home* page, it is possible to backup and restore the parameters and databases and to clear the databases. It can for example be used when information is to be copied from one ESS to another ESS, or to restore the database in the ESS. The format of the backup file is xxx.tar.gz.

There is also a backup/restore in the System Setup web page "xxx.xxx.xxx.xxx/admin". That is to be used when upgrading an ESS with an image, when an ESS module should be replaced with another ESS module in case of hardware failure, and to update the configuration in the ELISE.

To backup or restore, go to "Backup/Restore" in the left menu in the *Home* page.



Figure 23. Backup/restore of the settings in the ESS GUI.

Backup

- 1 Click "Backup".
- 2 In the dialogue window click "Save" and enter the file name and file path.

Restore

- 1 Click "Restore".
- 2 Locate the tar.gz file and click "Restore".

7.1 Clear Databases

This function is used when an empty configuration is required, for example when you want to restart the configuration from scratch. The old information can not be retrieved after a database is cleared. These are the databases that can be cleared:

- Users, Message Routing and Groups
- Fault Logs
- Activity Logs
- GUI Translations

Clear databases

Select databases to be removed. All contents will be discarded and databases are reset to default.
Note: Removing databases can take up to 15 seconds and affected components will be restarted!

- Message Routing and Users
- Fault Logs
- Activity Logs
- GUI Translations

Clear

129

- 1 Select database.
- 2 Click "Clear".
It can take up to 15 seconds to remove a database. Affected components will be restarted.

8 System Survey and Supervision

System survey and supervision of Unite modules are set up in the *System Overview* page. It is also possible to set up supervision of IP equipment, to monitor auxiliary equipment via set up inputs, monitor SNMP Traps, and to export site information.

8.1 System Survey

To start a system survey, click the "Survey System" button in the *System Overview* page, and all Unite modules connected to the LAN are surveyed. To survey one single module, enter the IP address for the module and click the "Survey Module" button.



Figure 24. Start of a system survey

When the system or a single module is surveyed, information about the module is shown. New modules that are found are shown in a separate list, *New Modules*. Modules that are lost since the last survey are shown in the list *Lost Modules*.

Module	IP Address	Host name	Status Since
NetPage	172.20.10.1	Netpage	
3.51	Service	Description	2006-09-20 13:01:25
8.10	S900	System 900 Interface	
ESS	172.20.10.47	ESS_Swe	
1.03	Service	Description	2006-09-20 13:01:25
8.04	S900	System 900 Interface	
	FaultHandler	System Fault Handler	

Figure 25. The new surveyed modules.

The survey request is sent out as a broadcast message, meaning that any module placed outside a router will not receive the request. If a module is placed outside the local LAN router, a specific request (Survey Module) to that module must be made for the first survey. Once the module has been added to the list of "Existing modules", it will be included in subsequent system survey requests. If an existing module is not answering on the broadcast message, a directly addressed survey request will always be sent.

8.2 Unite System Supervision

The ESS can supervise the modules that respond to a survey request. A request will be sent to the module with the specified interval, default set to 30 seconds. The ESS can send a supervision request (either to a Unite module or an ICMP ping) every 2 seconds, i.e. if the interval is set to 30 seconds up to 15 modules (Unite or IP Equipment) can be supervised. If this limit is exceeded, the interval will automatically be increased.

In the response, the module includes information about host name, software and OS versions, module key, licence, start-up time, and start-up cause. If the error relay is

released, the response will include this information also which will result in the status "Error" in the overview.




If the module does not answer on the request, the ESS will generate a persistent Status Log. It includes the module type, IP address and host name of the non-responding module. The default level is "Critical", but can be changed on the setup page. It is also possible to add a customized text to the Status Log. The persistent fault will be cleared when the ESS gets a response from the module.

When supervision is started/ended and when the supervision interval is changed, an Activity Log with information about the changes will be sent.

8.2.1 Adding a Module

The new modules detected in the system survey have to be added to the existing system by clicking the "Add" button. These modules will subsequently be supervised by default and shown in the list *Existing Modules*.

Existing Modules





Module	IP Address	Host name	Status	Since
ESS	172.20.9.145	ESS-145		
<input type="button" value="Setup"/> 				
B6-2.10	Service	Description		
8.21	S900	System 900 Interface		2006-10-12 14:17:04
	FaultHandler	System Fault Handler		
	ActivityLogger	System Activity Logger		

014

Figure 26. List of existing modules at a certain time

8.2.2 Status Symbols

When a system or module is supervised, a status symbol for each module is shown. There are four symbols describing the status of the module:

Symbol	Description
	Supervision OK
	Module lost
	Module error
	Module not supervised

8.2.3 Changing the Supervision Settings

Click "Setup" for the module whose supervision settings should be changed, see [figure 26](#) on page 24.

On the *Setup* page, it is possible to choose if the module should be supervised or not, and to set the interval (in seconds, default value is 30 seconds) at which the ESS sends out a module status request to the supervised module. The level that the fault shall be reported as can be changed and the Event description can be added to the Status Log. The interface description can also be edited on this page. There is also a direct link to the administration pages for basic configuration of the module.

Setup Parameters:

Supervised:	If module/equipment should be supervised or not.
Interval:	The time between supervision request.
Level:	The fault level to use in the transmitted Status Log.
Event Description:	A customized description that will be added to the Status Log.

Setup

Module information

Module: IMS
IP Address: 172.20.10.148
Host name: MDGW1

Software version: SU-1.00-8.3.3-A
OS version: 8.05-8.X.X-A
Module key:
Licence options:
Status: OK
Start time:
Start cause: Unknown

Notes

Supervision

Supervised: Yes No
Interval: (s)

Log Setup

Level

Event Description

Interfaces

Interface	Description	My description
S900	System 900 Interface	<input type="text"/>
DECT	DCT-1800-S gateway	<input type="text"/>
OAP	OAP Interface	<input type="text"/>

Additional Configuration

[Configure the module parameters](#)

6/13

Figure 27. The Setup page with module information.

8.2.4 System Overview

When all modules are set up for supervision, the *System Overview* page gives a snapshot of the system at the time stated uppermost on the page. To get current status of the system, click the "Update page" link and the status of the modules are updated in the list *Existing Modules*.

If a new system survey is wanted, click the "Survey System" button again. If any new modules have been added to the system since the last survey, they will be shown in the "New modules" list and can be set up to be supervised.

8.2.5 Removing Modules from the Overview

If a module is physically removed from the system and a new survey is made, the module is not automatically removed from the *System Overview* page. The result of the survey for that module will be "Module lost".

To remove the module from the *System Overview*, click the "Delete" symbol. A dialogue window opens, click "OK" to remove the module.

8.3 Supervision of IP Equipment

The ESS can supervise IP Equipment by sending ICMP ping requests. If the equipment does not answer on the sent request, a persistent Status Log will be generated. It includes the configured Equipment name and IP address or host name. The default level is "Error", but can be changed on the setup page. The persistent fault will be cleared when the equipment responds again.

The ESS can send a supervision request (either to a Unite module or an ICMP ping) every 2 seconds, i.e. if the interval is set to 30 seconds up to 15 modules (Unite or IP Equipment) can be supervised. If this limit is exceeded, the interval will automatically be increased.

Example: if the interval is set to 30 seconds as above, but the modules to supervise are 30, the interval will be increased to 60 seconds.

When supervision is started/ended and when the supervision interval is changed, an Activity Log with information about the changes will be sent.

To set up supervision, click *IP Equipment* in the left menu.



078

Figure 28. The IP equipment page.

8.3.1 Adding IP Equipment

- 1 Enter IP address or host name.
- 2 Click "Add Equipment" to add equipment to the survey.

IP Equipment




Module	IP Address	Status	Since	
	172.02.03.04		2006-10-16 10:30:35	<input type="button" value="Setup"/>

Enter IP or host name and press Add Equipment to start supervising new equipment.

110

Figure 29. Added equipment. The supervision status of the module is showing that the module is not supervised.

8.3.2 Status Symbols

Symbol	Description
	Supervision OK
	Equipment lost
	Not Supervised

8.3.3 Changing Supervision Settings

- 1 Click "Setup" to set up supervision parameters for the equipment.

Setup

Equipment information

Equipment:
IP Address:

Notes

Supervision

The equipment is supervised with ICMP ping

Supervised: Yes No

Interval: (s)

Log Setup

Level

Event Description



Figure 30. Setup page for IP equipment.

- 2 Enter a descriptive text in the Equipment field. Equipment is shown as Module in the Status Log.
- 3 Change IP address or host name if the address of the equipment has changed.

- 4 Select if the equipment should be supervised or not.
- 5 Enter the time between supervision requests.
- 6 Select fault level from the drop-down list to use in the transmitted Status Log.
- 7 Enter a description of the event.
- 8 Click "Save".

8.3.4 Removing IP Equipment

Remove IP equipment by clicking the "Delete" symbol. A dialogue window opens, click "OK" to remove the IP equipment.

8.4 Supervision of Auxiliary Equipment

The ESS can be configured to generate a Status Log when receiving an Input Activity. This can be used by equipment that indicates faults via a physical output to send faults to the Unite system. For each input that is monitored, equipment name, fault level and event description can be configured. It is also possible to set that the sent Status Log should be persistent. The persistent fault will be cleared when the input is deactivated. The inputs are defined on the *Home - I/O Setup* page.

When monitoring is started/ended, an Activity Log with information about the changes will be sent.

This page reflects system status at 2000-01-02 11:52:47 [Update page](#)

Auxiliary Equipment Monitoring

Input	Status	Since	
Internal Input 1		2000-01-02 09:12:51	<input type="button" value="Setup"/> <input type="button" value="X"/>

Internal Input 1

079

Figure 31. The Auxiliary Equipment page.

8.4.1 Adding Auxiliary Equipment

- 1 Select an Input from the drop-down list.
- 2 Click "Add Auxiliary Equipment" to add selected input.

This page reflects system status at 2005-08-30 10:24:05 [Update page](#)

Auxiliary Equipment Monitoring





Input	Status	Since	
Internal Input 1		2005-08-29 16:15:01	<input type="button" value="Setup"/> <input type="button" value="X"/>
Internal Input 2		2005-08-30 10:12:40	<input type="button" value="Setup"/> <input type="button" value="X"/>

Internal Input 1

111

Figure 32. Internal Input 2 has been added.

8.4.2 Status Symbols

Symbol	Description
	Monitored
	The input is not defined in the I/O setup.
	The auxiliary equipment has activated the input, i.e. signals a fault.
	Not Monitored

8.4.3 Changing Monitoring Settings

- 1 Click "Setup" to set up monitoring parameters.

Input:	The inputs are defined in the I/O setup page. The input can be changed, for example if the monitored equipment has been moved.
Monitoring:	If the input should be monitored or not.
Equipment Name:	Is shown as Module in the Status Log.
Level:	The level that the fault shall be reported as.
Persistent:	Fault remains until the input is not active any longer.
Event Description:	Is shown under Description for the Status log.

Setup

Input

Internal Input 1 ▾

Notes

Monitoring

Monitored: Yes No

Log Setup

Equipment Name

Level ▾ **Persistent**

Event Description

083

Figure 33. Monitoring setup page for auxiliary equipment.

- 2 Select input if the input should be changed. Information about changes can be written in the *Notes* box.
- 3 Select if the input shall be monitored or not. When starting to monitor inputs from the ESS, the status will always be OK regardless of the actual state of the input. This give that if the input is active when monitoring is started no Status Log is sent.
- 4 Enter the name of the equipment.
- 5 Select logging level from the drop-down list.
- 6 Mark the check-box *Persistent*, if a fault should remain until the input is not active any longer.
- 7 Enter the description of the event.
- 8 Click "Save"

8.4.4 Removing Auxiliary Equipment

Remove auxiliary equipment by clicking the "Delete" symbol. A dialogue window opens, click "OK" to remove the auxiliary equipment.

8.5 SNMP Traps

SNMP (Simple Network Management Protocol) can be used by IP equipment to communicate that there are for example faults in the equipment.

The ESS can be configured to generate a Status Log when receiving an SNMP Trap. The Status Log will include the IP address that the trap was sent from, and text entered in the configuration. The information received in the trap can be added to the configured text.

The default action is to generate a Status Log with level "Information" for every received trap. The log level can be changed in the Log Setup.

It is possible to add SNMP Trap actions to get different behaviour depending on the sender's IP address and the information in the trap. The actions will be matched in the order displayed on the overview page and only one action will be executed.

By using wildcard *, several IP addresses can be matched in one action, for example "172.20.*.*" matches all IP addresses starting with 172.20. Wildcard* can also be used to match parts of the SNMP Trap message, for example "Error*" matches all messages starting with the word Error while "*Error*" matches all messages including the word Error.

Received traps can be discarded by selecting "No Log" in the Log Setup. This can be used either to discard traps from a specified address or with a specific message, or in the default action to discard all traps that are of no interest (i.e. the ones that are not matched by the configured actions).

8.5.1 Management Information Base file

To find the Management Information Base file (MIB) click "ESS Basic Administration" in the left menu on the *Home* page. A new window opens.

