

arcutronix

@ccess the Ethernet

USER GUIDE

SCX2e
GS1



arcutronix GmbH
Deutschland

**Installation and
Operation Manual**

Version 1.6

SCX2e - System Controller

USER GUIDE



Covered Variants of SCX2e by this User Guide:

SCX2e	0903 - 3000 / GS1
SCX2e-WDM	0903 - 3010 / GS1

Covered Software Versions of SCX2e by this User Guide:

SW-Version (≥):	V 1_4_00
Boot-Loader (≥):	V 1_3

Part-Number (User-Guide):	0903 30 65
---------------------------	------------

Version:	V 1.6
----------	-------

Date of Issue:	2014-08-07
----------------	------------

Contacts

arcutronix GmbH
Garbsener Landstraße 10
D-30419 Hannover, Germany
Tel.: +49 (0)511 277- 2700
Fax: +49 (0)511 277- 2709
E-Mail: info@arcutronix.com
<http://www.arcutronix.com>

Copyright Note

© Copyright 2010, arcutronix GmbH. All rights reserved.

Restricted Rights Legend: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software Restricted Rights clause at DFARS 252.227-7013 and/or the Commercial Computer Software Restricted Rights clause at FAR 52.227-19(c) (1) and (2).

Document Contents

This document contains the latest information available at the time of publication. The content of this document is subject to change without prior notice. arcutronix reserves the right to modify the content at any time. arcutronix shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material. To request arcutronix publications or comment on this publication, contact a arcutronix representative or the arcutronix corporate headquarters. arcutronix may, without obligation, use or distribute information contained in comments it receives. Address correspondence to the attention of Manager, Technical Publications.

Trademarks

arcutronix is a registered trademark of arcutronix GmbH. All other products, trade names and services are trademarks, registered trademarks or service marks of their respective owners.

About this Book

Document Organization

This guide describes the hardware and software components of the SCX2e - System Controller. It provides information on configuration, system installation and technical data.

The intended audience of this document is anyone who is responsible for installing, maintaining or operating the SCX2e - System Controller. This person must be aware of the risks, affected with these actions and must be qualified and trained. **Observe the safety precautions in chapter “Safety, Instructions, Statements”.**

The manual is designed as printable book, therefore chapters start at an odd page (the last even page of the chapter before may be empty). The headlines of the pages contain chapter name, chapter count, and chapter headline. The foot lines of the pages contain chapter page count, the revision date and the document title.

Chapters

Chapter 0, **Safety, Instructions, Statements:** Handling, precautions, warnings.

Chapter 1, **Abstract:** General description of the SCX2e devices and applications for use.

Chapter 2, **Getting Started:** Short form about installation, mounting and configuration of SCX2e-family.

Chapter 3, **Hardware:** Description of hardware and front panel elements.

Chapter 4, **Functionality:** Switching, routing, agent.

Chapter 5, **SCX2e Web-OPI:** Control and configuration of the SCX2e.

Chapter 6, **SNMP and MIBs:** Remote monitoring of the SCX2e.

Chapter 7, **SSH and CLI:** Explains the SSH access to the SCX2e and the usage of the Command Line Interface (CLI).

Appendix A, **Technical Specifications:** Technical data of the SCX2e.

Appendix EC, **EC Declaration of Conformity:** Valid for the SCX2e product family.

Conventions

This manual uses the following text conventions to convey instructions and information:

Normal text is written in Albany font.

Commands and Arguments are done in `Courier New`.

Notes, cautions, and tips use these conventions and symbols:

NOTE: Means reader take note. Notes contain helpful suggestions or references to materials not contained in this manual.

WARNING:



DANGER

Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Release History

2014-08-07 Version 1.6 Editor: mjz
Added and changed the following topics:

- Correction of typos.

2012-12-11 Added and changed the following topics:

- Alarm-Management is improved now. The details are presented in chapter 4. The web-menus are slightly updated to the new features.

2011-11-25 Added and changed the following topics:

- New features added with SW-version 1_3_50.

2011-10-21 Added and changed the following topics:

- New features added with SW-version 1_3_40.
- Added SCX2e-WDM as new variant of ax agent-cards.

2011-09-06 Added and changed the following topics:

- New features added with SW-version 1_3_30.

- Q- and F-interface; IP-Defaults for MGMT2
- Spelling corrections

2011-03-18 Added and changed the following topics:

- ssh-support (chapter 7) added.
- Technical data (Appendix A) corrected.

2010-03-14 First issue of the SCX2e User Guide.

About this Book
Release History

Table of Contents

Document Organization	about-1
Chapters	about-1
Conventions	about-2
Release History	about-2

Chapter 0 Safety, Instructions, Statements

Safety Precautions	0-1
Power Precautions	0-1
Handling Precautions	0-1
Preventing Damage From Electrostatic Discharge	0-2
Card Protection	0-2
Grounding Procedure	0-2
Fibre Optic Precautions	0-3
Technical Instructions to User	0-4
Inspection	0-4
Commissioning	0-4
Cleaning	0-4
Quality	0-4
Repair	0-5
Disposal and Recycling	0-5
CE Conformity	0-5
Electromagnetic Immunity Statement	0-5
Instructions to User	0-5
Electromagnetic Emissions Statements	0-6

Chapter 1 Abstract

SCX2e Description	1-1
General	1-1
SCX2e Functions at a Glance	1-2
Alarm Conditions	1-2
IP-Port	1-3
SCX2e-WDM	1-3
Order Information	1-4
Accessories	1-5
Housings and Cables	1-5
SFPs (Small Form-factor Pluggable)	1-5

Chapter 2 Getting Started

Delivered Parts	2-1
-----------------------	-----

Preparing the Start-up	2-1
Operating Conditions	2-1
Ambient Conditions	2-1
SCX2e Mounting	2-2
Start-up of the SCX2e	2-2
Switching on the Device	2-2
Power-Up Sequence	2-3
LED Start-Up	2-3
Initial Configuration	2-6
Ethernet/IP-based Management Ports	2-6
Default IP-Address of the Device SCX2e	2-6
Default IP-Address of the Device SCX2e-WDM	2-6
Supported Protocols	2-7
Configuration Methods	2-7
Local and Remote Access	2-7
Web Access	2-8
SSH Access	2-8
Telnet Access	2-8
SNMP Access	2-8

Chapter 3 Hardware

List of System Components	3-1
SCX2e Front Panel	3-2
Front Views	3-3
SCX2e	3-3
SCX2e-WDM	3-4
Management Interfaces TCP/IP	3-4
MGMT Port 1	3-4
SCX2e	3-5
SCX2e-WDM	3-5
10/100BaseT (RJ45)	3-5
MGMT Port 2	3-6
SCX2e	3-6
SCX2e-WDM	3-6
10/100/1000BaseTX (RJ45)	3-7
100BaseFX (SFP) and 1000BaseFX (SFP)	3-8
Alarm Connector	3-8
Common Indicators	3-9
'ON' LED	3-9
'AGENT' LED	3-9
'WARN/ERR' LED	3-9
Reset Switch	3-9

Chapter 4 Functionality

Agent 4-1

SW-Update Server for Line-Cards 4-2

Miscellaneous Features 4-2

 Auto Negotiation 4-2

 IP-Addressing 4-4

 Management Ports MGMT 1 & 2 4-4

 DHCP and Manual Address Assignment 4-4

 F- and Q-Interface. 4-5

 DNS-Support. 4-5

Reset IP-Address to Default 4-6

Alarm Management 4-7

 Alarm Types 4-7

 Alarm States 4-8

 Not Available. 4-8

 Inactive 4-8

 Ignored 4-8

 Acknowledged. 4-9

 Warning. 4-9

 Error 4-9

 Alarm Acknowledgement Behaviour 4-9

 Keep Acknowledged Until Inactive 4-9

 Unacknowledge When Raising Severity 4-10

 Unacknowledge on State Change 4-10

 Example 4-10

 Alarm Properties 4-12

 Common Alarm Properties 4-12

 Digital Alarm Properties 4-12

 Analogue Alarm Properties 4-12

 Alarm Groups 4-13

 Global Alarm Status 4-13

Chapter 5 SCX2e Web-OPI

Access to the Device 5-1

 Local Management Interface 5-1

Security Issues 5-1

Login Screen. 5-2

Web-OPI's Body 5-3

 Navigation. 5-4

 Select a menu entry 5-4

 Page Update. 5-4

 Logout. 5-4

Rack View. 5-5

 Symbols of the Rack View 5-5

Card View SCX2e	5-6
General System Information	5-7
Rack Details	5-9
Inventory	5-10
Administration	5-12
User and Access Administration	5-13
Users and Passwords	5-15
SSH Access	5-19
SNMP Access	5-22
SNMP based SNMP parameter configuration	5-35
Port and IP Configuration	5-35
F- and Q-Interface	5-35
Edit Port Settings	5-37
Edit IP-Settings	5-38
SFP Information	5-40
Diagnostics	5-42
Date and Time Settings	5-43
Configuration Management	5-45
Recall Configuration ("Apply")	5-46
Firmware Update	5-48
HTTP FW-Update	5-49
SFTP FW-Update	5-51
TFTP FW-Update	5-52
Reset System	5-53
Selftest	5-55
Alarm Management	5-55
System Alarm Group	5-57
Detailed Alarm Settings	5-59
Port#2 SFP Alarm Group	5-60
Update Manager	5-62
Update Manager	5-63
Update Manager Device-Specific	5-63

Chapter 6 SNMP and MIBs

SNMP Access Generally	6-1
SNMPv2c	6-2
SNMPv3	6-2
Traps	6-2
Installation Prerequisites	6-3
Preparing the SNMP Management System	6-3
Management Information Bases (MIBS)	6-3

Chapter 7 SSH and CLI

Access to the Device	7-1
--------------------------------	-----

SSH connection	7-1
SSH connection with public keys	7-3
Security Issues	7-4
Command Line Interface (CLI)	7-4
CLI Editor Features	7-5
Context Sensitive Help	7-5
Command Syntax Check	7-5
Command Completion	7-5
Hot Keys	7-5
Commands	7-6
SCX2e-CLI Modes	7-8
Rackview - Mode	7-8
Example SHOW	7-8
Example SELECT	7-9
SELECT by rack/slot address	7-10
SELECT by name	7-10
SELECT by serial number	7-10
Cardview - Mode	7-10
Example CONFIG	7-11
Quick Usage Guide for CLI-Commands	7-14
Example for ssh-Script	7-15
Menu-Structure (Directory-Tree) of SCX2e	7-17

Appendix A Technical Specifications

SCX2e Hardware Specification	A-1
SCX2e Software Specification	A-6

Appendix EC EC Declaration of Conformity

Declaration of Conformity	EC-1
---------------------------------	------

List of Figures

Figure 1-1	SCX2e in ax 10-slot Chassis SRX10	1-1
Figure 1-2	SCX2e-WDM Remote Management Application	1-3
Figure 2-1	Slot for SCX2e in Rail 63	2-2
Figure 3-1	SCX2e HW Configuration	3-2
Figure 4-1	Agent Architecture	4-1
Figure 4-2	Acknowledge of Alarms	4-11
Figure 5-1	Login Screen	5-2
Figure 5-2	Web-OPI's Appearance	5-3
Figure 5-3	Rack-View	5-5
Figure 5-4	Card-View SCX2e	5-7
Figure 5-5	General System Information	5-8
Figure 5-6	Rack Details	5-9
Figure 5-7	Inventory	5-11
Figure 5-8	Administration	5-12
Figure 5-9	User and Access Administration	5-14
Figure 5-10	Users and Passwords	5-15
Figure 5-11	Add Account	5-16
Figure 5-12	Modify Account	5-18
Figure 5-13	SSH Access	5-19
Figure 5-14	SSH Password	5-21
Figure 5-15	SSH Password	5-22
Figure 5-16	SNMP Access, SNMP enabled	5-23
Figure 5-17	SNMP Users and Community	5-25
Figure 5-18	SNMPv2c Community	5-26
Figure 5-19	SNMPv3 User	5-27
Figure 5-20	SNMPv3 Edit User Settings	5-29
Figure 5-21	SNMP Trap Configuration	5-32
Figure 5-22	Edit SNMP Trap Receiver	5-34
Figure 5-23	Port and IP Configuration	5-36
Figure 5-24	Edit-Port-Settings	5-37
Figure 5-25	Edit-Port-Settings	5-39
Figure 5-26	SFP	5-40
Figure 5-27	SFP	5-42
Figure 5-28	Diagnostics	5-43

Figure 5-29	Date And Time Settings	5-44
Figure 5-30	Configuration Management	5-45
Figure 5-31	Recall Configuration	5-47
Figure 5-32	Update SCX2e-SW	5-49
Figure 5-33	Ongoing SCX2e-SW Update	5-50
Figure 5-34	TFTP Firmware Update	5-51
Figure 5-35	TFTP Firmware Update	5-52
Figure 5-36	Reset System, Immediate Reset	5-53
Figure 5-37	Reset System, @Specific Time	5-54
Figure 5-38	Selftest	5-55
Figure 5-39	Alarm Management	5-56
Figure 5-40	System Alarm Group Management	5-58
Figure 5-41	Temperature Threshold	5-60
Figure 5-42	SFP Alarm Group Management	5-61
Figure 5-43	Update Manager.	5-63
Figure 5-44	Update Manager Device-Specific.	5-64
Figure 6-1	The SNMP ax-MIB Tree (1.3.6.1.2.4.1.31507).	6-4
Figure 7-1	PuTTY ssh-Connection	7-2
Figure 7-2	Secure Shell.	7-2
Figure 7-3	Secure Shell - Public Key	7-3
Figure 7-4	Example Rackview Mode	7-9
Figure 7-5	Example Rackview Mode: SHOW command	7-9
Figure 7-6	Example Cardview-Mode: SHOW command	7-11
Figure 7-7	Menu Structure SCX2e	7-21

List of Tables

Table 0-1	Effects of Cleaning Liquids	0-4
Table 1-1	Order Matrix	1-4
Table 1-2	Accessories Housings & Cables	1-5
Table 1-3	Accessories SFPs	1-6
Table 2-1	Ambient Conditions	2-1
Table 2-2	SCX2e Front View	2-4
Table 2-3	LED Start-Up	2-5
Table 3-1	System Components	3-1
Table 3-2	SCX2e Front View	3-3
Table 3-3	SCX2e Front View	3-4
Table 3-4	Electrical Interfaces	3-5
Table 3-5	Pin Assignment Alarm Connector	3-8
Table 3-6	Restore IP-Settings	3-10
Table 4-1	Settings Auto-Negotiation	4-3
Table 4-2	Restore IP-Settings	4-6
Table 5-2	SCX2e Menu	5-7
Table 5-3	General System Information Menu	5-8
Table 5-4	Rack Details Menu	5-10
Table 5-5	Inventory Menu	5-11
Table 5-6	Administration Menu	5-13
Table 5-7	User Administration Menu	5-14
Table 5-8	Users and Passwords Menu	5-16
Table 5-9	Add Account Menu	5-17
Table 5-10	Change Password	5-18
Table 5-11	SSH Access	5-20
Table 5-12	SSH User Definition	5-21
Table 5-13	SNMP Access Menu	5-23
Table 5-14	SNMPv2c Community Configuration Menu	5-26
Table 5-15	SNMPv3 User Menu	5-28
Table 5-16	SNMPv3 User Settings Menu	5-29
Table 5-17	SNMPv3 Confidentiality	5-31
Table 5-18	SNMP Trap Configuration Menu	5-33
Table 5-19	Edit SNMP Trap Receiver Menu	5-34
Table 5-20	IP-Configuration Menu	5-36

Table 5-21	Port Configuration Menu	5-37
Table 5-22	IP-Port Configuration Menu	5-39
Table 5-23	SFP Details	5-41
Table 5-24	Date and Time Settings Menu	5-44
Table 5-25	Configuration Management	5-46
Table 5-26	Recall Configuration	5-47
Table 5-27	Firmware Update Menu	5-50
Table 5-28	Reset System Menu	5-54
Table 5-29	Alarm Management	5-56
Table 5-30	System Alarm Group Management	5-58
Table 5-31	SFP Alarm Group Management	5-61
Table 7-1	SCX2e CLI Hot Keys	7-5
Table 7-2	SCX2e CLI Commands	7-7
Table 7-3	Menu Indicators and corresponding CONFIG Commands	7-12
Table 7-4	Special CONFIG Commands	7-13
Table 7-5	Quick Reference	7-14
Table 7-6	Example for ssh-Script	7-15
Table A-1	Number of Interfaces	A-1
Table A-2	Power Requirements	A-1
Table A-3	Technical Data of the Interfaces	A-2
Table A-4	Display Functions	A-3
Table A-5	Mechanic and Environment	A-4
Table A-6	µController and Clock	A-4
Table A-7	Technical Data of the SCX2e - Software	A-6

Chapter 0

Safety, Instructions, Statements

Safety Precautions

The following sections provide the safety precautions for the supplied device. You must always observe the power precautions for the device. You must follow all warning notes to ensure that the procedures are performed safely. You must follow all caution notes to ensure that the device is operated correctly.

WARNING: Serious injury or loss of life is possible, if instructions are not carried out.

CAUTION: Serious damage or destruction is possible, if instructions are not followed.

NOTE: Before installing the device find out if any local technical rules must be observed. These may be defined by ANSI, ITU, IEC, your PTT, or other similar organizations.

Power Precautions



WARNING:

- Disconnect the power cord before opening the device.
- Always plug the power cords into properly grounded receptacles. An improperly wired receptacle could place hazardous voltage on the accessible metal parts of the device.
- Use only approved power cords.
- Use only manufacturer supplied power supplies.
- The power supply must match the power specifications for the device.
- Do not work on the equipment during periods of lightning activity.

Handling Precautions

Note: Precautions for transporting, installing, and operating the device:

- Avoid excessive shocks and vibrations. Install shock absorbers, if you need to use the device for mobile applications.
- Avoid contact with any liquid (e.g. water) or dust or dirt.
- Avoid exposing the device to excessive direct sunlight.

- Ensure sufficient cooling of the device.
- Prevent loose items from falling into the device.
- Always place protective covers on all fibre optic cables and connectors that are not in use to prevent breakage and contamination.
- Inspect all fibre optic connections and clean contaminated surfaces before use.
- Avoid damage to components when installing or setting switches or jumpers of the device.
- Attach a wrist strap and follow ESD procedures, see next paragraph.

Preventing Damage From Electrostatic Discharge



CAUTION: Discharge of static electricity (ESD) can damage or degrade electronic components. The electrostatic potential of a person can be several thousand Volt and a discharge to semiconductor components may have severe consequences. Observe the precautions below when you are handling any hardware with electronic components.

Card Protection

Each card is shipped in a separate, reusable, and anti-static shielding bag. Leave each card in its bag until you are ready to install it into the system. Do not remove the card from its bag unless you are grounded. Do not place a bag on exposed contacts where it can cause short circuits.

Grounding Procedure

Before attempting to install or remove any part of the chassis, ensure that you, the equipment chassis, and the rack mount cards are at ground potential to prevent electrostatic discharge (ESD). Electrostatic discharges can damage the components of the system. To place yourself at ground potential, connect the chassis with a ground wire or via the power cord with a grounded mains socket and clip your wrist strap to the chassis.

The following advice will help you to prevent ESD damage to electrical components:

- Always use an ESD wrist strap with a metal clip for grounding.
- Limit your movement as much as possible. Movement can cause a build-up of static electricity.
- Handle the system and its components carefully. Never touch the circuitry. Place your hands only on the edges, rails, or frame of the unit.
- Touch a spare component - while it is still in the anti-static wrapping - to an unpainted metal portion of the chassis for at least two seconds. This allows the static electricity to discharge harmlessly from your body and the spare.
- Install the spare directly into the chassis after removing it from the anti-static wrapping. Do not remove the anti-static wrapping until you are ready to do the install. If you must set down an unwrapped spare, set it down on an anti-static mat or on its anti-static wrapping.

Caution: Do not place the spare component on the top of the chassis (rack) or on a metal table. Either action could cause severe damage to the spare.

- Set down cards with their component sides face up.
- Be aware of weather conditions. Cold weather increases the likelihood of static electricity build-up.
- Be aware of your own conductivity level. Wear ESD shoes to diminish personal static electricity build-up. Wear e.g. an electrostatic dissipative lab coat.

Fibre Optic Precautions



Caution: An optical fibre may carry (invisible) light from the remote system.

This device may contain Laser Class 1 components, like laser transmitters or light emitting diodes LED (refer to technical data). Operating components emits (invisible) laser radiation. Be careful when you are working with these components. The following safety precautions must be followed when working with fibre optics and Laser Class 1 components:

WARNING: Do not look into the fibre optic output. Looking into the fibre optic output can cause injury to the eye. When observation is necessary eye protection must be worn and precautions must be taken to avoid exceeding the limits recommended in ANSI Z136.1-1981.

WARNING: Use caution when working with the laser components of the device. The device is designed to protect the user against optical powers beyond laser class 1.

WARNING: Ensure that the incoming signal from the remote device does not exceed the power defined for laser class 1 when the cabling is disconnected. The device will also become unsafe, if any unsafe equipment is connected to the system.

WARNING: Do not disconnect the fibre optic cables while power is applied. Disconnecting the fibre optic cables could expose the user to optical powers beyond laser class 1.



Caution: Use Of Controls Or Adjustments Or Performance Of Procedures Other Than Those Specified Herein May Result In Hazardous Laser Light Exposure.

CAUTION Laser Class 1. Complies with FDA radiation standards, 21CFR subcategory J. DANGER (Invisible) laser radiation when open and / or interlock defeated. Avoid direct exposure to beam!

Technical Instructions to User

Do not use this product for other applications than suggested in this manual!

The international standards and the technical rules of your local PTT company must be observed.

All interface cables to this equipment must be shielded and designed in accordance with proper EMI techniques to ensure compliance with EMC requirements. arcutronix will provide cable shielding specifications on request.

Inspection

Before commissioning, check the content of the consignment for completeness and note whether any damage has occurred during transport. If so, do not use the parts and contact your arcutronix representative.

Commissioning

Work may be carried out only by qualified personnel. The relevant precautions must be taken.

Cleaning



To clean the outer surfaces, use a soft damp (not wet) cloth. Do not let moisture go inside. Please consider the properties of the housing and other material used!

Table 0-1 Effects of Cleaning Liquids

Valuation	ABS/ABS+PC/PC/PPE+PS
well resistant	water, aqueous saline solutions, sud, diluted acid and alkali
conditionally resistant	alcohol, aliphatics, oil and fat
not resistant	concentrated mineral acid, aromatic and halogenated hydrocarbon, ester, ether, ketone

Quality



The quality management of arcutronix GmbH is certified to DIN ISO 9001:2000.

This product is manufactured to the arcutronix GmbH quality standards.

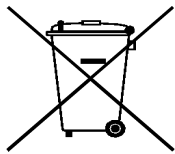
Repair

There are no repairable parts in the device. Defective parts must be sent to arcutronix GmbH for repair. The power supplies of a device may contain fuses. Blown-up mains fuses must be replaced by fuses of the same type and the same ratings. Using repaired fuses or short-circuit the fuse holder are not permitted.

Disposal and Recycling



This symbol on the product or on the packaging indicates that it can be recycled. To save our environment please hand it over to your next recycling point.



This symbol on the product or on its packaging indicates that it shall not be treated as household waste. Instead it shall be handled over to the applicable collection point for the recycling of electronic equipment.



For more detailed information about recycling contact your local city office, your waste disposal service or where you purchased the product.

CE Conformity



arcutronix products complies with the European standard regulation. They are tested to the Council guideline for harmonizing the legal regulations of the member states on electromagnetic compatibility.

Electromagnetic Immunity Statement

This equipment has been tested and found to comply with the limits of EN 50082-2 (Electromagnetic Immunity for heavy industry).

Instructions to User

All interface cables to this equipment must be shielded and designed in accordance with proper EMI techniques to ensure compliance with EMC requirements. arcutronix will provide cable shielding specifications on request.

Electromagnetic Emissions Statements

To achieve satisfactory EMC performance, all interface cables to this equipment must be shielded and designed in accordance with proper EMI techniques. Rack mount cards has to be inserted into the designated chassis. Chassis slots that are not used have to be covered with a blanking plate. The chassis must be bonded to earth. This is usually achieved by installing the power cord to the chassis. An extra earth terminal may be provided. If this device is used in a residential setting, resulting interference must be corrected by the user. Any user modification made to the unit voids the user's authority to operate the unit under the FCC rules.



WARNING: This is a Class A product. In a domestic environment, this product may cause interference in which case the user may be required to take adequate measure. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

United States Federal Communications Commission (FCC) Electromagnetic Emissions Statement

WARNING: This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions in this manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of the FCC Rules, which are designed to provide reasonable protection against such interference in which case the user at his own expense will be required to take whatever measures may be required to correct interference.

Canadian Department of Communications (DOC) Statement

WARNING: This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions in this manual, may cause interference to radio communications. This digital apparatus has been tested and does not exceed the Class A limits for radio noise for digital apparatus set out in the DOC Radio Interference Regulations. The regulations are designed to provide reasonable protection against radio noise interference in which case the user at his own expense will be required to take whatever measures may be required to correct interference.

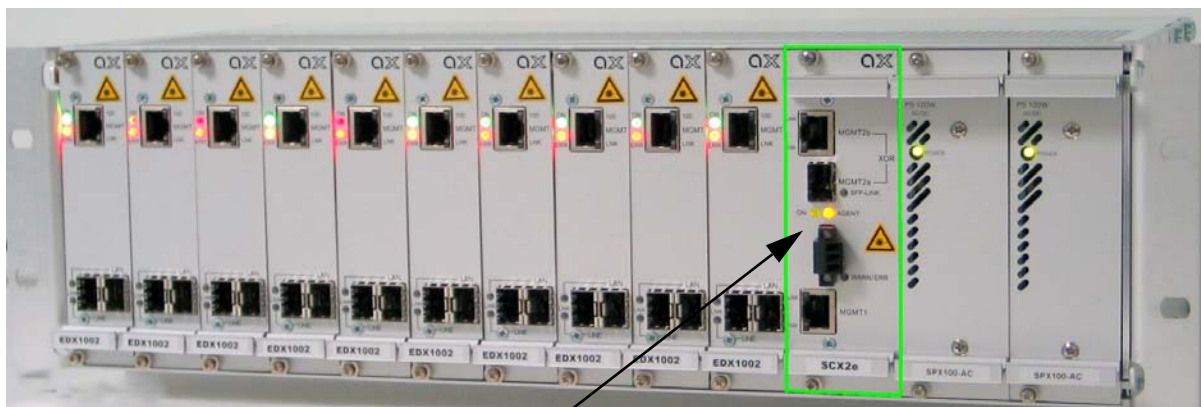
European Communities

WARNING: This equipment has been tested and found to comply with the limits of CISPR 22 and EN 55022 Class A for information technology equipment. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

SCX2e Description

General

The System Controller SCX2e is used to control and configure all types of managed arcutronix line-cards: Connectivity, Transport and Ethernet types. The SCX2e allows the administrator and operator to configure and monitor local as well as remote ¹ devices via one single access point.



SCX2e Agent

Figure 1-1 SCX2e in ax 10-slot Chassis SRX10

The System Controller SCX2e provides access by very different methods to fit it into a wide bunch of applications and management scenarios. Some of these are

- Web-GUI for an intuitive and user-friendly way,
- Command Line Interface for scripting and automation,
- SNMP-agent for alarm-push and integration in umbrella management systems,
- Fibre and copper ports, and
- SSH for high security.

1. Mainly the ax connectivity family does support remote inband access from local access point.

Web-GUI and local management assist a user friendly field installation and configuration. For SNMP management, several standard and product specific MIB files (Management Information Base) are provided.

SNMP management can be interconnected to any SNMP-compatible management software such as [HP Open View](#) and SNMPc ([Castle Rock](#)).

Remote SW-upload for SCX2e and each other component in the system rack is realized via HTTP or (T)FTP. After copying SW updates to SCX2e Flash File System updated files are loaded into agent and plugged modules on administrator request.

The in-band management capability, in combination with the System Controller SCX2e allow Carriers and ISPs to maintain and supervise all devices inside management system via single NMS access point. Trap signalling helps to detect errors in case of any failure or status change at the local or remote site.

SCX2e Functions at a Glance

The SCX2e rack agent allows the management of ax-chassis and expansion chassis equipped with rack mounted line-cards (LCs). It provides access by standard TCP/IP stack and any kind of management platform using SNMP, ssh or a web-browser. The chassis and the installed rack mount cards can be monitored and configured locally and remotely.

The SCX2e communicates with the arcutronix Multi Service System and installed rack mount cards and allows the following management features:

- Central management access device for system racks (SRX family)
- Auto-detection of equipped cards
- SW-upload for each component in a system rack via http or (T)FTP
- Flash File System, for saving new and old SW files of all plugged cards
- Various management access options: SNMP, Web-GUI, Telnet
- Power and Fan control functionality
- SNMP trap-signalling in case of local or remote status changes
- Discovery of system rack types
- Alarm relay - Enhanced alarm threshold selectable in addition to autonomous alarm function via alarm relay contacts on fan module
- Compact 3RU rack card
- Power supply via system racks (SRX)

Alarm Conditions

Alarm conditions can be detected depending on the settings made in the control software. Each SCX2e card monitors all power supplies and rack mount cards of the chas-

sis and the fan's function. If there is a failure recognized by an SCX2e card, an alarm will be set by the agent.

An alarm contact are used to execute an initiated alarm. The alarm contact is a part of the alarm output card or the fan module.

IP-Port

Two Ethernet ports are available. One is 10/100BaseT (RJ45), only, while the other is either twisted pair or optical access ("Combo-Port"). The two ports are used for IP-based communication. The IP-address has to be configured before usage.

SCX2e-WDM

The SCX2e-WDM agent is intended to offer remote management via an WDM-overlay network. A fibre based service, which needs remote management in the same fibre as the service itself, can make use of the WDM capability. Service traffic and management traffic is multiplexed on the same line without any interference or decrease of bandwidth.

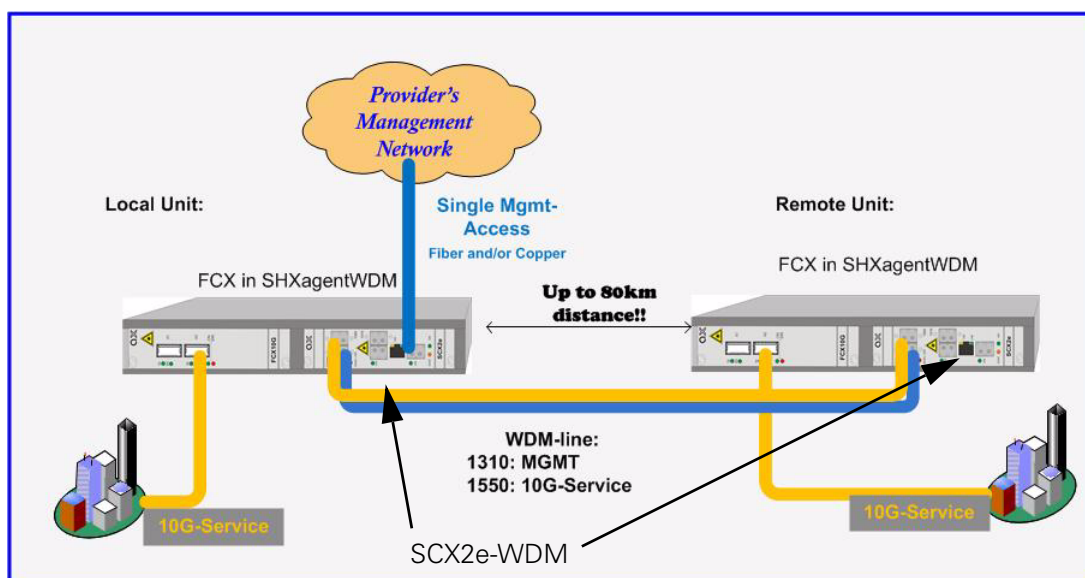


Figure 1-2 SCX2e-WDM Remote Management Application

The SCX2e-WDM is intended to be only used in the double-slot housing SHX3-SC, which is shown in the figure above, too.

The WDM filter is a pure passive component, which is mounted on the PCBA of SCX2e-WDM.

Order Information

For the time being, the SCX2e is the sole member of SCX2e - System Controller family.

Table 1-1 Order Matrix

Art.- No.	Short Name	Description
0903-3000	SCX2e	System Controller for connectivity system devices: <ul style="list-style-type: none">• SNMP, Web-GUI, ssh,• 1x GigE-Port (RJ45: 10/100/1000BaseT),• 1x GigE-Combo-Port (RJ45: 10/100/1000BaseT; SFP: 1000BaseX),• with alarm contact,• 3RU rack mount card.
0903-3010	SCX2e-WDM	System Controller for connectivity system devices: <ul style="list-style-type: none">• SNMP, Web-GUI, ssh,• 1x GigE-Port (RJ45: 10/100/1000BaseT),• 1x GigE-Port (SFP: 1000BaseX),• Onboard passive WDM filter (1310/1550nm std SM),• 3RU rack mount card.

Accessories

Housings and Cables

The arcutronix' Multi Service Platform offers a range of accessories for an easy and space saving installation of your device into 19" cabinets or as desktop / wall-mount installation.

Table 1-2 Accessories Housings & Cables

Art.- No.	Short Name	Description
0805-9000	SRX10	Rack mount shelf: <ul style="list-style-type: none">• 19" chassis• Height: 3RU• 10 slots for line-cards• 1 slot for management• 2 slots for modular AC (115/230V) and/or DC (-48V) power supplies
0717-9501	SHX3-SC	Standalone housing: <ul style="list-style-type: none">• 1x slot for 3RU line-card,• 1x slot for SCX2e-WDM Management card only,• max. 15W total power consumption,• VT100 Management port (D-Sub)• with alarm contacts, grounding bolt, ventilation,• integrated wide range power supply,• mains supply: 48VDC...110/230VAC,• DC jack included.
0500-001	PC-E	Power cord, European plug.
0500-002	PC-B	Power cord, Great Britain plug.

NOTE: All order matrices will be regularly updated. Asked your arcutronix representative for the latest publications.

SFPs (Small Form-factor Pluggable)

The SCX2e-series offers a number of SFP-slots (Small Form-factor Pluggable) for usage of a wide range of different optical transceivers. The small form-factor pluggable (SFP) is a compact, "hot-pluggable" optical transceiver used in optical communications for both telecommunication and data communications applications. The SFP transceiver is specified by a multi-source agreement ([SFP MSA]) between competing manufacturers.

Using the right SFP, the SCX2e can be used in different optical environments with different fibre-types (single-mode or multi-mode) and a wide range of distances.

SCX2e does support all optical modules, which are designed according the [SFP MSA]. For safe operation, arcutronix recommends the SFPs below. Please ask for special types, if required.

Table 1-3 *Accessories SFPs*

Short Name	Description
Optical Transceiver:	
100Base-FX:	
SFP-155-S13-10	Optical SFP Interface Module: 1310nm SM FO; Fast E, 155 Mbps transceiver; pluggable SFP footprint; LC connector; 10km.
SFP-155-S13-15	Optical SFP Interface Module: 1310nm SM FO; Fast E, 155 Mbps transceiver; pluggable SFP footprint; LC connector; 15km
SFP-155-S13-40	Optical SFP Interface Module: 1310nm SM FO; Fast E, 155 Mbps transceiver; pluggable SFP footprint; LC connector; 40km.
1000Base-SX/LX/LH/ZX	
SFP-1.25-S13-10	Optical SFP Interface Module: 1310nm SM FO; 1xFC, 1.25 Gbps transceiver; pluggable SFP footprint; LC connector; digital diagnostics; 10km.
Copper Transceiver (Triple-Speed SFP):	
SFP-1.25e	Electrical SFP Interface Module: Pluggable SFP module, for data rates of 1.25Gb/s bi-directional data links. - 1000BASE-T Copper port, RJ45 connector - compatible with the Gigabit Ethernet and 1000BASE-T standards as specified in IEEE 802.3 - digital diagnostic supported.

Chapter 2

Getting Started

For the start-up of the SCX2e please follow the directions in this chapter. You must keep the operating conditions specified for the devices. In the following read about the start-up preparation, the start-up itself, and the possibility to automate the start-up.



WARNING: Read the safety notes at the beginning of this manual carefully before you start the device!

Delivered Parts

Please check if all the items listed below are included in your delivery. Your delivery includes:

- An SCX2e System Controller Card
- Short User-Information

Preparing the Start-up

Before you switch on the device you need to check the operating conditions and install the SCX2e into the chassis or the desktop-housing.

Operating Conditions

Read the operating conditions specified in this section carefully to avoid damages to the device or connected systems.

Ambient Conditions

The ambient conditions, which must be maintained for the SCX2e, are shown in Table 2-1.

Table 2-1 Ambient Conditions

Operating Temperature	5°C to 40°C
Max. Relative Humidity (non-condensing)	85% (30°C)

Table 2-1 Ambient Conditions (continued)

Input Voltage	+5V DC
Power Consumption	< 7 VA ⁱ

i. Depends on the given variant.

CAUTION: If operating limits are exceeded, malfunctions and permanent damage to the equipment may result.

NOTE: In order to operate the various interfaces, please ensure that the plugs are firmly engaged in the sockets.

SCX2e Mounting

To mount the SCX2e into the chassis please follow the subsequent step-by-step instructions.

1. Disconnect all cables from the SCX2e before mounting the device.
2. Place the SCX2e right way up on a table with the front panel looking in your direction.
3. Insert the SCX2e that way into the chassis as shown below. Use slot with the rail number 63!

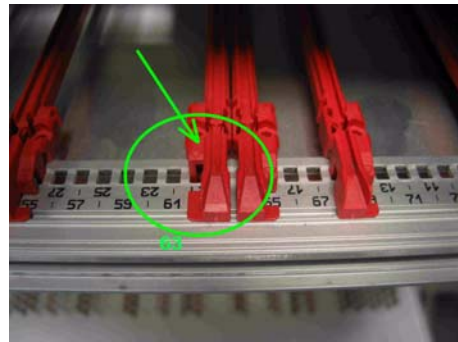
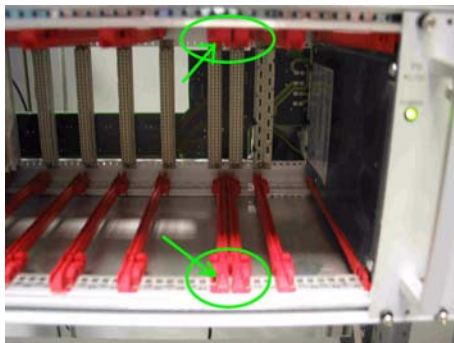


Figure 2-1 Slot for SCX2e in Rail 63

4. Mount the SCX2e to the chassis using the provided screws.
5. Connect the interface cables to the SCX2e.

Start-up of the SCX2e

Switching on the Device

Switching on the SCX2e, please observe the following instructions:

1. Connect the mains cable to the chassis containing the SCX2e.
2. Plug the mains plug of the mains cable in a Home Office socket.

After power is connected to either chassis or housing, the device boots its software automatically. No extra switch has to be activated. During the boot-process all internal components are roughly tested and the device is initialized. The last setup is restored; in case the unit starts the first time, it starts with the factory defaults.

The boot-process is indicated by the blinking ON-LED and takes about half a minute (see “Power-Up Sequence” below). At the end of this process the unit is fully operational. If there are any settings, which need special adoption, different to the default, the configuration can start now.

Power-Up Sequence

After providing power to the SCX2e, the device will be powered up. The start-up will take several seconds, while internal SW is started and some tests are done to verify the SCX2e is not damaged and proper operation can be guaranteed.

The power-up sequence is indicated by special behaviour of the LEDs. After finishing the start-up, the LEDs will operate “normal” and indicate status and alarms of the unit, as written in this book.

The special behaviour of the LEDs allow to user to

1. check, whether all LEDs are operating well and
2. see when the unit’s start-up is finished and it is operational.

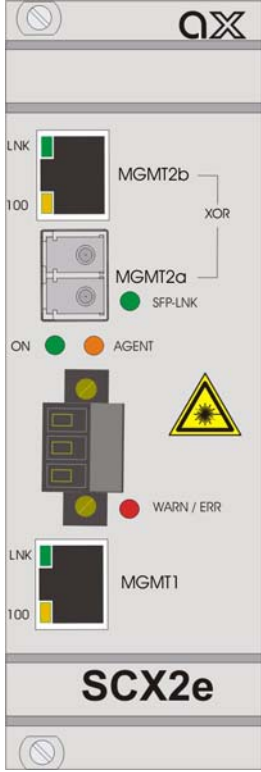
LED Start-Up

In the front plate, four categories of LEDs are grouped together:

- Power-LED (green)
- Configuration LED (yellow)
- Alarm-LED (red)
- Ethernet LEDs, build-in RJ-45 connectors and beside SFP

See the following table for the categories:

Table 2-2 SCX2e Front View

View	Product Number & Details
	<p>Mounting screw in SRX. Handle w/o Label.</p> <p>1x 10/100/1000BaseT Management Port (Part of Combo Port 2), 2x integrated LEDs.</p> <p>1x 100FX/1000FX Management Port (Part of Combo Port 2) + 1x LINK-LED</p> <p>1x ON-LED + 1x Agent-LED.</p> <p>1x Alarm Connector. 1x Alarm-LED.</p> <p>1x 10/100BaseT Management Port (Port 1), 2x integrated LEDs.</p> <p>Handle with Label. Mounting screw in SRX.</p>

NOTE: The SCX2e-WDM front plate is slightly different. The alarm connector and Copper I/F MGMT1 is missing. As the behaviour of the LEDs is the same, the SCX2e-WDM will not be depicted here. See Chapter 3, SCX2e-WDM for details.

The flow of these LED groups is depicted in the following table.

Table 2-3 LED Start-Up

State	ON-LED	Agent-LED	Alarm-LED	Ethernet-LEDs
S1 “Boot-Seq.”, (after Power On) Duration: ~5sec	LED is blinking fast	LED are ON	LED is ON	All LEDs are OFF
S2 “Boot-Finished” Duration: ~2sec	LED is ON	LED is OFF	LED in ON	All LEDs are OFF
S3 “Start Linux” Dur.: ~1 sec	LED is blinking slowly	LED is ON	LED in ON	All LEDs are OFF
S4 “Test-Eth-LEDs”	LED is blinking slowly	LED is ON	LED in ON	All LEDs of Port 2 are ON ⁱ
O1	LED is ON	Normal operation = Agent-Mode (ON).	Normal operation = Alarm status of the card/rack is shown.	Normal operation = Link and traffic of Ethernet-connections are shown.
O2 (IP-Reset)	LED is ON	IP-Reset (blinking).	Normal operation = Alarm status of the card/rack is shown.	Normal operation = Link and traffic of Ethernet-connections are shown.

i. The LEDs of Port1 are not part of the LED-test.

Note: Sx = Startup state; O1 = Operational State reached.

Initial Configuration

The initial configuration can be done like all other configuration settings. There are several ways to get contact to the device, which are explained in more detail later on. Here, only a short overview to the possible options of access are given.

Ethernet/IP-based Management Ports

A lot of protocols can be used for configuration, which are based on the TCP/IP stack: Telnet, SSH and SNMP. The access to these protocol-stacks are achieved via the available management interfaces. These are either the out-of-band interfaces (called "MGMT1" and "MGMT2").

MGMT1 is dedicated to act as a local management interface, in the so-called F-mode. This is used to directly connect your PC/Laptop to this interface. It provides an IP-address to the PC/Laptop via DHCP and makes it very easy to communicate with the device.

MGMT2 is intended to be used as a remote management port, to integrate the device in an (overlay) management network, where a DSCP-server is running and the configuration is administrated from central place. This is called a Q-interface.

Both default settings of the management interfaces can be changed to fit into the given environment and needs.

Default IP-Address of the Device SCX2e

The two Ethernet ports MGMT1 and MGMT2 do have different factory settings concerning their IP-settings.

Per default MGMT1 does have a fixed IP-address and is acting as DSCP allow easy initial connection and configuration:

- Default IP (MGMT1): 192.168.0.100/24
- Default GW (MGMT1): empty

MGMT2 asks for an IP address via DHCP. The DHCP server has to be connected to "MGMT2" port. As long as there was no DHCP available, yet, the unit uses the following default IP-address:

- Default IP (MGMT2): DHCP-client (no default IP-address)
- Default GW (MGMT2): from DHCP (empty)

If the IP-address shall be assigned manually, then the settings can be changed and a fixed IP-address can be assigned in the configuration menu.

Default IP-Address of the Device SCX2e-WDM

The two Ethernet ports MGMT1 and MGMT2 do have different factory settings concerning their IP-settings.

Per default MGMT1 does have a fixed IP-address and is acting as DSCP allow easy initial connection and configuration:

- Default IP (MGMT1): 192.168.0.100/24
- Default GW (MGMT1): empty

MGMT2 asks for an IP address via DHCP. The DHCP server has to be connected to "MGMT2" port. As long as there was no DHCP available, yet, the unit uses the following default IP-address:

- Default IP (MGMT2): DHCP-client (no default IP-address)
- Default GW (MGMT2): from DHCP (empty)

If the IP-address shall be assigned manually, then the settings can be changed and a fixed IP-address can be assigned in the configuration menu.

Supported Protocols

When using the in-band or out-of-band management interfaces, three protocol applications can be used:

- SNMP
- Telnet
- SSH (secure shell)
- Web-GUI

Configuration Methods

After successful start-up process, the unit is ready for communication and configuration. A default setup is available as factory settings, but special settings can be done via several ways and methods. These will be depicted hereafter. All configuration settings are made by using the management user I/Fs. For the system configuration you can choose one of the following configuration methods:

Local and Remote Access

The SCX2e has two Ethernet I/Fs, which can be used for local and/or remote access. Local access means the direct connection of a Laptop and/or PC, while remote access is via LAN or WAN connection from somewhere else.

Remote access allows the user to communicate with the SCX2e and maintain the chassis via a long distance. The SFP-port or other Ethernet-based transmission systems can be used to hub the SCX2e into your local environment. The SCX2e can easily integrated in umbrella management system or the EM-function can be used, just as if the user is standing in front of the unit.

Web Access

A Web-based GUI is available to configure and maintain the SCX2e locally and/or remote. Two Ethernet-ports are available, which can be used. Port 1 is a pure 10/100BaseT copper port (CAT5 cable) while port 2 is a so-called “Combo-Port” (up to 1Gbps). One can choose to use the copper or fibre option. When a SFP is plugged into the SFP-slot, the RJ45 is automatically disabled, even when no FO signal is detected!

1. Connect your PC / Laptop / LAN via any Ethernet cable (cross-over or straight) to the port.
2. The SCX2e port1 is configured to act as an DHCP-server and will advertise the connected PC / Laptop an IP-address in the same subnet, as itself (192.168.1.100/24). To use this feature, the PC / Laptop has to be configured as DHCP client. (See Chapter 4, DHCP and Manual Address Assignment for details.)
3. Open your standard internet browser (e.g. Firefox) and enter in the address field **192.168.1.100**. The html-based GUI will allow easy configuration settings.

SSH Access

Secure Shell or SSH is a network protocol that provides secure communication between two computers. If SSH is used correctly, no eavesdropping or tampering with your data is possible, unless you are under attack by an immortal miscreant with extraordinarily powerful computers. Typically, SSH is used to securely log in to remote machines in order to execute commands.

See “SSH Access” on page 5-19 for configuration and Chapter 7, SSH and CLI, for details.

Telnet Access

Telnet access is not supported. Please use SSH access for Command Line Access via TCP/IP.

SNMP Access

The SCX2e offers an on-board SNMP manager, which can be contacted by any available MIB-browser and/or SNMP manager. It supports SNMPv2c as well as SNMPv3 protocol, as defined by IEEE.

As SNMP access is based on TCP/IP suite, the communication is possible via the “Web-OPI” port as well as via the inband / remote access. For normal use, SNMP makes sense for the remote access, but local access is possible.

The TCP-settings are the same as written above for the other ways of access. An easy and quick setup is implemented. See “SNMP Access” on page 5-22 for configuration and Chapter 6, SNMP and MIBs, for details.

Chapter 3

Hardware

This chapter provides information on the System Controller (SCX2e) of the arcutronix Multi Service System with all the function indicators and external interfaces.

The SCX2e is a compact unit. All external connection points for control elements are accessible on the front panel. The indicator elements are also on the front panel.

List of System Components

The SCX2e contains the following system components:

Table 3-1 System Components

	Component	Description
1a	Processor (Local Control Point LCP)	The SCX2e is based on a PowerQuick platform with an MPC8313E from Freescale. This CPU integrates a 32 bit power PC architecture and is clocked with 33MHz.
1b	Flash	The 64MByte non-volatile flash memory contains the program code for the operating functionality of the device as well as the system configuration. The software can be updated or added directly through the interfaces of the device. Therefore, it is not necessary to replace memory modules (for example EPROMs).
1c	SDRAM	The 128MByte main memory allows an high efficient operation of the CPU. The operating system (an embedded Linux distribution) will first be copied from the Flash memory to the SDRAM and then started from there.
2	NMS-Port1	10/100BaseT for local access.
3	NMS-Port2	10/100/1000BaseT Combo port for local and remote access.
4	Alarm-Relay plus Alarm-LED	The alarm relay and LED show the status of the unit.
5	USB-Hub	24-Port USB-Hub to backplane. USB is the physical layer to the line-cards.

Table 3-1 System Components (continued)

	Component	Description
6	DC/DC-Converter	The DC/DC converter is an own developed block, which generates all required voltage-levels out of the incoming 5V from backplane. It is temperature protected to prevent the device from damage.
7	Backplane Connector	Via the backplane connector the SCX2e is connected to all line-cards, the Power-Supply and optional fan unit.
8	Reset-Switch	If the IP-address has been forgotten or lost, this switch can be used to recall the default IP-addresses: MGMT Port1: 192.168.1.100 MGMT Port2: no default IP-address. MGMT-port2 waits for a DHCP-server to get an IP-address.

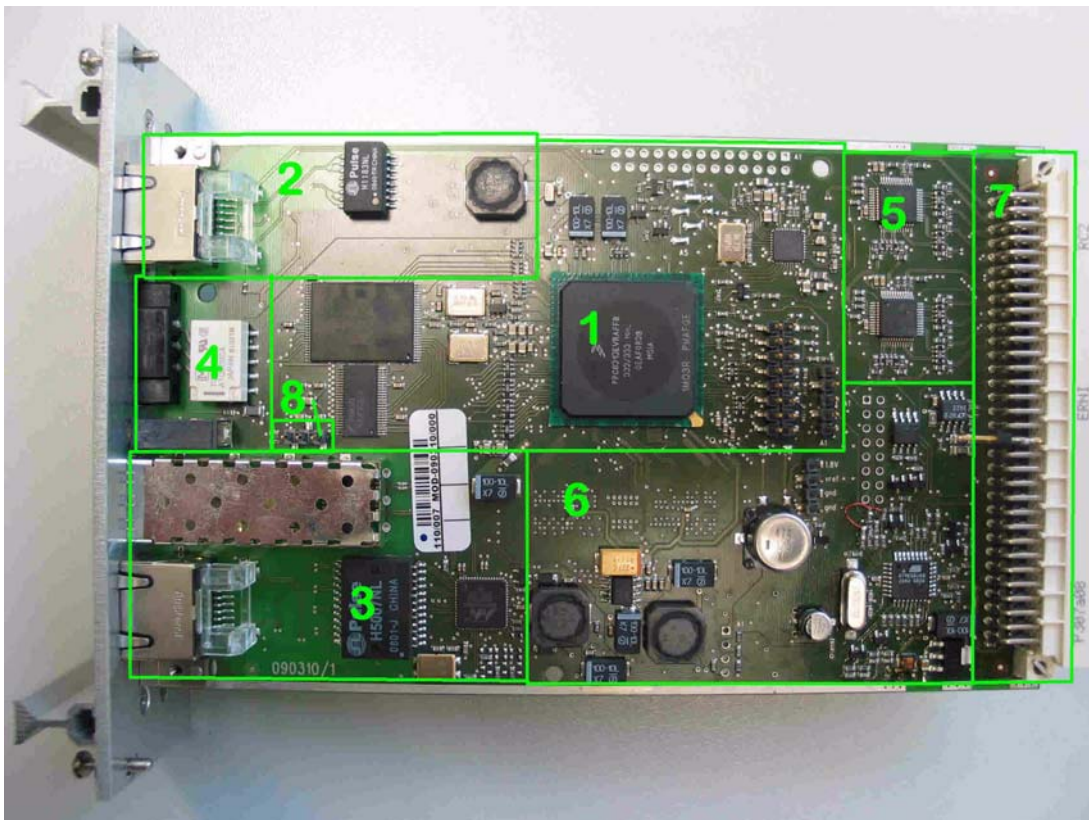


Figure 3-1 SCX2e HW Configuration

SCX2e Front Panel

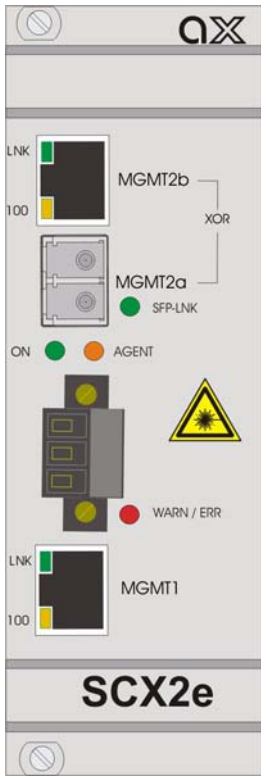
The SCX2e series offers on the front side the connectors for user control interfaces plus a number of LEDs to show status of unit and interfaces.

Front Views

SCX2e

Table 3-2 provides information on the connectors, indicators, and controls of the SCX2e System Controller:

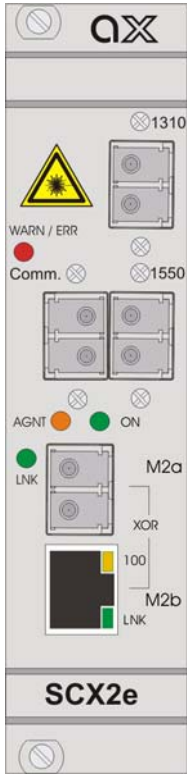
Table 3-2 SCX2e Front View

View	Product Number & Details
 <p>The diagram shows the front panel of the SCX2e System Controller. At the top, there is a mounting screw and a label 'Handle w/o Label'. Below this are two management ports: MGMT2b (a 10/100/1000BaseT port with two LEDs) and MGMT2a (a 100FX/1000FX port with one LINK-LED and an SFP-LNK port). Below these are two LEDs: a green ON LED and an orange AGENT LED. In the center is an alarm connector with a yellow warning triangle and a red WARN / ERR LED. At the bottom are another management port MGMT1 (a 10/100BaseT port with two LEDs) and another mounting screw with a label 'Handle with Label'.</p>	<p>Mounting screw in SRX. Handle w/o Label.</p> <p>1x 10/100/1000BaseT Management Port (Part of Combo Port 2), 2x integrated LEDs.</p> <p>1x 100FX/1000FX Management Port (Part of Combo Port 2) + 1x LINK-LED</p> <p>1x ON-LED + 1x Agent-LED.</p> <p>1x Alarm Connector. 1x Alarm-LED.</p> <p>1x 10/100BaseT Management Port (Port 1), 2x integrated LEDs.</p> <p>Handle with Label. Mounting screw in SRX.</p>

SCX2e-WDM

Table 3-2 provides information on the connectors, indicators, and controls of the SCX2e System Controller:

Table 3-3 SCX2e Front View

View	Product Number & Details
 <p>The image shows the front panel of the SCX2e system controller. At the top, there is a mounting screw hole and the 'αX' logo. Below the logo, there is a yellow laser warning triangle with a red dot, labeled 'WARN / ERR'. To the right of the warning triangle is a WDM-Port labeled '1310'. Below the warning triangle is a red LED labeled 'Comm.' and a green LED labeled 'ON'. To the right of the 'Comm.' LED is a WDM-Port labeled '1550'. Below the 'Comm.' LED is an orange LED labeled 'AGNT' and a green LED labeled 'LNK'. To the right of the 'AGNT' LED is a 100FX/1000FX Management Port labeled 'M2a'. Below the 'LNK' LED is a 10/100BaseT Management Port labeled 'M2b'. The 'M2a' port has a yellow LED labeled '100' and a green LED labeled 'LNK'. The 'M2b' port has a green LED labeled 'LNK'. At the bottom of the panel, there is a 'SCX2e' label and another mounting screw hole.</p>	<p>Mounting screw in SHX. Handle w/o Label.</p> <p>1x WDM-Port (1310nm) to MGMT2a</p> <p>1x Alarm-LED.</p> <p>1x WDM-Port (1550nm) to line-card, 1x WDM-Port (1310+1550).</p> <p>1x ON-LED + 1x Agent-LED.</p> <p>1x 100FX/1000FX Management Port (Port 2) + 1x LINK-LED</p> <p>1x 10/100BaseT Management Port (Port 1), 2x integrated LEDs.</p>
	<p>Handle with Label. Mounting screw in SHX.</p>

Management Interfaces TCP/IP

The SCX2e does have two independent management interfaces called “MGMT 1” and “MGMT 2”. MGMT 1 is a pure copper based Ethernet port with a maximum speed of 100Mbps. MGMT 2 is a combo-port, which is the offer to use either the copper interface or the SFP-based interface. The SFP-based interface will mostly be used for fibre optic data transmission. Port MGMT 2 has a maximum speed of 1000Mbps.

MGMT Port 1

MGMT1 is dedicated to act as a local management interface, in the so-called F-mode. This is used to direct connect your PC/Laptop to this interface. It provides an

IP-address to the PC/Laptop via DHCP and makes it very easy to communicate with the device.

SCX2e

The default IP-settings of port MGMT1 are:

IP-address: 192.168.1.100/24.
Mode: F-interface (acts as an DHCP-server)

SCX2e-WDM

The default IP-settings of port MGMT1 are:

IP-address: 192.168.0.100/24.
Mode: internal interface to remote site.


10/100BaseT (RJ45)

The SCX2e does have one electrical Fast-Ethernet port to be used for local management access ("MGMT 1"). The interface has indicators to give information on the Link state (LNK) and activity (ACT). The device negotiates the operating mode of the corresponding interface automatically with the remote station using Auto Negotiation (if activated). Half-duplex and full-duplex connections are supported. You will find more configuration information in the section "Copper Ethernet Port" on page 5-42. The data rate is either 10 Mbit/s or 100 Mbit/s. The protocol is according to IEEE 802.3 10BaseT or 100BaseTX. Auto negotiation and auto crossover are supported.

Table 3-4 Electrical Interfaces

Item	Values
Standards:	IEEE802.3, 802.3u, 801.1 p&Q
Ports:	up to 8x 10/100BaseT
Data rate:	10Mbit/s or 100Mbit/s auto negotiation, full- or half-duplex, bandwidth limitation
Range:	Up to 100m over UTP-5 cable
Connector s:	RJ-45 8-pin

The connector is a RJ-45 plug with 2 LEDs, which indicate established Link (green LED on the left side) and the data transport (activity) (yellow LED, right). The pin assignment of the RJ45 is as follows:

RJ-45	Pin	Assignment
LED:	1	TD+
green	2	TD-
yellow	3	RD+
LNK	4	-
ACT	5	-
	6	RD-
	7	-
	8	-

- The green LED (left, 'LNK') indicates, when the link is established and packets are transferred.
- The yellow LED (right, 'ACT') indicates a received or transmitted Ethernet frame.

The device is able to recognize

- a polarity inversion of the receiving signals (RD+ <--> RD-)
- a crossover of transmitting/receiving signals (RD+/RD- <--> TD+/TD-)

and corrects it automatically to ensure that the operation continues smoothly. This allows the usage of 1:1 cables in any case.

CAUTION: For access it is recommended to use twisted-pair cables of the category 5 and an impedance value of 100 Ω . The maximum cable length is 100 metres. Using cables of lower quality or different impedances may result in a restriction of the maximum cable length. In addition the employment of unshielded cables can have negative effect on the reliability of the data transmission.

MGMT Port 2

MGMT2 is intended to be used as a remote management port, to integrate the device in an (overlay) management network, where a DSCP-server is running and the configuration is administrated from central place. This is called a Q-interface.

SCX2e

The default IP-settings of port MGMT2 are:

IP-address: <empty>
Mode: Q-interface (acts as an DHCP-client)

SCX2e-WDM

The default IP-settings of port MGMT2 are:


IP-address: 192.168.0.100/24.
Mode: F-interface (acts as an DHCP-server)

10/100/1000BaseTX (RJ45)

The SCX2e provides one copper Gigabit Ethernet interface as part of combo-port MGMT 2. Separate indicators give information on the Link state (LNK) and activity (ACT) of the interface. The device negotiates the operating mode of the corresponding interface automatically with the remote station using Auto Negotiation (if activated). Half-duplex and full-duplex connections are supported. You will find more configuration information in the section “Copper Ethernet Port” on page 5-42. The data rate is either 10 Mbit/s, 100 Mbit/s or 1000 Mbit/s. The protocol is according to IEEE 802.3. Auto negotiation and auto crossover are supported.

NOTE: If the SCX2e detects an SFP in the adjacent copper-port, will be disabled! If a SFP is detected and there is no link established on the FO, the LNK-LED of the SFP will blink.

The connector is a RJ-45 plug with 2 LEDs, which indicate established Link (green LED on the left side) and the data rate (green LED, right). The pin assignment is as follows:

RJ-45	Pin	Assignment
LED:	1	BI_DA+
green	2	BI_DA-
yellow	3	BI_DB+
LNK	4	BI_DC+
ACT	5	BI_DC-
	6	BI_DB-
	7	BI_DD+
	8	BI_DD-

- The green LED (left, 'LNK') indicates the speed of the link:
 - 1x blink = 10Mbps
 - 2x blink = 100Mbps
 - 3x blink = 1000Mbps
- The yellow LED (right, ACT) indicates, when the link is established and packets are transferred.

The device is able to recognize

- a polarity inversion of the receiving signals (RD+ <--> RD-)
- a crossover of transmitting/receiving signals (RD+/RD- <--> TD+/TD-)

and corrects it automatically to ensure that the operation continues smoothly. This allows the usage of 1:1 cables in any case.

CAUTION: For access it is recommended to use twisted-pair cables of the category 5 and an impedance value of 100 Ω. The maximum cable length is 10 metres. Using cables of lower quality or different impedances may result in a restriction of the maximum cable length. In addition the employment of unshielded cables can have negative effect on the reliability of the data transmission.

100BaseFX (SFP) and 1000BaseFX (SFP)

The SCX2e offers one optical SFP port, which can be equipped with an 100BaseFX or an 1000BaseFX module according the SFP industry standard. For the interface one indicator give information on the Link state (LNK).

- The green LED ('LNK') indicate(s) that the optical link is established.
- If a SFP is detected in the SFP-slot and there is no link established, yet, the LNK-LED is blinking. This is to indicate that the copper port is disabled, as the SFP is plugged.

For copper SFPs, auto-neg 10/100/1000 is supported. Please ask arcutronix, which vendors are supported for copper SFP.

NOTE: SCX2e detects automatically, when a SFP (copper or fibre) is plugged. In this case the combo port does automatically switch off the copper part!

Alarm Connector

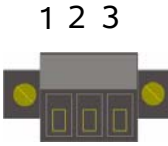


An alarm connector is used in order to indicate an alarm of the system.

NOTE: Not available on the SCX2e-WDM.

Normally a line, fan and/or power failure sets the system to alarm status. Please check manual of installed devices, which additional events can cause an alarm.

Table 3-5 shows the alarm connector settings.

Table 3-5 Pin Assignment Alarm Connector

	Normal status	Alarm status	Pin	Connect to:
			:	Normally open "NO"
			1	Centre contact
			2	Normally closed
			3	"NC"

NOTE: The contact is galvanic separated. The contact rating allows a resistive load with max. 1 A, 30 V AC/DC.

Common Indicators

‘ON’ LED

The green ‘PWR’ LED indicates that the power supply of the SCX2e is available and the DC/DC converter is operating well.

‘AGENT’ LED

The yellow ‘AGENT’ LED indicates that the SCX2e is operated in main agent mode. For future purposes it is possible to change mode into sub-agent behaviour. This is not implemented yet. So for the time being, this LED will always be on.

In case the unit is configured to reset the IP-addresses to the defaults, the AGENT-LED will blink. Blinking of the AGENT-LED is the indicator for IP-reset. See Chapter 4, **Reset IP-Address to Default** for details.

‘WARN/ERR’ LED

The red ‘WARN/ERR’ LED indicates that there is a problem on the unit. Solid on is an error state, while blinking is an alarm state indicator.

NOTE: Only when the unit is in error state, the relay will be closed.

Reset Switch

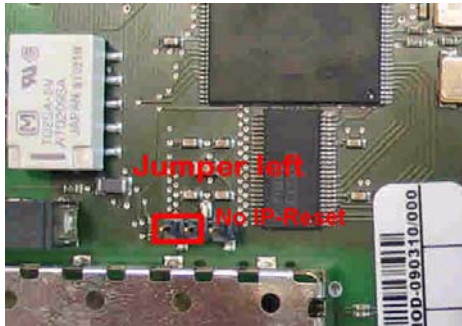
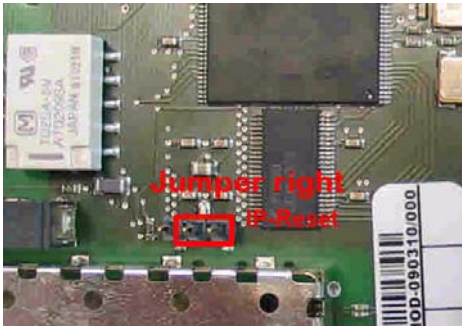
A small reset switch is placed on the top side of the unit. This switch is dedicated to reset the IP-address of the MGMT port (local management port) to the factory defaults. In case you have lost the IP-address of the unit, please reset the IP-address to enable further configuration. When the switch is closed, the AGENT-LED is blinking to indicate this special status.

The default IP-address of the MGMT port 1 is 192.168.1.100/24.

The default IP-address of the MGMT port 2 is <empty> (DHCP-client).

How to reset the addresses will be depicted in all details in Chapter 4, **Reset IP-Address to Default**.

Table 3-6 Restore IP-Settings

Normal Operation	IP-Reset
	

Chapter 4 Functionality

Agent

The task of the SCX2e as an agent in the provider's network is to provide a single management interface for configuration and maintenance of the ax system.

The SCX2e collects all information of the ax MSP (Multi Service Platform) and gives access to it by different possible protocols, which are used as northbound interface. In the same way, the SCX2e allows access to all managed objects and their change and supervision.

An agent does normally do not send any information by default, but only reacts upon request of the management system. The SCX2e can be configured to inform the management system spontaneously by sending traps to several receivers so changes and alarms can be recognized very quick.

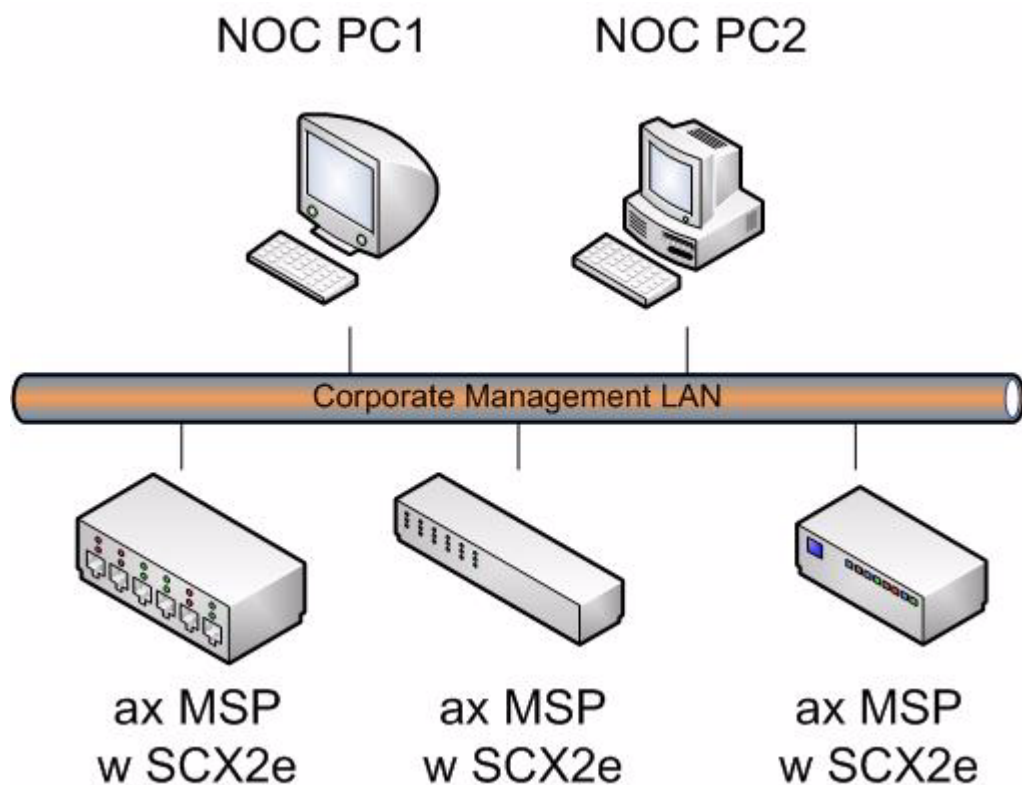


Figure 4-1 Agent Architecture

SW-Update Server for Line-Cards

The SCX2e is not only an agent but offers also the possibility to act as a hub for SW-update. It can store several different SW-files for the installed line-cards (LC) and the admin can choose time and version of a new file to be installed.

The SCX2e keeps track on the versions and which file may be valid for which LC so it is very easy to keep control. New files can easily uploaded to the file-server of SCX2e via HTTP or TFTP.

Miscellaneous Features

Auto Negotiation

Modern ethernet interfaces support a mechanism called Auto-negotiation to allow connection of ports with different capabilities. During the auto-negotiation process the common speed (10, 100 or 1000Mbps) and the duplex mode (full duplex or half duplex) are defined for the established link.

Auto-negotiation is part of IEEE 802.3, the Ethernet standard. It was first defined in 1995 as IEEE 802.3u and was an optional implementation. Unfortunately at this time the standard gave partly space for interpretation and so different implementation in older equipment can be found. In 1998 the debatable portions were eliminated and a year later the standard was extended for Gigabit-Ethernet.

In the market, there is still a lot of the older equipment, where auto-negotiation was not clear defined, so there may occur problems when devices try to do auto-negotiation. So some devices do still expect to “talk” auto-neg, even when the port’s speed and duplex mode are strictly defined by the user. For this reason, SCX2e supports to enable and/or disable the auto-neg communication, when the port’s speed or duplex mode is not really matter of negotiation but fixed by the user.

Please see table below for the possible settings and the resulting behaviour.

Table 4-1 Settings Auto-Negotiation

Setting (Port Speed)	Speed	Result	
		Duplex	Remark
Automatic	10, 100 or 1000 Mbps ⁱ	Full or Half Duplex ⁱⁱ	Full Auto-neg takes place; no limitations are given. The variable "Autonegotiation" is not changeable, but always "ON".
10 Half Duplex	10 Mbps	Half Duplex	Auto-neg communication with peer can be enabled via the "Autonegotiation" variable.
10 Full Duplex	10 Mbps	Full Duplex	Auto-neg communication with peer can be enabled via the "Autonegotiation" variable.
100 Half Duplex	100 Mbps	Half Duplex	Auto-neg communication with peer can be enabled via the "Autonegotiation" variable.
100 Full Duplex	100 Mbps	Full Duplex	Auto-neg communication with peer can be enabled via the "Autonegotiation" variable.