- 1 Click "Documents"
- 2 Click "Ascom unite mib" in the left menu

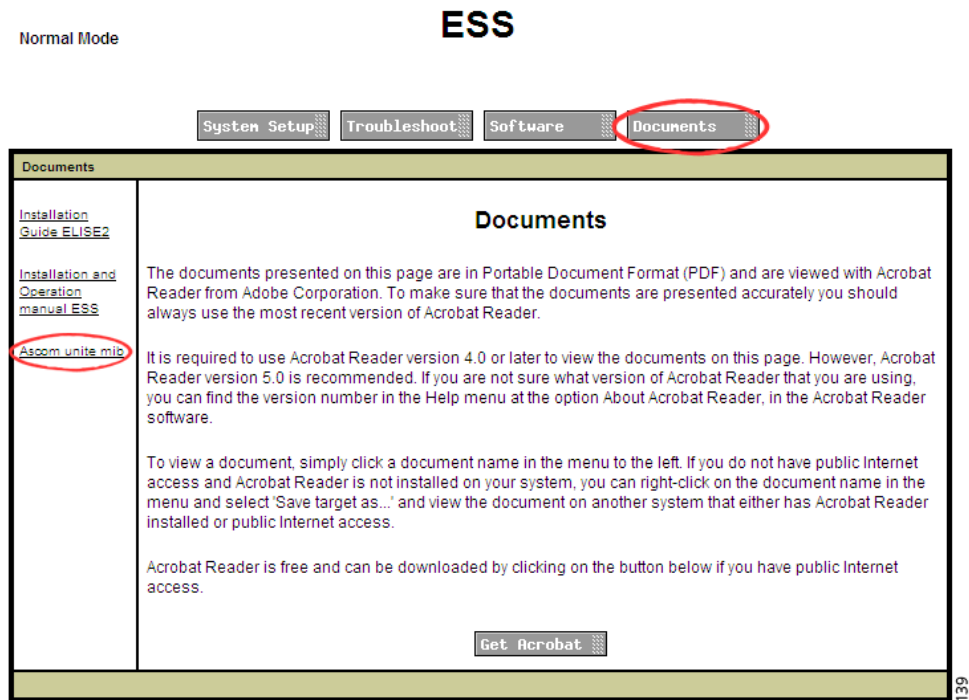


Figure 34. Where to find the MIB file.

8.5.2 Information Received in Traps

The information about which traps the sending equipment can send, is defined by the MIB (see [8.5.1 Management Information Base file](#) on page 33) set by the equipment vendor. A received trap includes a hierarchically structured number called object identifier (OID) and optional variables.

For example, traps sent from Airespace equipment will have an OID starting with 1.3.1.6.4.1.14179, where 1.3.1.6.4.1 identifies that it is an enterprise specific trap and 14179 stands for Airespace.

When the ESS receives a trap, it creates a string starting with the OID followed by a hyphen (-). Any received variables are added to the string after the hyphen. The filter set up in the SNMP trap action is matched against the created string.

Example:

When a Cisco access point restarts, a trap with OID 1.3.6.1.4.1.9.0.0 is sent. The first variable holds the uptime for the access point. The ESS creates a string with the following appearance; 1.3.6.1.4.1.9.0.0-4 days, 21:56:52.90.

When setting up the SNMP trap actions, consult the MIB provided by the vendor for more information about the traps. In addition, set up the default action to include the received information in the sent Status Log and force the equipment to generate traps to get detailed information.

8.5.3 Default SNMP Trap Action

The default action will be matched for all traps that are not matched by any other actions that are set up. In the Status Log, the module will be set to "-" and the IP address and Event Description will be copied from the received trap.

SNMP Trap Actions

Module	IP Address	Filter	Enabled	
DEFAULT			✓	<input type="button" value="Setup"/>

133

Figure 35. The default setting for SNMP trap action.

Change Status Level

- 1 Click "Setup".

Default SNMP Trap Action Setup

Log Setup

Information ▼

Event Description

Include trap data

132

Figure 36. The default SNMP trap is enabled to receive information.

- 2 Select which level the sent Status Log should have, or select "No Log" to not generate a Status Log when a trap only matching the default action.
- 3 Enter an event description to be included in the Status Log.
- 4 Mark the check-box *Include trap data*, if received trap data should be included in the log message.
- 5 Click "Save".

8.5.4 Add/Change SNMP Trap Action

This is used when SNMP traps from specific modules or with certain messages should be handled individually. The IP address in the received trap should match the defined pattern and/or the trap message should match the pattern set up in the filter. By selecting "No Log" in the Log Setup, traps matching the set up conditions can be discarded.

Module: A name that identifies the equipment that sent the SNMP trap.

- IP Address: The IP address that should match the address of an incoming SNMP trap.
- Filter: A text that should match the message of an incoming SNMP trap .
- Enabled: If enabled, incoming SNMP traps will be matched with the IP address and the filter condition that is set.
- Level: The level that the fault shall be reported as.
- Event Description: The information will be added to the Status Log.
- Include trap data: The received trap data will be included in the log message.

SNMP Trap Action Setup

Module:

IP Address:

Filter:

Notes

Action Conditions

Enabled: Yes No

Log Setup

▼

Event Description

Include trap data

134

Figure 37. The action is setup to receive SNMP trap with the status Warning.

- 1 Enter a name that describes the sender of the SNMP traps.
- 2 Enter the IP address pattern that should match the IP address in the received trap.
- 3 Enter a text that should match the trap message. Wildcard (*) can be used to match a part of the received message. Leave the field empty if the trap should be received regardless of the trap message.
- 4 Select if the action should be enabled to not.
- 5 Select which level the sent Status Log should have or select "No Log" to not generate a Status Log when a trap matching the conditions is received.
- 6 Enter an event description to be included in the Status Log.

- 7 Mark the check-box *Include trap data*, if received trap data should be included in the log message.
- 8 Click "Save".

8.5.5 Removing SNMP Trap Action

Remove SNMP trap action by clicking the "Delete" symbol. A dialogue window opens, click "OK" to remove the SNMP trap action.

8.6 Site Information

In the site information page, it is possible to export information about the site to a text file. Information about the modules and the supervised equipment will be included in the text file as well as the last 100 status logs.

Site Information

Notes



The screenshot shows a text area for entering notes, with a vertical scrollbar on the right side. Below the text area are two buttons: "Save" and "Undo".

Export

Click button to export information about the site to a text file. Information about existing, lost and new modules as well as information about supervised equipment will be included.

Export

080

Figure 38. Site information page.

The *Notes* field can be used to describe the system. These notes will also be included in the exported site information.

The exported file will be stored as an XML file.

9 Fault Handling

To be able to use the Fault Handler functions in the ESS, all concerned modules must be configured to send their status log messages to the ESS. For more information, see [2.7.1 Sending Status Log Messages to the ESS](#) on page 7.

The functions in the Fault Handler are:

- System status presentation
- Storing of the last 1000 received Status Logs
- Trigger conditions and action settings on faults
- Summary fault action settings on persistent faults
- Exporting the fault log in CSV format
- Clear all non-active faults
- Block repeated faults for a time period

9.1 Nomenclature

Trigger: A set of conditions that is used to match specific fault messages that have been sent to the Fault Handler.

Action: Events that can be started as a response to a trigger matching a fault message. That is; sending a message to a Call ID defined in the UNS, activating an output or the error relay, and sending SNMP Trap and E-mail.

Fault action: A set of triggers that starts one or several actions

9.2 Active Faults

When clicking on the "Fault Handler" tab in the top menu, the *Active Fault* page is displayed. Active Faults page is where the last 100 received active persistent fault logs are listed. For more information about the fault log, see to [9.3 ESS Fault Log File](#) on page 40.

The following information is shown for each fault:

- Time when the fault occurred
- Level of the fault:
 - Critical error
 - Error
 - Warning
- Description of the fault, as defined in the module
- Type of module
- IP address and host name of the module that generated the fault

By expanding the fault in the list, additional information about the fault is shown containing:

- Fault ID
This is used to reference a persistent fault when it later is reset
- Fault code
- Description of the fault code
- Extended address information showing the system, bus type and module address
In the figure below the system is 00, the bus type is 1 and the module address is 0A

This page reflects the active faults at 2004-04-20 10:21:20 [Update Page](#)

Active Faults

Active Faults: 1 - 5

[Expand all entries](#)

Time	Level	Description	Module	Address	
2004-05-26 09:07:16	Error	Supervision	T942CEN	172.20.9.127	✗
		Other communication interruption		FI-Elise	
ID: 10A	3-1-C	Module status C, for module 0A on A-bus in system 00		00-1-0A	
2004-04-15 18:37:44	Error	Fault in module/component	REX	172.20.9.134	✗
		Major Base Station Error		Elise	
2004-04-15 17:39:34	Error	Fault in module/component	REX	172.20.9.134	✗

Error Relay

017

Figure 39. The Active Faults page

The fault will remain in the list until the module sends a status message confirming that the module is working properly again. It is also possible to delete the fault in the list by clicking the delete symbol.

The active faults list page has to be manually updated by clicking the "Update Page" link uppermost on the page.

On this page, the error relay can be reset.

9.2.1 Module Fault List

A module fault list exists for each module in the system, which shows codes and statuses etc. for each module. The "Module Fault List" is found in the administration web page under "Troubleshoot".

9.3 ESS Fault Log File

The ESS fault log is a centralised log file and shows a complete log of the faults in the system. Every time a fault message is generated in the system, information about the fault is written to the log file. The maximum number of entries in the log file is 1050. When the log file is full, the 50 oldest entries are removed.

The first 25 log entries are shown in the *Fault Handling* page. To get the following 25 log entries, click the "Next" link.

The following levels exist in the fault log:

- Information
- Individual reset
- All OK
- Critical error
- Error
- Warning

Fault Log

Entry 1 - 25 [Next](#)




[Expand all entries](#)

Time	Level	Description	Module	Address
⊕ 2004-04-06 08:33:07	Warning	Supervision Application restarted	IMS	172.20.9.134 Elise
⊕ 2004-04-06 08:24:30	Error	⚡ Supervision Lost link to DECT	IMS	172.20.9.134 Elise
⊕ 2004-04-06 08:23:43	Warning	Fault in module/component Minor CPU Error	REX	172.20.9.134 Elise
⊕ 2004-04-06 08:23:04	Error	⚡ Supervision Lost link to DECT	IMS	172.20.9.134 Elise
⊕ 2004-04-06 08:22:02	Warning	Fault in module/component Minor CPU Error	REX	172.20.9.134 Elise
⊕ 2004-04-06 08:22:02	All Ok	⊗ No error	REX	172.20.9.134 Elise

8

Figure 40. Example of ESS fault log.

9.3.1 Symbols used in the Fault Log

Symbol	Description
	Active persistent fault
	Persistent fault that has been handled
	Reset message, no fault exists

To get more detailed information about the events, it is possible to expand the log entries by clicking the "Expand all entries" link. Single log entries can be expanded by clicking the individual plus symbol.

9.3.2 Block Repeated Faults

If a Status Log is received repeatedly, i.e. a Status Log with the same content and from the same Unite Address, it can be blocked for a set period of time. Repeated Status Logs can occur in the system for example if a Unite module sends Activity Logs to an ESS that has no licence to handle Activity Logs. Persistent Status Logs and reset of persistent faults will never be blocked.

The ESS will discard all blocked Status Logs that are received during the set time, i.e. if the timeout is set to 10 minutes and the Status Log is received once every minute, every tenth Status Log will be stored in the ESS. No actions will be executed for the discarded Status Logs.

The ESS keeps track of up to 100 different Status Logs and the timeout is set individually for each one of them.

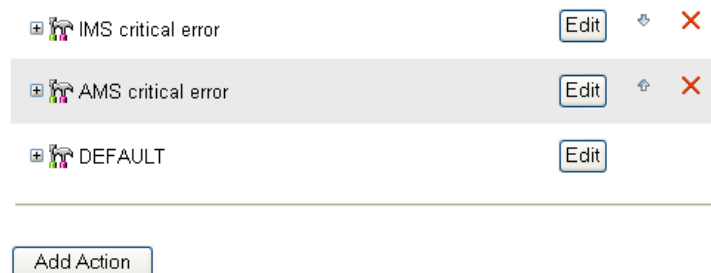
The timeout is set on the "Admin Log" page, see [9.6 Admin Log](#) on page 48.









9.4 Trigger Conditions and Actions

Settings of trigger conditions and actions are made in the *Actions* page. When the page is opened, a list of all existing actions is shown.

Fault Actions

Fault Actions will be matched in listed order. When a trigger condition matches the incoming fault message, the following actions will not be matched.



  IMS critical error	Edit		
  AMS critical error	Edit		
  DEFAULT	Edit		

018

Figure 41. Overview of Fault Handling Actions

The action with the highest priority is shown first in the list, i.e. at the top. The actions are processed by the Fault Handler in priority order. The Fault Handler only processes the first action that matches the incoming fault message, that is, only one action will be processed for each fault message. The priority order can be changed by using the arrows.

An action can be deleted by clicking the delete symbol.

9.4.1 Default Action

The *Default* action is triggered on all faults that have not been processed by any of the previous actions. In the *Default* action, it is only possible to set actions since it is automatically triggered on all remaining faults. The *Default* action cannot be deleted and is automatically placed last in the action list.

9.4.2 Add a Fault Action

- 1 To add a new action, click "Add Action".
- 2 Enter the name of the action (mandatory) and additional text, if wanted, in the *Notes* field.

New action

Action Name

IMS critical error

Notes

019

Figure 42. Action name

Trigger Conditions

- 3 Enter the trigger conditions. The trigger can include either host name, IP address type of module or level of the fault. The type of module is found in the *System Overview* page.

At least one of the three fields *Hostname/IP address*, *Module* or *Level* must be entered to create a trigger.

- 4 The action can have more than one trigger. To add more triggers, click "Add Trigger".