Table 4-1 Settings Auto-Negotiation (continued)

Setting (Port Speed)	Result		
	Speed	Duplex	Remark
1000 Half Duplex ⁱⁱ	1000 Mbps	Half Duplex	Auto-neg communication with peer can be enabled via the "Autonegotiation" variable.
1000 Full Duplex ⁱⁱ	1000 Mbps	Full Duplex	Auto-neg communication with peer can be enabled via the "Autonegotiation" variable.

i. Depending on ports capability and auto-negotiation result.

ii. Depending on auto-negotiation result. All SCX2e ports do support full duplex mode.

IP-Addressing

The SCX2e can be managed either from the "MGMT 1" and/or "MGMT 2" port. For either method a management IP-address is used and this can be freely configured. The two IP-addresses have defaults, when delivered.

Management Ports MGMT 1 & 2

The two ports are dedicated to be used for local and remote management access and the default settings are as following:

- MGMT 1
 - Default IP-address: 192.168.1.100/24
 - Default GW: empty
 - Default Mode: Act as DHCP-Server
- MGMT 2
 - Default IP-address: <empty>
 - Default GW: empty
 - Default Mode: Act as DHCP-Client

DHCP and Manual Address Assignment

The IP-address of the two management ports can be assigned by an DHCP-server or manually. If an DHCP-server is used, it must be connected to the interface. If no DHCP-server is available for this interface (or just not reachable), the unit starts with the Default IP-address of the interface (see above).

Note: We have sometimes seen problems with DHCP communication over some available USB-to-Ethernet adaptors. This problem is not related to SCX2e, but the implementation of these adaptors. Best results is reached with onboard Ethernet-ports.

After assignment of the management IP-address (via DHCP or manually) the SCX2e is reachable within the existing IP-network. It makes no difference whether the communication runs over the MGMT or LINE-IF. Of course, the LINE-IF uses a VLAN tagged communication method, whilst the MGMT uses an untagged communication method.

F- and Q-Interface

F- and Q-interface are two different behaviours of a management interface port.

The behaviour of an interface configured as “F-interface”, is defined by ITU for local access. The F-interface implementation of arcutronix does incorporate a DHCP-server, which makes it very easy to connect your laptop via Ethernet-cable. In your standard laptop configuration, it will get a valid IP-address from the SCX2e and the IP connection can be used.

Just enter “http://ax-SCX2e.mgmt.ax” into your web-browser and the web-connection is established.

NOTE: The DHCP-server can only assign one(!) IP-address, so it makes no sense to connect a complete LAN to this port, using the SCX2e as DHCP-server for the LAN!

If the interface shall be used for remote access, the proper configuration will be “Q-interface”. In Q-interface mode, the SCX2e will act as a DHCP-client and gets an IP-address via the connected network (as long as a DHCP-server is setup somewhere in the network).

DNS-Support

The Domain Name System (DNS) is a hierarchical naming system for computers, services, or any resource participating in the Internet. It associates various information with domain names assigned to such participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices world-wide. An often used analogy to explain the Domain Name System is that it serves as the “phone book” for the Internet by translating human-friendly computer hostnames into IP addresses. For example, *www.example.com* translates to *208.77.188.166*.

SCX2e does support DNS infra-structure to support easy access to the devices after IP address assignment. The SCX2e will inform the DHCP about its name (= serial number) and with this information, the DHCP server will inform the DNS about the logical name and the assigned IP-address.

An example is shown below. The SCX2e with serial number **ax12345678** has been assigned the IP-address **192.10.4.10**. A ping-command will result in the following:

```
C:\> ping ax12345678
```

```
Ping ax12345678 [192.10.4.10] with 32 bytes data:  
  
Reply from 192.10.4.10: Bytes=32 Time<1ms TTL=128  
Reply from 192.10.4.10: Bytes=32 Time<1ms TTL=128  
Reply from 192.10.4.10: Bytes=32 Time<1ms TTL=128  
Reply from 192.10.4.10: Bytes=32 Time<1ms TTL=128  
  
Ping-Statistics for 192.10.4.10:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% Loss),  
  
C:\>
```

Reset IP-Address to Default

In case the given IP-address of the SCX2e is lost or forgotten, there is a way to reset it to the factory default, so communication can start again and a new IP-address can be assigned. The reset will stop the operation of the SCX2e, but as communication is anyhow not longer possible, this is not relevant. The services (of the line-cards) are NOT effected by the reset!

In the following the 4 steps to reset the IP-address to defaults will be shown. The defaults are:

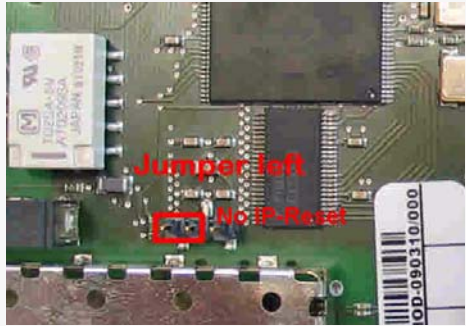
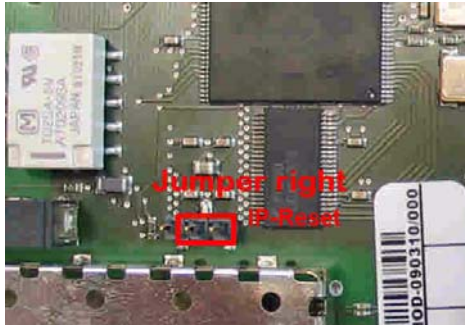
The default IP-address of the MGMT port 1 is 192.168.1.100/24.

The default IP-address of the MGMT port 2 is <empty>.

1. Place Reset-Jumper

Remove the SCX2e from the chassis and place the jumper on the reset-switch as shown:

Table 4-2 Restore IP-Settings

Normal Operation	IP-Reset
	

2. Start again and Login with Default IP-address

Plug the unit back to the chassis and let it start. After successful boot-process, the AGENT-LED will blink permanent. This is the indicator for IP-RESET-mode.

Now you can connect to the unit with the default IP-addresses and log onto the device just as before.

After login, change IP-settings of the ports as required. The new settings are stored automatically.

NOTE: After changing the IP-addresses to the new values, you might loose contact. In this case you have to re-establish communication with the new settings, if further settings are required to do.

3. Remove Reset-Jumper and Start again

To leave the IP-RESET-mode remove the unit again and remove the reset-jumper. After restart, the new settings are valid.

NOTE: If you do not remove the Reset-jumper, the SCX2e will have the default IP-addresses again after any reboot! You can see the IP-RESET-mode, when the AGENT-LED is blinking.

Alarm Management

The SCX2e does have an outstanding alarm management, which allows users to get a quick overview of the current device status, but also to get detailed information about individual alarm states. The alarms are grouped by function or hardware component, each group can be configured and acknowledged as group. Or one can navigate into the groups and configure each alarm in detail for the personal preferences.

Alarm Types

In general terms, an alarm monitors the value of a certain quantity for exceptional values. If such an exceptional value is detected, the alarm condition is said to be active. Depending on the configuration of the alarm, this may cause the alarm to become active as well.

There are two fundamentally different types of quantities that can be monitored by alarms. The first one are quantities that have a well-know set of discrete states, some of which may represent exceptional values. An example is the link state of an ethernet interface which may have the states "Link Up", "Link Down", and "Port Disabled". Here "Link Down" represents the exceptional value that causes the alarm condition to become active. Alarms that monitor these discrete-state quantities are called **digital alarms**.

The second type of quantities represent physical quantities that usually vary continuously. Here, exceptional values are defined in terms of thresholds that limit the acceptable operational range for the physical quantity. Depending on the quantity being monitored, the device checks upper and/or lower bounds for the acceptable operational range and allows to define the corresponding threshold values. An example of this type of variables is the device temperature, for which an acceptable operational range may be defined as -20°C ... 60°C. Alarms that monitor these continuously varying quantities are called **analogue alarms**.

NOTE: For analogue alarms it is possible to define the warning level at a higher value than the error level. E.g. for the temperature it is possible to define the warning @60°C and the error @55°C. This is not forbidden by the system, as there might be customer's reason to do so.

Alarm States

The state of each alarm is determined by several factors.

The first one is the **alarm condition**. The alarm condition can be unavailable which means that the quantity being monitored is not well-defined, which may occur due to the current device configuration. In case of the Ethernet interface example above, the link status is not defined if the Ethernet port is disabled by the administrator. The alarm condition can also be active or inactive, which indicates that the monitored quantity has an exceptional value or indicates normal operational conditions, respectively.

The second factor that affects the alarm state is the alarm configuration. It may affect the state of the alarm when the alarm condition becomes active, but it may also define parameters for detecting the alarm condition:

- Alarm configuration can force the alarm condition to be ignored.
- Alarm configuration can limit the severity of an active alarm.
- Alarm configuration specifies the severity with which an active digital alarm is reported.
- Alarm configuration specifies the Hold Time for an active alarm.
- Alarm configuration specifies the thresholds and hysteresis used to detect alarm conditions for analogue alarms.

The third factor that affects the alarm state is alarm acknowledgement. Once the device operator has received knowledge of the occurrence of an active alarm, he can indicate this to the ENX device by acknowledging the alarm. The ENX device will then ignore this alarm in the calculation of the global device alarm state so that newly occurring alarms will immediately be brought to the operators attention.

Given all the influences explained above, the alarm can be in one of the following states:

Not Available

This indicates that the alarm condition is not available. The alarm is always considered to be inactive in this case and the corresponding alarm state value is "n.a."

Inactive

This indicates that the alarm condition is inactive. The alarm is always considered to be inactive in this case and the corresponding alarm state value is "Ok".

Ignored

This indicates that the alarm condition is active, but the alarm condition was configured to be ignored. The alarm is always considered to be inactive in this case and the corresponding alarm state value is "Ignored".

Acknowledged

This indicates that the alarm condition is active and the alarm is not configured to be ignored. However, the device operator has acknowledged the alarm and the corresponding alarm state value is “Acknowledged”.

Warning

This indicates that the alarm condition is active and the alarm is considered to be active, having a severity of “Warning”.

This state occurs for analogue alarms if a warning threshold has been crossed, but the corresponding error threshold is not yet reached. This state occurs for digital alarms if the alarm was configured to be a “Warning” by the device administrator.

A warning level usually indicates that the device is operating close to the limits of the operational parameters and that actions should be taken to ease the situation.

Error

This indicates that the alarm condition is active and the alarm is considered to be active, having a severity of “Error”.

This state occurs for analogue alarms if an error threshold has been crossed. It occurs for digital alarms if the alarm was configured to be an “Error” by the device administrator.

An error level usually indicates that the device is operation outside of the limits of the operational parameters and that the device is no longer operating reliably.

Alarm Acknowledgement Behaviour

Any active alarm can be acknowledged by the device operator. Even though the alarm condition is still active, this has the effect of making the alarm “silent” by excluding it from the global device alarm state calculation. Informally speaking, this makes the alarm a “known problem”.

It may happen that the alarm severity changes while the alarm is acknowledged. In case of analogue alarms this may happen if an additional threshold is crossed, whereas for digital alarms it implies a configuration change. In any case, the severity of the acknowledged alarm may either increase (from “Warning” to “Error”) or decrease (from “Error” to “Warning”). Any other value (“Ignored”, “Inactive” or “Not Available”) means that the alarm becomes inactive.

The device administrator can select from three different policies that decide whether the alarm gets reactivated by the alarm severity change or remains acknowledged. This is a global setting and valid for all alarms.

Keep Acknowledged Until Inactive

This policy keeps acknowledged alarms in their acknowledged state until the alarm becomes inactive. Neither the increase nor the decrease of the alarm severity have any effect.

Unacknowledge When Raising Severity

This policy keeps the alarm acknowledged as long as “the situation gets better”. When the severity decreases from “Error” to “Warning”, the alarm remains acknowledged. However, if the situation gets worse and the alarm severity increases from “Warning” to “Error”, the alarm is reactivated and brought again to the device operators attention. This is the default behaviour.

Unacknowledge on State Change

This policy will always reactivate an acknowledged alarm whenever the alarm severity changes.

Example

The next figure displays an example, of temperature alarm and the behaviour when alarm is raised, acknowledged and raised again.

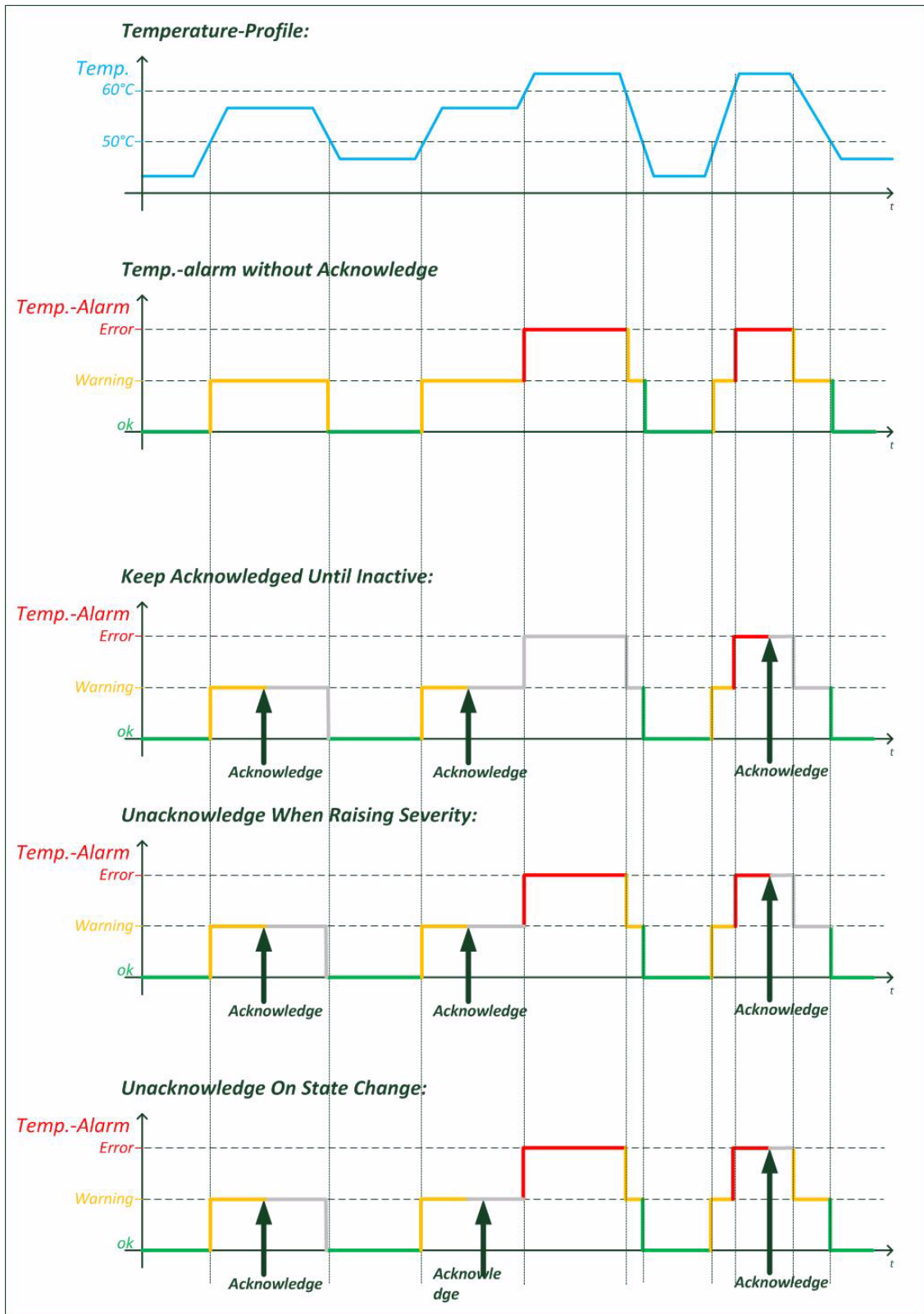


Figure 4-2 Acknowledge of Alarms

Alarm Properties

Each alarm has a certain set of properties associated with it that depends on the alarm type (analogue or digital alarm).

Common Alarm Properties

These properties are defined for both, analogue and digital alarms.

- Alarm Group: the group that the alarm belongs to (see below).
- Alarm Name: a descriptive name of the alarm.
- Alarm Value: the current value of the observed quantity.
- Alarm State: the current alarm state.
- SNMP Notification: whether to generate SNMP traps if the alarm state changes (editable).
- Hold Time: The hold time indicates the minimum time an alarm is active after rising. This is to reduce the number of alarms in a certain time-frame and to tune the system to special requirements.

Digital Alarm Properties

Digital alarms have one further property:

- Alarm Severity: the device administrator must decide for each digital alarm whether it represents an error condition, a warning condition, or an ignorable condition (editable).

Analogue Alarm Properties

Besides the common alarm properties, analogue alarms have the following properties as well:

- Overrun Warning Threshold: If the physical quantity has a meaningful upper limit for its operational range, the threshold above which the alarm becomes active with "Warning" severity (editable).
- Overrun Error Threshold: If the physical quantity has a meaningful upper limit for its operational range, the threshold above which the alarm becomes active with "Error" severity (editable).
- Underrun Warning Threshold: If the physical quantity has a meaningful lower limit for its operational range, the threshold below which the alarm becomes active with "Warning" severity (editable).
- Underrun Error Threshold: If the physical quantity has a meaningful lower limit for its operational range, the threshold below which the alarm becomes active with "Error" severity (editable).
- Hysteresis: A hysteresis applied to threshold values when checking whether an active alarm condition is cleared (editable).

Alarm Groups

Due to the large number of alarms already defined, the alarms are divided into a number of different alarm groups. These alarm groups serve multiple purposes:

- Logical subdivision of alarms for a better overview.
 - Alarms are grouped by function or hardware component they refer to (e.g. “System Alarms” for general device management alarms, “Clock Alarms” for SyncE and PTP-related alarms, ...)
- Alarm status summary.
 - The alarm group keeps track of the most severe alarm state of any alarm in the group and provides the current number of alarms that are ignored, acknowledged, or are active with “Warning” or “Error” severity.
- Easy acknowledgement of multiple alarms.
 - All alarms within an alarm groups can be acknowledged with a single action.
- Limiting the alarm severity of multiple alarms.
 - The alarm group defines a maximum alarm severity setting that overrides the alarm severity of all alarms in the alarm group.

Global Alarm Status

The SCX2e device provides a summary of all alarms. Besides showing the number of acknowledged alarm and active alarms with “Warning” or “Error” severity, the global (overall) alarm status keeps track of the maximum severity of any active alarm. Furthermore, the global alarm status is reflected by the ALM-LED on the front panel of the device and the alarm relay.

The ALM-LED will be turned on if the global alarm state is “Error”, it will blink if the global alarm state is “Warning” and be turned off otherwise.

The alarm relay will be activated if the global alarm state is “Error” and be deactivated otherwise.

Chapter 5

SCX2e Web-OPI

The SCX2e can be configured via a html-based Web-OPI (Operator Interface). Just a standard web-browser is needed and an IP-connection to the device. This chapter will explain how to connect to the Web-OPI and its usage.

Access to the Device

The SCX2e Web-OPI can be accessed via the both management ports (called “MGMT1” and “MGMT2” interface). Both interfaces use different IP-addresses, but the behaviour and the usage from html-point of view is just the same.

Local Management Interface

The Web-OPI ports on the front panel can be used to have local or remote management access (F- and Q-interface). The Web-OPI ports offer plain TCP/IP connection, no VLAN is expected to be seen here.

As the Web-OPI “MGMT1” port act as a DHCP-server by default (F-interface mode), just connect your PC/Laptop to this interface. If your PC/Laptop is configured to use “Automatic IP-address”, which is standard today, it will be configured correct and management access can start immediately.

Just enter

```
http://192.168.1.100 or  
http://ax-SCX2e.mgmt.ax
```

in the web-browsers address field and the login screen will appear.

Security Issues

The Web-OPI is accessible via any TCP/IP link to the device, so it might be that other persons than the intended ones get connection and will see the login screen. To avoid forbidden configuration or burglary of information, the access is protected against intruders via username and password.

Any time you connect or reconnect to the initialized SCX2e the login-window is displayed and a password request turns up on the terminal.

Be careful with passwords! If you write them down, keep them in a safe place. Do not choose strings easy to hack. In particular, do not use the default strings which were valid when you received the device.

Do not forget your password. If you forget your password the device will be rendered useless and will have to be sent back to the factory for basic re-configuration.

NOTE: Three different access-level are selectable with different access rights:

1. Guest (only view)
2. User (view and modify)
3. Admin (full access inclusive user administration)

If the device is started-up the very first time, only the user “admin” is defined. See in “User and Access Administration” on page 5-13, how to define the other users and how to change the user password.

Login Screen

After a management connection has been established towards the SCX2e, the login screen is displayed. The management software may be accessed by the user with different access levels (see “Security Issues” on page 5-1).

The Login screen is shown in the figure below. The user selects his login level from the following menu by entering the corresponding user name and password.

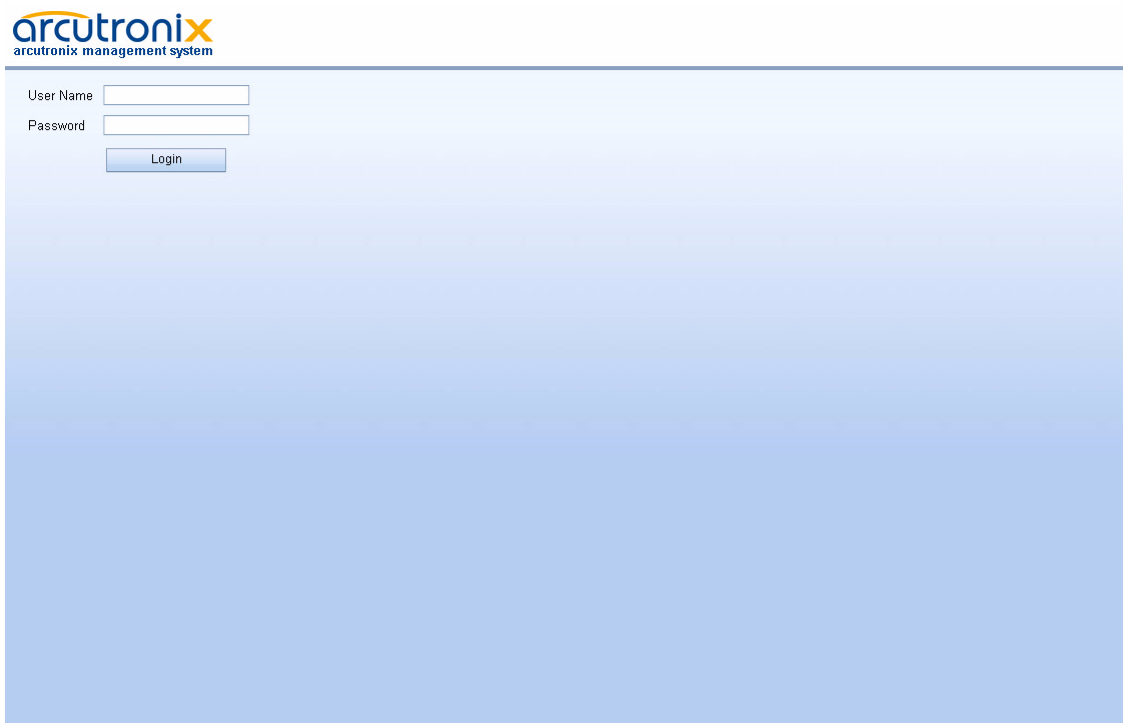


Figure 5-1 Login Screen

A user name and a valid password have to be entered before access to configuration parameters is granted. The default user name and password are as follows:

User: admin
Password: private

CAUTION: It is strongly advised to change these passwords in the USER ADMINISTRATION menu after the first login.

If the device is started-up the very first time, the only user 'admin' is defined with the password 'private', which should be changed immediately after login. The password is not displayed, each character is replaced by an asterisk (*). An error message will be displayed for any unsuccessful login (the application continues with the login menu).

NOTE: Be careful, when typing user and password. The Web-OPI is case-sensitive.

Web-OPI's Body

After Login, the SCX2e Web-OPI is seen in its full glance. The Web-OPI is designed according the latest rules for web-based GUIs and you will find it very easy to navigate.

The Web-OPI's body is divided in 5 major parts, which are shown in the next figure and will be explained a little bit after this.

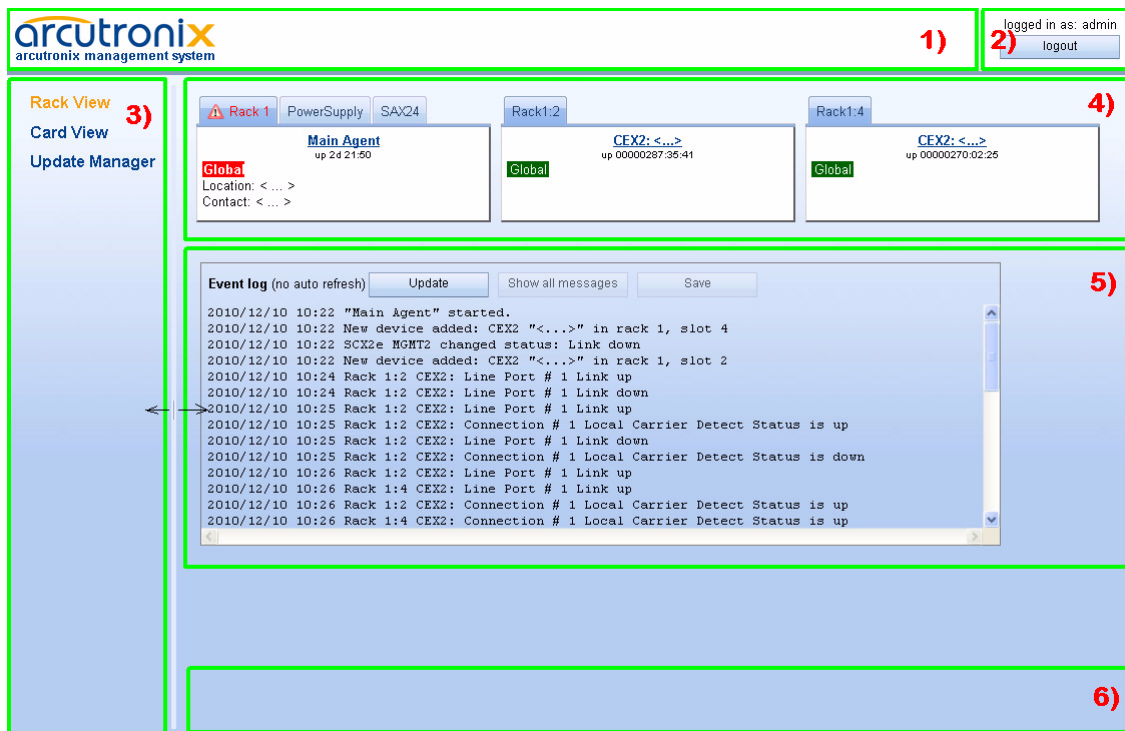


Figure 5-2 Web-OPI's Appearance

1. Logo and Name Area.
2. Login-Area: Info, who is logged in and a button for Logout.
3. Explorer Bar: Navigating in the Web-OPI is easy with the Explorer-Bar. The settings are grouped in different categories, which can be exploded and collapsed.
4. Main-Area: This is the area, where all the information is listed and the configuration can be changed and adopted. The next chapter will mainly handle the settings in the Main-Area.
5. Alarm-Table: Summary of all events and alarms.
6. Info-Bar: Here status and error-messages are shown.

Navigation

The Web-OPI is a graphic user menu. The best way to navigate between the different pages is to use your mouse. Open and collapse the menus in the Explorer-Bar (see above) and select the page, you want to see and/or edit.

Select a menu entry

When you move the mouse-pointer over the explorer-bar, you can see the pointer change its face: When you move the pointer over a selectable item, it will look like a this:



, if there is no selectable value, it is standard (normally arrow):



When you want to open or select the given entry, press the left button on your mouse to complete the selection.

The selected menu-entry is displayed in orange-coloured text, while all the others are marked blue (see Figure 5-2).

In some cases, you will find lists to select an entry. Use also the mouse-pointer to navigate in these list. Press Enter, when the right entry is highlighted to select it.

Page Update

To update the actual menu, just use your browser's reload button.

Logout

Use the Logout-Button to terminate the session and leave the unit. Never forget to log-out, as otherwise unauthorized persons could get access to the unit and damage your services.

The auto-logout feature adds additional security in case the regular logout has been forgotten.

Rack View

After the login, the Rack-View will be displayed, which provides a general overview of the ax MSP rack, where the SCX2e is plugged.

All discovered cards and their actual status are shown as overview with short information like serial number, user's given name, slot-ID and up-time.

Move the mouse over one of the shown cards and you can enter the Card-View of the device.






The screenshot shows the Arcutronix management system interface. The top left features the Arcutronix logo and the text 'arcutronix management system'. The top right shows 'logged in as: adm' and a 'logout' button. The main interface is divided into a sidebar on the left with 'Rack View', 'Card View', and 'Update Manager' options. The central area displays three rack views: 'Rack 1' (PowerSupply) with a 'Global' status icon, 'Rack 1.1' (FCX10G: FCX10G-Vodafone) with a 'Global' status icon, and 'Rack 1.2' (CSX4: <...>) with a 'Global' status icon. Below these, 'Rack 1.10' (EDX1008: <...>) is shown with a 'Global' status icon. At the bottom, an 'Event log' window displays a list of system events with timestamps and descriptions, such as 'Web login from 192.168.1.154: admin (admin)' and 'New device added: EDX1008 <...> in rack 1, slot 10'.

Figure 5-3 Rack-View

Symbols of the Rack View

Each plugged module (line-card etc.) in the sub-rack does have an rectangular diagram in the rack-view. On top of the diagram one or more flags are seen to indicate that this diagram contains more information. The flag shows the status of the card in a small icon. If there is no icon to see, all is fine and the card is working without any problems.

Table 5-1 Status-Symbols

Symbol	Prio	Meaning
none (empty)	0	Everything is fine. No problems detected.
	4	Alarm-Symbol. The device has detected at least one active alarm.
	2	Alarm-Acknowledged Symbol. The device has at least one alarm, which is already acknowledged by user.
	3	Warning-Symbol. The device has detected at least one active warning.
	1	Warning-Acknowledged Symbol. The device has at least one alarm, which is already acknowledged by user.
	5	Removed-Symbol. The device was removed or fails. If the device shall be removed permanently, please delete the diagram from rack-view.

As there can be only one symbol at the time, there is a priority. Depending on the priority of the event, the symbol with the highest priority is shown. This starts with the "Removed" and ends up with none-symbol, which indicates All-Good.

Card View SCX2e

To enter the card view of one of the discovered devices just select this device in the Rack-View or in the Explorer-Bar. The cards individual menu appears. As all cards do have different appearance, not all of them can be shown in detail here. Only the SCX2e will be depicted here after.

The main Card-View is displayed, which provides a general overview of the menu structure.

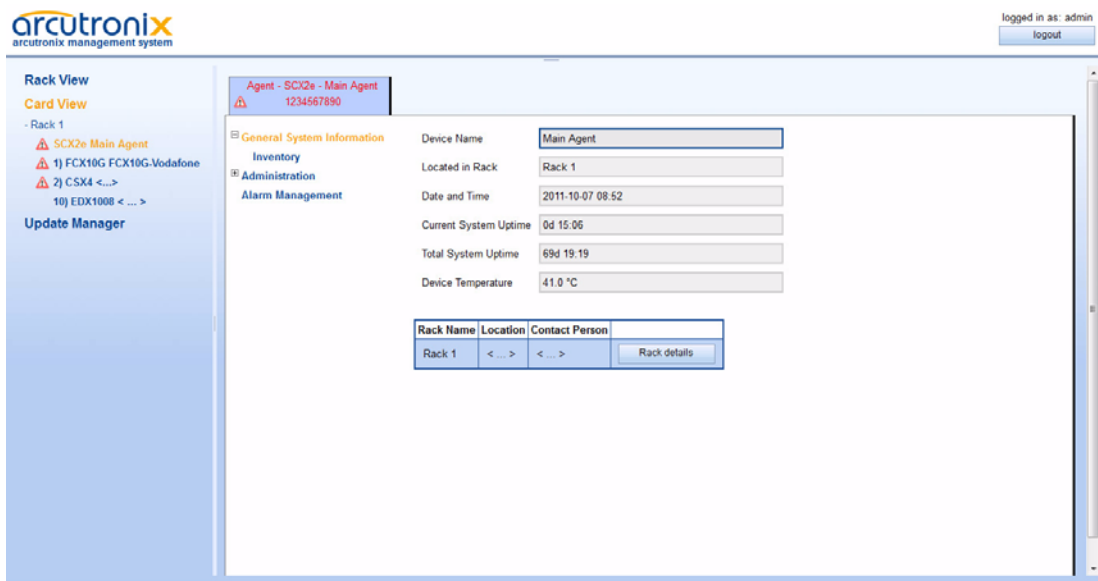


Figure 5-4 Card-View SCX2e

Select a menu line in the “Explorer-Bar” to open the selected submenu or to logout from the SCX2e’ Web-OPI.

Table 5-2 provides information on the menu.

Table 5-2 SCX2e Menu

Parameter	Description	Format	Default
General System Information	Set and get global static information.	Menu	
Administration	Configuration of global parameters.	Menu	
Alarm Management	Configuration of alarm handling.	Menu	

General System Information

Select “General System Information” to access the General System Information. The following will be displayed:

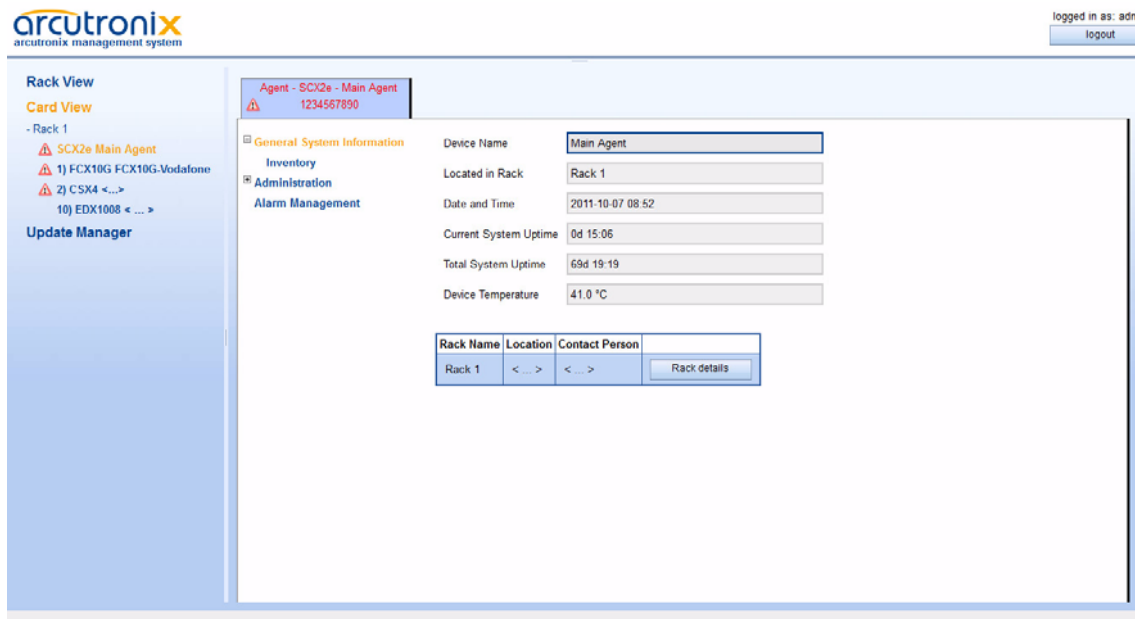


Figure 5-5 General System Information

This menu contains the general system information of the SCX2e device and system. Table 5-3 provides information on the menu.