Trigger

Host name/IP Address	Module	Level
	IMS	Critical

Add Trigger

020

Figure 43. Trigger conditions.

- 5 Define actions that indicate the fault, see descriptions on how to configure below.

- 6 Click "Save", located at the bottom of the page. The fault action is saved and added before the default action in the list on the *Actions* page. By expanding the fault action, the triggers and actions are shown.
- 7 If needed, change the priority of the fault action by clicking the arrow symbols on the right side of the edit button.

Fault Actions

Fault Actions will be matched in listed order. When a trigger condition matches the incoming fault message, the following actions will not be matched.

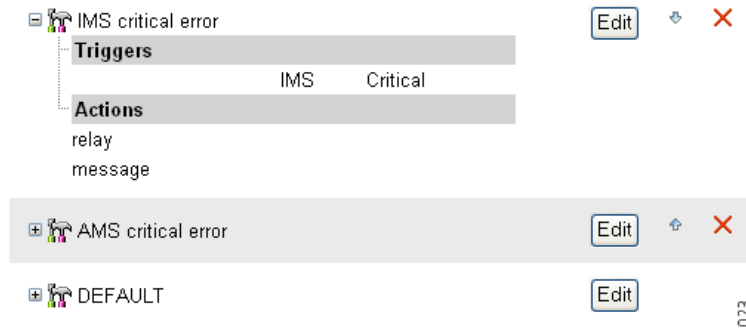


Figure 44. Expanded action list

It is possible to edit a fault action by clicking the "Edit" button. A View/Edit page opens with the same functionality as in the New Action page described above.

9.4.3 Message Action

- 1 Click "Add message" to define a message to send. Enter the Call ID (must be defined in the UNS, see [10.3 Call IDs](#) on page 54) and the message text.

Actions

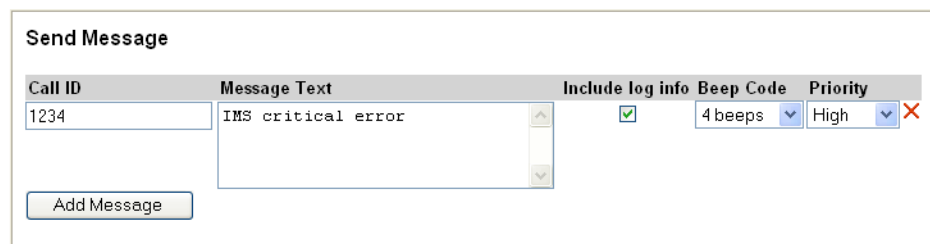


Figure 45. Defining the message to be sent.

- 2 Mark the *Included log info* check-box to add the fault information to the message text.
- 3 Select the beep code level.
- 4 Select the priority level.
- 5 Click "Add Message" again to add another message to send.

9.4.4 E-mail Action

To be able to send E-mail from the Fault Handler, the IP address/host name of the mail server must be set up in the System Setup, see [2.5 Sending E-mail](#) on page 5.

- 1 Click "Add Email" to define an e-mail to send.

084

- 2 Enter e-mail addresses and any addresses that should receive a copy.
- 3 Enter a subject and a message text.
- 4 Mark the Include log info check-box to add the fault information to the message text.

9.4.5 SNMP Trap Action

The ESS uses the Ascom Unite MIB (see [8.5.1 Management Information Base file](#) on page 33) when sending traps.

The sent trap includes a hierarchically structured number called object identifier (OID) and optional variables. The OID for the sent trap is 1.3.6.1.4.1.27614.1.2.1.2.0.1.

- 1 Click "Add SNMP trap" to define a SNMP trap to send.

075

Figure 46. Send SNMP Traps.

- 2 Enter the IP address that the trap is to be sent to.
- 3 Enter the text that should be sent.
- 4 Mark the *Include log info* check-box to add the fault information to the message text.
- 5 Select SNMP version.
- 6 Click "Add SNMP trap" again to send another SNMP trap.

9.4.6 Output Action

- 1 Select the output to be activated and click "Add".

The outputs are configured on the *I/O Setup* page, see [6 I/O Setup](#) on page 19. The state is set to the opposite of the inactive state when activated. For example, if output 2 is set to low in inactive state, the output will automatically be set to high when activated.

- 2 Set the duration in seconds. The output can be manually reset from the I/O setup page.

Activate Output

Output	Duration (s)
Internal Output 1	

Internal Output 1

Error Relay

Indicates Fault	Duration (s)
<input type="checkbox"/> Yes	

BusLogger

Store logs
<input type="checkbox"/> Yes

022

Figure 47. Activation of outputs.

9.4.7 Error Relay Action

- 1 Mark the check-box *Indicates Fault* if the error relay should indicate faults.
- 2 Set the duration in seconds. This field is mandatory when the check-box is marked. The error relay will be released when activated. The error relay can be manually reset from the Active Faults page.

9.4.8 BusLogger Action

The BusLogger is used for error tracking in System 900 and Unite systems. An action in the Fault Handler can trigger the BusLogger to save current log information to disk, to prevent it from being overwritten.

Mark the check-box to make the BusLogger tool save current log information when the trigger is matched.

9.5 Summary Faults Actions

In the *Summary Fault Actions* page, it is possible to set actions to start when the first persistent fault occurs and/or when there are no remaining persistent faults. The actions that can be set are:

- Activating error relay and outputs set up on the I/O Setup page for the defined time or as long as there are persistent faults.
- Sending messages when the first fault occurs and when no faults remain.
- Sending SNMP traps when the first fault occurs and when no faults remain.
- Sending E-mail when the first fault occurs and when no faults remain.

9.5.1 Activating Error Relay/Outputs

Summary Fault Status indicated by

Indicates Fault	Duration (s)
<input checked="" type="checkbox"/> Yes	60

Output	Duration (s)
Internal 1	

Internal 2

Figure 48. Summary fault actions.

Error Relay

- 1 To activate the error relay, mark the check-box for *Indicates Fault*.
The error relay will be released when activated.
- 2 Set the duration in seconds. If duration is not set, the error relay will be released until no persistent faults remain.
- 3 Click "Save" at the bottom of the page.

The error relay can manually be reset from the *Active Faults* page.

Outputs

- 1 Select an output and click "Add".
- 2 Set the duration in seconds. If the duration is not set, the output is active until no persistent faults remain.
- 3 Click "Save" at the bottom of the page.

The outputs can manually be reset from the " I/O Setup" page. See also [6 I/O Setup](#) on page 19.

9.5.2 Sending Messages

First Persistent Fault

Action on First Persistent Fault

Call ID	Message Text	Beep Code	Priority
9371	Very bad	3 - Normal	High

Add Message

Add E-mail

Add SNMP trap

Figure 49. Action on First Persistent Fault.

- Click "Add Message" in the *Action on First Persistent Faults* section to send a message for the first persistent fault. See also [9.4.3 Message Action](#) on page 43.
- Click "Add E-mail" if an e-mail notification should be sent. See also [9.4.4 E-mail Action](#) on page 43.
- Click "Add SNMP trap" to send a SNMP trap. See also [9.4.5 SNMP Trap Action](#) on page 44.

No Remaining Faults

Action on No Remaining Persistent Faults

Call ID	Message Text	Beep Code	Priority
9371	Very good	3 - Normal	High

Add Message

Add E-mail

Add SNMP trap

Save Cancel

Figure 50. Action on No Remaining Faults.

- Click "Add Message" in the *Action on No Remaining Persistent Faults* section to send a message when all persistent faults are resolved. See also [9.4.3 Message Action](#) on page 43.
- Click "Add E-mail" if an e-mail notification should be sent. See also [9.4.4 E-mail Action](#) on page 43.
- Click "Add SNMP trap" to send a SNMP trap. See also [9.4.5 SNMP Trap Action](#) on page 44.

9.6 Admin Log

In the Admin Log page, it is possible to export the log file to CSV (Comma Separated Values) file format, and to clear the status log file from non-active faults. A timeout can be set to block repeated Status Logs i.e. the fault will be discarded and no actions will be executed.

Export

- 1 Click "Export".
- 2 Click "Save" in the dialogue window and enter the file name (default name statuslog.csv) and the file path.

Clear Status Log

- 1 Click "Clear".
- 2 Click "Yes" in the dialogue window to remove all non-active faults from the status log file.

9.6.1 Timeout

- 1 Enter the timeout in minutes (0-1000 minutes), the default value is 10 minutes. If no Status Logs should be blocked, set the timeout to 0.
- 2 Click "Set timeout" to save the setting.

10 Message Routing

The *Message Routing* function is divided into two main parts:

- Number Plan (UNS)
- Message Router

Number Plan (UNS)

The number plan translates Call IDs to Unite destination addresses. Every Call ID corresponds to a Number/Address (for example a pocket unit call number or an e-mail address) to which a message is sent. In the Number Plan, all Call IDs must be defined. A Call ID can either be numerical or a text string.

The following list gives an example of a number planning table (the destination address format is written as Number/Address → Category where category stands for an IP address with a service, for example Number/Address → 172.23.9.151/DECT).

Call ID	Destination Address
7123	9123 → DECT phone
8123	9123 → Pager
Lars	9401 → DECT phone

Message Router

The Message Router is used to route messages to destinations, depending on the diversion conditions that have been set up. Messages can be diverted to other users or systems, if the receiving unit is out of range or absent.

The Message Router can divert the messages directly to a user, or use the Number Plan for looking up the destination addresses. The Message Router can divert a message to up to 10 individual destinations depending on licence.

10.1 Message Routing Functions

The *Message Routing* function consists of:

- View/Edit Call ID
search, view, edit and set up diversion conditions for individual Call IDs and Call ID Ranges
- Add IDs
add individual Call IDs to the number plan
- Add Multiple IDs
individual Call IDs are created for each defined number in a given range
- Delete Multiple IDs
individual Call IDs, in a given range, are deleted from the number plan
- Call ID Ranges
add Call ID ranges that correspond to a range of destinations and set up diversion conditions for the ranges
- Work Shifts
set up work shifts for the system
- Search Diversions
search, view and edit diversion conditions
- Category Setup
set up of system categories
- Import/Export
import and export of the Number Plan database

To set up a diversion, the following work flow is recommended:

- 1 Set up categories
- 2 Add Call IDs
- 3 Set up diversions

10.1.1 Symbols Used in the Message Routing Function











Symbol	Description
	Diversion exists
	Primary destination
	Secondary destination
	Destination enabled
	Add a condition
	Edit a condition
	Delete a condition/destination
	Absent diversion
	Not reachable diversion
	Out of range diversion

Figure 51. Symbols used in Message Routing

Edit or Delete a category

- To edit a category click "Edit" and enter new data. Click "Save".

Category Setup

Category Description	IP Address	Service	Service Extension	Properties
IMS Phonebook	1.1.1.1	Phonebook		<input type="button" value="Edit"/> <input type="button" value="X"/>
DECT Gbg	172.02.02.04	DECT		<input type="button" value="Edit"/> <input type="button" value="X"/>
<input type="text" value="System 900"/>	<input type="text" value="172.20.13.250"/>	<input type="text" value="S900"/>	<input type="text" value="category=A"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="button" value="Save"/> <input type="button" value="Cancel"/>
				<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="button" value="Save"/> <input type="button" value="Cancel"/>
— Fetch information from System Overview <input type="button" value="v"/>				

027

Figure 53. Category setup page in edit mode.

- To delete a category, click the "Delete" symbol.

10.2.2 Default Category

In the *Category Setup* page, it is possible to choose one category to be the default category. The default category is used when the number plan receives a request with no match for Call ID. The response from the Number Plan will then be "Call ID" → default category.

- To add a default category click "Change Default".

Default Category

If there is no match in the number plan database, the default category will be used when the response is sent, for example if the request is for the Call ID "1000" and there is no match, the response will be 1000@default.

Category Description	IP Address	Service	Service Extension
DECT GBG	172.20.9.146	DECT	<input type="button" value="Change Default"/> <input type="button" value="X"/>

028

Figure 54. Default category

- Select the category from the drop-down list and click "Save".

10.2.3 Predefined Categories

A category for the IMS Phonebook is predefined in the ESS. If the system does not include an IMS, the category can be deleted.

A special IP address (1.1.1.1) is used for the phonebook category. When the ESS gets a number plan look-up request for a Call ID with this category, the ESS will respond with the requesting modules IP address.

Example:

An IMS with IP address 172.30.5.123 sends a Call ID request to the ESS. In the ESS number plan the Call ID corresponds to the category "IMS Phonebook". The category is defined as "1.1.1.1/Phonebook". The ESS will send the number plan look-up response "172.30.5.123/Phonebook" to the IMS.

If several systems use the same phonebook, for example a DECT and a VoWiFi system, the special address should be changed to the IP address of the phonebook service, typically one of the IMS's or the global phonebook. The result is that all phonebook requests will be sent to the specified address instead of the IMS sending the number plan look-up request.

10.3 Call IDs

The number plan is set up with help of the following information:

- Call ID: Numerical or a text string.
Description: Description of the Call ID.
Number/Address: The Number/Address in the carrier system, for example a phone number in a DECT category or an e-mail address in a MailGate category.
Category: Defined in *Category Setup*.

10.3.1 Add a Call ID

- 1 Click "Add IDs" in the left menu.
- 2 Enter data in the fields and click "Save".

Add Call IDs to Number Plan

Call ID	Description	Number/Address	→ Category
9525	Evas Dect phone	9524	→ DECT GBG

Empty Copy previous Increment previous

029

Figure 55. Call ID added to the number plan.

- 3 Click "Add row" for each additional Call ID. Select either:
 - Empty (default)
 - Copy previous
 - Increment previous, increases the Call ID and Number/Address with 1 for each added row, all other fields remain. Only works for numerical Call IDs and Numbers.
- 4 Enter data and click "Save".

10.3.2 Call ID Ranges

Adding a range of Call IDs to the number plan is done in the *Call ID Ranges* page. A range has to be numerical and two ranges cannot overlap. Individual IDs always override an ID in a range.

The ranges are defined with help of the following fields:

- First Call ID: The first Call ID in the range, must be numerical.
Last Call ID: The last Call ID in the range, must be numerical.
Description: Description of the range.
First Number: The number corresponding to the first Call ID, must be numerical.
Category: Defined in *Category Setup*.

Add Call ID Ranges

- 1 Click "Call ID Ranges" in the left menu.
- 2 Enter data in the fields and click "Save".

Call ID Ranges

Note that individual Call IDs always override IDs in the ranges

First Call ID	Last Call ID	Description	First Number	→	Category		
300	399	Dect Main Office	300	→	Dect Main Office	Edit	Diversion
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	→	- select category	Save	Cancel

030

Figure 56. Adding a Call ID range.

Edit or Delete Call ID Ranges

- To edit a Call ID Range, click "Edit" and enter new data. Click "Save".
- To delete a Call ID Range, click the "Delete" symbol.

It is possible to set diversion conditions on the range by clicking the "Diversion" button. For more information about setting up diversions, see [10.6.3 Adding Range Diversions](#) on page 61.

To set up diversion to an individual Call ID in a range, the Call ID must first be set up as an individual Call ID. See [10.6 Diversions](#) on page 58.

10.3.3 Search, View and Edit Call IDs

- Click "View/Edit IDs" in the left menu.

Search, View and Edit IDs

Call ID	Number/Address	Category	Call IDs/page	
<input type="text"/>	<input type="text"/>	→ All	4	<input type="button" value="Search"/>

Search result

Search results 1-4 (32)

[1..4](#) [5..8](#) [9..12](#) [13..16](#) [17..20](#) [21..24](#) [25..28](#) [29..32](#) [Next](#)

Call ID Ranges

Call ID Range	Description	Number/Address Range →	Category
No match			
<input type="button" value="Add Range"/>			

Individual Call IDs

Call ID	Description	Number/Address →	Category	
111		111 → 900-116		<input type="button" value="Edit"/> <input type="button" value="Diversion"/> <input type="checkbox"/>
112		112 → 900-116		<input type="button" value="Edit"/> <input type="button" value="Diversion"/> <input type="checkbox"/>
113		113 → 900-116		<input type="button" value="Edit"/> <input type="button" value="Diversion"/> <input type="checkbox"/>
5533 > System 900 Interface	helens pager	5533 → System 900 Interface		<input type="button" value="Edit User"/>
<input type="button" value="Add Call ID"/>				

031

Figure 57. Search result of 4 Call IDs.

The first 50 Call IDs in the number plan are displayed by default, but the amount of displayed Call IDs can be changed at *Call IDs/page*.

Call ID ranges are always displayed before the individual Call IDs. Click the "Next" link to get the following Call IDs.

The "Diversion" button enables diversion setup, see [10.6 Diversions](#) on page 58. If a Call ID already has a diversion setup, this is shown by the Diversion exists symbol.

Call IDs connected to Users are displayed in the list but cannot be edited on this page, instead click "Edit User" to open the User Setup page. See [14.3 User Administration](#) on page 91.

Search for a Call ID

- Enter any of the fields *Call ID*, *Number/Address* or *Category*. Click "Search". As wildcard, use "*" or "%". Enter the number of Call IDs to show per page. The result is shown on the same page.

Edit Call ID

It is possible to edit a user by clicking "Edit User".

- To edit any Call ID, click "Edit" and enter new data. Click "Save".

Predefined Call IDs

A Call ID for the IMS phonebook is predefined in the ESS. The Call ID corresponds to the default address of the phonebook, "999999". If the address of the phonebook should be altered, the Call ID has to be updated.

Note: For phonebook Call IDs the Number/Address has to be undefined.

10.4 Add Multiple IDs

Multiple Call IDs can be added as individual Call IDs to the number plan. If any of the Call IDs already exist, a fault message will appear with a list of failing Call IDs.

- 1 Click "Add Multiple IDs" in the left menu.

Add multiple Call IDs to Number Plan

Individual Call IDs will be created for each number defined below. Maximum 1000 Call IDs can be added.

First Call ID	Last Call ID	Description	First Number	→ Category
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	→ Dect Factory ▼

100

Figure 58. Add multiple ID page.

- 2 Enter data in the fields and select category. Up to 1000 Call IDs can be added at the same time.
- 3 Click "Save".

10.5 Delete Multiple IDs

- 1 Click "Delete Multiple IDs" in the left menu.

Remove multiple Call IDs from Number Plan

Individual Call IDs in range specified below will be deleted from the Number Plan. Maximum 1000 Call IDs can be removed.

First Call ID	Last Call ID
<input type="text"/>	<input type="text"/>

101

Figure 59. Delete multiple ID page.

- 2 Enter data in the fields. Up to 1000 Call IDs can be removed at the same time.
- 3 Click "Delete".

10.6 Diversions

The Message Router can divert the messages with direct addressing or using the Number Plan for address look up. When direct addressing is used, the call address in the diversion condition does not have to be defined in the Number Plan. The category must however always be defined in the Number Plan.

The diversion is defined by a diversion condition and a destination on diversion.

- Condition: Three conditions are available:
- Absent, the pocket unit is reported absent
 - Out of range, the unit (phone, pager) is out of range
 - Not reachable, covers all message delivery failures, absent and out of range included.
- Work Shift: In addition to set up work shift, the following alternatives can be selected:
- Always, the message will be sent regardless of active Work Shift.
 - Between shift, to prevent messages from being undelivered if no Work Shift is active.
- Device: - Select a Call ID, only applicable if setting up diversions for a user.
- Manual, manually enter a Call ID and interface.
- Number/Address: A Call ID in the number plan or a number/address
- Category: Must be defined in the *Category Setup*.
If the Number Plan is used for address look up, the category "Number plan" is used. If the message is diverted with direct addressing, the selected category is used.

10.6.1 Individual Diversion Set Up

To set up an individual diversion, go to the *View/Edit IDs* page. Diversions can also be set up from the user setup page.

- 1 Locate the Call ID to be diverted, for example by searching as described in [Search for a Call ID](#) on page 56.
- 2 Click "Diversion".

The *Setup Diversion* page for the call number is opened and the primary destination is automatically created. The message will always be sent to this number.

It is not possible to edit the primary destination.

[Go back](#)

Setup diversion for 111

Database utilization: 0.0%.



032

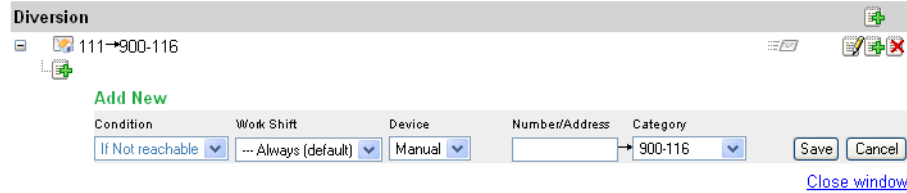
Figure 60. Setup diversion.

- 3 Click the "Add" symbol after the primary destination to add the first conditional diversion.

[Go back](#)

Setup diversion for 111

Database utilization: 0.0%.



033

Figure 61. Add new diversion.

Enter diversion condition and the destination on diversion.

For Call IDs belonging to an user, additional devices can be selected in the "Device" drop-down list. By selecting "Manual", any Call ID in the number plan can be used for diversion.

- 4 Enter data in the fields and click "Save".

10.6.2 Diversion Chains

It is possible to add up to 10 diversions in a diversion chain. For every new diversion click the "Add" symbol after the diversion condition. For example, to add a diversion to the *Not Reachable* condition in the figure below, click the "Add" symbol in the grey field after the destination address (in the example below, 1234 → Number plan).

Setup diversion for 5678

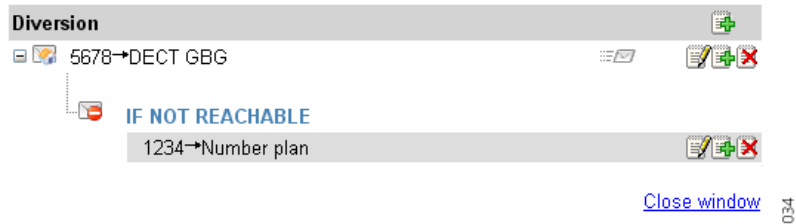


Figure 62. Diversion chains set up.

To add a diversion on the same level as the *Not Reachable* condition, click the "Add" symbol after the primary destination (5678 → Dect GBG).

To add an unconditional diversion, click the top "Add" symbol. A secondary destination is created, meaning that all messages are directed to the primary and to the secondary destination. The secondary destination can also have conditional diversions.

It is also possible to set up diversions that depend on work shifts.

After adding the destinations and conditions, the diversion chain could look like this:

Setup diversion for 5678

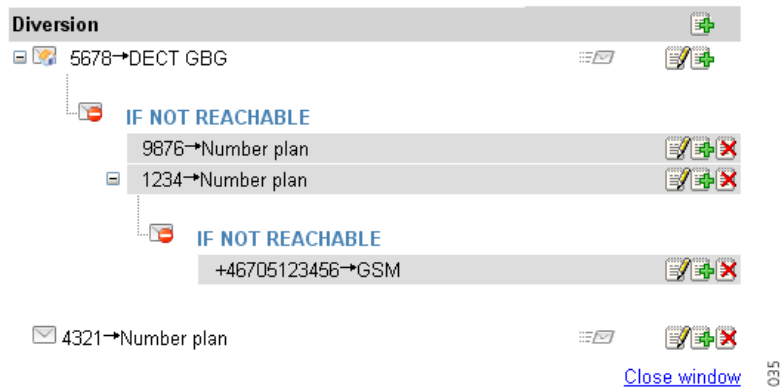


Figure 63. Example of a diversions chain.

It is possible to collapse and expand the diversions by clicking the plus and minus symbols in the view.

The diversions can be edited by clicking the "Edit" symbol and deleted by clicking the "Delete" symbol.

When there is at least one secondary destination, it is possible to temporarily disable top level destination by clicking the "Edit" symbol and then marking the "Disable" radio button. At least one destination must always be enabled.

10.6.3 Adding Range Diversions

To add a range diversion, use the same procedure as for adding individual diversions.

- 1 To set up a range diversion, go to the *View/Edit IDs* page.
- 2 The ranges are shown in the list. Click "Diversion".
The *Setup Diversion* page for ranges is shown. The primary destination is not editable.
- 3 Click the "Add" symbol to enter a diversion condition. Click "Save".

Setup diversion for range 9301-9400

Note that individual Call IDs always override IDs in the ranges

Database utilization: 0.1%.

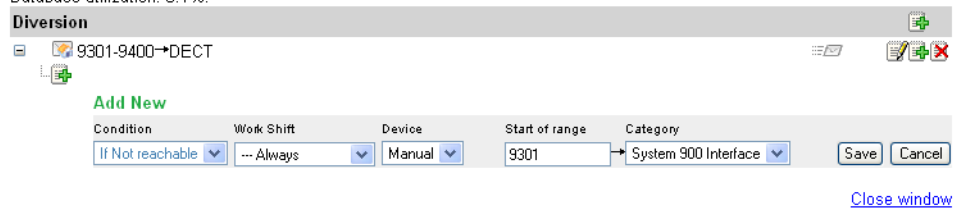


Figure 64. Set up diversion for a range.

It is possible to have up to 10 range diversions in a chain. It is also possible to add diversions on different levels in the chains in the same way as for individual diversions, see [10.6.2 Diversion Chains](#) on page 60.

10.6.4 Search Diversions

- 1 To search for a number/address that is included in different diversions, click "Search Diversion" in the left menu.
- 2 Enter a search criteria in any of the fields "Destination No./Address" or "Category" and click "Search". As a wild card, use "*" or "%".

The search result shows all entries where the search criteria is included. The diversion information can be expanded and collapsed by clicking the plus and minus symbols.

Search diversions

Search in which diversions a number/address is included.

Destination No./Address	Category	
<input type="text" value="5678"/>	<input type="text" value="All"/>	<input type="button" value="Search"/>

Search result

Call ID Destinations

5678	-	+	5678→DECT GBG	<input type="button" value="Edit"/>
			<ul style="list-style-type: none"> 9876→Number plan 1234→Number plan 4321→Number plan 	

1 entries matched your query. Results: 1

037

Figure 65. Diversion search result.

10.7 Import/Export

To import or export individual Call IDs and categories, go to "Import/Export" in the left menu. The data is exported as a CSV file. The main purpose with this function is to make it easier to add entries to the number plan. An exported file is to be edited and then imported into the ESS again. It is not recommended to import an old CSV file if Call IDs and categories have been changed in the ESS in the meantime (it could cause strange behaviour in the ESS).

Note: It is not possible to add new categories in the imported CSV file, new categories can only be added in the ESS GUI.

Export

- 1 Click "Export". In the dialogue window, click "Save".
- 2 Enter file name and file path and click "Save".