Table 5-3 General System Information Menu

Parameter	Description	Format	Default
Device Name	Description/comment of the device/application.	Display/Input (up to 32 characters)	< ... >
Located in Rack	Present device location.	Display	no default
Date and Time	The current date and time of the device. Press on the time-value and a drop-down menu is shown to select the time.	Display	no default
Current System Uptime	The time since the last system reboot.	Display	no default
Total System Uptime	Overall sum of system uptime.	Display	no default
Device Temperature	Measured temperature on SCX2e in Celsius.	Display	no default

Table 5-3 General System Information Menu (continued)

Parameter	Description	Format	Default
Rack Details	Opens a new menu to enter the rack's details like location, contact person etc.	Menu	
Inventory	Opens the Inventory menu.	Menu	

Rack Details

Selecting “Rack Details” leads to the details menu, which provides information on the rack. The values can be changed to make identification more easy.

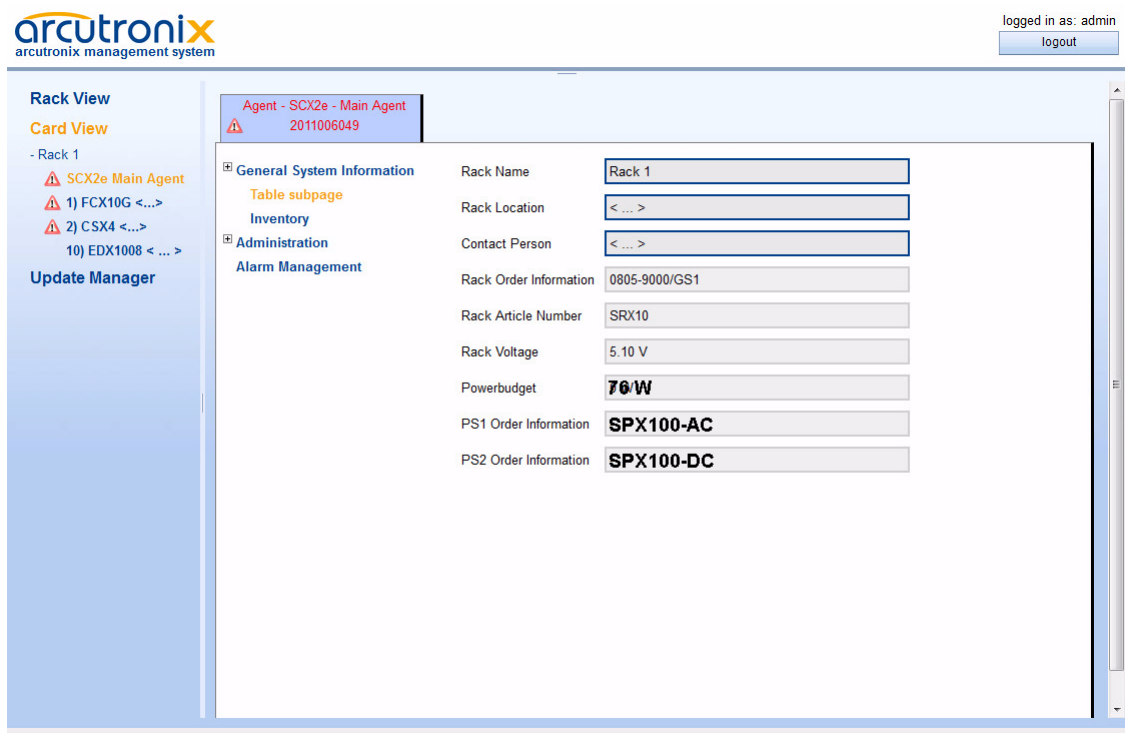


Figure 5-6 Rack Details

This menu contains the general system information of the SCX2e device and system. Table 5-3 provides information on the menu.

Table 5-4 Rack Details Menu

Parameter	Description	Format	Default
Rack Name	Description/comment of the rack.	Display/Input (up to 32 characters)	Rack1
Rack Location	Description/comment of the rack.	Display/Input (up to 32 characters)	< ... >
Contact Person	Description/comment of the rack.	Display/Input (up to 32 characters)	< ... >
Rack Order Information	Details about the rack's order code.	Display	Depending on used Rack.
Rack Article Number	Details about the rack's order code.	Display	Depending on used Rack.
Rack Voltage	The measured value of the power bus on the backplane.	Display	no default
Power Budget	The calculated power budget. This depends on the used power supplies and the number and type of plugged cards.	Display	no default
PS1 Order Information	Details about the power supply, plugged in PS-slot1.	Display	Depending on used PS.
PS2 Order Information	Details about the power supply, plugged in PS-slot2.	Display	Depending on used PS.

Inventory

Selecting "Inventory" leads to the Inventory menu, which provides information on the device. These are factory settings which can only be read.

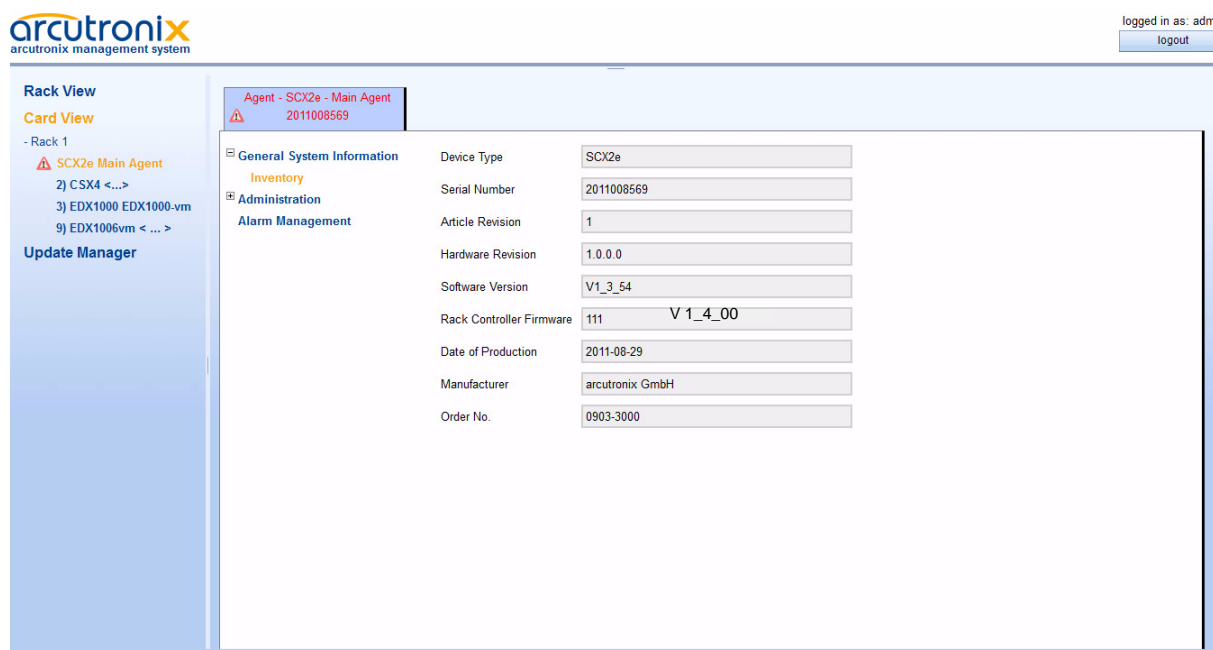


Figure 5-7 Inventory

Table 5-5 provides information about the content.

Table 5-5 Inventory Menu

Parameter	Description	Format	Default
Device Type	Indicates the device type.	Display	SCX2e
Serial Number	Serial number of the device.	Display	Depends on the factory settings
Article Revision	The release number of the device.	Display	Depends on the factory settings
Hardware Version	Revision of the loaded system software.	Display	Depends on the hardware
Software Version	Revision of the loaded system software.	Display	Depends on the loaded software
Rack Controller Firmware	Revision of the installed RC-FW.	Display	Depends on the loaded firmware
Date of Production	Date of the device's production.	Display	Depends on the factory settings

Table 5-5 Inventory Menu (continued)

Parameter	Description	Format	Default
Manufacturer	Manufacturer of the Device (normally arcutronix GmbH).	Display	arcutronix GmbH
Order Number	Order information for the device.	Display	Depends on the device's type. See Order Matrix (Table 1-1 on page 1-2).

Administration

Select "Administration" in the Explorer bar and the Administration menu will be displayed. This menu allows to configure the general device settings.

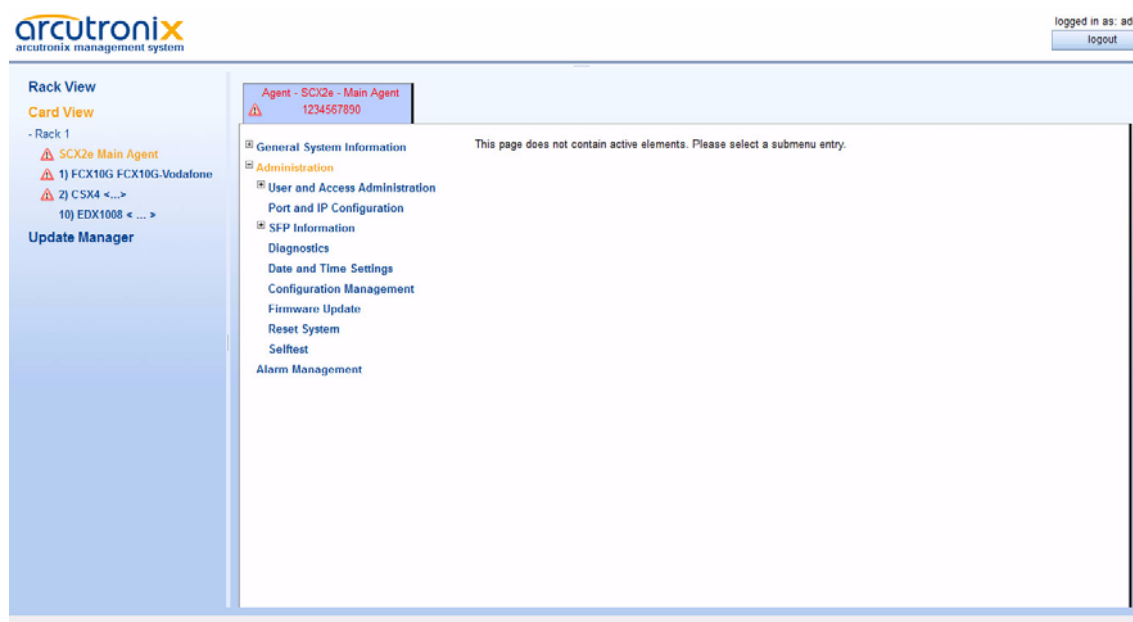


Figure 5-8 Administration

Table 5-6 provides information on the menu.

Table 5-6 Administration Menu

Parameter	Description	Format	Default
User and Access Administration	Administration of users, access levels and passwords.	Menu	
Port and IP Configuration	Configuration of the Ethernet interfaces ("MGMT"-ports).	Menu	
SFP Information	If a SFP is plugged in port 2, the SFP vendor information is displayed.	Menu	
Diagnostics	Ping a remote IP-address to verify the IP settings and proper infra-structure.	Menu	
Date and Time Settings	Configure system date and time.	Menu/Display	displays actual time and date
Configuration Management	Store and Recall configurations.	Menu	
Firmware Update	Update of SCX2e software and firmware.	Menu	
Reset System	Opens the Reset System menu.	Menu/Display	No reset scheduled
Selftest	Start the self-test of the unit.	Menu	

User and Access Administration

Select "Access Administration" in the Administration menu and press the Enter key. The Access Administration menu will be displayed:

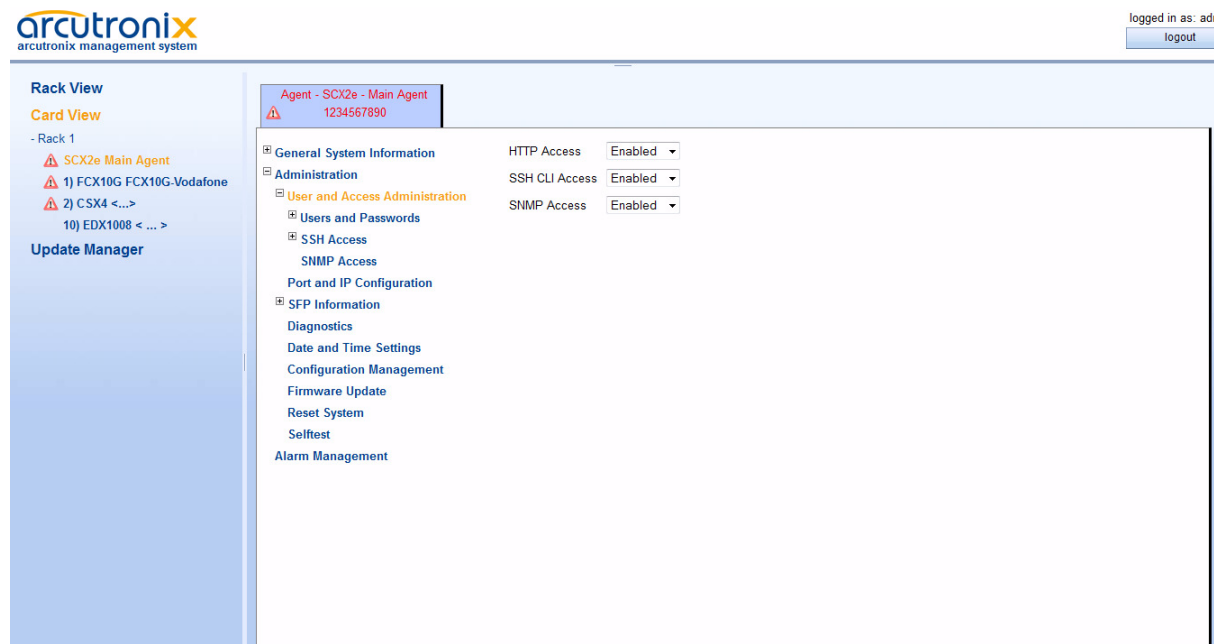


Figure 5-9 User and Access Administration

The menu gives a quick overview and configuration option for the different ways of access to the unit. Three entries can be seen for the varying access methods. Each of them can be disabled and enabled individually.

NOTE: At least one access method **MUST** be enabled! If you want to disable the last one, this will be prohibited. A window will pop up to inform you.

Table 5-7 provides all information on the menu.

Table 5-7 User Administration Menu

Parameter	Description	Format	Default
HTTP Access	Enable or Disable the management access via HTTP (Web-GUI).	PullDown-Menu <ul style="list-style-type: none"> • Disabled • Enabled 	Enabled
SSH CLI Access	Enable or Disable the management access via SSH.	PullDown-Menu <ul style="list-style-type: none"> • Disabled • Enabled 	Enabled
SNMP Access	Enable or Disable the management access via SNMP.	PullDown-Menu <ul style="list-style-type: none"> • Disabled • Enabled 	Enabled
Users and Passwords	Configuration of user- names and passwords.	Menu	

Table 5-7 User Administration Menu (continued)

Parameter	Description	Format	Default
SSH Access	Configuration of the ssh-access to the unit.	Menu	Enabled
SNMP Access	Configuration of the SNMP access to the device.	Menu/Display	Enabled

Users and Passwords

This menu gives the administrator the capability to add/remove users and change their passwords if necessary. The maximum number of possible users defined for SCX2e is 99.

On top of the page is a list with all configured users and their read- and write-authorization. Each user’s account can be disabled, if this is temporarily required. To delete a configured user-account for ever, just use the delete button.

Note: The Default user “admin” can not be deleted.

The list has only one entry after first start-up and/or “Load Default Cfg”. This entry is the user “admin”.

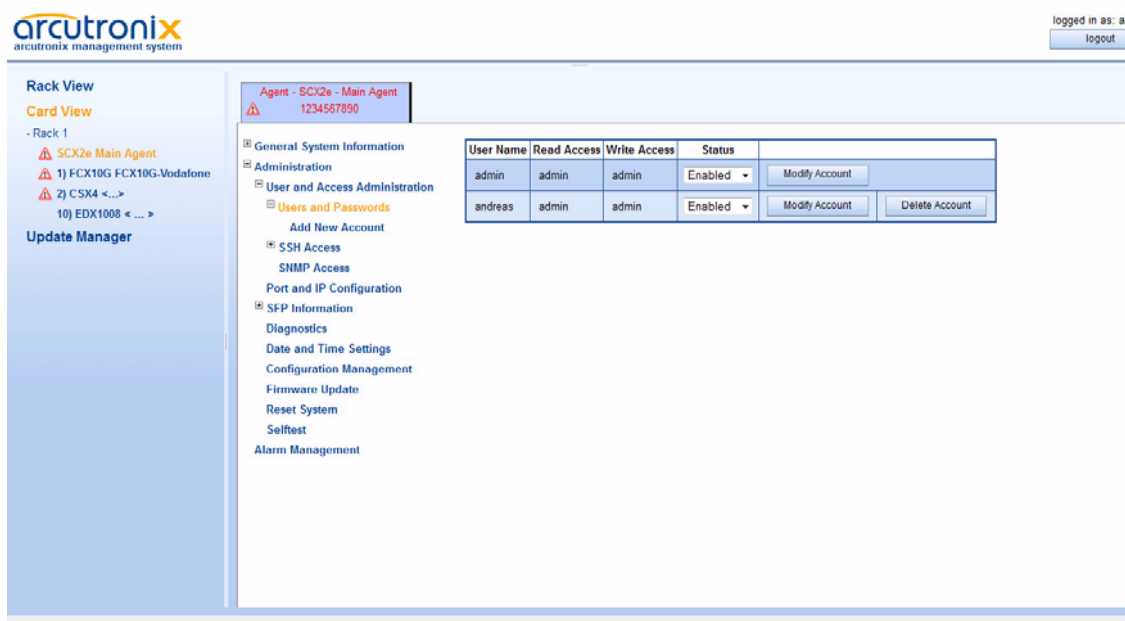


Figure 5-10 Users and Passwords

Table 5-8 provides information on the menu.

Table 5-8 Users and Passwords Menu

Parameter	Description	Format	Default
Add New Account	Add an user account.	Menu	
Delete Account	Select an user of the list and click on the button. After this confirm the action.	Select Button/Confirm	
Modify Account	Select an user of the list and click on the button. After this the Modify Account menu opens.	Select Button / Menu	

Add New Account

Select “Add New Account” in the explorer bar. The following menu will be displayed:

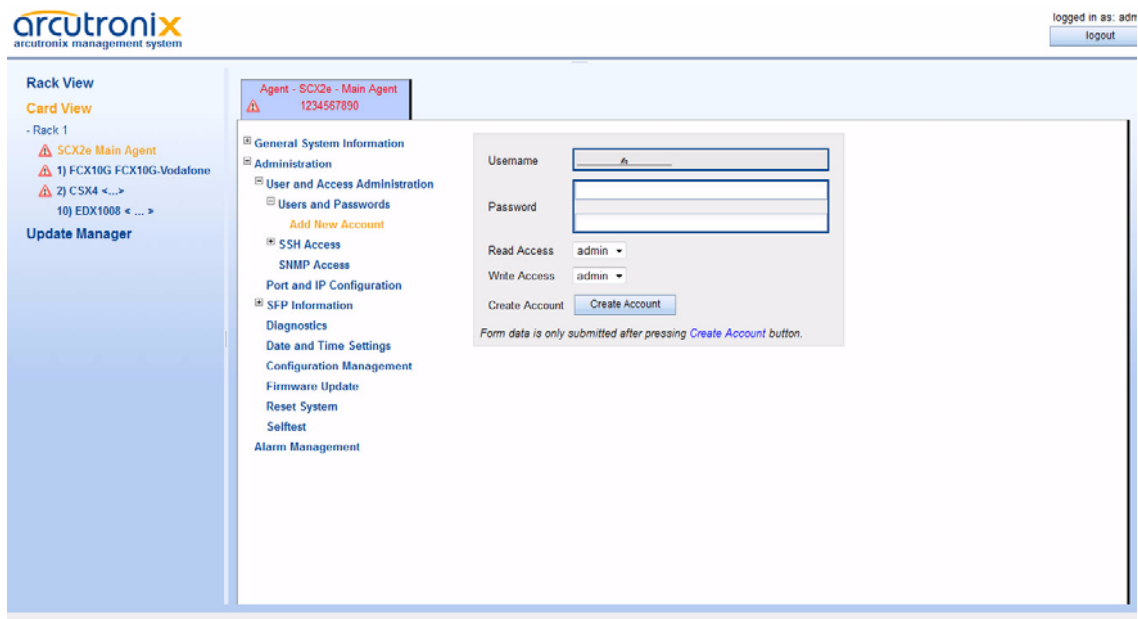


Figure 5-11 Add Account

Table 5-9 provides information on the menu.

Table 5-9 Add Account Menu

Parameter	Description	Format	Default
Username ⁱ	Enter name of new user.	Display/Input	< ... >
Password ⁱⁱ	Definition of a new password.	Input	no default
Retype Password	Retype field for the new chosen password.	Input	no default
Read Access	The read access level is allocated.	PullDownMenu <ul style="list-style-type: none"> • admin • user • guest 	Unknown
Write Access	The write access level is allocated.	PullDownMenu <ul style="list-style-type: none"> • admin • user • guest 	Unknown
Create Account	Press button to confirm new user data. See in the bottom row, whether the creation was successful.	Confirm Button	

i. The user name must consist of less than 33 characters (<=32). The following characters are allowed: '0-9', 'a-z', 'A-Z', ' _'.

ii. The password must consist of more than 4 and less than 16 characters (5<= n <=15). The following characters are allowed: '0-9', 'a-z', 'A-Z', ' _'.

Note: The maximum number of different users is 99.

Note: You can check, whether the operation succeeded in the Chapter 5, Users and Passwords Menu (page 5-15). There you can see all created users and their read- and write-permissions.

Modify Account

Select “Modify Account” of one of the users in the list for modification. Any member of the user-group “admin” may change the selected accounts membership in a user-group. E.g. change the account “test” to be in user-group “user” instead of “guest”.

To change the user’s password, the user must be logged in to the system. It is not possible to change any user’S password but by the user itself!

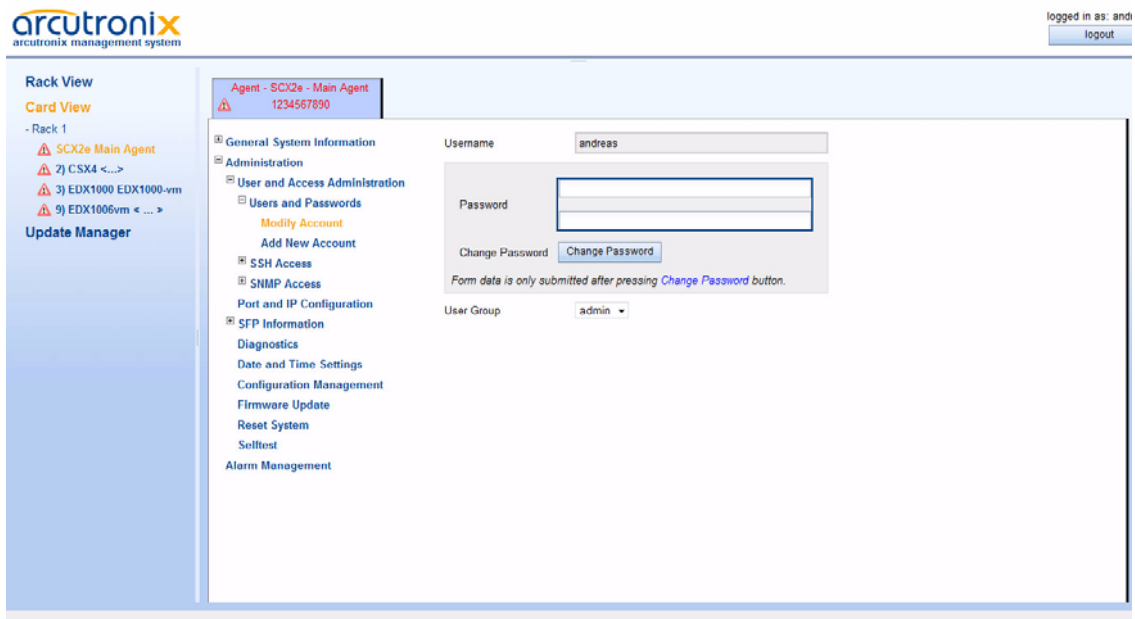
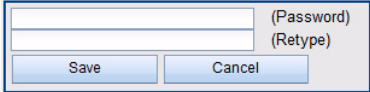
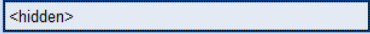


Figure 5-12 Modify Account

Table 5-10 provides information on the menu.

Table 5-10 Change Password

Parameter	Description	Format	Default
Username	User's name.	Display	no default
New Password ⁱ	The user's password. The password must be entered twice for verification. Please retype it in the bottom field:	Input	no default
			
	<p>If a valid password is stored on the device, it will be shown as <hidden> to avoid phishing:</p> 		
User Group ⁱⁱ	The new read/write access level be allocated.	PullDownMenu	old value
		<ul style="list-style-type: none"> • admin • user • guest 	

i. Only visible, if the logged-in user is the same as the selected one modifying.

ii. Only visible, when the selected account is NOT the default ADMIN-account.

NOTE: If a user has forgotten its password, nobody can reset it to any default. In this case, the user’s account must be deleted and re-added with (new) password.

Delete Account

Any listed user may be deleted by “admin” user-group. If the button “Delete Account” is pressed, a verification window is opened for security reasons.

SSH Access

This menu offers the possibility to configure the SSH settings, like passwords and keys. If required by the user, the SSH access can be disabled at all, to avoid illegal access to the device. In factory default, the SSH access is enabled.

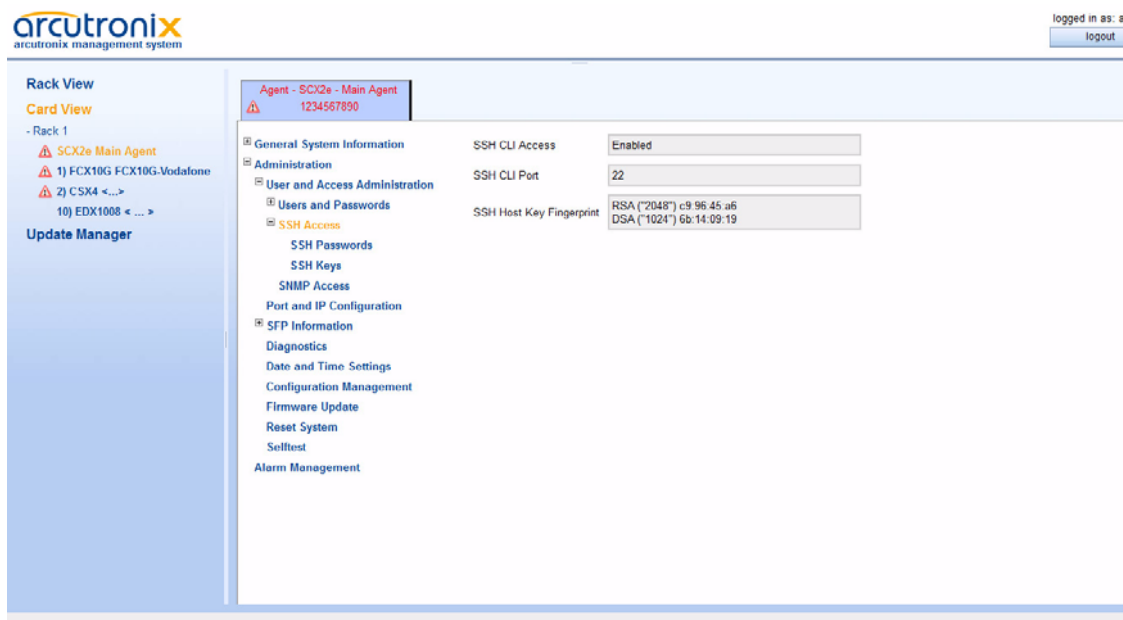


Figure 5-13 SSH Access

Table 5-11 provides information on the menu.

Table 5-11 SSH Access

Parameter	Description	Format	Default
SSH Access	Indicator, whether the SSH access is enabled or disabled. The setting can be changed in the higher level.	Display	Enabled
SSH CLI port	TCP port for SSH communication. standard value defined by IANA is 22. Note: The value can only be changed, when the SSH-access is disabled.	Port-Number	22
SSH Host Key Fingerprint	Value of the RSA and DSA key. Only the first 4 words are given. A new key can be added in the menu "SSH Keys".	Display	
SSH Passwords	Sub-Menu to select the way how to authenticate at the SSH server (SCX2e). For details on the possible options see Chapter 7, SSH and CLI.	Sub-Menu	
SSH Key	Sub-Menu to upload a public SSH key if available.	Sub-Menu	

SSH Passwords

This menu offers the possibility to configure the SSH passwords. Three possible ways of authentication are foreseen:

- Disable the usage of passwords for SSH access.
- Use the same users and passwords are configured for the Web-OPI access (see chapter "Users and Passwords" on page 5-15.
- Use a special global SSH-connection password, which can be configured here, when this option is selected.

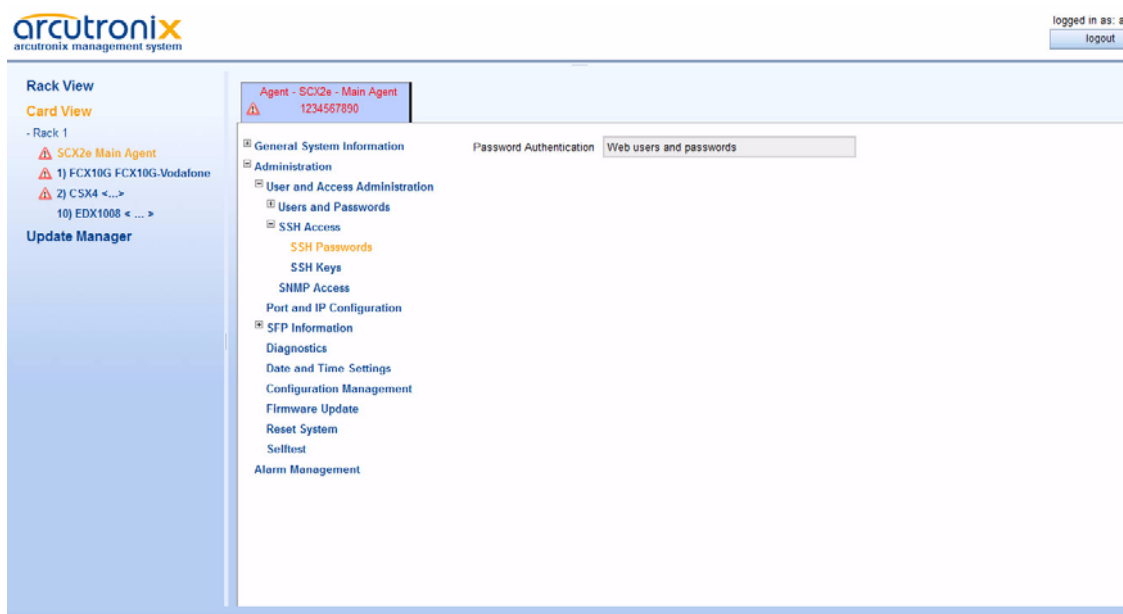


Figure 5-14 SSH Password

Table 5-12 provides information about the menu.

Table 5-12 SSH User Definition

Parameter	Description	Format	Default
Password Authentication	<p>Pulldown Menu to select the how to authenticate at the SSH server (SCX2e).</p> <p>For details on the possible options see Chapter 7, SSH and CLI.</p> <p>Note: The value can only be changed, when the SSH-access is disabled.</p>	<p>PullDown Menu</p> <ul style="list-style-type: none"> • "Password authentication disabled" • "Web users and passwords" • "Use global SSH connection password" 	"Web users and passwords"
Global Access Password	<p>Here one can define a global ssh-user(name) and his global ssh-password. Define this, when "Use global SSH connection password" is selected in the line above.</p>	<ul style="list-style-type: none"> • 1st row: Username (e.g. "ssh-admin") • 2nd row: Password (e.g. "ssh-private") 	empty

SSH Keys

This menu offers the possibility to upload a SSH key via file-transfer. The file with the ssh-key can be selected via explorer window and then uploaded to be stored on the device.

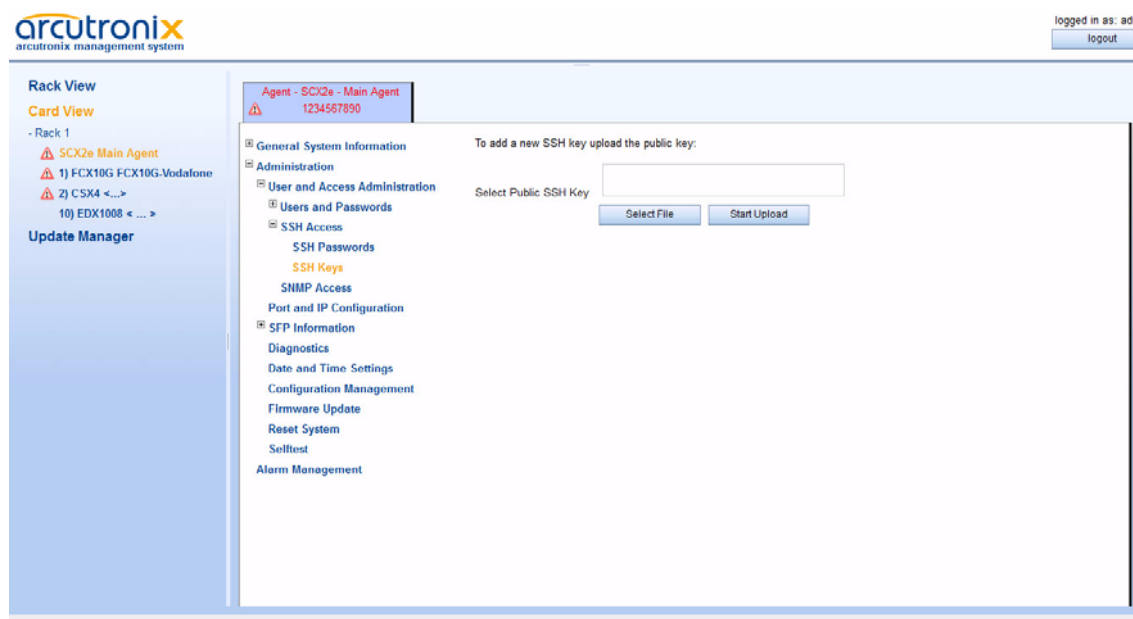


Figure 5-15 SSH Password

SNMP Access

This menu offers the possibility to configure the SNMP settings, like communities and trap-receivers. If required by the user, the SNMP access can be disabled at all, to avoid illegal access to the device. In factory default, the SNMP access is disabled.

The configuration of SNMP security parameters and SNMP trap receivers can be done two ways with differing complexity, either via Web GUI/CLI or via SNMP. By default, configuration of these parameters via Web GUI/CLI is active. Both configuration modes are mutually exclusive, e.g. when Web/CLI configuration is enabled, the same parameters cannot be changed via SNMP and vice versa.

It is assumed that the reader is familiar with the configuration of SNMP security parameters and SNMP trap receivers.

WARNING: When switching from Web/CLI based configuration of SNMP security parameters and SNMP trap receivers to SNMP based configuration, the device only accepts access by SNMPv2 communities or SNMPv3 users that have previously been configured via Web/CLI. It is important that at least one SNMPv2 community or one SNMPv3 user have been added so that initial access to the device via SNMP is possible for further configuration.

WARNING: When switching from SNMP based configuration of SNMP security parameters and SNMP trap receivers to Web/CLI based configuration, all SNMPv2 community settings, SNMPv3 user settings and SNMP trap receiver settings are lost and need to be re-configured using the Web/CLI interface.

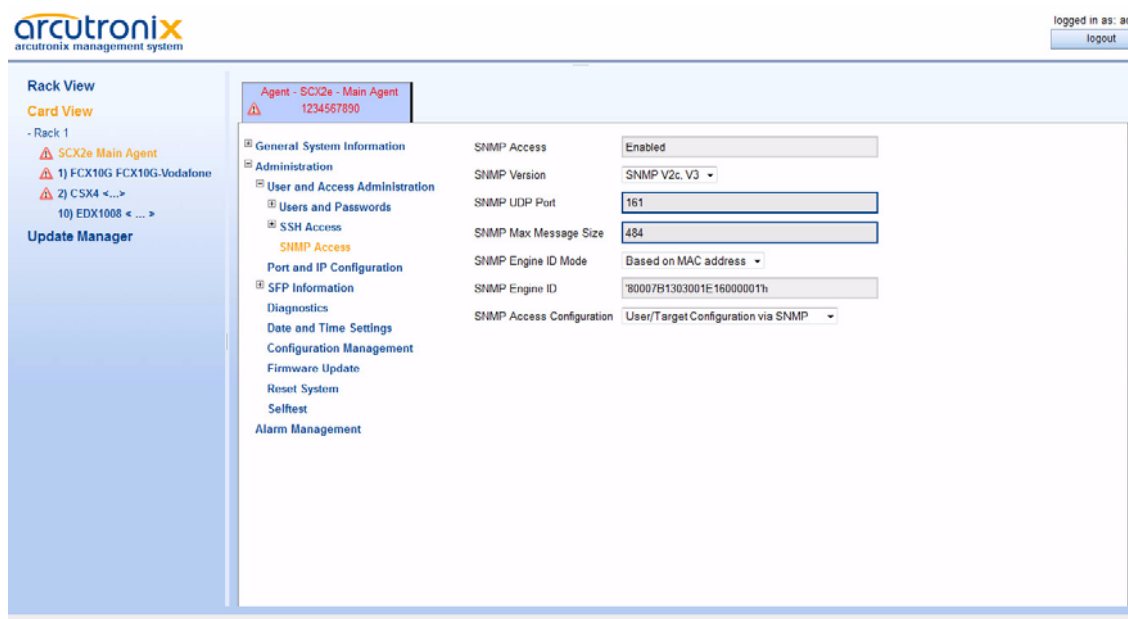


Figure 5-16 SNMP Access, SNMP enabled

Table 5-13 provides information on the menu.

Table 5-13 SNMP Access Menu

Parameter	Description	Format	Default
SNMP Access	Indicator, whether the SNMP access is enabled or disabled. The setting can be changed in the higher level.	Display	Enabled
SNMP Version	Select the SNMP version to be used	PullDown Menu <ul style="list-style-type: none"> • SNMP v2c • SNMPv3 • SNMPv2c & v3 	SNMPv2c & v3
SNMP UDP Port	Enter the UDP-Port to be used for SNMP-Traps. (1-65535)	Port-Number	161
SNMP Max Message Size	Maximum numbers of data transferred within a get-bulk request.	Integer	484

Table 5-13 *SNMP Access Menu (continued)*

Parameter	Description	Format	Default
SNMP Engine ID Mode	Select, how the SNMP Engine ID is assigned.	PullDown Menu <ul style="list-style-type: none"> Automatically Based on MAC Address Bases on sysName 	Based on MAC Address
SNMP Engine ID	The local engine ID is defined as the administratively unique identifier of an SNMPv3 engine, and is used for identification, not for addressing.	Engine ID	
SNMP Access Configuration	Defines how to perform detailed SNMP configuration.	PullDown Menu <ul style="list-style-type: none"> User/Target Configuration via Web/CLI User/Target Configuration via SNMP 	User/Target Configuration via Web/CLI
SNMP Users	Add, change and delete the communities and the related access levels.	Menu	
SNMP Traps	Add, change and delete the Trap receivers.	Menu	

NOTE: SNMP is based on IP based data transmission. Make sure the IP configuration is correct and a Default-GW is defined.

SNMP Users and Community Configuration Menu

This menu lists the defined SNMP community strings (SNMP v2c) or SNMP users (SNMP v3) and allows to add, change and delete these settings. Each SNMP community/user can be assigned with an access level, which grants rights for set- and/or get-commands.

Select the v2c-community or v3-users in the explorer bar. If there are not both protocols defined, only the selected one is displayed.

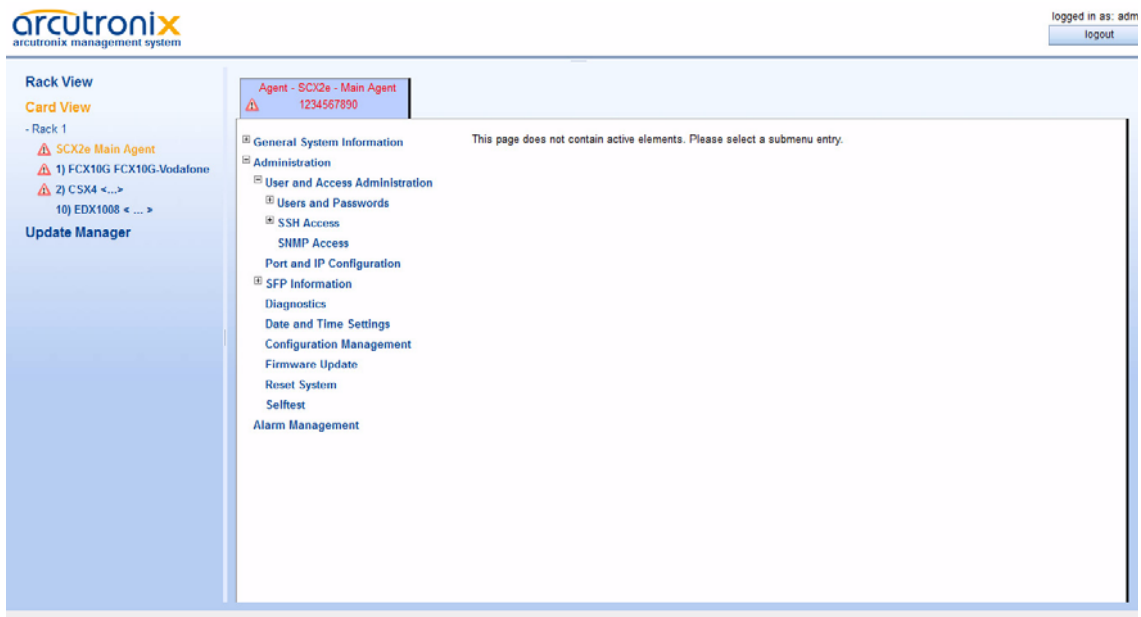


Figure 5-17 SNMP Users and Community

SNMP V2 Communities

This page shows all currently known SNMPv2 communities along with their access permissions, provided that Web/CLI based configuration of security parameters is enabled. Known communities can be enabled, disabled or deleted, new SNMPv2 community strings can be added using the “Add Community” button below the list.

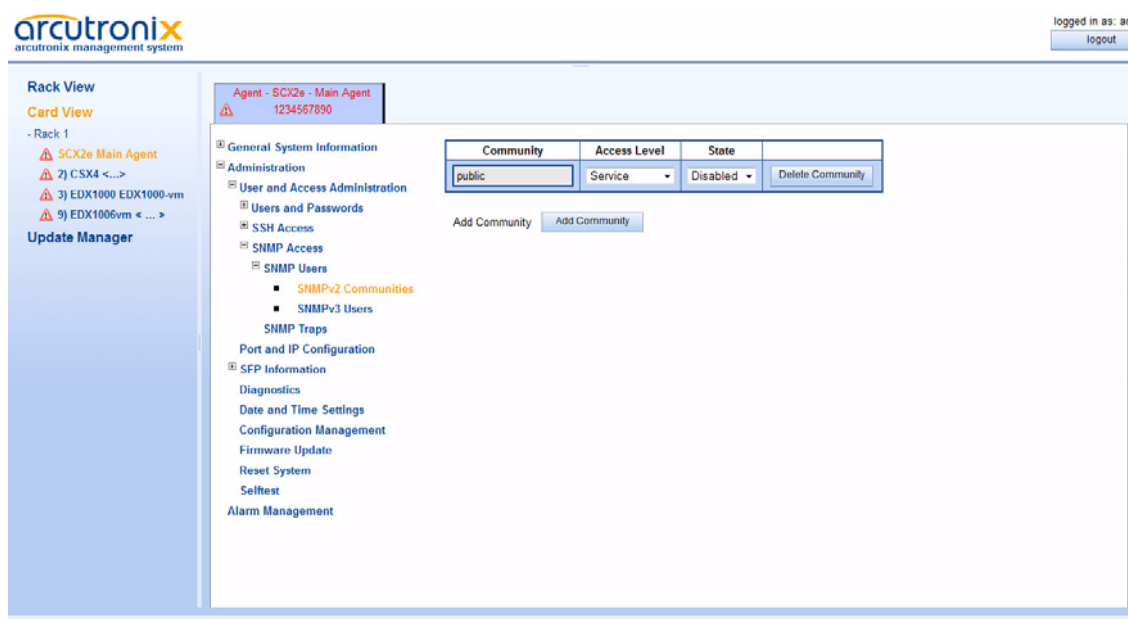


Figure 5-18 SNMPv2c Community

Table 5-14 provides information on the menu.

Table 5-14 SNMPv2c Community Configuration Menu

Parameter	Description	Format	Default
Community	Click on the name of the community (e.g. public) to edit it.	SelectList/Menu	
Access Level	Define the access level for this community.	PullDown Menu <ul style="list-style-type: none"> • Administrator • Service • Monitor 	Service
State	Enable / disable the community.	PullDown Menu <ul style="list-style-type: none"> • Enabled • Disabled 	Enabled
Delete Community	Press Enter and select an entry in the (scroll) list. After this confirm the action.	Select/Confirm	
Add Community	Add a new SNMP community.	Action	

NOTE: When “Add Community” is selected, a new entry in the list above is created: “public”, with access level *Service*. Please adapt the settings of the new community. The new community’s default status is *Disabled!*

SNMP V3 Users

This page shows all currently known SNMPv3 users along with their access permissions and authentication parameters. The columns in this table have the following meaning:

- Name: the SNMPv3 user name (also used as security name)
- Passphrase: the SNMPv3 authentication mode supported for this user (HMAC-MD5/SHA1 authentication with pass phrase or no authentication)
- Access Level: the level of access permissions of the SNMPv3 user
- Encryption: the encryption mode that is supported for the SNMPv3 user (DES/AES encryption with Passovers or no encryption)
- State: whether the SNMPv3 user is enabled or disabled
- Edit Settings: allows to change the user's name and security parameters
- Delete Entry: delete the SNMPv3 user

It is possible to add additional SNMPv3 users to the device by using the “Add User” button below the list. The newly added user will immediately appear at the bottom of the list (with all fields set to default values). Use the “Edit Settings” button in the new user's entry to adjust the settings as required.

The screenshot shows the Arcutronix management system interface. The main content area displays the configuration for a specific agent (SCX2e - Main Agent, ID: 1234567890). Under the 'SNMP Users' section, there is a table with the following data:

Name	Authentication	Access Level	Encryption	State		
public	HMAC-MD5	Service	No Encryption	Disabled	Edit Settings	Delete Entry

Below the table, there is an 'Add User' button. The left sidebar shows the navigation menu with 'SNMP Users' selected.

Figure 5-19 SNMPv3 User

Table 5-15 provides information on the menu.

Table 5-15 *SNMPv3 User Menu*

Parameter	Description	Format	Default
Edit Settings	Press Button and select an entry in the (scroll) list. After this the Edit SNMP User menu opens.	SelectList/Menu	
Delete Entry	Press Enter and select an entry in the (scroll) list. After this confirm the action.	SelectList/Confirm	
Add User	Add a new SNMP user.	Action	

NOTE: When “Add SNMPv3 User” is selected, a new entry in the list above is created: “guest”, with access level *Guest*. Please select after this the “Edit Settings” to adapt the settings of the new user. The new user’s default status is *Disabled!*

NOTE: Please note that SNMPv3 users and Web/CLI users are distinct in the sense that SNMPv3 users do not automatically get Web/CLI access with the same user name/password and vice versa.

Edit Settings

This menu allows to adjust the security settings of an SNMPv3 user. The configuration menu are shown in Table 5-16.

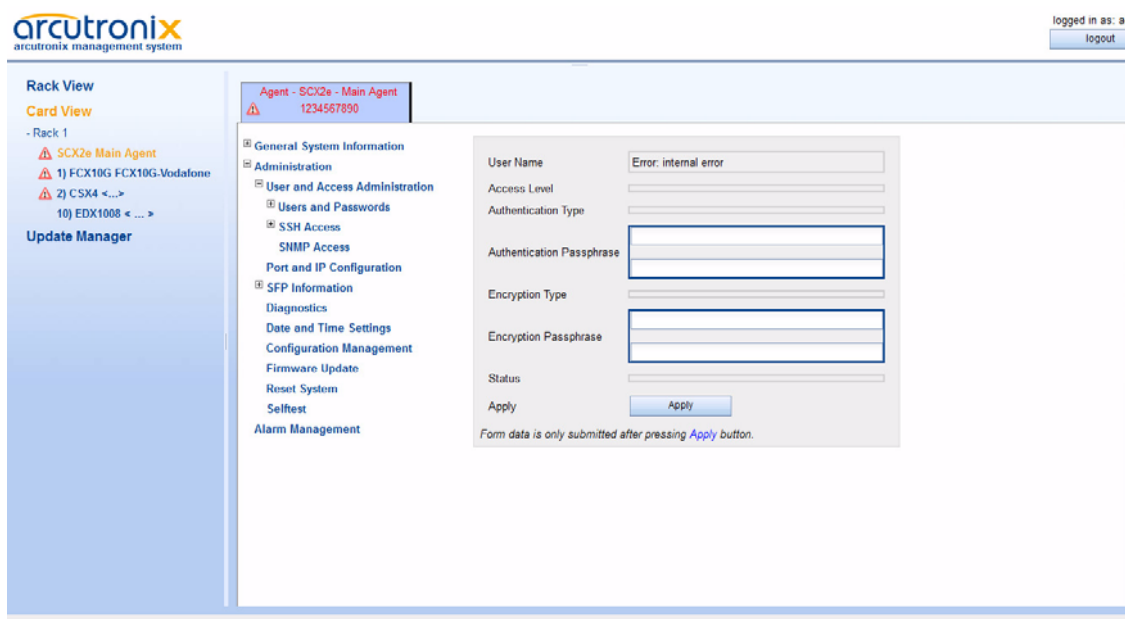


Figure 5-20 SNMPv3 Edit User Settings

Table 5-16 SNMPv3 User Settings Menu

Parameter	Description	Format	Default
User Name	The “User-based Security Model” (USM) user name. In SNMPv3, the user name is also used as security name.	string	empty
Access Level	The level of access permission of the SNMPv3 user.	PullDown Menu <ul style="list-style-type: none"> • Administrator • Service • Monitor 	Service
Authentication Type	This settings determines the authentication method to use for authenticating messages of this user. It is shown in the “Passphrase” column of the user list.	PullDown Menu <ul style="list-style-type: none"> • No Authentication • HMAC-MD5 • HMAC-SHA 	HMAC-MD5

Table 5-16 SNMPv3 User Settings Menu (continued)

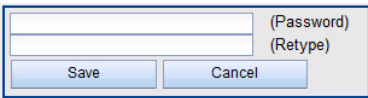
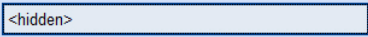
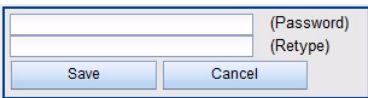

Parameter	Description	Format	Default
Authentication Passphrase	<p>When the authentication method is set to “Passphrase (MD5)” or “Passphrase (SHA1)”, enter the user's password here. The password will be used to generate an authentication key according to RFC3414.</p> <p>The passphrase must be entered twice for verification. Please retype it in the bottom field:</p>  <p>If a valid passphrase is stored on the device, it will be shown as <hidden> to avoid phishing:</p> 	string	empty
Encryption Type	This setting determines whether to accept encrypted SNMP messages of this user and which encryption algorithm is in use (DES/AES).	PullDown Menu <ul style="list-style-type: none"> • No Encryption • DES Encryption • AES Encryption 	No Encryption

Table 5-16 SNMPv3 User Settings Menu (continued)

Parameter	Description	Format	Default
Encryption Passphrase	<p>When the encryption algorithm is set to DES or AES encryption, enter the password for message decryption here. The password will be used to generate a decryption key according to RFC3414.</p> <p>The passphrase must be entered twice for verification. Please retype it in the bottom field:</p> 	string	empty
	<p>If a valid passphrase is stored on the device, it will be shown as <hidden> to avoid phishing:</p> 		
Status	When Status is set to Disabled, no messages in behalf of this user will be accepted.	PullDown Menu <ul style="list-style-type: none"> • Enabled • Disabled 	Disabled
Apply	<p>The changes can be made permanent using the “Apply” button.</p> <p>If you do not want to confirm your settings, just press the “Back” button in your web-browser.</p>		

The settings “Passphrase Type” and “Encryption Type” determine the maximum confidentiality of SNMP messages in behalf of the user that the device will accept. The following rules apply:

Table 5-17 SNMPv3 Confidentiality

Authentication	Encryption	Accepted SNMP Messages
enabled	enabled	noAuthNoPriv; authNoPriv authPriv

Table 5-17 SNMPv3 Confidentiality (continued)

Authentication	Encryption	Accepted SNMP Messages
enabled	disabled	noAuthNoPriv; authNoPriv
disabled	disabled	noAuthNoPriv

The selection of OIDs visible/writable to the user depends on the access permission level as well as the SNMP message confidentiality.

SNMP Traps

This menu show various settings related to SNMP trap receivers. The generation of SNMP Authentication-Traps can be enabled or disabled. Furthermore, the list of currently known trap receivers (e.g. management stations) is visible.

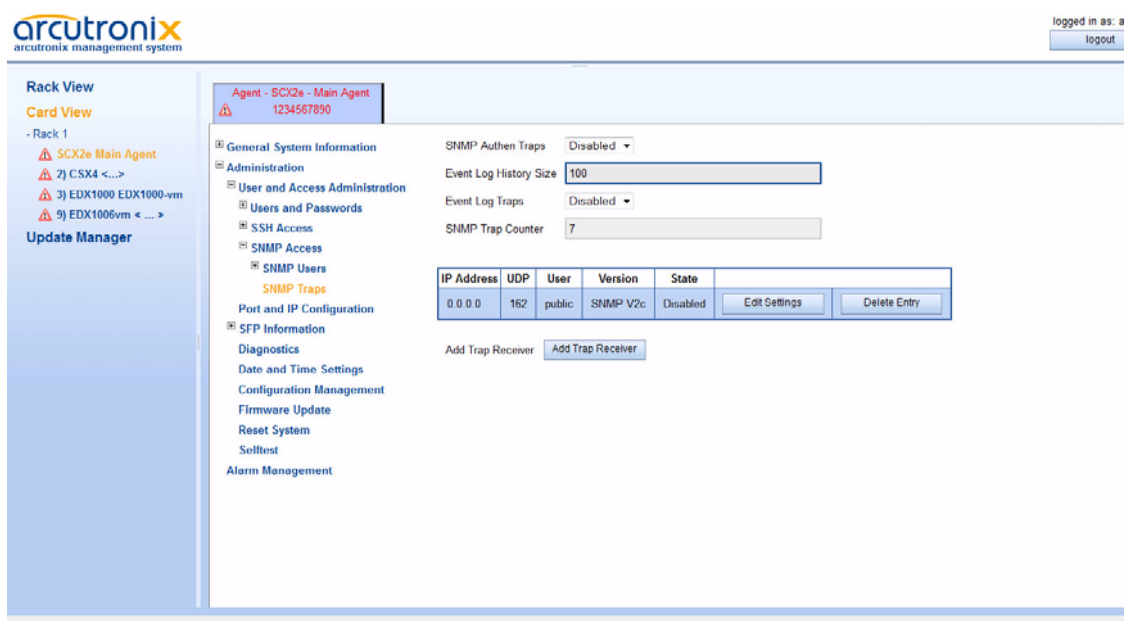


Figure 5-21 SNMP Trap Configuration

At the head of the page the defined SNMP trap receivers and the associated information are shown in a list.

In Default configuration, no trap receivers are defined.

The columns in the trap receiver list have the following meaning (see Table 5-18):

Table 5-18 *SNMP Trap Configuration Menu*

Parameter	Description	Format	Default
SNMP Authen Traps	When an SNMP agent receives a request that does not contain a valid community name or the host that is sending the message is not on the list of acceptable hosts, the agent can send an authentication trap message to one or more trap destinations	PullDown Menu <ul style="list-style-type: none">• Disabled• Enabled	Enabled
Event Log History Size	Defines the size of the Event Log History. The Event Log may be read out via the axCommon.MIB	Number	100
Event Log Traps	A trap can be enabled, at any time an event is written into the log file.	PullDown Menu <ul style="list-style-type: none">• Disabled• Enabled	Enabled
SNMP Trap Counter	Counter of all outgoing traps	Display	7
Edit Settings	Press Button for an entry in the list. After this the Edit SNMP Trap Receiver menu opens.	Select Button/Menu	
Delete Entry	Press Button and the related entry will be removed from the list.	Select Button/Confirm	
Add Trap Receiver	Add a new SNMP Trap Receiver.	Action	

NOTE: When “Add Trap Receiver” is selected, a new entry in the list above is created. Please select after this the “Edit Settings” menu to adapt the settings of the new receiver.

Edit SNMP Trap Receiver

Pressing the “Edit Settings” button in the trap receiver table opens a new menu:

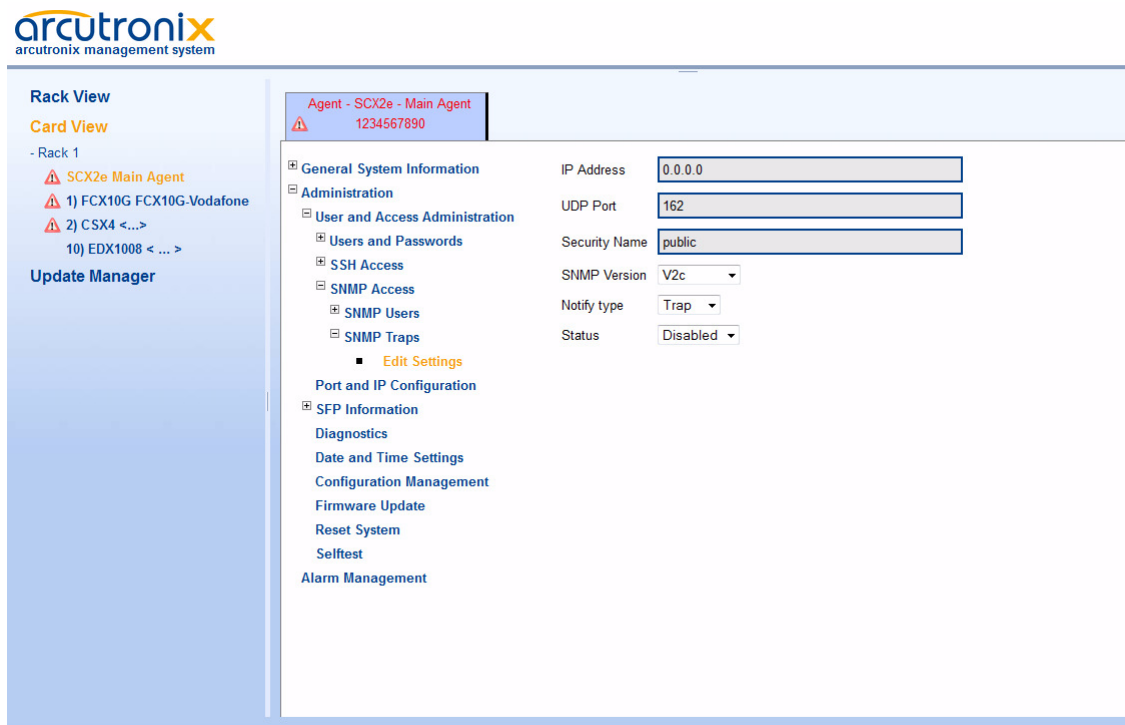


Figure 5-22 Edit SNMP Trap Receiver

Table 5-19 provides information on the menu.

Table 5-19 Edit SNMP Trap Receiver Menu

Parameter	Description	Format	Default
IP Address	The IPv4 address of the management station to which the traps should be sent.	Input	0.0.0.0
UDP Port	The port number where the management station expects SNMP traps. Normally Port 162 is ok.	Input	162
Security Name	The name of an SNMPv2 community or SNMPv3 user on which behalf the trap message is generated. ⁱ	Input	public

Table 5-19 Edit SNMP Trap Receiver Menu (continued)

Parameter	Description	Format	Default
SNMP Version	Whether to generate SNMPv2 or SNMPv3 trap messages.	PullDownMenu <ul style="list-style-type: none">SNMP v2cSNMP v3	SNMP v2c
Status	Whether this management station will receive any traps or not.	PullDown Menu <ul style="list-style-type: none">EnabledDisabled	Enabled

i. The SNMPv3 user or SNMPv2 community must have been configured on this device in advance, because further security parameters are taken from the user or community settings.

It is possible to add further management stations to the list of trap receivers using the “Add Trap Receiver” button below the list.

SNMP based SNMP parameter configuration

When the SNMP based SNMP parameter configuration is being enabled, all settings regarding SNMPv3 Users, SNMPv2 communities and SNMP trap that have been configured via Web/CLI are transferred to the corresponding data tables in the relevant MIBs and made available for changes. At the same time, modification of this data via Web/CLI is being prohibited.

The configuration of all SNMP parameters can then be done using SNMP operations on the following MIBs:

- SNMP-COMMUNITY-MIB
- SNMP-USER-BASED-SECURITY-MIB
- SNMP-VIEW-BASED-ACM-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB

for which full support is available.

Port and IP Configuration

Use this menu to configure the IP parameters of the two management ports. These ports are designed for local access via a laptop for mainly service and craft people as well as for remote connection from central NOC.

F- and Q-Interface

See Chapter 4, IP-Addressing for details about F- and Q-interface.

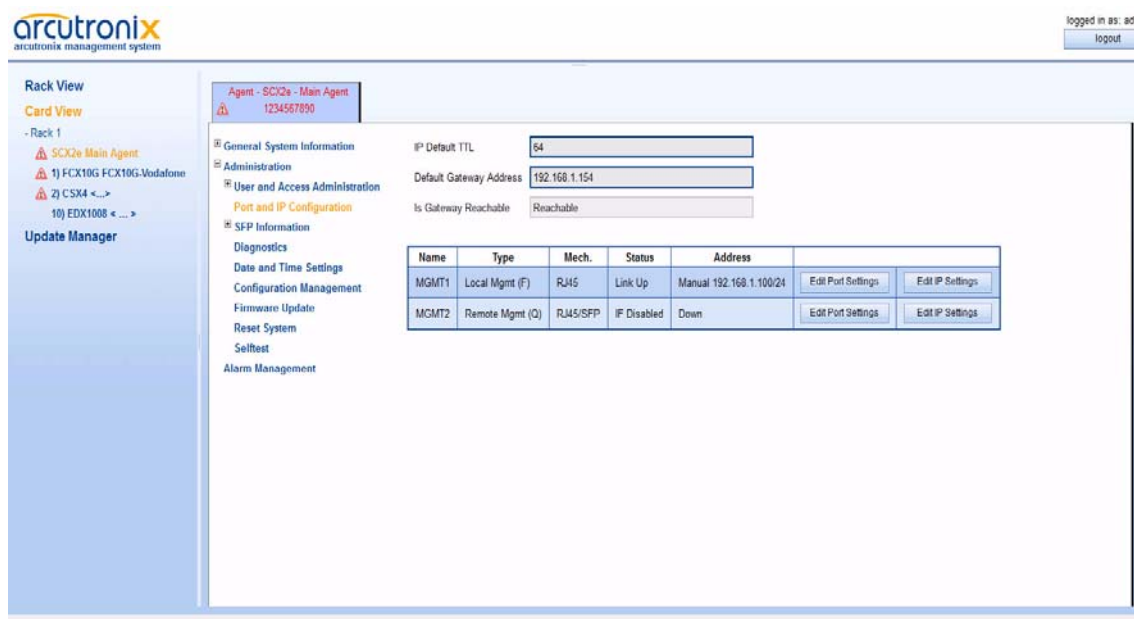


Figure 5-23 Port and IP Configuration

Table 5-20 provides information on the menu.

Table 5-20 IP-Configuration Menu

Parameter	Description	Format	Default
IP Default TTL	Default Time-to-Life value for all outgoing IP packets	Integer	64
Default Gateway Address	Address of the Default Gateway.	IP-address	0.0.0.0
Is Gateway Reachable	Check, whether the Default Gateway is reachable with the actual IP settings.	Display	

Below the above mentioned 3 entries a quick overview of all management (Ethernet) ports is given.

Press the “Edit Port Settings” to change the HW settings of a port.

Press the “Edit IP Settings” to change the IP settings of a port.

Warning: Any changes of the IP parameters may lead to contact loss with the device. Be careful when changing this attributes.
In case you made any changes a new connection using the changed IP settings might be necessary.

Edit Port Settings

Use this menu to change the HW-settings and behaviour of the ports. The menus for the different ports (Copper, Fibre or Combo) are almost similar.

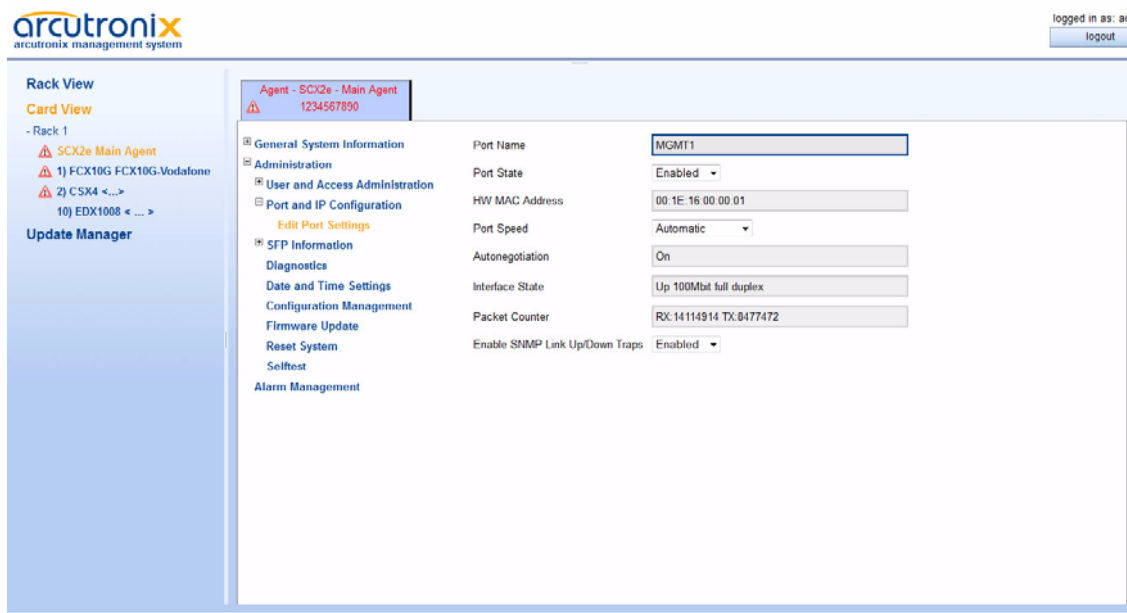


Figure 5-24 Edit-Port-Settings

Table 5-21 provides information on the menu.

Table 5-21 Port Configuration Menu

Parameter	Description	Format	Default
Port Name	Name for this port.		MGMTi
Port State	Enables or disables the local management port.	PullDownMenu • Enabled • Disabled	Enabled
HW MAC Address	Displays the MAC address of the local management port.	Display	00:1E:16:aa:bb:cc
Port Speed	Configures the data transmission mode for the selected Ethernet port. ⁱ	PullDown Menu • Automatic • 10 Half Duplex • 10 Full duplex • 100 Half Duplex • 100 Full duplex	Automatic

Table 5-21 Port Configuration Menu (continued)

Parameter	Description	Format	Default
Autonegotiation	Autonegotiation handling can be invoked, even when a fixed Port Speed (see above) is selected. when Port Speed is “Automatic”, this entry is always ON.	PullDown Menu • On • Off	On
Operation Mode ii	Indicates, whether the Combo-Port (port2) has indicated a plugged SFP or not. If an SFP is plugged the display is 100FX or 1000FX, otherwise it is called Copper .		
Interface State	Indicates, whether the port is up, down or disabled.	Display	
Packet Counter	Counter for transmitted (TX) and received (RX) Ethernet-frames on the port.	Display	
Enable SNMP Link Up/Down Traps	Enables or disables the capability to send traps when the link state is changed.	PullDownMenu • Enabled • Disabled	Enabled

i. See Table 4-1 for explanation on the settings.

ii. This menu item is only visible for port 2.

Edit IP-Settings

Use this menu to change the IP-settings and behaviour of the ports. The menus for the different ports (Copper, Fibre or Combo) are almost similar.

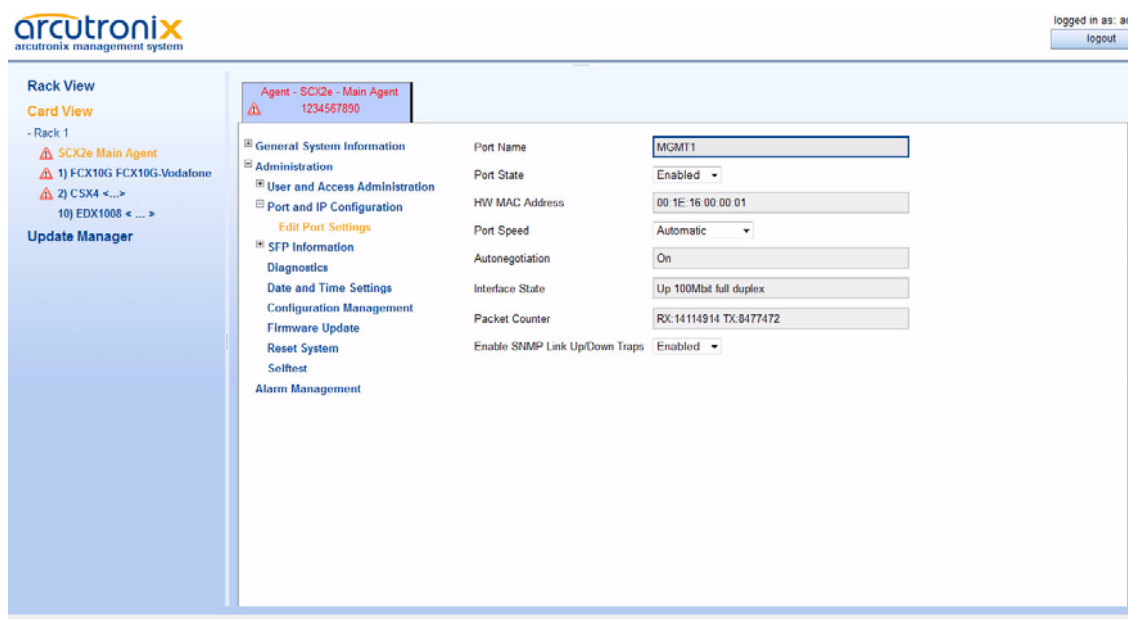


Figure 5-25 Edit-Port-Settings

Table 5-21 provides information on the menu.

Table 5-22 IP-Port Configuration Menu

Parameter	Description	Format	Default
Port Name	Name for this port.	String	MGMTi
Interface Type	Defines the IP behaviour of the port. Either local interface (F-interface) or remote access (Q-interface).	PullDownMenu <ul style="list-style-type: none"> • Local Mgmt (F) • Remote Mgmt (Q) 	MGMT1: Local Mgmt (F) MGMT2: Remote Mgmt (Q)
IP Address Assignment	Defines the IPv4 address assignment. The Pulldown menu offers different entries, depending on the selected Interface Type (F- or Q-interface).	PullDown-Menu F-Interface: <ul style="list-style-type: none"> • Manual • Provide DHCP Server Q-Interface: <ul style="list-style-type: none"> • Manual • From DHCP Server • From DHCP Server/ Auto IP 	F-IF: Provide DHCP Server Q-IF: From DHCP Server

Table 5-22 IP-Port Configuration Menu (continued)

Parameter	Description	Format	Default
IP Address	Configuration of the device's IPv4 address.	Display/Input	MGMT1: 192.168. 1.100 MGMT2: <empty>
Network Mask	Configuration of the device's IPv4 network mask. When an IPv4 address is entered, a suggested network mask will be displayed.	Display/Input	255.255. 255.0

SFP Information

Port2 of the SCX2e is build as a Combo-Port. It can be used as copper or fibre I/F (SFP). It supports 100BaseFX as well as 1000BaseFX SFP modules. If a SFP is plugged, the internal information, provided by the SFP, can be read here.