Import

Click "Browse" to locate the CSV file, then click "Import". The information in the database will be exchanged with the contents of the imported file if updates have been made. The import result, for example entries that have been added, is displayed. The import result is available in English only and cannot be translated.

To import a complete CSV file can take some time, to minimize the time for example import only the new or changed Call IDs. It is not possible to import ranges or default category.

11 Work Shifts

Messages can be diverted to different Call IDs depending on active work shift. The work shifts are set up with day of week and time. The work shifts can also overlap, i.e. different work shifts can be used for different users. It is also possible to set the work shifts to be continuously On or Off, which makes it possible to test the system independent of time and day. It is also a way to solve temporary changes to shifts due to for example holidays.

- 1 Click "Work Shifts" in the left menu of the *Message Routing* tab to open the page.

Work Shifts

Name	Days	Time	Mode	
weekdays 1	Mon,Tue,Wed,Thu,Fri	06.00-15.00	Time	 
<input type="button" value="Add"/>				

072

Figure 66. Work shift page.

- 2 Click "Add" to set up a new work shift.

- Shift Name: The name of the work shift.
- Mode: Predefined values;
Time,
On – Enabled, regardless of time
Off – Disabled
- Days: Check-boxes to select which days the work shift is active.
- Start Time: When the shift shall start, for example 08.00.
- Stop Time: When the shift shall end, for example 00.00.

Work Shift Setup

Work Shift Name

Mode

Days
 Monday Tuesday Wednesday Thursday Friday
 Saturday Sunday

Start Time **Stop Time**

073

Figure 67. Work shift setup page.

- 3 Enter the name of the work shift.
- 4 Select shift mode.

- 5 Mark the check-boxes to select days.
- 6 Enter start time for the shift.
- 7 Enter end time for the shift.
- 8 Click "Save".

12 Group Handling

In Group Handling, groups for the complete system are gathered and administrated in one place. The overview page gives a list of all group numbers that exist in the system.

12.1 Group Handling Functions

The *Group Handling* functions consist of:

- Add/Edit Broadcast Group IDs
set group Call ID and select which categories to include
- Add/Edit Multicast Group IDs
set group Call ID, which categories that are included in the group and add group members
- Add/Edit Group IDs
set group Call ID, add members to the group and configure whether diversion is allowed for included members or not.

To be able to add Broadcast/Multicast Groups IDs there must be categories that support the corresponding function. If no such category exist, then the feature will be disabled.

12.1.1 Symbols Used in the Group Handling










Symbol	Description
	Group ID
	Broadcast ID
	Multicast group ID
	Handset added but not yet programmed
	Unsuccessful programming
	Handset removed from group but not yet programmed
	Unprogrammed members
	Activation of one/several members failed
	Activation of group failed - carrier interface problem

Figure 68. Symbols used in Group Handling.

12.2 Create a Multicast Group ID

Groups

Create new:

Existing groups

Number of small groups: 1 (500), Number of large groups: 0 (50)

Type	Call ID	Description	
	5050	Group A	<input type="button" value="View/Edit"/>

Figure 69. Create Groups.

- 1 Click "Multicast Group ID".

- Call ID: Numerical or a text string.
- Description: Description of the Call ID.
- Group Number: The telephone number that is defined in the number plan for the radio exchange, max. 6 characters.
- Category: Defined in *Message Routing, Category Setup*.

Create Multicast ID

Call ID	Description
<input type="text" value="9099"/>	<input type="text"/>
Group Number	
<input type="text" value="5050"/>	

Included Categories

Security Group

Member Administration

Call ID
<input type="text" value="9099"/>
<input type="button" value="Add row"/>

Figure 70. Create a Multicast Group ID.

- 2 Enter data in the fields, *Call ID*, *Description* and *Group Number*.
- 3 Select category/categories.
- 4 Add Call ID members, i.e. the handsets that shall belong to the group. Members can be added manually, or by using the Call ID search function.

12.2.1 Call ID Search

- Click, "Call ID Search...".

Call ID: Numerical or a text string.
Number/Address: The Number/Address in the carrier system, for example a phone number in a DECT category or an e- mail address in a MailGate category.
Category: Must be defined in *Message Routing, Category Setup*.

Call ID Number/Address Category

 All Search

053

Figure 71. Call ID search.

- Enter the fields and choose *Category*.
The fields can also remain empty and only categories can be selected. Then all Call IDs in that Category will be shown.
 - Click "Search".
The search dialogue is replaced with the search result. In the search result page, click "Add" to include the corresponding Call ID in the group.
- 5 Click, "Save and Activate".
The included Call IDs have to exist as individual Call IDs in the Number Plan. If they does not exist in the Number Plan, an error message is displayed when the group is saved. The missing Call IDs can easily be added from the error message pop-up.

12.3 Create a Broadcast ID

Groups

Create new:

Existing groups

Number of small groups: 1 (500), Number of large groups: 0 (50)

Type	Call ID	Description	
	5050	Group A	<input type="button" value="View/Edit"/>

051

Figure 72. Create Broadcast IDs.

- 1 Click "Broadcast ID"

Call ID: Numerical or a text string.
Description: Description of the Call ID.

Create Broadcast ID Y

Call ID	Description
<input type="text" value="5050"/>	<input type="text"/>

Included Categories

All Pocket Units within selected category are included in the group.

Security Group

054

Figure 73. Create a Broadcast ID.

- 2 Enter the fields *Call ID* and *Description*.
- 3 Select *Included Categories*.
- 4 Click "Save".

12.4 Create a Group ID

Groups

Create new:

Existing groups

Number of small groups: 1 (500), Number of large groups: 0 (50)

Type	Call ID	Description	
	5050	Group A	<input type="button" value="View/Edit"/>

051

Figure 74. Create Group ID.

- 1 Click "Group ID".

Call ID:	Numerical or a text string, case insensitive.
Description:	Description of the Call ID.
Diversion permitted for included members:	Yes - Group message will be delivered as any other messages. No - no diversion will be made for group messages.

Create Group ID

Note that it will take some time to send a message to a large group as one message per Call ID will be transmitted. Multicast groups are available in this system, and it can be a good solution for large groups. [More information](#)

Call ID	Description
5050	Group A

Diversion permitted for included members
 Yes No

Member Administration

Call ID	
9099	
9098	
9097	

Empty Copy previous Increment previous

055

Figure 75. Create Group IDs.

- 2 Enter data in the fields *Call ID* and *Description*.
- 3 Select "Yes" or "No", if diversions should be permitted for included members.
- 4 Add Call ID members, i.e. the handsets that shall belong to the group. Members can be added manually, or by using the Call ID search function. See [12.2.1 Call ID Search](#) on page 68.
- 5 Click "Save".
The Call IDs should exist in the number plan, if not, a dialogue window opens where you can either add the Call IDs to the number plan or just save the group, it will then use the Call ID within a range or the default Category.

12.5 View and Edit Groups

Existing groups

Number of small groups: 2 (500), Number of large groups: 0 (50)

Type	Call ID	Description	
	GbgStaff	All personnel ATAB Gbg	<input type="button" value="View/Edit"/>
	Integration	Integration Section	<input type="button" value="View/Edit"/>
	SysDesign	System Design Section	<input type="button" value="Activate"/> <input type="button" value="View/Edit"/>

056

Figure 76. View and edit existing groups.

12.5.1 View and Edit Multicast Group ID

- 1 Click "View/Edit", see figure 76.

Edit Multicast Group ←

Call ID: 7078 Description:

Group Number: 3033

Included Categories

SMS Dect
 Security Group

Member Administration

Call ID	
9086	×
9087	×

Add row

Call ID Search... Save and activate Save Cancel

057

Figure 77. Administration page, Multicast group ID.

- 2 Edit the group..
- 3 Click "Save and activate".

12.5.2 View and Edit Broadcast ID

- 1 Click "View/Edit".

Edit Broadcast →

Call ID: 9899 Description:

Included Categories

All Pocket Units within selected category are included in the group.

P-Sök Mölndal
 Security Group

Save Cancel

058

Figure 78. Administration page, Broadcast ID.

- 2 Edit the group.
- 3 Click "Save".

12.5.3 View and Edit Group ID

Edit Group

Note that it will take some time to send a message to a large group as one message per Call ID will be transmitted. Multicast groups are available in this system, and it can be a good solution for large groups. [More information](#)

Call ID	Description
<input type="text" value="5050"/>	<input type="text" value="Group A"/>

Diversion permitted for included members
 Yes No

Member Administration

Call ID	
<input type="text" value="9099"/>	<input checked="" type="checkbox"/>
<input type="text" value="9098"/>	<input checked="" type="checkbox"/>
<input type="text" value="9097"/>	<input checked="" type="checkbox"/>

Empty Copy previous Increment previous

059

Figure 79. Administration page, Edit Group.

- 1 Click "View/Edit".
- 2 Edit the group.
- 3 Click "Save".

13 Activity Logging

To be able to use the activity log functions in the ESS, each module must be set up for logging. See [2.7.2 Sending Activity Log Messages to the ESS](#) on page 8.








To be able to view activities stored on the ESS, it is also necessary to install the Java Runtime Environment to run the Activity Log Viewer. To find this, go to www.java.com. For software version see [1.1.1 PC Requirements](#) on page 2.

The functions in the *Activity Log* are:



- Log View – to view and search for activities that are stored in the ESS.
- Filter Setup – to limit the number of stored activities.
- Printer Setup – to activate the printer function and to limit the number of printed activities.
- Log Export Setup – automatic and manual export.

13.1 Log View

13.1.1 Symbols used in the Activity Log Viewer

Symbol	Description
	Related Activities
	Search
	Cancel search
	Update view continuously
	Stop updating view
	Print search result
	Log out

13.1.2 Log information

Symbol	Description
	Error, did not reach destination.
	Extended log. These logs are for quick information and are not stored in the database.

13.1.3 View Activity Logs

Click the "Activity Log Viewer" button in the Activity Log tab. Enter User ID and Password,

and click "OK".

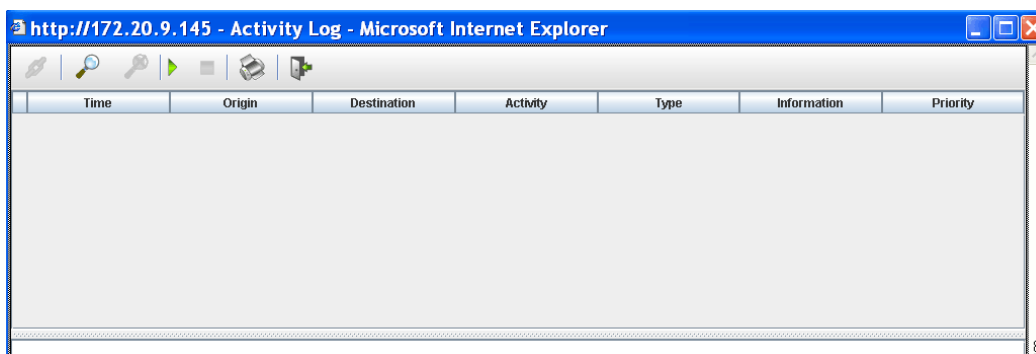


Figure 80. The activity log view.

It is possible to search for stored logs and view incoming activity logs continuously.

13.1.4 Search

From the Activity Log Viewer, it is possible to search for activities that are stored in the ESS by choosing; time period, priority level, kind of activity etc. For priority and activity it is possible to specify if searching for all priorities or activities, or searching for a specific priority or activity. Specific information in the activity can also be searched, for example a subject or body or a specific Call ID .

- 1 Click the search symbol.

Date:	The date interval when the activities where logged. Default is the current date as both start and stop.
Time:	The time interval when the activities where logged. Default Start time: 00:00:00 Default Stop time: 23:59:59
Number of lines:	A numerical value between 1 and 1000. The default value is 100.
Priority:	The message priority; Low, Normal, High and Alarm. A combination can be selected by using "Shift" or "Ctrl".
Information:	A specific text in the activity log, for example a subject or body. Supported characters: Latin-1
Activity:	The different activities, for example Message, Input Activity. A combination can be selected by using "Shift" or "Ctrl".
Origin:	A specific origin such as; Call ID, User, Number/Address, IP Address.
Destination:	A specific destination such as; Call ID, User, Number/Address or IP Address.

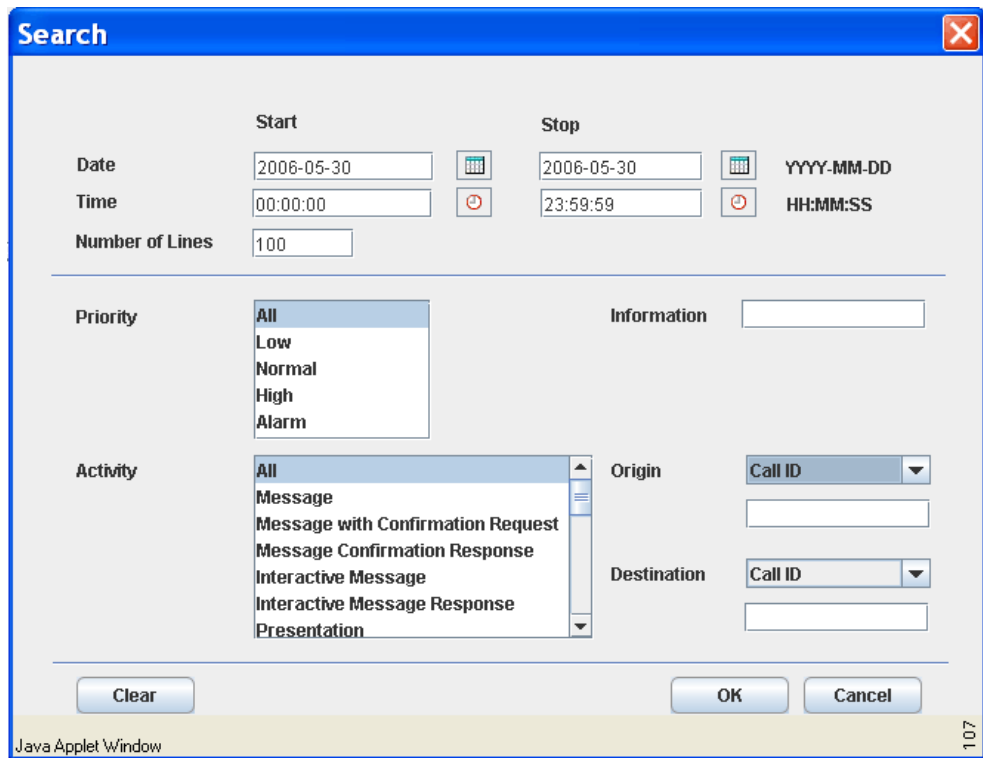


Figure 81. Search for activity logs.

- 2 Enter start date or click the "calendar" button to select the date. The time can be changed by clicking the "clock" button.
- 3 Change the number of lines if you want more or less than 100 activities to be displayed.
- 4 Select/specify the search criteria, *All* is set by default, but you can specify *Priority*, *Activity*, *Origin*, *Destination* and *Information*. When searching for specific *Origin*, *Destination* and/or *Information*; enter a number or a text in the corresponding text field.
- 5 Click "OK".

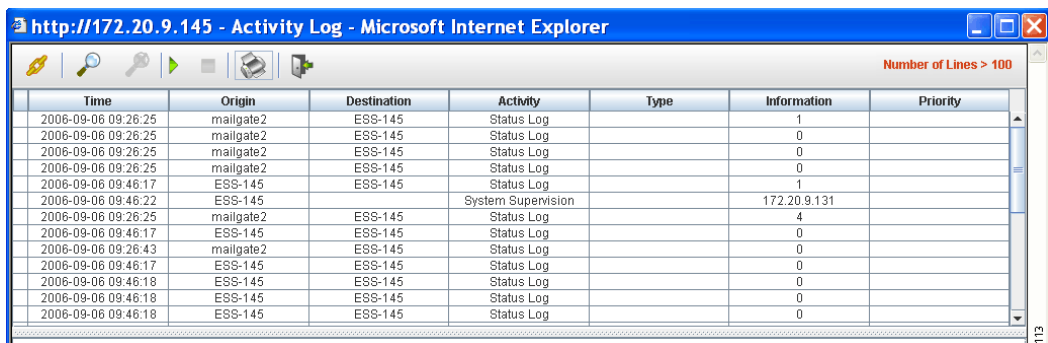


Figure 82. Search result of activity logs.

During the search, it is possible to interrupt the search operation by clicking the stop search symbol. An ongoing search is indicated with a symbol in the upper right corner. When the result of activities is displayed, the number of returned lines is displayed in the upper right corner. If more lines than displayed is available in the database, the

information will be replaced with Number of Lines > X in red colour, where X is the number of requested lines.

When marking a log, more information about the log will be found below the list, see [figure 83](#).

13.1.5 Print Search Result

The table with search result can be printed by clicking the printer icon, see [13.1.1 Symbols used in the Activity Log Viewer](#) on page 74. The details for a specific activity log can be printed by marking the log, right click and selecting Print Details from the displayed menu.

13.1.6 View Related Activities

To view related activities, for example all actions that have been taken as a result of an incoming alarm, click the activity log, and then click the related activity icon in the top menu. (It is also possible to double-click the actual activity to open the related activity view or to right click the activity log, and choose *Related Activities* from the displayed menu.)

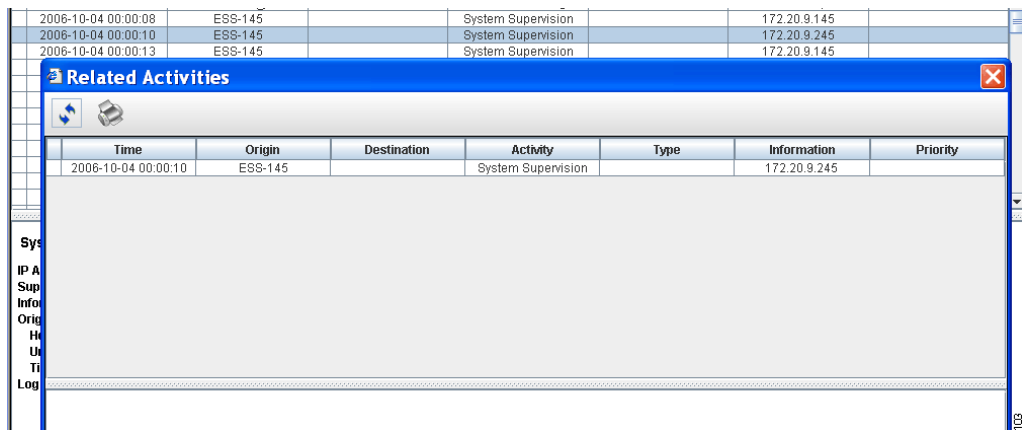


Figure 83. Related activity view.

13.1.7 Print Related Activities

The table with the related activities can be printed by clicking the printer icon, see [13.1.1 Symbols used in the Activity Log Viewer](#) on page 74. The details for a specific activity log can be printed by marking the log, right click and selecting Print Details from the displayed menu.

13.1.8 Continuous Log View

By clicking the "Update view continuously" icon, the activity logs will be displayed when received by the ESS. The logging can be stopped by clicking the "Stop updating view" icon. It is also possible to pause by marking the check-box *Lock scrolling*.

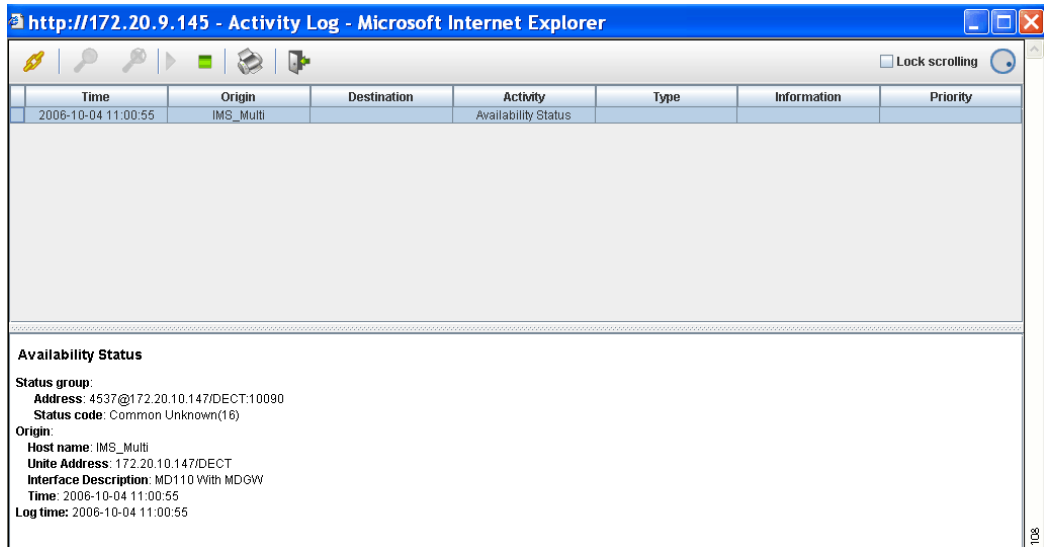


Figure 84. The information of the most recent activity logs are viewed.

The symbol located next to the check-box *Lock scrolling*, indicates that the continuous view is activated.

When the extended activity log is enabled for a module, the symbol for extended activity logs will show up in front of incoming intermediate logs. This log is only for quick information, a "real" activity log will appear shortly after. See also [14.1 Symbols](#) on page 89.

13.2 Filter Setup

Filter Settings

Messages

Message Priority
Store messages with specified priorities.

Low Normal High Alarm

180

Figure 85. The Filter Setting page, showing the basic filter setting.

The filter settings are divided into basic settings and advanced settings. With the basic settings, it is possible to store activities based on set priority. This concerns messages,

messages with confirmation, interactive messages and responses on messages, all other types of activities will be stored. In the advanced settings, it is possible to configure whether or not to store depending on receiver/sender, and type of activity.

13.2.1 Basic Filter Settings

All check-boxes for priority are marked as default, see [figure 85](#) on page 78, which means that all messages will be stored. The different priorities are:

- Low
- Normal
- High
- Alarm

Note: Alarm refers to the message priority *Alarm*.

Discard Messages with specified Priority

- 1 Unmark the check-boxes for message priorities that are not going to be stored.
- 2 Click "Save". See [figure 85](#).

13.2.2 Advanced Filter Settings

Click the "Advanced Filter Settings" to open the page.

It is possible to discard or to store activities sent from/to an IP address and a service. It is also possible to select specific activities to be discarded regardless of sender/receiver.

Discard (default):	All activity logs will be stored if nothing else is specified. If Discard is marked, and <i>IP Address/Service</i> is specified - all activities from/to the specified service or module will not be stored.
Store:	Only activities from/to listed services will be stored.
IP Address/Service:	On the format: xxx.xxx.xxx.xxx/service

Advanced Filter Settings

Activities sent from/to a service within a module can be discarded or stored in the log. If "Discard" is selected, all activities from/to the specified service and module will be lost. If "Store" is selected, only activities from/to listed services will be stored, i.e. activities from/to any other services will be lost.

Discard Store

IP Address/Service

✘

Select activities to include in the log. Discarded activities will be lost.

Store

Alarm	
Alarm Acknowledge	
Alarm System 900	
AvailabilityStatus	
Call Setup	

Discard

--

Discard administration events

063

Figure 86. Advanced filter setting page.

Store Activities for a Specific IP Address/Service

- 1 Mark "Store".
- 2 Enter the IP address and service.

Note: All activities sent from another address/service than specified will be lost.

- 3 Click "Save".

Discard all Activities from/to a Specific IP Address/Service

When *Discard* is selected together with a specified IP address and service, all activities from/to the specified service on the module will be filtered out and lost.

- 1 Mark "Discard".
- 2 Enter the IP address and service.
- 3 Click "Save".

Discarding Activities based on Type

It is possible to discard activities regardless of the sender/receiver. By default, the following activity types are discarded; Availability Status, Location Data, Presentation and Presentation Response.

- 1 Select activities from the *Store* box that should not be included in the log.
- 2 Move the activities into the *Discard* box with the arrow button, see [figure 86](#).
- 3 Click "Save".

13.3 Printer Setup

Log information can be printed to the locally connected printer. For information about how to install the printer, see [2.6 Printing Log Information](#) on page 6. There are two different printing modes, a standard printing mode and an extended printing mode. Depending on printing mode selection there is different data content sent to the printer handler application. See below for details.

Standard printing mode – One line of content

Date, Time, Origin, Destination (final), Status, Activity Type and Information.

Extended printing mode – Two lines of content

Line 1 contains:

Date, Time, Origin, Destination (first), Destination (final), Status, Activity Type, Priority.

Line 2 contains:

LogID, Message Reference and Information.

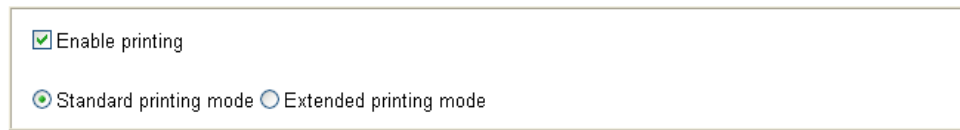
For both modes, the Origin and Destination contains either "User", "CallID", "Surveyed host name" or "Unite address".

Between each data there is one space character.

Depending on the printer configuration, a line that is longer than the paper width will appear truncated or with line wrap.

Note: Only activities that are stored in the ESS are printed.

Printer settings



The screenshot shows a rectangular box containing two lines of text. The first line is "Enable printing" with a checked checkbox to its left. The second line is "Standard printing mode" with a selected radio button to its left, followed by "Extended printing mode" with an unselected radio button to its left.

131

Figure 87. Enable printing for standard printing mode.

- 1 Mark the *Enable printing* box.
- 2 Select printing mode.
- 3 Click "Save".

13.3.1 Customized Printer Setup

There are different settings that can be made to prevent that all logs are printed:

- Print messages with specified priorities only
- Print activities from/to specified services (IP address/Service) only or do not print activities from/to specified services.
- Select which activities to print and discard the others
- Select not to print administration events

Printer settings

Enable printing

Basic mode Extended mode

Note that the settings on the "Filter Setup" page will affect this page as well. No logs that are discarded due to rules on that page will be printed

Print messages with specified priorities.

Low Normal High Alarm

Activities sent from/to a service within a module can be printed. If "Do Not Print" is selected, all activities from/to the specified service and module will not be printed. If "Print" is selected, only activities from/to listed services will be printed, i.e. activities from/to any other services will not be printed.
Warning! Selecting "Print" and not adding any services will result in no logs being printed.

Do Not Print Print

Add address

Select activities to be printed..