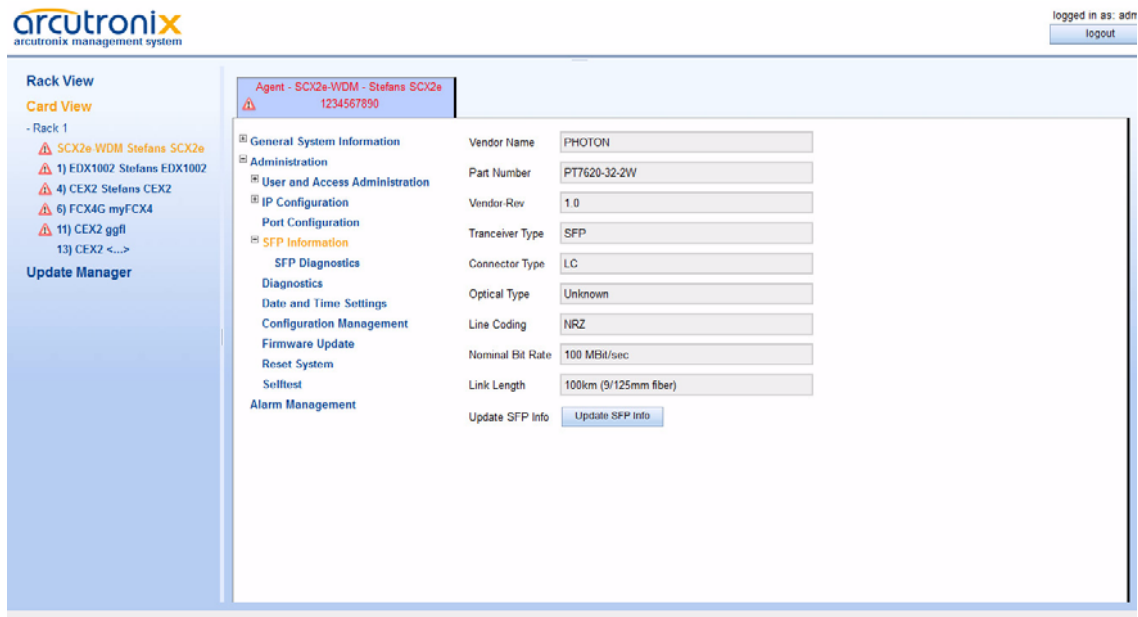


Figure 5-26 SFP

NOTE: All displayed values depending on the SFP. arcutronix cannot ensure the correctness of this values.

Table 5-23 provides information about the.

Table 5-23 SFP Details

Parameter	Description	Format
SFP Info for Port	Presents the name of the elected SFP.	Display
Detected Type	The Detected Type specifies the physical device plus the service purpose.	Display
Vendor Name	The vendor name is a 16 character field. The vendor name is the full name of the corporation, a commonly accepted abbreviation of the name of the corporation, the SCSI company code for the corporation, or the stock exchange code for the corporation.	Display
Serial No	The vendor serial number (vendor SN) is a 16 character field. A value of all zero in the 16-byte field indicates that the vendor SN is unspecified	Display
Part Number	The vendor part number (vendor PN) is a 16-byte field, defining the vendor part number or product name. A value of all zero in the 16-byte field indicates that the vendor PN is unspecified.	Display
Connector Type	The connector value indicates the external optical cable connector provided as the media interface.	Display
Optical Type	These are the optical interface(s) that is (are) supported by the transceiver.	Display
Line Coding	The encoding value indicates the serial encoding mechanism that is the nominal design target of the particular transceiver.	Display
Nominal Bit Rate	The nominal bit (signalling) rate (BR, nominal) is specified in units of 100 MBd, rounded off to the nearest 100 MBd. A value of 0 indicates that the bit rate is not specified and must be determined from the transceiver technology.	Display
Link Length	This value specifies link length that is supported. The given link length is valid for the optical cable specified in quote signs.	Display

Table 5-23 SFP Details (continued)

Parameter	Description	Format
Date Code	The date code is an 8-byte field that contains the vendor's date code in ASCII characters. The date code is mandatory.	Display
Wave Length	Denotes nominal transmitter output wavelength at room temperature.	Display

SFP Diagnostics

More detailed information about the inventory data of a plugged SFP can be found here.

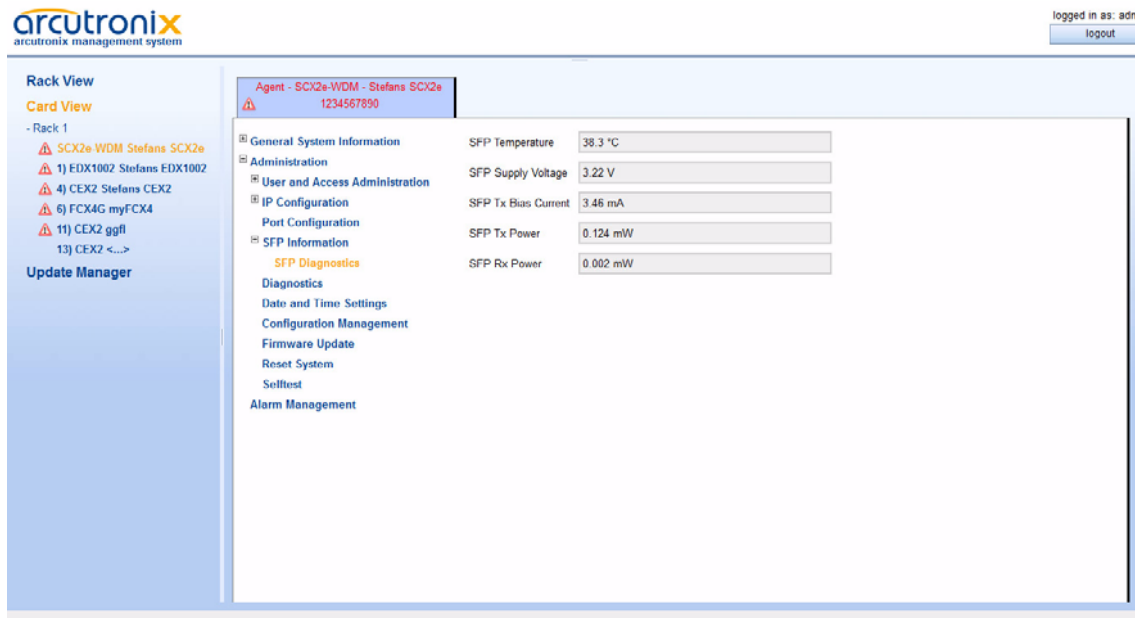


Figure 5-27 SFP

NOTE: All displayed values depending on the SFP. arcutronix cannot ensure the correctness of this values.

Diagnostics

The Diagnostics can be used to check the IP settings and reachability of remote devices. Using the ICMP (Internet Control Message Protocol) a remote router can be “pinged” and the route traced.

Just enter the remote router’s IP-address and the select either “Ping”, “Trace-route/UDP” or “Traceroute/ICMP”. The result is given in the line below called “Ping Result”.

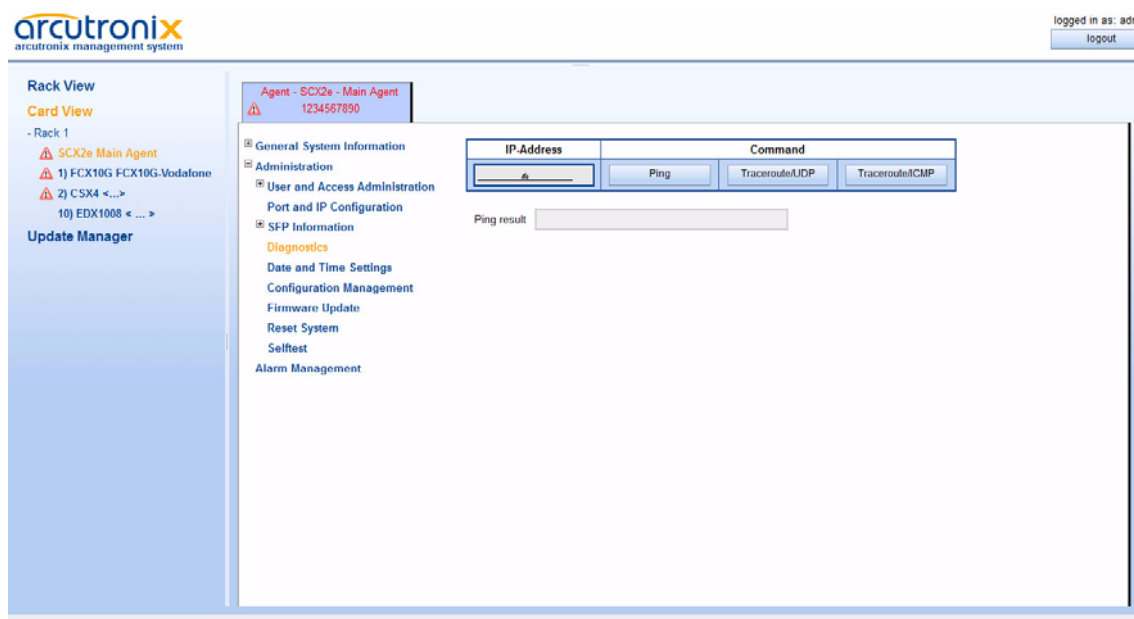


Figure 5-28 Diagnostics

Date and Time Settings

Use this menu to set the date, time, and time zone for the device. The date and time can be configured manually or via NTP².

For manual setting, the entry for the NTP server must be empty. For automatic setting, a NTP-server's IP-address must be assigned.

2. NTP = Network Time Protocol, IETF RFC 1305

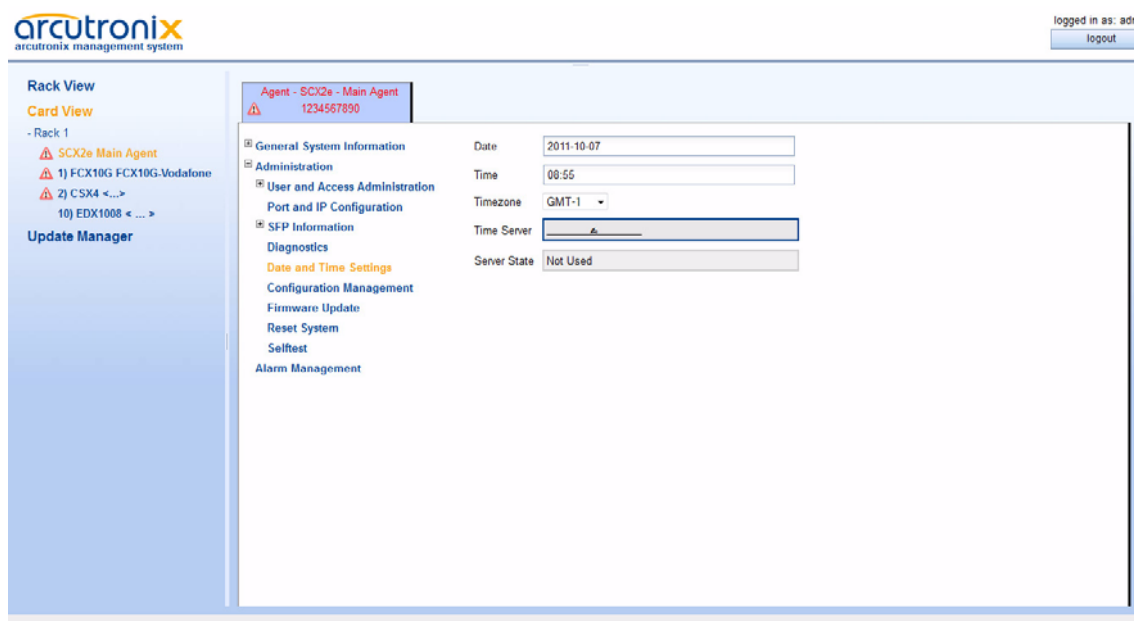


Figure 5-29 Date And Time Settings

Table 5-24 provides information on the menu.

Table 5-24 Date and Time Settings Menu

Parameter	Description	Format	Default
Date	Indicates the current device's date (dd.mm.yyyy).	Display/Input	no default
Time	Indicates the current device's time (hh:mm:ss).	Display/Input	no default
Time Zone	Indicates the relative time deviation to UTC ⁱ , i.e. '-1' for Berlin.	PullDown Menu	UTC
Time Server	If there is a time server, you may enter its IPv4 address in this fields ⁱⁱ .	Display/Input	no default
Server State	This entry does indicate the result and progress of time synchronization.	Not used Not available Connecting Synchronizing Lost sync Synchronized	Not used

i. UTC = Universal Time Coordinated

- ii. The SCX2e expects an NTP-server.

Configuration Management

Use this menu to store and recall different configurations. The actual configuration can be stored at any time and later recalled to switch between different settings. Also the Factory Default can be redressed, if required.

When a stored configuration (Default config or any other) is to be recalled, one can decide, whether all variables are redressed, or to keep some settings. This is helpful to keep the IP-address for example or the actual defined users and passwords.

Configurations can not only be stored locally on the SCX2e, but externally on a server or PC. So one has the possibility to up- and download files to save them externally and/or to use stored files as “master-config-file” for other devices. This makes it easier to put lots of units in operation with a common configuration.

For transferring the configuration files to and from the unit, the HTTP file transfer is used. HTTP file transfer refers to the transfer of large files through a computer's web browser. Although similar, HTTP works in a slightly different way to FTP as it is a 'state-less' protocol and only acts on isolated commands and responses. HTTP file transfer has been developed as a simple alternative to FTP when no FTP clients are required, all your customer needs is access to a web browser and they are able to send large files.

NOTE: A configuration-file does always use the extension *.cfgx and carries some internal check-words to make sure that no illegal configuration can be installed on the unit.

The screenshot shows the Arcutronix management system interface. The top right corner indicates the user is logged in as 'adm' with a 'logout' button. The left sidebar contains navigation options: 'Rack View', 'Card View', 'Rack 1', 'SCX2e Main Agent', '1) FCX10G FCX10G-Vodafone', '2) CSX4 <...>', '10) EDX1008 <...>', and 'Update Manager'. The main content area is titled 'Agent - SCX2e - Main Agent' with ID '1234567890'. It features a tree view of configuration categories: General System Information, Administration, User and Access Administration, Port and IP Configuration, SFP Information, Diagnostics, Date and Time Settings, Configuration Management (highlighted), Firmware Update, Reset System, Selftest, and Alarm Management. The 'Configuration Management' section contains a table:

Name	Date	Action
Current Configuration	2011/10/07 08:56:41	Save Configuration
Factory Default Configuration	--	Apply

Below the table, there is an 'Import Configuration' section with a text input field and two buttons: 'Select File' and 'Start Upload'.

Figure 5-30 Configuration Management

Table 5-25 provides information about the.

Table 5-25 Configuration Management

Parameter	Description	Format
Current Configuration	This is the actual configuration of the unit. Press the “Save Configuration” -Button and it will be stored in the device. The new storage will be added to the list, where one can provide special name to it.	Action
Factory Default Configuration	The Factory Default, as defined in the SW. Press “Apply” to recall this configuration.	Action
Any additional entry	Up to 10 possible entries to show different configurations, which were stored as “Current Configuration”. A meaningful name can be given. Press “Apply” to recall this configuration.	Action
Download xxx.cfgx	Download the configuration called “xxx” to your PC or management system via http. This is good for more secure storage and/or to use the configuration on a different device.	Action
Delete Configuration	Press “Delete Configuration” to remove the selected entry from the system.	Action
Select File	Select File button to open browsers window to file explorer, when http-file transfer is enabled.	Action
Start Upload	To start the http file transfer.	Action

Recall Configuration (“Apply”)

When a stored configuration (Default config or any other) shall be recalled, it might be reasonable to keep some actual settings, e.g. IP-address or defined users and passwords. This can be configured in the sub-menu.

To make it more comfortable for the user, all the specific settings can be configured to the same behaviour in one step (“Preset Configuration Components”) or each setting can be configured individually.

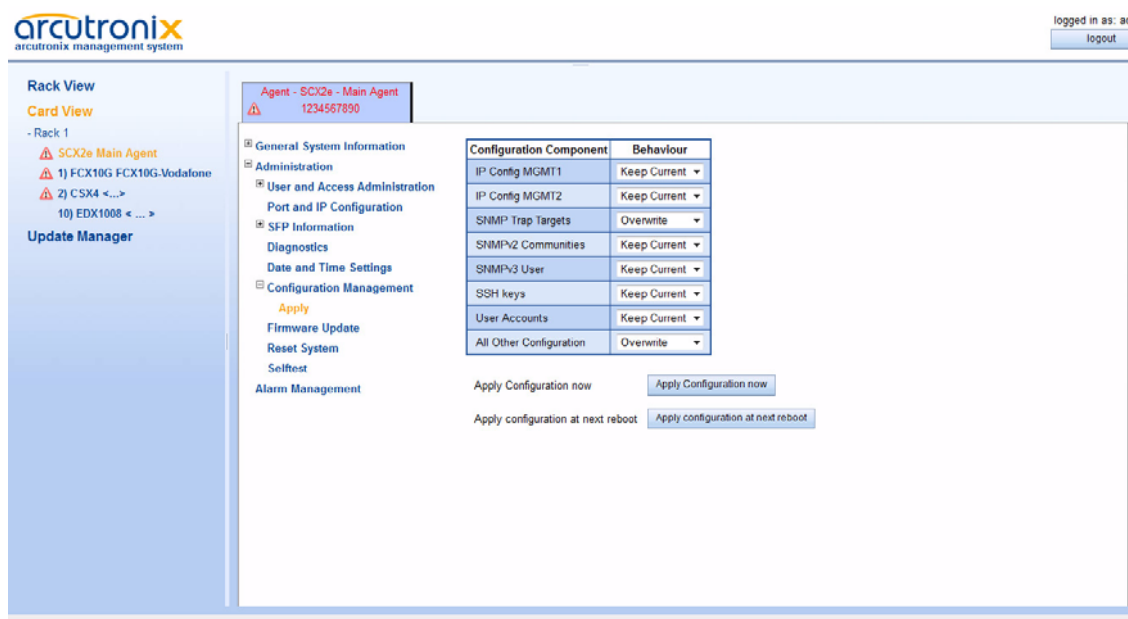


Figure 5-31 Recall Configuration

Table 5-26 provides information on the menu.

Table 5-26 Recall Configuration

Parameter	Description	Format	Default
IP Config MGMT1	The IP- (and VLAN-) settings for outband management.	PullDown-Menu <ul style="list-style-type: none"> Overwrite Keep Current 	Keep Current
IP Config MGMT2	The IP- (and VLAN-) settings for inband management.	PullDown-Menu <ul style="list-style-type: none"> Overwrite Keep Current 	Keep Current
SNMP Trap Targets	The IP settings for SNMP-trap receivers.	PullDown-Menu <ul style="list-style-type: none"> Overwrite Keep Current 	Overwrite
SNMPv2 Communities		PullDown-Menu <ul style="list-style-type: none"> Overwrite Keep Current 	Overwrite
SNMPv3 Users		PullDown-Menu <ul style="list-style-type: none"> Overwrite Keep Current 	Overwrite

Table 5-26 Recall Configuration (continued)

Parameter	Description	Format	Default
SSH Keys		PullDown-Menu • Overwrite • Keep Current	Keep Current
User Accounts		PullDown-Menu • Overwrite • Keep Current	Keep Current
All Other Configuration		PullDown-Menu • Overwrite • Keep Current	Overwrite
Apply Configuration Now	Press this button to invoke the new configuration. A reset of the system will be done and the new configuration is in place after.	Action	no default
Apply Configuration at next start	Press this button to invoke the new configuration after next reset. The reset may be defined in the Reset System menu.	Action	no default

Firmware Update

Use this menu to specify the protocol, the file and the server, where the new software is stored. In addition you can specify when the new software is invoked.

Two different protocols are supported to update the SCX2e Firmware:

- HTTP - Hyper Text Transfer Protocol as used for Web-Pages,
- SFTP - SSH File Transfer Protocol as used for ssh-connections.
- TFTP - Trivial File Transfer Protocol as used for IP-connections.

HTTP file transfer refers to the transfer of large files through a computer's web browser. Although similar, HTTP works in a slightly different way to FTP as it is a 'stateless' protocol and only acts on isolated commands and responses. HTTP file transfer has been developed as a simple alternative to FTP as no FTP clients are required, all your customer needs is access to a web browser and they are able to send large files.

Trivial File Transfer Protocol, more commonly referred to as TFTP is a very basic and more traditional method used to transfer large files over an IP network, such as the internet. Although simple, TFTP servers can be the ideal solution to cater for smaller business file transfer as the software itself can be sourced at little to no cost, providing you with the extra funds needed to adapt the system to suit your requirements.

HTTP FW-Update

HTTP FW-Upload is the default for SCX2e Update, as the standard management connection is based on http. Select the “Protocol” entry to HTTP, if not done yet, and the following menu will appear.

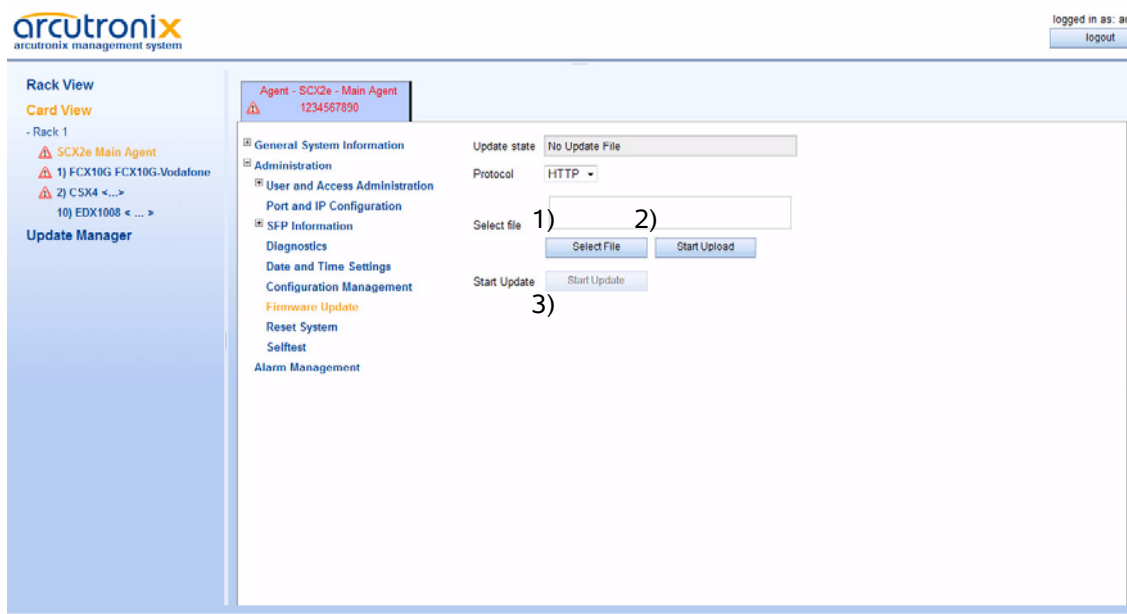


Figure 5-32 Update SCX2e-SW

3 steps to update the SCX2e software:

1. First select the upload file
2. Then press “Start Upload” to begin with the file-transfer. A progress bar will be popped to show the file transfer.

NOTE: If the upload did not take place or it failed, the next step (start the update process) can not be invoked.

3. After successful file-upload, the update process can be started, at any time, whenever it is required. Just press the “Start Update” button and it begins. The progress is shown in the field “Update Progress”.

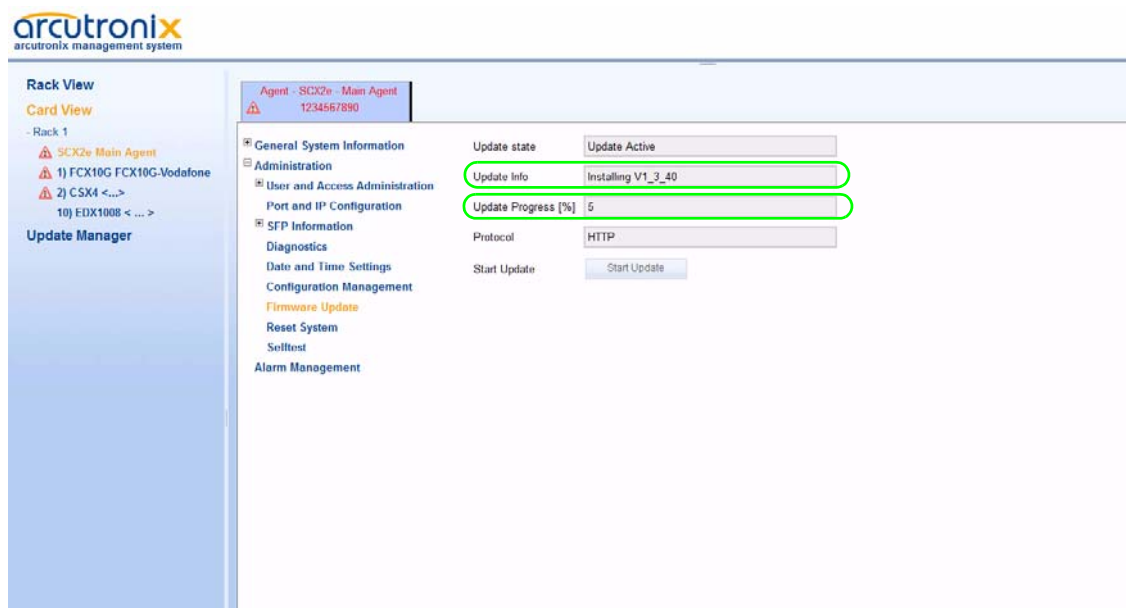


Figure 5-33 Ongoing SCX2e-SW Update

Table 5-27 provides all the information on the menu.

Table 5-27 Firmware Update Menu

Parameter	Description	Format	Default
Protocol	Select the used protocol.	PullDown Menu <ul style="list-style-type: none"> • HTTP • SFTP • TFTP 	HTTP
Select File	Press on the “Select File” Button and enter the file’s name and path.	Display/Input	no default
Update State	Indicates the progress of update (Idle Active Sending Restart Command... Sending Reboot Command... Update finished Update failed).	Display	Idle
Start Download	Starts the firmware update.	Action	

NOTE: After successful installation of the new FW, the SCX2e will reboot to finish the update progress. After the reboot reconnecting to the unit might be necessary. Just press the reload-button in your web-browser to reconnect again to the unit.

SFTP FW-Update

SFTP Firmware Update gives more security and features to the update process. The protocol is not stateless, one can better see, whether the file-transfer process was successful or not. SFTP is using SSH as transport layer, so one can use the benefits in security of the SSH protocol. To avoid immediate update of the FW, in the SFTP-style a date/time combination can be defined to do the update in a “service-window” to minimize impacts for the service.

Change the “Protocol” entry to SFTP, if not done yet, and the following menu will appear.

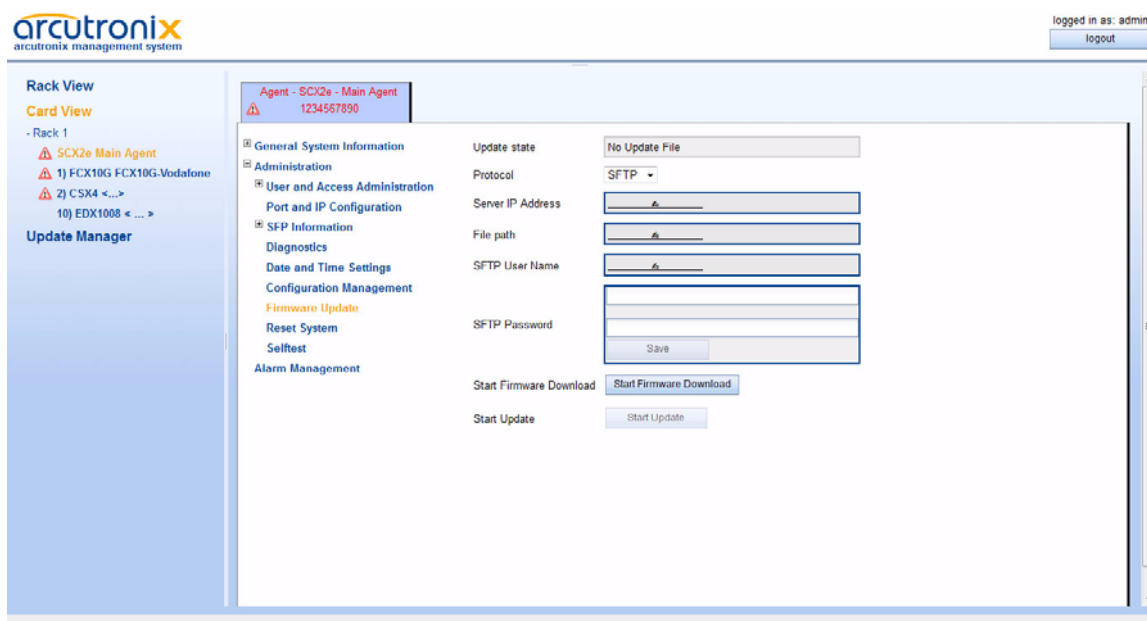


Figure 5-34 TFTP Firmware Update

Note: When you want to restart the device at a specified time, you first have to configure the device’s correct time and date (see “Diagnostics” on page 5-42).

The Error State line will display the reason.

Critical Error, write failed	The device may be unusable after power-off.
Error, write failed	Download failed, old software is usable.
Error, download data invalid	The download files cannot be read or are not found (check the path).
Software up to date	Download is not executed.

NOTE: After successful installation of the new FW, the SCX2e will reboot to finish the update progress. After the reboot reconnecting to the unit might be necessary. Just press the reload-button in your web-browser to reconnect again to the unit.

TFTP FW-Update

TFTP Firmware Update gives more security and features to the update process. The protocol is not stateless, one can better see, whether the file-transfer process was successful or not. To avoid immediate update of the FW, in the TFTP-style a date/time combination can be defined to do the update in a “service-window” to minimize impacts for the service.

Change the “Protocol” entry to TFTP, if not done yet, and the following menu will appear.

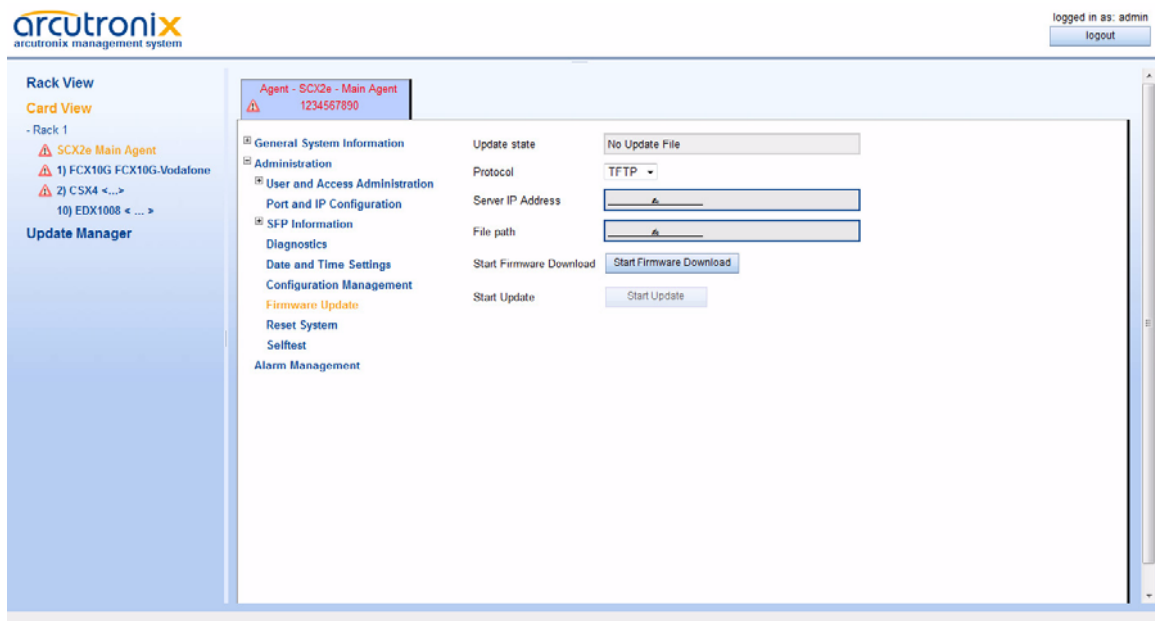


Figure 5-35 TFTP Firmware Update



Note: The Specfile’s path has to be specified with slash (/), when used on a Windows based TFTP-server. Otherwise the TFTP-server can not locate the correct file.
Format: `root/./SCX2e/dlimage.spec`

Note: When you want to restart the device at a specified time, you first have to configure the device’s correct time and date (see “Diagnostics” on page 5-42).

The Error State line will display the reason.

Critical Error, write failed	The device may be unusable after power-off.
Error, write failed	Download failed, old software is usable.

Error, download data invalid The download files cannot be read or are not found (check the path).

Software up to date Download is not executed.

NOTE: After successful installation of the new FW, the SCX2e will reboot to finish the update progress. After the reboot reconnecting to the unit might be necessary. Just press the reload-button in your web-browser to reconnect again to the unit.

Reset System

Use this menu to reset the SCX2e manually immediately or at a scheduled time.