Print		Do Not Print
Alarm		Presentation
Alarm Acknowledge		Presentation Response
Alarm System 900		
Availability Status		
Call Setup		

Do not print administration events

Save Cancel

125

Figure 88. The Printer Setup page.

13.3.2 Print Messages with Specified Priority

- 1 Deselect check-boxes for message priority that shall not be printed. See [figure 88](#).
- 2 Click "Save"

13.3.3 Discard/Print Activities for a Specific IP Address/Service

- 1 Select *Do Not Print* or *Print*, see [figure 89](#) on page 83.
- 2 Click "Add address"

Activities sent from/to a service within a module can be printed. If "Do Not Print" is selected, all activities from/to the specified service and module will not be printed. If "Print" is selected, only activities from/to listed services will be printed, i.e. activities from/to any other services will not be printed.
Warning! Selecting "Print" and not adding any services will result in no logs being printed.

Do Not Print Print

IP Address/Service

100.10.20.250/DECT X

Add address

126

Figure 89. IP address and service added.

- 3 Enter the IP Address and Service.
- 4 Click "Save".

13.3.4 Print Activities based on Type

Select activities to be printed.

Print

- Alarm
- Alarm Acknowledge
- Alarm System 900
- Availability Status
- Call Setup

Do Not Print

- Presentation
- Presentation Response

Do not print administration events

Save Cancel

Figure 90. Activity and administrative events that shall not be printed.

- 1 Select the activity from the *Print* box that should not be printed.
- 2 Move the activities to the *Do Not Print* box by clicking the arrow pointing right. See [figure 90](#).
- 3 Click "Save".

13.3.5 Discard Administration Events

- 1 Mark the check-box *Do not print administration events* if those events are not to be printed. See [figure 90](#).
- 2 Click "Save".

13.4 Log Export Setup

The Log Export Setup page is used for export of stored activities, either manually or automatically in CSV or XML file format. Automatic export can be sent to an FTP server or attached to an e-mail. Manual export is used when a certain time period of the activity log should be exported. The automatic export is used when the activity log should be exported regularly, for example the same time every day. On this page, it is also possible to clear the Activity Log database.

To open the administrate activity log page click *Administrate Log* in the left menu.

Administrate Activity Log

Clear Activity Log

Manual Export

Export to File
Export activities within specified time

Start date and time
2006 June 01 00:00

End date and time
2006 June 01 14:13

File format
CSV

Export

Automatic export

Export type
No export

Max size of export file (in kB) **File name**
1024 LogExport.csv

Export to File
Add FTP entry

Export as E-mail
Add e-mail entry

Save Cancel 006

Figure 91. Administrate activity log page.

13.4.1 Manual Export

The manual export includes stored activities within specified time period.

Start date and time: For example, 2005, June, 04, 14.30

End date and time: For example, 2005, June, 05, 02.00

File format: Export in the format CSV or XML.
If the log file should be analysed with the Log Analyser, then XML format should be chosen. Otherwise the choice of format is dependent of the tool that should be used for analysing the data.

The screenshot shows a web-based form for manual export. It is titled "Manual Export" and has a sub-header "Export to File" with the instruction "Export activities within specified time". The form is organized into three main sections: "Start date and time", "End date and time", and "File format". Each section contains input fields for year, month, day, and time. The "Start date and time" fields are set to 2006, June, 01, and 00:00. The "End date and time" fields are set to 2006, June, 01, and 14:13. The "File format" is a dropdown menu currently set to "CSV". At the bottom of the form is an "Export" button. A small number "067" is visible in the bottom right corner of the form's border.

Figure 92. Example of manual export.

- 1 Enter the start date and time.
- 2 Enter the end date and time.
- 3 Select file format.
- 4 Click "Export".

A dialogue window will open where the activity log can be saved to the local file system.

13.4.2 Automatic Export

The automatic export can be done regularly or when the database is full. If the exported data exceeds maximum file size, the data will be divided into several files.

Export type: Predefined values to choose from, for example; No export, Database full only, Daily, Hourly etc.

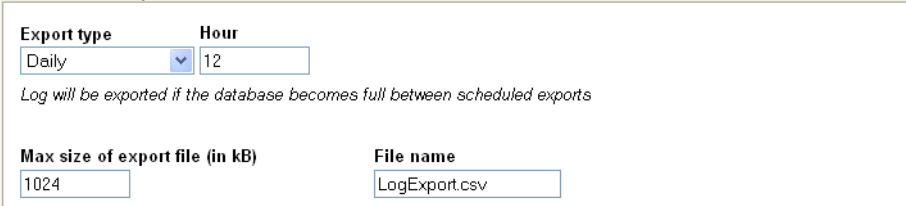
File size: 100 - 30 000 kB. Enter max. size in kB of exported file. If file becomes larger, exported data will be divided into multiple files or e-mails.

File name: File name to use when exporting the activity log.
A time-stamp and a counter is added after the file name for each new file that is exported.

- 1 Select the export type, it is by default set to *No export*. Depending on the chosen value, the page will look different.

- 2 Enter time data in the fields, if the chosen export type is time based.

Automatic export



The screenshot shows a configuration form for automatic exports. It has two columns: 'Export type' and 'Hour'. Under 'Export type', there is a dropdown menu with 'Daily' selected. Under 'Hour', there is a text input field with '12'. Below these fields is a note: 'Log will be exported if the database becomes full between scheduled exports'. At the bottom, there are two more fields: 'Max size of export file (in kB)' with a text input field containing '1024', and 'File name' with a text input field containing 'LogExport.csv'.

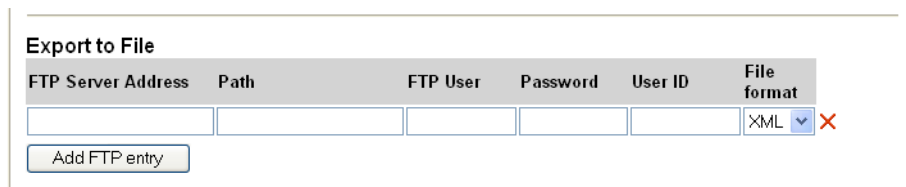
Figure 93. An example when the log will be exported daily at 12:00.

- 3 Enter the maximum file size in kB.
- 4 Enter the file name.

Export to File

- 1 Click "Add FTP entry".

- FTP Server Address: IP address for the FTP server.
- Path: The path to a directory on the FTP server where exported files should be placed.
- FTP User: User name to log in to the FTP server.
- Password: Password for entered user.
- User ID: User ID to use when exporting data. If a User ID is entered, only activities that the user has the right to view will be exported. Leave field empty to export all activities. See [14.2.3 Edit Log View Rights](#) on page 91 for more information.
- File format: Export in the format CSV or XML.
If the log file should be analysed with the Log Analyser, then XML format should be chosen. Otherwise the choice of format is dependent of the tool that should be used for analysing the data.



The screenshot shows the 'Export to File' configuration form. It has a table with six columns: 'FTP Server Address', 'Path', 'FTP User', 'Password', 'User ID', and 'File format'. Each column has a corresponding text input field. The 'File format' field has a dropdown menu with 'XML' selected. Below the table is a button labeled 'Add FTP entry'.

Figure 94. Add FTP entry is opened.

- 2 Enter data in the fields, see [figure 94](#).
- 3 Select file format.
- 4 Click "Save", see [figure 91](#) on page 85.

Export as E-mail

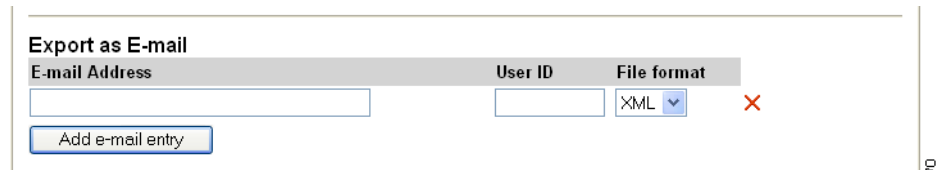
To be able to export via E-mail, the IP address/host name of the mail server must be set up in the System Setup, see [2.5 Sending E-mail](#) on page 5.

- 1 Click "Add E-mail entry".

E-mail Address: Destination address for the export.

User ID: User ID to use when exporting data. If a User ID is entered, only activities that the user has the right to view will be exported. Leave field empty to export all activities. See [14.2.3 Edit Log View Rights](#) on page 91 for more information.

File format: Export in the format CSV or XML.
If the log file should be analysed with the Log Analyser, then XML format should be chosen. Otherwise the choice of format is dependent of the tool that should be used for analysing the data.



The screenshot shows a web form titled "Export as E-mail". It contains three input fields: "E-mail Address", "User ID", and "File format". The "File format" field is a dropdown menu with "XML" selected. To the right of the dropdown is a red "X" icon. Below the fields is a button labeled "Add e-mail entry".



Figure 95. Add E-mail entry opened.

- 2 Enter data in the fields, see [figure 95](#).
- 3 Select file format.
- 4 Click "Save", see [figure 91](#) on page 85.

14 Users

This is where to administrate Users and User Teams. Users are used in the Unite system for individual log in and authorisation to for example Log View.

14.1 Symbols

Symbol	Description
	Show members
	Edit User/User Team








14.2 User Teams

Access rights within the system are given to User Teams. In the ESS, messaging rights and log view rights are set up to different User Teams. One user can belong to several User Teams. Click "User Teams" in the left menu to access the configuration page.

User Teams

Authorisation

Administration

User Teams	
default	
ward 1	  
ward 2	  

065

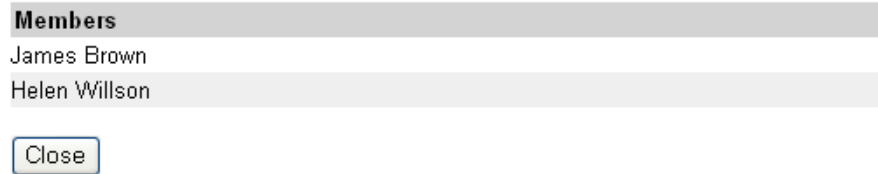
Figure 96. The Authorisation page for User Teams.

There is a *default* User Team that is used for logs without any connection to a user, for example a message that is sent to a portable device that does not belong to any user.

Show Members

It is possible to see which members that are assigned to a specific User Team by clicking the "Show members" symbol. User Team assignment is handled from the User Setup pages, see [14.3 User Administration](#) on page 91 for more information.

ward 2



095

Figure 97. Showing members in ward 2.

14.2.1 Add User Team

- 1 Click "Add new"

Add User Team

Name

Save Cancel

087

Figure 98. Naming the User Team.

- 2 Enter the name of the User Team. The name must be unique.
- 3 Click "Save".

14.2.2 Edit Messaging Rights

- 1 Click "Messaging".

Messaging

Mark the check-box in front of the User Team(s) that shall be changed. Select a User Team, and click Add/Remove to change the groups authorities.

Mark all Unmark all

User Team	Authorities
<input type="checkbox"/> ward 1	ward 1
<input checked="" type="checkbox"/> ward 2	ward 1

ward 1 Add Remove Close

086

Figure 99. The Messaging rights page.

In the Messaging rights page, it is possible to edit the authorities for the User Teams. These settings limit the number of addresses that are displayed in for example Netpage.

Add Messaging Rights

- 2 Mark one or more User Team check-boxes and select from the drop-down list which User Team they should be able to send message to.
- 3 Click "Add".
- 4 Click "Close" when finished.

Remove Messaging Rights

- 1 Mark one or more User Team check-boxes and select from the drop-down list which User Team that should be removed.
- 2 Click "Remove".
- 3 Click "Close" when finished.

14.2.3 Edit Log View Rights

Click "Log View".

Log View

Mark the check-box in front of the User Team(s) that shall be changed. Select a User Team, and click Add/Remove to change the groups authorities.

Mark all Unmark all

User Team	Authorities
<input type="checkbox"/> ward 1	default
<input type="checkbox"/> ward 2	ward 1

ward 2

080

Figure 100. Log View Rights page.

In the Log View rights page, it is possible to edit the authorities for the User Teams. These settings restricts which activity logs that will be shown to the user in the Activity Log Viewer, and can also be used to restrict which activities that are exported to a specified destination.

Adding or removing log view rights is done in the same way as in messaging rights, see [14.2.2 Edit Messaging Rights](#) on page 90.

14.3 User Administration

The User Administration page gives an overview of set up users. For each user, it is displayed which teams the user belongs to, and which Call IDs that are associated with the user. By default, ten users per page is displayed. When searching for users, the number can be changed.

Click "Administration" in the left menu.

User Administration

Users/Page: Last Name

Name	Member of User Teams	Call IDs	
James Brown	ward 1, ward 2	1	 

Search results 1-1 (1)

092

Figure 101. The User administration page with one user shown.

- When searching for users, these data can be entered:
 - Number of users to display per page
 - Last Name, First Name, Title or User ID

The wildcard "*" can be used by itself to search for all users (which is the same as leaving the field empty), or after a letter to search for all names that for example starts with A (A*).

- It is possible to edit an existing user by clicking the "Edit User" symbol.

14.3.1 Add Users

A device Call ID in the number plan can be connected to a user to make it possible to send messages to the user. Groups configured in *Group Handling*, can be added as users to make it possible to send messages to the groups from for example XGate. When several users should be added, the "Add Multiple Users" function can be used. The user is set up in the same way, but when saving the user the Add User page is displayed instead of the overview page. To facilitate adding users that are members of the same teams, the settings made for the previous user are copied.

- 1 Click "Add User" or "Add Multiple Users".

User ID: The User ID must be unique.

Password: No restriction of figures. The password is used for logging in to the Activity Log Viewer. It is also used in other applications like, for example, XGate and NetPage.

Confirm Password: The same as password.

User Setup

The screenshot shows the 'User Setup' page with the following fields and sections:

- First Name:** Helen
- Last Name:** Willson
- Title:** Technical Admin
- User ID:** HWi
- Password:** [masked]
- Confirm Password:** [masked]
- User Teams:** Select which User Teams this user should be a member of.
 - Available:** Doctors, Nurses Ward A, Nurses Ward B, Porters, Ward C
 - Member of:** Head nurses
- Call ID Table:**

Call ID	Description
helen	Helen Willson

Buttons: Save, Cancel

Figure 102. User Setup page, where membership and Call IDs can be added .

- 2 Enter data in the fields.
- 3 Select from the *Available* box which User Teams the user should be a member of, and move it to the *Member of* box, by clicking the arrow pointing right. See [figure 102](#). A User Team can also be removed from a user, by using the arrow button pointing left to move the selected User Team from *Member of* to *the Available* box.
- 4 Enter the user's Call ID. If the user already has an individual Call ID defined in the number plan, it can be used by entering the already existing Call ID. This makes it possible to move any set up diversions to the user in an easy way. See [figure 102](#).
- 5 Click "Save".

If the Call ID was not configured in the number plan, a pop-up where a device address can be added is displayed, see [figure 103](#). Either a new device can be added or an existing Call ID can be used. When a User Call ID has been added, at least one device or group must be added for the Call ID to function correctly. If a group should be connected to the user, click "Close" and follow the instructions in [Add Group Call ID](#) on page 95.

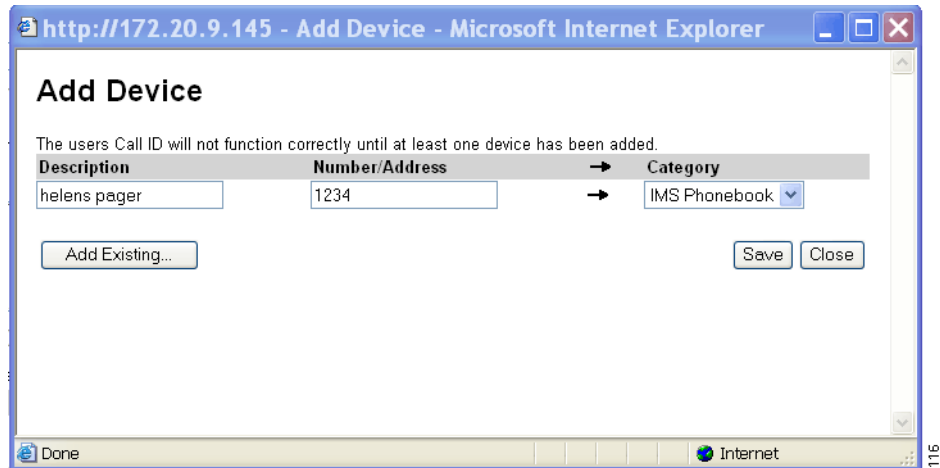


Figure 103. Add devices.

Add Device

- 1 Enter description for the device.
- 2 Enter the number or address for the device.
- 3 Select category for the device.
- 4 Click "Save".

It is also possible to use an existing device by clicking "Add Existing..".

- Enter data in the fields or leave it empty to get all Call IDs, and click "Search".

Search results 1-4 (4)

Call ID	Description	Number/Address →	Category	Is Diverted	User ID	
999999	IMS Phonebook		→ IMS Phonebook			Add
Carol	carols detc phone	9206	→ Dect Main Office		CMc	Info
5533 > System 900 Interface	helens pager	5533	→ System 900 Interface		Hwi	Info
steven	stevens Dect phone	9255	→ Dect Factory			Add

[Close](#)

Figure 104. Search result of individual Call IDs.

It is only individual Call IDs that will be shown. Call IDs in a range will not be included.

Call IDs with an "Info" button instead of an "Add" button means that the Call ID is already connected to a user or that the Call ID is diverted. The Call ID has to be removed from the other user or the diversions have to be removed before the device can be added to this user.

- Click "Add" for the Call ID that corresponds to the user's device.

Add Group Call ID

Groups must first be defined in the *Group Handling*, see [12 Group Handling](#) on page 65 before they can be added to a user.

- 1 Click "Add Group...". A window will open where to search for Call IDs.
- 2 Enter data in the fields or leave it empty to get all groups, and click "Search".
- 3 Click "Add" for the group Call ID that is going to be used.

The screenshot shows a 'User Setup' form with the following sections:

- Personal Information:**
 - First Name: Group
 - Last Name: fire brigade
 - Title: (empty)
- User ID and Password:**
 - User ID: Groupfd
 - Password: (empty)
 - Confirm Password: (empty)
- User Teams:**

Select which User Teams this user should be a member of

Available	Member of
Head nurses	ward 1
TestTeamA	
TestTeamB	
ward 2	
Ward A	

Navigation buttons: up, down, left, right arrows.
- User Call ID:**

The Call ID that is used when sending messages to the user

Call ID	Description	Actions
2001	Group fire brigade	Edit Diversion X
- Devices:**

Define any devices that the user has. The first Call ID is the users main device.

Call ID	Description	Actions
1000		X

Buttons: Add New..., Add Existing..., Add Group...

Figure 105. The User Setup has been defined and the Group device information have been added.

When a group has been added, it is no longer possible to add any more devices or groups for the user. However it is possible to add additional Call IDs, see [14.3.3 Additional User Call IDs](#) on page 97.

Set up Diversions

It is now possible to set up diversions for the user.

- 1 Click "Diversion". See figure 107.

Setup diversion for helen w



Figure 106. Setup diversion for the device Call ID.

- 2 Diversions are done in the same way as in the Message Routing configuration, see [10.6 Diversions](#) on page 58 on how it is done.

14.3.2 Add Additional Devices to Users

The user can have several devices, where the first one is the main device. It is possible to change which device that should be the main one.

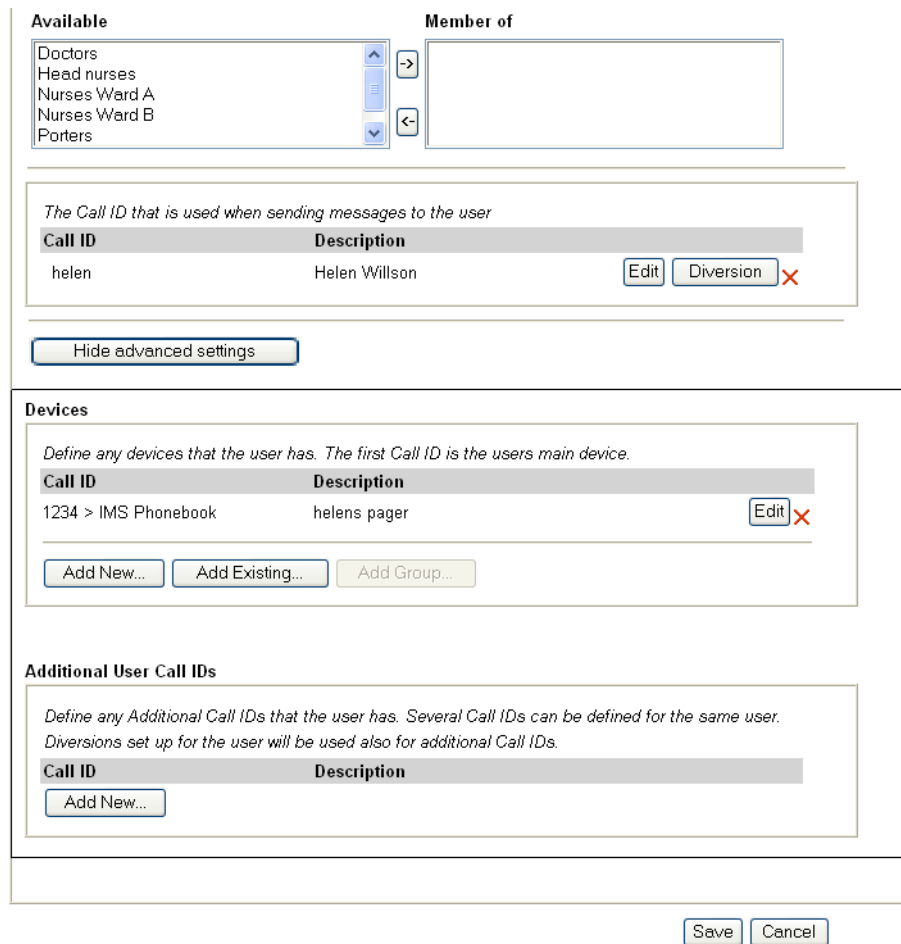


Figure 107. An added device.

To add more devices and additional user Call IDs, click Show Advanced Settings.

Add New Device

If the device Call ID is not defined in the number plan it can be added from the User Setup pages.

- 1 Click "Add New...". A page where a device Call ID can be added to the number plan will be opened. See [figure 103](#) on page 94 and also how it is done.
- 2 Click "Save".

When at least two devices are added, it will be possible to change which device that should be used as the main device by clicking "Use as main". The main device is placed first in the list.

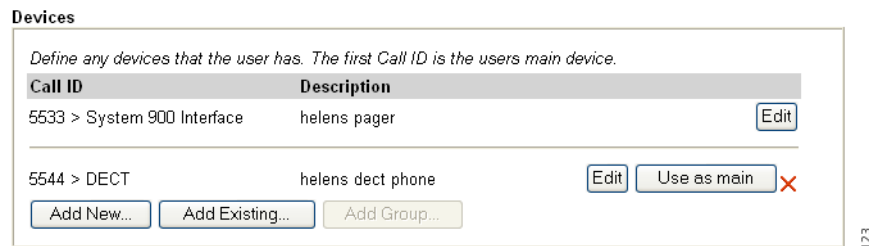


Figure 108. Two devices added.

Add Existing Device

If the device Call ID is already defined in the number plan, it is possible to add that device by clicking "Add Existing...". A window will open where to search for Call IDs, see [figure 104](#) on page 94.

14.3.3 Additional User Call IDs

A user can have several Call IDs. Independent of which user Call ID that is used, a message will always be sent to the main device.

- 1 Click "Add new".

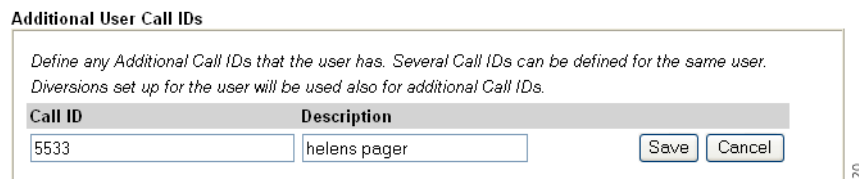


Figure 109. Add additional User Call ID.

- 2 Enter the data in the fields and then click "Save".

15 Clock Synchronisation

The time for modules in a system can be synchronized.

For configuration of clock synchronisation, see the *Installation Guide, ELISE2, TD 92232GB*.

16 Document History

For details in the latest version, see change bars in the document.

Version	Date	Description
F	12 May 2009	<ul style="list-style-type: none">• Document History chapter added.• Information added about Ascom Unite MIB in 9.4.5 SNMP Trap Action on page 44.• Minor changes and clarifications in following chapters: 8.3 Supervision of IP Equipment on page 27, 9.2 Active Faults on page 38 and 10.7 Import/Export on page 62
G	2 March 2010	Chapter 8.5.1 Management Information Base file on page 33 added.

17 Related Documents

Installation Guide, ELISE2	TD 92232GB
Installation and Operation Manual, Remote Management Client	TD 92256GB
Function Description, Activity Logging in Unite	TD 92341GB
Function Description, Remote Management	TD 92257GB
Function Description, System Supervision and Fault Handling in Unite	TD 92252GB
Function Description, Message Routing in Unit	TD 92254GB
System Description, Unite	TD 92243GB
Data Sheet, Enhanced System Services, ESS	TD 92250GB

Appendix A: ESS and IT Security

The following ports on the ESS are open:

Port	Application or unit	Transport protocol
22	SSH (Secure Shell)	TCP
25	Simple Mail Transfer Protocol (SMTP)	TCP
53	Domain Name Server (DNS)	UDP
80	Web traffic	TCP
113	Authentication	TCP
123	Network Time Protocol (NTP)	UDP
162	Simple Network Management Protocol (SNMP)	UDP
3217	Unite traffic	UDP
10101	Remote connection - TCP and RS232 conversion	TCP
10103	Remote connection - Communication between Remote Access Client and Remote Access Server	TCP
10130	Applet communication (Activity Log Viewer)	TCP

On the following ports, the ESS is open for File Transfer Protocol (FTP) traffic:

Port	Application or unit	Transport protocol
20	FTP (<i>outgoing traffic</i>)	TCP
21	FTP (<i>outgoing traffic</i>)	TCP
45100-45110	FTP (<i>incoming traffic</i>)	TCP

On the following ports, the ESS permits traffic to be forwarded to the requested IP address:

Port	Application or unit	Transport protocol
80	Web traffic	TCP
10101	Remote connections	TCP

Traffic is forwarded on ports opened for remote connection. See [3 Remote Connection](#) on page 10.

ICMP packets are forwarded.

Note: When "Activity Log" data is exported, either manually by using a web browser or automatically by e-mail or ftp, the information is not encrypted.