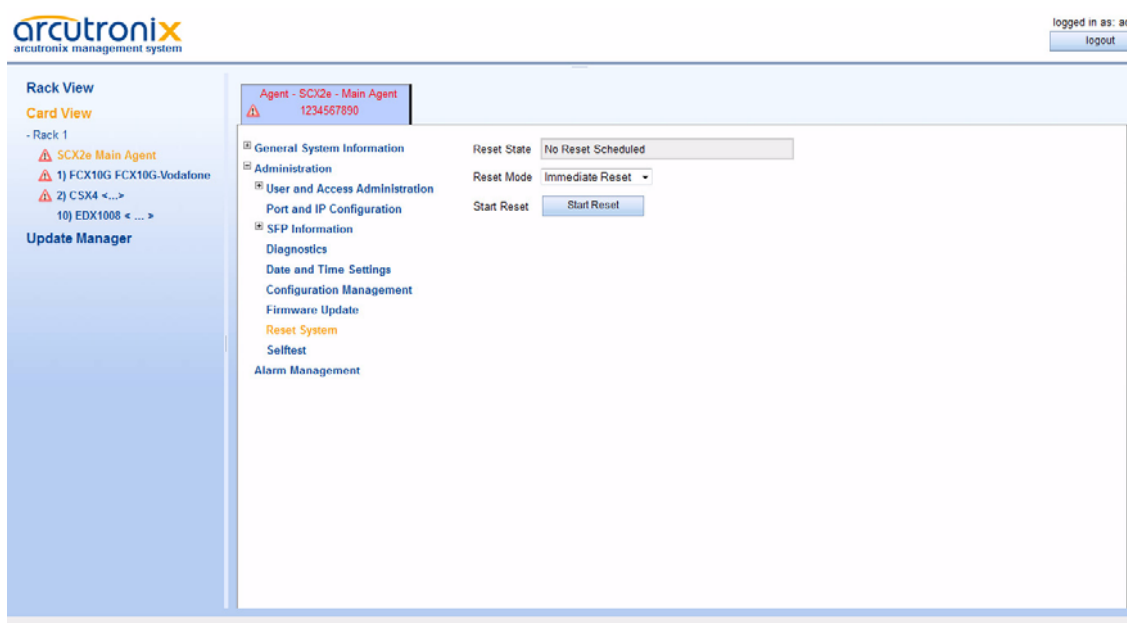


Figure 5-36 Reset System, Immediate Reset

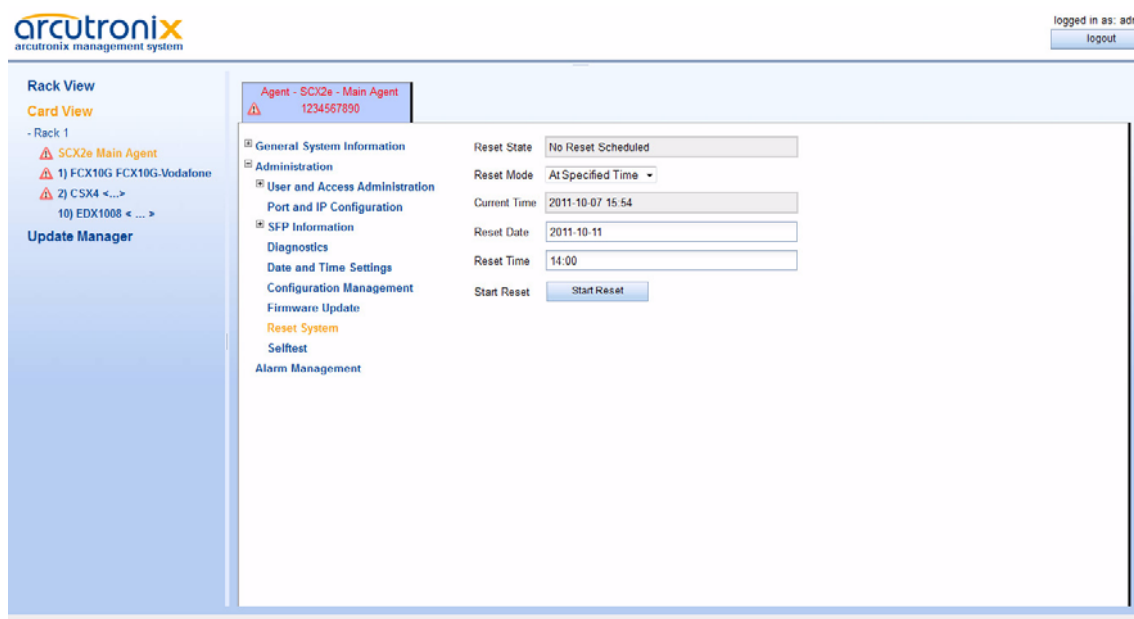


Figure 5-37 Reset System, @Specific Time

Table 5-28 provides information on the menu.

Table 5-28 Reset System Menu

Parameter	Description	Format	Default
Reset State	Indicates the device's reset state (No reset scheduled System is going down... Reset scheduled).	Display	No reset scheduled
Reset Mode	Defines the device's reset mode.	PullDownMenu • At specified Time • Immediate Reset	Immediate Reset
Current Time ⁱ	Indicates the current device's date and time (dd.mm.yyyy hh:mm:ss).	Display	no default
Reset Date ⁱ	Enter the date for restart (dd.mm.yyyy).	Display/Input	no default
Reset Time ⁱ	Enter the time for restart (hh:mm:ss).	Display/Input	no default

Table 5-28 Reset System Menu (continued)

Parameter	Description	Format	Default
Reset System	Press Enter to confirm the settings.	Confirm	
Error State	Indicates the result of an system reset (Ok Reset Date/Time is in the past Reset Date/Time does not exist Not allowed (download active).	Display	no default

i. This menu item is only visible, when the Reset Mode is set to "At specified time".

Selftest

The Selftest can be used to check, whether the unit is still working well. After starting the self-test the status and results are shown in the entries below.

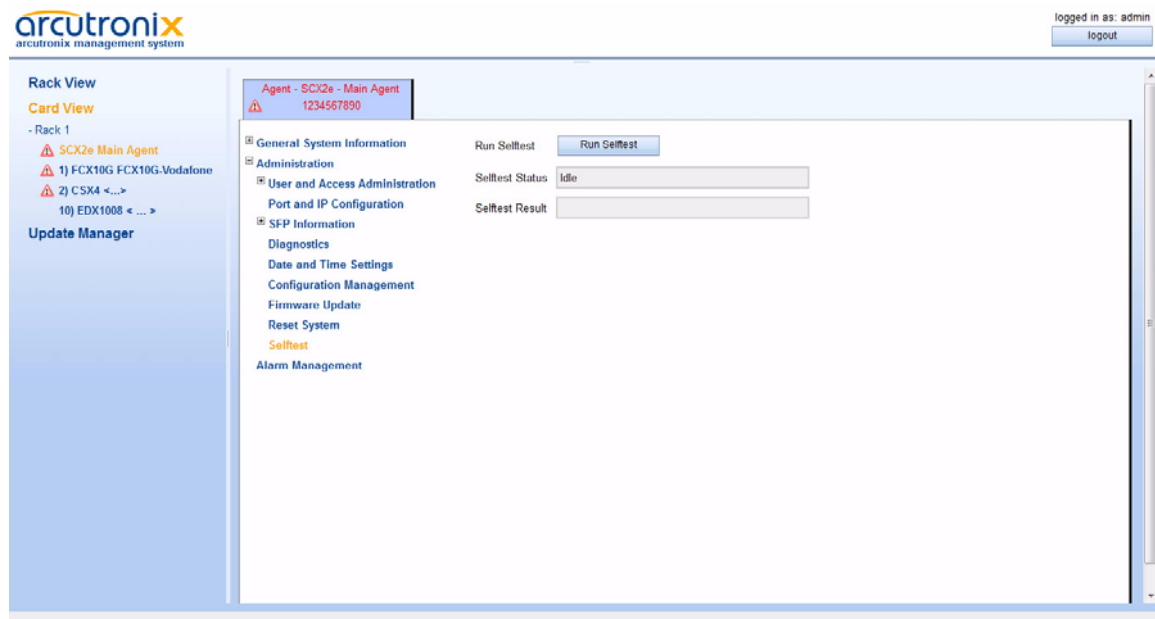


Figure 5-38 Selftest

Alarm Management

The Alarm Management view is designed to give a quick and detailed overview to the status of the SCX2e, the chassis and the line-cards. Many details about usage of the Alarm Management is given in "Alarm Management" on page 4-7. Please read this chapter before using the Alarm Management.

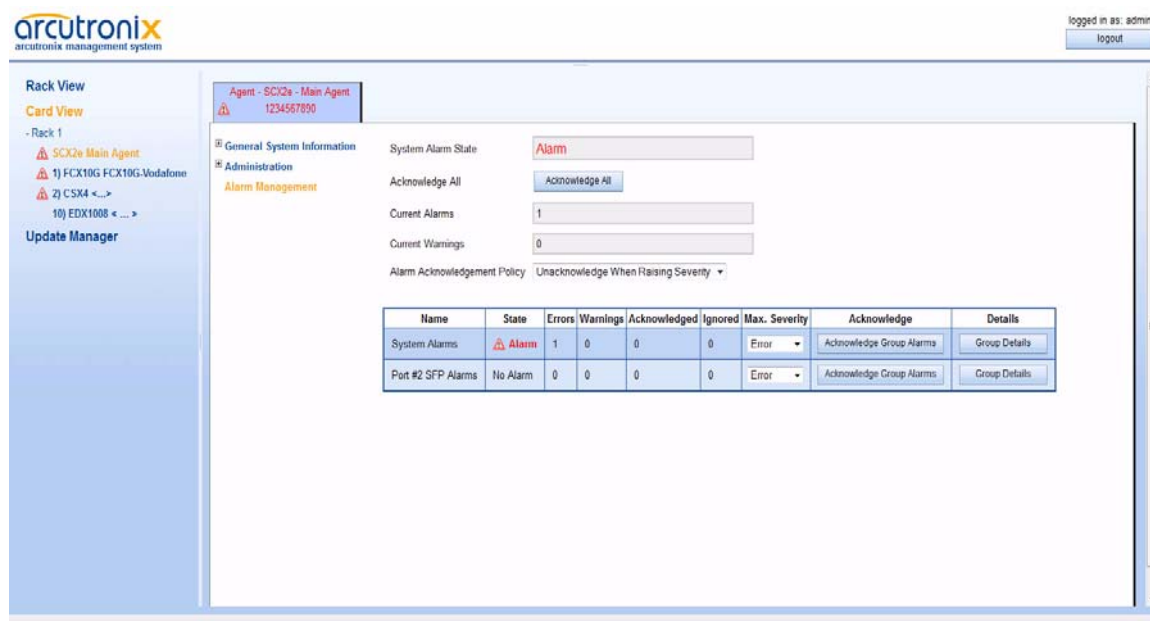


Figure 5-39 Alarm Management

On the top of the menu the summary of alarms and warnings is presented. If there is any active alarm or warning, this is shown here. One can press the “Acknowledge All”-button to affirm that all these problems are noted (and accepted). This will stop the alarm/warning condition of the SCX2e, e.g. the LED and alarm relay status are reseted.

As there are many different alarms, several alarm-groups were defined.

1. System Alarm Group
2. SFP Alarms

The alarms in these groups can be acknowledged together and the max. severity level can be defined. If for example the Systems Alarm Group has a max. severity level of “Warning”, no “Error” can be raised from any group member.

Each alarm can be configured to trigger an SNMP-trap, when the alarm state is changing (alarm raise and fall). This can be done inside the different alarm groups.

Table 5-31 provides information on the menu of the Alarm Management.

Table 5-29 Alarm Management

Parameter	Description
System Alarm State	Status of the unit. This status is shown on the ALM-LED and in case of Alarm, the relay is closed.
Acknowledge All	Press button to confirm the alarms.
Current Alarms	Summary (number) of all active alarms.

Table 5-29 Alarm Management (continued)

Parameter	Description
Current Warnings	Summary (number) of all active warnings.
Alarm Acknowledgement Policy	<p>What shall be done, when an alarm/warning has been acknowledge by administrator:</p> <p>Keep Acknowledged until Inactive:</p> <ul style="list-style-type: none">The acknowledge alarm/warning will be kept in this status, until the alarm-cause is gone. <p>Unacknowledged when raising Severity:</p> <ul style="list-style-type: none">The acknowledge alarm/warning will be kept in this status, until the severity gets worse. (Default) <p>Unacknowledged on State Change:</p> <ul style="list-style-type: none">The acknowledge alarm/warning will be kept in this status, until the alarm-cause changes its state.

System Alarm Group

The System Alarm Group incorporates all the system alarms:

- Line alarm from the line-cards,
- Reset state of the SCX2e,
- Status of interfaces MGMT1 and MGMT2,
- Temperature and
- Rack voltage.

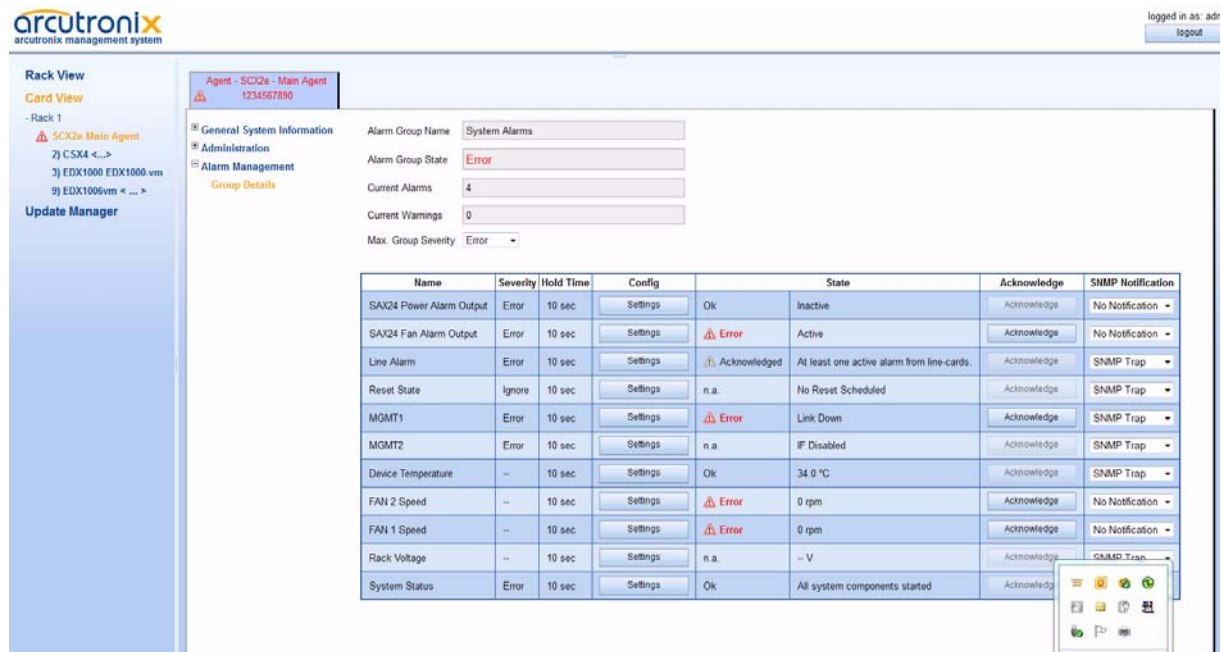


Figure 5-40 System Alarm Group Management

Table 5-31 provides information on the menu of the System Alarm Group Management.

Table 5-30 System Alarm Group Management

Parameter	Description
SAX24 Power Alarm Output ⁱ	The SAX24 module does have its own power supervision unit, which monitor the voltage on the backplane. If this unit detects a problem, the SAX24 Power Alarm can be raised. It can be configured to be used with error or warning level.
SAX24 Fan Alarm Output	The SAX24 module does have its own fan supervision unit. If this unit detects a problem, the SAX24 Fan Alarm can be raised. It can be configured to be used with error or warning level.
Line Alarm	A summary of all active alarms of the line-cards. Each line-card (LC) can be configured individually to raise alarms depending on the status. If an alarm is raised, the LC will announce this to the SCX2e on an accumulative signal, which is presented here.
Reset State	The “Reset States Alarm“can be raised, when a reset is scheduled. It can be configured to be used with error or warning level.
MGMT1 State	The “MGMT1 Status Alarm” can be raised, when the MGMT1 is in error. It can be configured to be used with error or warning level.

Table 5-30 System Alarm Group Management (continued)

Parameter	Description
MGMT2 State	The “MGMT1 Status Alarm” can be raised, when the MGMT1 is in error. It can be configured to be used with error or warning level. As MGMT2 is a combo port, either the copper or the fibre part can be sourcing the alarm.
Device Temperature	Value of the rack’s temperature. The warning and alarm level can be configured separately. It can be configured to be used with error or warning level.
FAN 2 Speed	The fan rotation on the SAX24 module is measured and supervised by the rack control unit of the SCX2e. If this unit detects a too low speed it can raise an alarm. It can be configured to be used with error or warning level.
FAN 1 Speed	The fan rotation on the SAX24 module is measured and supervised by the rack control unit of the SCX2e. If this unit detects a too low speed it can raise an alarm. It can be configured to be used with error or warning level.
Rack Voltage	Backplane voltage, which feeds the rack. The warning and alarm level can be configured separately for low voltage as well as for too high voltage. The value should be 4.9V ... 5.1V.
System Status	This alarm raises, when an error occurred during start of the system or on run-time. When the system detects any application that cannot be started or must be stopped due to HW problem, the alarm raises. It can be configured to be used with error or warning level.

i. Only visible, when a SAX24 module is plugged into the chassis.

In the overview tablet, the details for the events and configuration concerning severity is given. Events can be configured in the “Settings” submenu for more details.

Detailed Alarm Settings

Each alarm can be configured in detail to set the severity and hold-time. For analogue alarms the limits for warning and error-level can be defined. All alarms do have predefined settings, which can be normally left untouched.

The severity defines whether the alarm

- to be ignored,
- to be a warning or
- to raise an error.

Some events need thresholds to know when a warning and when an error must be raised. E.g. the thresholds for temperature in the picture below:

Warning = 50 °C; Alarm = 60 °C

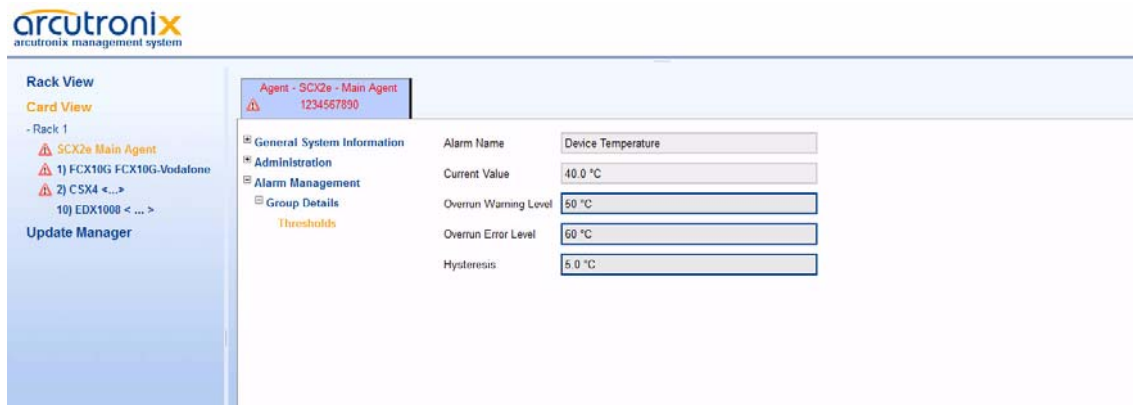


Figure 5-41 Temperature Threshold

NOTE: For analogue alarms it is possible to define the warning level at a higher value than the error level. E.g. for the temperature it is possible to define the warning @60°C and the error @55°C. This is not forbidden by the system, as there might be customer’s reason to do so.

The “Alarm Hold Time” is the amount of time, for which an alarm will be active after rising. No change in the status will be indicated during hold time.

Port#2 SFP Alarm Group

The SFP Alarm Group incorporates all the alarms related to SFP (of port MGMT2):

- RX and TX power,
- TX bias current,
- SFP supply voltage and
- SFP temperature

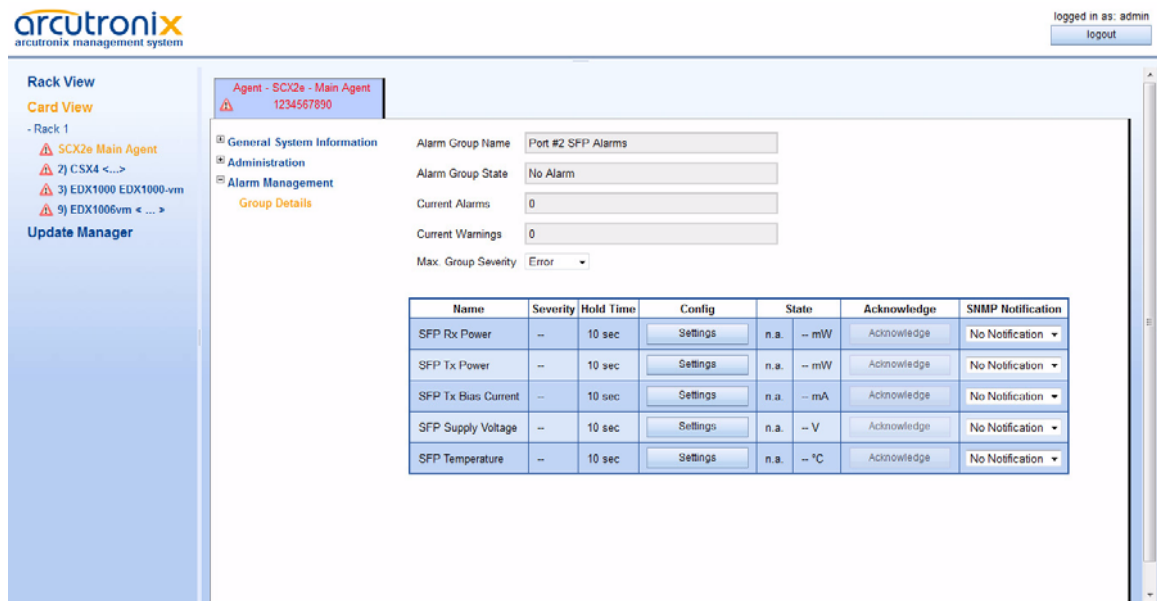


Figure 5-42 SFP Alarm Group Management

Table 5-31 provides information on the menu of the Alarm Management menu.

Table 5-31 SFP Alarm Group Management

Parameter	Description
SFP Rx Power ⁱ (mW)	<p>The “SFP RX Power Alarm” can be raised, when the SFP’s RX power is below a configurable value (Thresholds). The warning and alarm level can be configured separately. The allowed value depends on the used SFP.</p> <p>Here all values are used in mW units.</p>
SFP Tx Power ⁱ (mW)	<p>The “SFP TX Power Alarm” can be raised, when the SFP’s TX power is below a configurable value (Thresholds). The warning and alarm level can be configured separately. The allowed value depends on the used SFP.</p> <p>Here all values are used in mW units.</p>
SFP TX Bias Current ⁱ (mA)	<p>The “SFP TX Bias Alarm” can be raised, when the bias current of the SFP’s TX is below a configurable value (Thresholds). The warning and alarm level can be configured separately. The allowed value depends on the used SFP.</p>

Table 5-31 SFP Alarm Group Management (continued)

Parameter	Description
SFP Supply Voltage ⁱ (V)	The “SFP Supply Voltage Alarm” can be raised, when the power supply of the SFP is below a configurable value (Thresholds). The warning and alarm level can be configured separately. The allowed value depends on the used SFP. Common value should be 3.3V +/- 5%.
SFP Temperature ⁱ (°C)	The “SFP Temperature Alarm” can be raised, when the temperature of the SFP is above (or below) a configurable value (Thresholds). The warning and alarm level can be configured separately.

i. Only valid, when the plugged SFP supports digital diagnostic functions (DDF) according [SFP MSA].

In the overview tablet, the details for the events and configuration concerning severity is given. Events can be configured in the “Settings” submenu for more details. See “Detailed Alarm Settings” on page 5-59.

Update Manager

The Update-Manager is the menu to govern the update files and the time of update and installation for line-cards.

NOTE: The Update Manager is only used for the line-cards. For updating the SW of the SCX2e, please use the “Firmware Update” as written in “Firmware Update” on page 5-48.

All the available update-files are grouped together for the different types of line-cards. This makes it easier to handle and makes sure not to install wrong files on the line-cards.

Any information of the installed files (date, size etc.) are shown in the table and, if available, also the release notes.

Update Manager

arcutronix
arcutronix management system

logged in as: admin
logout

Rack View
Card View
Update Manager
+ CSX4
+ EDX1008
+ FCX10G

1)

Update Manager

Upload section and disk space

Upload new update file

Device	Total space (MByte)	Space left (MByte)
Main Storage on SCX2e	34	26

Select File Upload File

2)

3)

Available update files

Filename	Release Notes	Build Date	Filesize (kByte)	Designated for
266000AB11.BIP	N/A	Sep 16 2008	189	CSX4, softwarefamily 2660
266000AB12.BIP	N/A	Apr 24 2009	190	CSX4, softwarefamily 2660
CSXA001V04.BIP	N/A	Apr 13 2010	301	CSX4, softwarefamily CSXA
CSXANB1V04.BIP	N/A	Jul 31 2010	302	CSX4, softwarefamily CSXA
edx-V2_1_15p20-vm.zip	Release Note	Mar 9 2010	6401	EDX, softwarefamily EDX

Figure 5-43 Update Manager

The Update Manager is divided in 3 sections:

1. On the left side is the Explorer Bar.
The Explorer Bar shows all plugged device-types, grouped together according their nature of software. See below for a list of available device-groups.
The right side is divided in two parts, the Upload Section and the File Section:
2. The Upload Section offers the possibility to upload new Update-files for line-cards and gives an overview to available and remaining disk space on the SCX2e. If there is not enough disk-space left, one can deallocate memory by deleting older update-files (see below).
3. The File Section is a list of all stored update-files with the corresponding information and release notes. If an older version of update-file is not longer needed or disk-space must be deallocated, one can do this here with the help of the “Delete File” button.

Update Manager Device-Specific

For each group of devices, which do use the same update-file, an entry in the left Explorer Bar is shown. When selecting one entry here, the device-specific menu is shown. This menu is organized in the same way for all different groups of devices. The

reduction to possible selectors and update-combinations makes it easier to handle the update process. Less problems and errors will occur with this concept.

In the following the update menu for CFX-devices will be shown, but the explanations are valid for all groups.

The screenshot shows the Arcutronix management system interface. The top right corner indicates the user is logged in as 'admin' with a 'logout' button. The left sidebar contains navigation options: 'Rack View', 'Card View', 'Update Manager', and 'CFX2'. The main content area is titled 'Update Manager for device of type CFX2' and is divided into four sections:

- Registered devices in Rack:** A table listing devices with columns for Position, Info, Softwareversion, and Status. Each row has a 'Select this device' checkbox and a 'Ready for Update' status. A 'Select all devices' checkbox is at the bottom.
- Update control for selected devices:** A form with fields for 'Start update immediately' (checkbox), 'or select date (YYYY-MM-DD)' (text input), 'and time (hh-mm)' (text input), 'Select the update file' (dropdown menu), and a 'Start Update' button.
- Available update files:** A table listing update files with columns for Filename, Release Notes, Build Date, Filesize (kbyte), and Designated for. Each row has a 'Delete File' button.
- Upload section and disk space:** A section for uploading new update files, including a 'Select File' button, an 'Upload File' button, and a table showing disk space usage for 'Main Storage on SCX2e'.

Figure 5-44 Update Manager Device-Specific

The Update Manager Device-specific is divided in 4 sections:

1. In the table on the top, one can see all plugged devices, which belong to this SW-update group. In the column “Select this device” one can decide, which of the plugged devices shall get an SW-update. The button “Select all devices” helps for quick selection.
2. The second table is to schedule the update and to select, which update-file has to be used. It can be either an immediate update or one can specify and time/date in the future. Press “Start Update” to take the settings in place and launch the timer (if required).
3. The table called “Available update files” is a list of all locally stored update-files for the selected group. An overview on the available information is given.

This list is the same as File Section in the Upload Manager, reduced to the selected group of devices.

4. On the bottom the Upload Section, as depicted in the Upload Manager, an overview of the available and free memory space is presented. In addition one can start a new file upload from here.

Note: One can upload here any file. If the uploaded is not fitting to the selected upload-group, it will not be shown, unless one select the right group or change into the Upload Manager.

Chapter 6

SNMP and MIBs

This chapter provides information on the SNMP and the management information bases (MIBs) used by the SCX2e.

SNMP Access Generally

The growing global network 'Internet' was the home of plans to simplify network maintenance by defining a maintenance protocol, which would allow network managers to control network equipment via the network itself. This protocol was given the name SNMP (Simple Network Management Protocol). As the name implies, SNMP was originally planned as an intern solution. However, SNMP became widely used and is now a universal standard.

What is the difference between equipment with and without SNMP? Generally, SNMP featured equipment has:

- Added intelligence to talk SNMP and to get and set unit parameters
- An own unique network address
- Some kind of local management port

Network management by SNMP requires at least two partners:

- Network equipment with SNMP software, called 'agent'
- A network station, running some kind of network management software

The two partners communicate via the net using SNMP. The network management station sends configuration commands and data requests to the network equipment. The network equipment responds to requests by sending the requested data. Additionally, traps are triggered by certain events in the network equipment. Traps are data packets containing information about these events. Their destination is a (or multiple) network management station, where the information is collected. SNMP traps enable an agent to notify the management station(s) of significant events by way of an unsolicited SNMP message.

Network configuration information, in particular configuration commands, is sensitive data and must therefore be protected against prying eyes. SNMP deals with this problem by implementing something called a 'community'. A community is comparable to a password and gets attached to each SNMP message. The attached community allows the receiving SNMP partner to decide if the transmitting partner is allowed to force the execution of the command.

The arcutronix Multi Service System supports two versions of SNMP: SNMPv2c (version2, community-based) and SNMPv3.

SNMPv2c

Community-Based Simple Network Management Protocol version 2, or SNMPv2c, is defined in IETF RFC 1901-RFC1908. SNMPv2c revises version 1 and includes improvements in the areas of performance, confidentiality, and manager-to-manager communications. It introduced GETBULK, an alternative to iterative GETNEXTs for retrieving large amounts of management data in a single request. SNMPv2c uses the same simple community-based security scheme as the former variant SNMPv1. While officially only a “Draft Standard”, this is widely considered the de facto SNMPv2 standard.

SNMPv3

SNMPv3 makes no changes to the protocol aside from some addition of cryptographic security. SNMPv3 primarily added security and remote configuration enhancements to SNMP. Security has been the biggest weakness of SNMP since the beginning. Authentication in SNMP Versions 1 and 2 amounts to nothing more than a password (community string) sent in clear text between a manager and agent.

Each SNMPv3 message contains security parameters which are encoded as an octet string. The meaning of these security parameters depends on the security model being used.

SNMPv3 provides important security features:

- Confidentiality - Encryption of packets to prevent snooping by an unauthorized source.
- Integrity - Message integrity to ensure that a packet has not been tampered with in transit including an optional packet replay protection mechanism.
- Authentication - to verify that the message is from a valid source.

Traps

SNMP encourage trap-directed notification. The idea behind trap-directed notification is as follows: if a manager is responsible for a large number of devices, and each device has a large number of objects, it is impractical for him to poll or request information from every object on every device. The solution is for each agent on the managed device to notify the manager without solicitation. It does this by sending a message known as a trap of the event or NOTIFICATION.

After receiving the event, the manager displays it and may choose to take an action. For instance, the manager can poll the agent directly, or poll other associated device agents to get a better understanding of the event.

Trap-directed notification can result in substantial savings of network and agent resources by eliminating the need for frivolous SNMP requests. However, it is not possible to totally eliminate SNMP polling. SNMP requests are required for discovery and topology changes. In addition, a managed device agent can not send a trap, if the device has had a catastrophic outage.

Installation Prerequisites

This section provides the installation prerequisites for SNMP.

Prerequisites for SNMP management:

- A management station with an Ethernet 10/100BaseT respectively RS232 interface.
- Management software for SNMP management (e.g. SNMPc, HP Openview).
- A VT100 compatible terminal or PC with terminal software (only used for initial installation).

Preparing the SNMP Management System

Before managing the SCX2e by SNMP, one has to prepare the SNMP management system. First install the MIBs for the SCX2e and second configure the correct access parameters.

You can download the MIB from the ax intranet (www.arcutronix.com/customer):

Login: **User = p49170644-0**
 Password = 1qayxsw2

A MIB (Management Information Base) is a kind of database, which tells the network management station about specific capabilities of the new equipment. Add the contained MIBs to the MIBs already known to your management system. Generally, you have to recompile the MIB database to include the new information.

Configure your management station to use SNMPv2c for read and write access mode and enter the community strings for read/write and read-only access.

Management Information Bases (MIBS)

The MIBs (Management Information Bases) define the variables which are used to control a (SNMP-) device or to retrieve operational data from the device. The MIB consists of collections of managed objects identified by object identifiers (see below). MIBs are accessed using the simple network management protocol (SNMP). A managed object (sometimes called a MIB object or an object) is one of a number of characteristics of a managed device.

System MIB variables are accessible through SNMP as follows:

- Accessing a MIB variable—Function is initiated by the SNMP agent in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- Setting a MIB variable—Function is initiated by the SNMP agent in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

SNMP and MIBs

Management Information Bases (MIBS)

An object identifier (OID) uniquely identifies a MIB object on a managed network device. The OID identifies the MIB object's location in the MIB hierarchy, that can be depicted as a tree with a nameless root. The levels of which are assigned by different organizations, such as IANA. This model permits management across all layers of the OSI reference model.

The MIBs for arcutronix's SNMP management are based on the arcutronix naming convention. The root-OID tree structure is accessible via

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).arcutronix(30507)

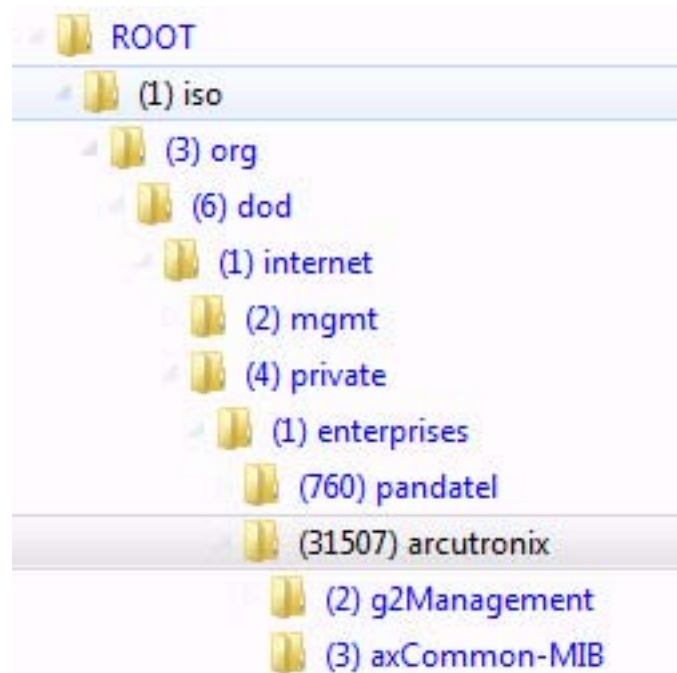


Figure 6-1 The SNMP ax-MIB Tree (1.3.6.1.2.4.1.31507)

Each number in the OID corresponds to a level of MIB hierarchy. For example, the OID 1.3.6.1.4.1.31507.3.xyz represents the .xyz with the location in the MIB hierarchy as follows. (Note that the numbers in parentheses are included to help show correspondence to the MIB hierarchy. In actual use, OIDs are represented as numerical values only.)

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).arcutronix(31507).axCommon-MIB(3).nn-MIB

The format of the MIBs as well as global sections are defined in the SNMP standard. MIBs are written in a special language (ASN 1) and are plain ASCII text. Thus they can be read using any available editor.

The MIBs can be enhanced at any time, so please refer to the MIBs itself for documentation.

Chapter 7

SSH and CLI

The SCX2e can be configured via a text-based Command Line Interface (CLI), which can be reached over a Secure Shell (SSH) connection. Only a SSH-client and an IP-connection to the device is needed. This chapter will explain how to connect to the CLI/SSH and its usage.

Access to the Device

The SCX2e CLI can be accessed either via the two (local) management ports (called "MGMT1" and "MGMT2" interface). Both interfaces use different IP-addresses, but the behaviour and the usage from SSH/CLI point of view is just the same.

SSH connection

There are many SSH client-SW on market, which are mainly freeware. We at arcutronix use normally the putty-ssh client and or the Tera Term. All the following examples are related to puTTY-ssh and/or TeraTerm-ssh.

To connect to the SCX2e SSH-server establish a link via TCP/IP:

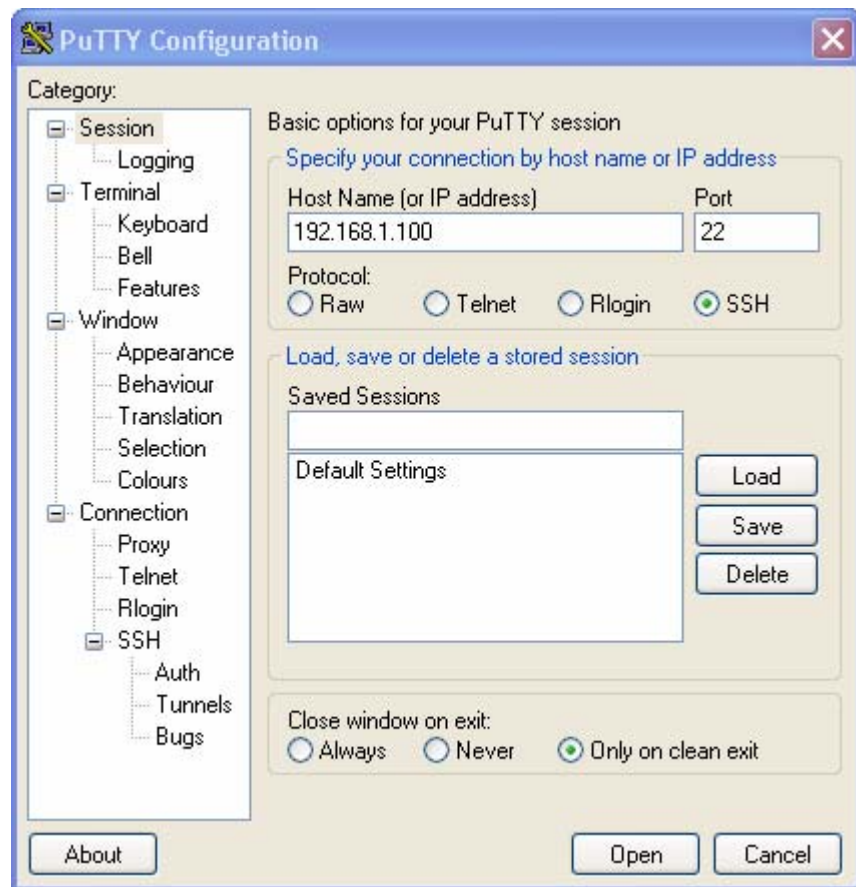


Figure 7-1 PuTTY ssh-Connection

After pressing “Open”, the Secure Shell will be opened and a prompt is visible.



Figure 7-2 Secure Shell

Now enter the username, which shall be used for the communication (e.g. admin) and enter the password (e.g. private).

The next message is "Welcome <username> !" and the connection is established.

SSH connection with public keys

A more secure method of authentication is through the use of RSA keys. The basic principle is as follows: RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.

Any host to which the user wants to connect must be aware of his public RSA key, as the server uses it during the authentication process. The user must place his public key living on the originating client machine, into his own `authorized_keys` file on the server.

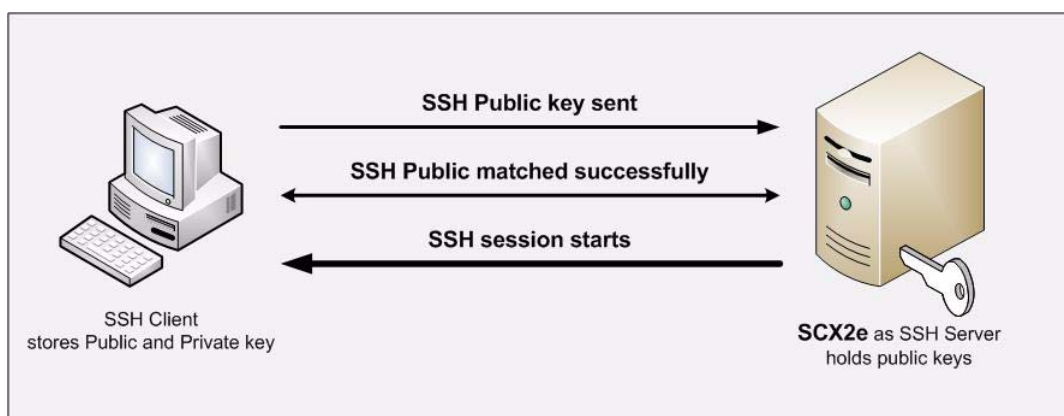


Figure 7-3 Secure Shell - Public Key

When he wants to connect to that server, ssh will first negotiate an encrypted session, then send the server the client's public key. The server checks that the public key is in the user's `authorized_keys`. If so, the server sends the client a challenge (a random number encrypted with the user's public key). If the client can then send back the random number decrypted, it has just proven that it has the private key (there is no other way to decrypt the challenge number), and is therefore authentic.

The user's private key is a very sensitive piece of data - with it, anyone can connect to any host on which the corresponding public key is in the `authorized_keys`. Therefore, the user's private key is never written to disk decrypted.

Public key authentication solves this problem. You generate a key pair, consisting of a public key (which everybody is allowed to know) and a private key (which you keep secret and do not give to anybody). The private key is able to generate signatures. A signature created using your private key cannot be forged by anybody who does not have that key; but anybody who has your public key can verify that a particular signature is genuine.

The Authentication layer uses one or more of the following authentication methods to validate the user:

1. Password Authentication
2. RSA/DSA Public-Key Authentication
3. Kerberos Authentication
4. Host-based Client Authentication

We have focused only on the RSA Public-Key based Authentication in this process.

Security Issues

The SSH/CLI is accessible via any TCP/IP link to the device, so it might be that other persons than the intended ones get connection and will see the login prompt. To avoid forbidden configuration or burglary of information, the access is protected against intruders via username and password.

Any time you connect or reconnect to the initialized SCX2e the login-window is displayed and a password request turns up on the terminal.

Be careful with passwords! If you write them down, keep them in a safe place. Do not choose strings easy to hack. In particular, do not use the default strings which were valid when you received the device.

Do not forget your password. If you forget your password the device will be rendered useless and will have to be sent back to the factory for basic re-configuration.

NOTE: Three different access-level are selectable with different access rights:

1. Guest (only view)
2. User (view and modify)
3. Admin (full access inclusive user administration)

If the device is started-up the very first time, only the user “admin” is defined. See in “User and Access Administration” on page 5-13, how to define the other users and how to change the user password.

Command Line Interface (CLI)

The CLI is organized just in the same way as the Web-OPI. It has the same menu-structure and options. The “navigation” within the CLI-menus and the access to the management-variables will be depicted in the next chapter.

CLI Editor Features

Context Sensitive Help

SCX2e-CLI offers context sensitive help. This is a useful tool for a new user because at any time during an ssh-session, a user can type a question mark (?) to get help. Two types of context sensitive help are available - word help and command syntax help.

Word help can be used to obtain a list of commands that begin with a particular character sequence. To use word help, type in the characters in question followed immediately by the question mark (?). Do not include a space before the question mark. The router will then display a list of commands that start with the characters that were entered.

Command syntax help can be used to obtain a list of command, keyword, or argument options that are available based on the syntax the user has already entered. To use command syntax help, enter a question mark (?) in the place of a keyword or argument. Include a space before the question mark. The router will then display a list of available command options with <cr> standing for carriage return.

Command Syntax Check

If a command is entered improperly (e.g. typo or invalid command option), the CLI will inform the user and indicate where the error has occurred.

Command Completion

Commands can not be abbreviated but commands and keywords can always be completed with <TAB>. For example, you can abbreviate the "config" command to "c<TAB>" because "config" is the only command that begins with "c" and the <TAB> will complete it. If there are more than one possible completion, the CLI will show them to give you help. For example, "s<TAB>" can be "show" and/or "select". Both commands will be shown.

Hot Keys

For many editing functions, the SCX2e-CLI editor provides hot keys. Table 7-2 lists some editing short-cuts that are available.

Table 7-1 SCX2e CLI Hot Keys

Hot Key	Description
Delete	Removes one character to the right of the cursor.
Backspace	Removes one character to the left of the cursor.
TAB	Completes a partial command.
Ctrl-A	Moves the cursor to the beginning of the current line.
Ctrl-B	Moves the cursor one word to the left.
Ctrl-D	Removes one character to the right of the cursor.

Table 7-1 SCX2e CLI Hot Keys (continued)

Hot Key	Description
Ctrl-I	Finishes a partial command.
Ctrl-J	Repeats the last command.
Ctrl-H	Removes one character to the left of the cursor.
Ctrl-N	Erases a line.
Ctrl-M	<CR>.
Up Arrow	Allows user to scroll forward through former commands.
Down Arrow	Allows user to scroll backward through former commands.

NOTE: The most helpful Hot-Key is the TAB. It allows inexperienced users to complete commands, gives correct syntax and shows possible entries at all stages!

Commands

Once an ssh-session is established, one can navigate within SCX2e-CLI like in a hierarchically structured tree. The structure is the same as for the Web-OPI. Command options and applications vary depending on position within this hierarchy.

To assist users in navigation through SCX2e-CLI, the command prompt will change to reflect the position of a user within the command hierarchy. This allows users to easily identify where within the command structure they are at any given moment. Also a <Tab> shows all possible options at the given position. This gives easy possibility to identify “Tab-by-Tab” the correct command.

NOTE: A <blanc> inside a string must be preceded by a back-slash (\) or the string must be wrapped by quotes. E.g.

```
$> mode "Rack View"          or  
$> mode Rack\ View
```

The “Tab-by-Tab”-feature helps here a lot to build always the correct syntax.

Table 7-2 is a summary of commands and the corresponding syntax.

Table 7-2 SCX2e CLI Commands

Command	Syntax / Explanation
help	<p>help [COMMAND]</p> <hr/> <p>HELP is in any context available and lists the possible commands in the given context. If HELP is used with a command, it shows the syntax of the command together with a short help-text.</p> <ul style="list-style-type: none"> • ARG COMMAND - any available command.
log	<p>log</p> <hr/> <p>LOG shows the last entries of agent's log file.</p>
config	<p>config [go up root SUBPAGE set OPTION VALUE do COMMAND [OPTION]]</p> <hr/> <p>CONFIG shows and changes configuration settings. Configurations are grouped and this command can also be used to display/change configuration group. Without an argument CONFIG shows the current configuration group and its settings/subgroups.</p> <ul style="list-style-type: none"> • ARG go up root SUBPAGE - Go to another config page. Choose a SUBPAGE from the current config page, go UP to the parent page or go to the ROOT page. Type config to see available subpages (marked with '>'). • ARG set OPTION VALUE - Set a new VALUE for a writable OPTION • ARG do COMMAND - Execute a config command (displayed with config as [Command]) • ARG OPTION - Show config OPTION
select	<p>select [agent [rack RACK] slot SLOT serial SERIAL DEVICENAME]</p> <hr/> <p>SELECT a device which should be configured in Cardview-mode.</p> <ul style="list-style-type: none"> • ARG agent - Select the agent card. • ARG rack RACK - Select device from RACK (integer). • ARG slot SLOT - Select device in slot SLOT (integer). • ARG serial SERIAL - Select device with serial number SERIAL. • ARG DEVICENAME - Select device DEVICENAME.
show	<p>show</p> <hr/> <p>SHOW presents the information about all available racks.</p>
mode	<p>mode [MODE]</p> <hr/> <p>With MODE one can easily switch between RACKVIEW and CARDVIEW.</p> <ul style="list-style-type: none"> • ARG MODE - Select mode MODE; available modes are: <ul style="list-style-type: none"> - MODE Card View - MODE Rack View

Table 7-2 SCX2e CLI Commands (continued)

Command	Syntax / Explanation
quit	quit
	Quit the current CLI session.

SCX2e-CLI Modes

Two modes are defined for the SCX2e-CLI:

- Rackview-Mode and
- Cardview-Mode

Rackview-mode is to get mainly information about the rack, the plugged cards, power supply etc. In Cardview-mode one can select one single card and gets direct access to it. One can configure, supervise and control cards only in Cardview-mode. To switch between the two modes, one has to use the `mode` command.

Rackview - Mode

In the Rackview-mode, one can get information about (all) the discovered racks and plugged cards.

NOTE: Rackview-mode is the Default after first login.

The Rackview-mode can be reached from any point within the CLI using the command `MODE`:

```
cardview $> mode Rack\ View
rackview $>
```

In Rackview-mode no settings or changes are possible. One can see all racks and cards and has the option to navigate to one of the discovered cards via “select”-command or to change to CardView-mode via “mode”-command.

Example SHOW

The following rack is given with cards plugged:

- 1x FCX4G (slot1)
- 1x FCX10G (slot2)
- 1x CSX4-E1 (slot4)
- 1x EDX1000 (slot7)
- 1x SCX2e
- 1x PS (slot ps1)

- 1x SAX24 (rear-side)

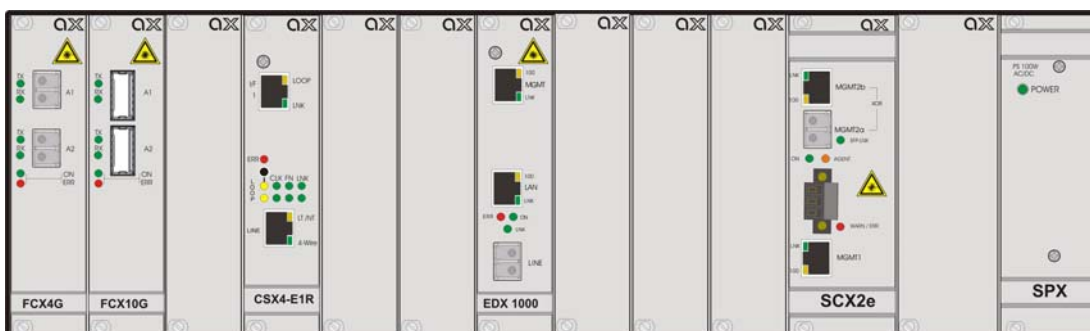


Figure 7-4 Example Rackview Mode

When entering “show” in the Rackview-mode, the following information is given:

```
Administrator: Windows PowerShell
rackview $> show
Rack 1 SCX2e "Main Agent": #2010003256, up 1d 04:18
      PowerSupply: up
      SAX24: up
Rack1:1 FCX4G "FCX4G-Test": #2010005684, up 00000000:00:51
Rack1:2 FCX10G "FCX10G-Vodafone": #2010005945, up 00000674:00:08
Rack1:4 CSX4 "CSX4-ax": #2010006389, up 00000089:01:24
Rack1:7 EDX1000 "EDX1000-vm": #2010002229, up 0d 00:02
rackview $>
```

Figure 7-5 Example Rackview Mode: SHOW command

All units are shown in a table with their

- Rack:Slotaddress,
- Type,
- Device-Name (if available): “name”,
- Serial Number (if available): #nnnnnnnnnn,
- Up-Time.

For the last entry (EDX1000) the 5 groups are separated by the green lines.

Example SELECT

The command SELECT gives you the chance to change into the Cardview-mode of a single card. If you want to select the EDX1000 in the example above, the following ways are possible.

SELECT by rack/slot address

```
rackview $> select rack Rack1 slot 7  
Rack1:7 EDX1000-vm [] $>
```

SELECT by name

```
rackview $> select EDX1000-vm  
Rack1:7 EDX1000-vm [] $>
```

SELECT by serial number

```
rackview $> select serial 2010002229  
Rack1:7 EDX1000-vm [] $>
```

The 3 ways are identical by result. The mode is changed to Cardview-mode and the device is selected.

The device-names “agent” and “Main Agent” are predefined to get quick access to the SCX2e card itself.

```
rackview $> select agent  
Agent SCX2e “Main agent”$>
```

Cardview - Mode

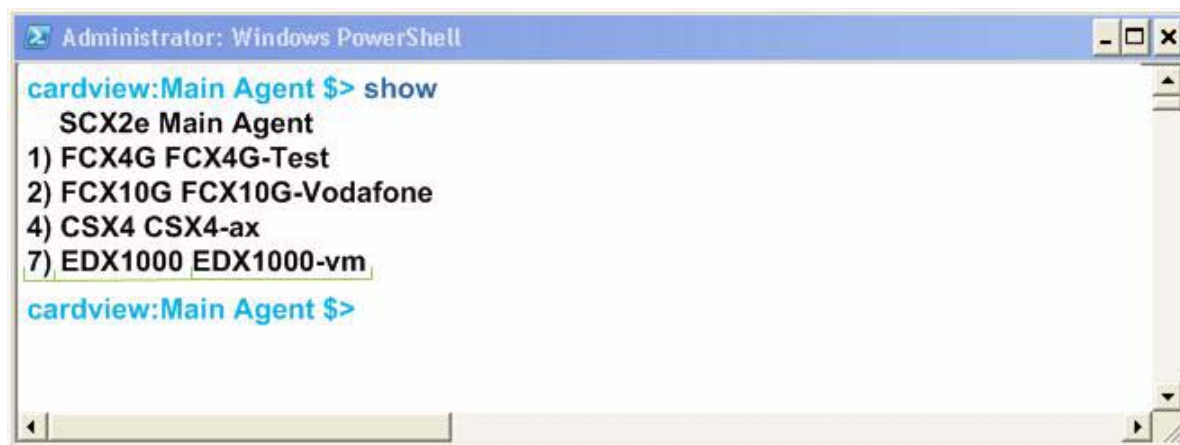
The Cardview-mode can be reached from any point within the CLI using the command MODE:

```
rackview $> mode Card\ View  
Agent SCX2e “Main Agent” $>
```

or by using the SELECT command (see examples above):

```
rackview $> select EDX1000-vm  
Rack1:7 EDX1000-vm [] $>
```

In the Cardview-mode each plugged and discovered (line-) card can be monitored and configured. When in Cardview-mode, the result of the command SHOW is slightly different than in Rackview-mode. In the example above (Figure 7-4) the result would like this:



```
Administrator: Windows PowerShell
cardview:Main Agent $> show
  SCX2e Main Agent
  1) FCX4G FCX4G-Test
  2) FCX10G FCX10G-Vodafone
  4) CSX4 CSX4-ax
  7) EDX1000 EDX1000-vm
cardview:Main Agent $>
```

Figure 7-6 Example Cardview-Mode: SHOW command

As already a dedicated card (and rack) is selected in Cardview-mode, only the cards in the same rack are visible and the information of the rack is not shown in Cardview-mode.

NOTE: The default card, which is selected, when no other card is explicitly selected is the agent card.

All units are shown in a table with their

- Slot-address,
- Type,
- Device-Name (if available): name

For the last entry (EDX1000) the 3 groups are separated by the green lines.

Example CONFIG

The command CONFIG is the most mighty tool in the SCX2e CLI. It is only available in Cardview-mode and gives access to the menu-structure of the selected card. The menu-structure of the individual card-types can vary. Please refer to the individual manuals of the different cards to get more information on the different menu-structures.

Within this document, the following examples will mostly depend on the SCX2e itself. The menu-structure of the SCX2e is shown in “Menu-Structure (Directory-Tree) of SCX2e” on page 7-17.

When entering the command CONFIG apart in any context (of the Cardview-mode), the available menu-entries are shown:

```
Agent SCX2e "Main Agent" / $> config
--Login
> General System Information
> Administration
> Alarm Management
> Firmware Update
```

The first 1-2 signs in the resulting overview are type-indicators which shows what can be done with this entry and which `config`-command can be used.

Table 7-3 Menu Indicators and corresponding CONFIG Commands

Type	Explanations / Examples
--	<p>Headline:</p> <p>This is the name of the shown menu. Nothing can be done with CONFIG; it is only a text.</p> <p>Example:</p> <pre>\$> config --LOGIN . . \$></pre>
>	<p>Sub-Menu:</p> <p>">" indicates a sub-menu, which can be accessed via</p> <p><code>CONFIG GO <sub-menu-name></code></p> <p>Example:</p> <pre>\$> config --Login > General System Information > Administration > Alarm Management > Firmware Update \$> config go Administration /Administration \$></pre>
*	<p>Changeable Management Variable</p> <p>"*" indicates a menu-entry which can be changed via</p> <p><code>CONFIG SET <variable-name> <value></code></p> <p>Example:</p> <pre>/General System Information \$> config --General System Information * Device Name: "Main Agent" . . . /General System Information \$> config set Device\ Name "New Name" /General System Information \$> config --General System Information * Device Name: "New Name" . . . /General System Information \$></pre>

Table 7-3 Menu Indicators and corresponding CONFIG Commands (continued)

+ Command
 “+” indicates a command-entry which can be invoked via
 CONFIG DO <command-name>
 Example:

```

/Administration/Reset System $> config
--Reset System
  Reset State: No reset scheduled
* Reset Mode: Immediate reset
+ [Start Reset]
/Administration/Reset System $> config do Start\ Reset

```

blanc Read-Only Variable
 No sign (or blanc character “”) indicates a read-only variable which can be read via
 CONFIG <variable-name>
 Example:

```

/General System Information $> config
--General System Information
.
.
.
Device Temperature: "35.5"
.
/General System Information $> config Device\ Temperature
"35.5"
/General System Information $>

```

There are some special CONFIG commands, which help to navigate:

Table 7-4 Special CONFIG Commands

Type	Explanations / Examples
	<p>Go back one directory in the directory-tree of the selected device in Cardview-mode.</p> <p>Example:</p> <pre> /Administration/Reset System \$> config go up /Administration \$> config go up \$> </pre>
	<p>Goto root directory of the selected device in Cardview-mode.</p> <p>Example:</p> <pre> /Administration/Reset System \$> config go root \$> </pre>

Quick Usage Guide for CLI-Commands

Table 7-5 Quick Reference

Select Agent:

```
$> select agent
```

Select Card in Slot 1:

```
$> select slot 1
```

Select Local/Remote Instance of Connectivity Products:

```
$> config go Local  
$> config go Remote
```

Show options in actual menu:

```
$> config
```

Change (User-) Name (e.g. FCX10G): [Local -> Maintenance -> General Information -> User Name]

```
$> config go root  
$> config go Local  
$> config go Maintenance  
$> config go General\ Information  
$> config set User\ Name "new Name"
```

Reboot Device (e.g. FCX10G): [Local -> Maintenance -> Update]

```
$> config go root  
$> config go Local  
$> config go Maintenance  
$> config go Update  
$> config set Reboot\ flash\ 1\ software
```

View Alarms (e.g. FCX10G): [Local -> System Monitor]

```
$> config go root  
$> config go Local  
$> config go system\ Monitor  
$> config
```

Clear Alarms (e.g. FCX10G): [Local -> System Monitor -> Clear Current Alarms]

```
$> config go root  
$> config go Local  
$> config go system\ Monitor  
$> config set Clear\ Current\ Alarms clear_now
```

Go back 1 Step in Menu:

```
$> config go up
```

Table 7-5 Quick Reference (continued)

Go back to Top-Level Menu (/):

```
$> config go root
```

Example for ssh-Script

TeraTerm and other ssh-clients are supporting scripting to execute commands in always the same way. In the following, a short example for an TeraTerm-script is given to show the initial setup to a host and how to enter some simple commands.

The script will do the following:

1. Connect to the device (192.168.0.100) with username “admin” and password “private” using ssh2
2. Change to Cardview-mode of SCX2e,
3. Change the units name to “test-unit with new name”,
4. Disconnects the session.

Table 7-6 Example for ssh-Script

Step	Code
0	<pre>;; Tera Term Macro ;; ===== ;; file __prog_SCX2e.ttl ;; ;; desc Example for Teraterm programming-file. ;; ===== ;; HISTORY ;; ;; 2011-02-21 arcutronix GmbH Initial Version ;; ;; =====</pre>
1	<pre>;; open Tera Term ;; connect '192.168.0.100 /ssh /2 /auth=password /user=admin /passwd=private</pre>
2	<pre>wait 'rackview \$> ' sendln 'mode "Card View" ' wait '\$>' sendln 'select agent'</pre>

SSH and CLI

Example for ssh-Script

Table 7-6 Example for ssh-Script (continued)

```
3  wait ' $>'
   sendln 'config go "General System Information"'
   wait ' $>'
   sendln 'config set "Device Name" "test-unit with new name"'

4  pause 1
   disconnect 0
   end
```

Menu-Structure (Directory-Tree) of SCX2e

Level	1	2	3	4	5	6	7	8	9	Comment
--	LOGIN									
>	General System Information									
	*	Device Name								
		Located in Rack								
		Date and Time								
		Current System Uptime								
		Total System Uptime								
		Device Temperature								
L		Rack Name		Location		Contact Person				List of Entries w 3 columns.
	>	Rack details								
	*	Rack Name								
	*	Rack Location								
	*	Contact Person								
		Rack Order Information								
		Rack Article Number								
		Rack Voltage								
		Powerbudget								
		PS1 Order Information								
		PS2 Order Information								
		FAN 1 Speed								
		FAN 2 Speed								
	>	Inventory								
		Device Type								
		Serial Number								
		Article Revision								
		Hardware Revision								
		Software Version								
		Software Details								
		Date of Production								
		Manufacturer								
		Order No.								
>	Administration									
	>	User and Access Administration								
	*	HTTP Access								
	*	SSH CLI Access								
	*	SNMP Access								
	>	Users and Passwords								
	L		User Name		Read Access		Write Access		*Status	List of Entries w 4 columns.
	>	Modify Account								
		Username								
]	Change Password								
	*	Password								
	*	Read Access								
	*	Write Access								
	+	Delete Account								
	>	Add New Account								
]	Create Account								
	*	Username								
	*									
	*	Read Access								
	*	Write Access								
	>	SSH Access								

continues on next page ...

SSH and CLI
Menu-Structure (Directory-Tree) of SCX2e

... continues from previous page

	SSH CLI Access				
	* SSH CLI Port				
	SSH Host Key Fingerprint				
	> SSH Passwords				
	* Password Authentication				
] Change Password				
	*				
	> SSH Keys				
	L Cipher Bits Key ID *User *Comment *Used as *Status Delete				List of Entries w 8 columns.
	+ Delete Key				
	* Select Public SSH Key				
	> SNMP Access				
	SNMP Access				
	* SNMP Version				
	* SNMP UDP Port				
	* SNMP Max Message Size				
	* SNMP Engine ID Mode				
	* SNMP Engine ID				
	* SNMP Access Configuration				
	> SNMP Users				
	> SNMPv2 Communities				
	L *Community *Access Level *State				List of Entries w 3 columns.
	+ Delete Community				
	+ Add Community				
	> SNMPv3 Users				
	L Name Authentication Access Level Encryption *State				List of Entries w 5 columns.
	> Edit Settings				
] Apply				
	* User Name				
	* Access Level				
	* Authentication Type				
	* Encryption Type				
	* Status				
	+ Delete Entry				
	+ Add User				
	> SNMP Traps				
	* SNMP Authen Traps				
	* Event Log History Size				
	* Event Log Traps				
	* INFO Message Traps				
	* ERROR Message Traps				
	* ALARM Message Traps				
	SNMP Trap Counter				
	L IP Address UDP User Version Type State				List of Entries w 6 columns.
	> Edit Settings				
	* IP Address				
	* UDP Port				
	* Security Name				
	* SNMP Version				
	* Notify Type				
	* Status				
	+ Delete Entry				
	+ Add Trap Receiver				
	> Port and IP Configuration				
	* IP Default TTL				

continues on next page...

... continues from previous page

		* Default Gateway Address				
		Is Gateway Reachable				
	L	 Name Type Mech. Status Address 			List of Entries w 5 columns.	
		> Edit Port Settings				
		* Port Name				
		* Port State				
		HW MAC Address				
		* Port Speed				
		* Autonegotiation				
		Operation Mode			only for SCX2e	
		Interface State				
		Packet Counter				
		* Enable SNMP Link Up/Down Traps				
		> Edit IP Settings				
		Port Name				
		* Interface Type				
		* IP Address Assignment				
		* IP Address				
		* Network Mask				
		DHCP Server				
		DHCP Server State				
		DHCP Default Gateway			/	
		> IP Configuration				
		* IP Default TTL			\	
		* Default Gateway Address				
		Is Gateway Reachable				
		> MGMT Interface				
		HW MAC Address				
		* Interface Type				
		* IP Address Assignment				
		* IP Address				
		* Network Mask				
		DHCP Server				
		DHCP Server State			only for SCX2e-WDM	
		DHCP Default Gateway				
		> Port Configuration				
	L	 Name Status Mech. 			List of Entries w 3 columns.	
		> Edit Port Settings				
		* Port Name				
		* Port Speed				
		* Autonegotiation				
		Operation Mode				
		Interface State				
		Packet Counter				
		* Port State			/	
		> SFP Information				
		Vendor Name				
		Part Number				
		Vendor-Rev				
		Tranceiver Type				
		Connector Type				
		Optical Type				
		Line Coding				
		Nominal Bit Rate				
		Link Length				

continues on next page...

SSH and CLI
Menu-Structure (Directory-Tree) of SCX2e

... continues from previous page

		+ Update SFP Info			
		> SFP Diagnostics			
		SFP Temperature			
		SFP Supply Voltage			
		SFP Tx Bias Current			
		SFP Tx Power			
		SFP Rx Power			
		> Diagnostics			
		L *IP-Address Command			List of Entries w 2 columns.
		+ Ping			
		+ Traceroute/UDP			
		+ Traceroute/ICMP			
		Ping result			
		> Date and Time Settings			
		* Date			
		* Time			
		* Timezone			
		* Time Server			
		Server State			
		> Configuration Management			
		L *Name Date Action			List of Entries w 3 columns.
		> Apply			
		L Configuration Component *Behaviour			List of Entries w 2 columns.
		+ Apply Configuration now			
		+ Apply configuration at next reboot			
		+ Save Configuration			
		+ Delete Configuration			
		* Import Configuration			
		> Firmware Update			
		Update state			
		Update Info			
		Update Progress [%]			
		* Protocol			
		* Select file			
		* Server IP Address			
		* File path			
		* SFTP User Name			
		+ Start Firmware Download			
		+ Start Update			
		> Reset System			
		Reset State			
		* Reset Mode			
		Current Time			
		* Reset Date			
		* Reset Time			
		+ Cancel Reset			
		+ Start Reset			
		> Selftest			
		+ Run Selftest			
		Selftest Status			
		Selftest Result			
		> Alarm Management			
		System Alarm State			
		+ Acknowledge All			
		Current Alarms			

continues on next page...

... continues from previous page

	Current Warnings						
	* Alarm Acknowledgement Policy						
	L Name State Errors Warnings Acknowledged Ignored *Max. Severity Acknowledge Details						List of Entries w 5 columns.
	+ Acknowledge Group Alarms						
	> Group Details						
	* Alarm Group Name						
	Alarm Group State						
	Current Alarms						
	Current Warnings						
	* Max. Group Severity						
	L Name *Config State Acknowledge *SNMP Notification						List of Entries w 5 columns.
	> Thresholds						
	Alarm Name						
	Current Value						
	* Overrun Warning Level						
	* Overrun Error Level						
	* Underrun Warning Level						
	* Underrun Error Level						
	* Hysteresis						
	+ Acknowledge						

Figure 7-7 Menu Structure SCX2e

Appendix A

Technical Specifications

SCX2e Hardware Specification

Table A-1 to Table A-6 provide the general technical data of the SCX2e - System Controller.

Table A-1 Number of Interfaces

Type		
SCX2e-Family		
Number of Interfaces		
SCX2e	1x Fast Ethernet 10/100BaseT (RJ45),	General Purpose
	1x Gigabit Ethernet 10/100/1000BaseT (RJ45) or	General Purpose (Combo Port)
	1x Gigabit Ethernet 1000BaseFX/TX (SFP),	General Purpose (Combo Port)
	1x Alarm Connector	NOC (normal open)
SCX2e-WDM	1x Fast Ethernet 10/100BaseT (RJ45),	Local Management-I/F.
	1x Gigabit Ethernet 1000BaseFX/TX (SFP),	Remote Management-I/F via WDM
	1x passive WDM-Filter (1310 + 1550nm, SM, SC-connector)	Overlay network for remote Management.

Table A-2 Power Requirements

Type
Power Supply

Table A-2 Power Requirements (continued)

Type		
Type:	DC	
Input voltage:	+5VDC	+/- 5%
Connector:	Via backplane	

Power Requirements ⁱ			
Device	w/o SFP	With Standard SFP(s) (700mW)	Max. power to be used by SFP(s)
SCX2e	4.0 VA	4.7 VA (1x SFP)	1.8 VA
SCX2e-WDM	4.0 VA	4.7 VA (1x SFP)	1.8 VA

i. The total power need depends on the used SFP(s).

Table A-3 Technical Data of the Interfaces

Type	
Interfaces	
Fast Ethernet Interfaces (Copper)	
Type:	IEEE 802.3 (full- and half-duplex, Autonegotiation)
Data-rate	10 or 100Mbps
Connection type:	Twisted-Pair interface (TP)
Function, electrical values, pin assignment:	according to IEEE 802.3i (10BaseT), IEEE 802.3u (100BaseTX)
Impedance:	100 Ohm (balanced)
Connector:	8 pin RJ-45 connector according to ISO 8877
Fast Ethernet Interfaces (SFP)	
Type:	IEEE 802.3 (full- and half-duplex, Autonegotiation)
Connection type:	Fibre Optics (FO), SFP
Function, electrical values:	IEEE 802.3u (100BaseFX, 100BaseSX, 100Base-BX, 100Base-LX10)
Connector:	LC

Table A-3 Technical Data of the Interfaces (continued)

Type	
SFP:	According to SFP MSA, Rev 4.5, Aug. 31, 2006 All vendors supported. Max. 100 insertion / extraction.
Gigabit Ethernet Interface (Copper)	
Type:	IEEE 802.3 (full- and half-duplex, Autonegotiation)
Connection type:	Twisted-Pair interface (TP)
Function, electrical values:	according to IEEE 802.3i (10BaseT), IEEE 802.3u (100BaseT) IEEE 802.3ab (1000BaseT)
Impedance:	100 Ohm (balanced)
Connector:	8 pin RJ-45 connector according to ISO 8877
Gigabit Ethernet Interface (SFP)	
Type:	IEEE 802.3 (full-duplex)
Connection type:	Fiber Optics (FO), SFP
Function, electrical values:	IEEE 802.3z (1000Base-X)
Connector:	LC or RJ45
SFP:	According to SFP MSA, Rev 4.5, Aug. 31, 2006 All vendors supported. Max. 100 insertion / extraction.
Alarm Connector	
Alarm Connector:	RIA (3 pin)

Table A-4 Display Functions

Type	
Display Functions	
System:	LEDs for operating and error status
Fast Ethernet interfaces:	LEDs for Link Status and 10/100Mbps recognition (only TP ports)

Table A-4 Display Functions (continued)

Type	
Gigabit Ethernet interfaces:	LEDs for Link Status and 10/100/1000Mbps recognition (only TP ports)

Table A-5 Mechanic and Environment

Type	
Mechanics	
Design:	AgentCard for rack-mount chassis or desktop housing
Dimensions:	190 x 130 x 30mm
Weight:	180g
Cooling:	Convection cooling through ventilation slots in the housing environment
Operation:	ETS 300 019: class 3.1
Transport:	ETS 300 019: class 2.1
Storage (in packing):	ETS 300 019: class 1.1
EMC	
	EN 55022:1998 + A1:2000 class B
	EN 61000-3-2:2000
	EN 61000-3-3:1995 + A1:2001
Product Security	
Electrical security:	EN 60950
Sound emission:	None (no build-in fan)
Conformity:	CE

Table A-6 μ Controller and Clock

Type	
Electronics	
Main processor:	32 Bit power PC, Freescale MPC8313E

Table A-6 μ Controller and Clock (continued)

Type	
Non-volatile memory:	64 MB
Main memory:	128 MB SDRAM
Real Time Clock	
Accuracy	10ppm (<1sec/day)
Hold Time (without ext. power)	min. 11 days

SCX2e Software Specification

Table A-7 provides the general technical data of the SCX2e - System Controller.

Table A-7 Technical Data of the SCX2e - Software

Type		
SCX2e		
General Information		
Valid SW-Version for this manual: V 1_4_00 ⁱ		
Switching, VLAN		
Interfaces:	2x MGMT/LAN: 10/100/1000BaseTX, 100BaseFX, 1000Base-X	
Standards		
Internet Protocol:	IPv4	
	IPv6	
IP-address assignment:	manually	
	DHCP	RFC 2131
	IPv6 Auto-Conf	RFC 2462
SNMP:	SNMPv2c	RFC 1901, RFC 1905, RFC 1906
	SNMPv3	IETF RFC 3410 - RFC 3418
	SNMPv2-MIB	RFC 3418
	RMON MIB (rmon1, rmon2, rmon3, rmon4 and rmon9)	
	IF-MIB	RFC 2863
Secure Shell (ssh)	SSHv1	draft-ylonen-ssh-protocol-00.txt
	SSHv2	RFC 4250 - RFC 5256
TFTP		RFC 1350
SFTP		draft-ietf-secsh-filexfer-02.txt
http	http /1.1	RFC 2616

i. If you use higher SW-version, please check with arcutronix or your local partner, whether there is a new release of the manual available.

Appendix EC EC Declaration of Conformity



Declaration of EC-Conformity

We arcutronix GmbH
Garbsener Landstr. 10
D – 30419 Hannover
Germany

declare under our sole responsibility that the product group

Name: SCX – System Controller
Members: SCX2, SCX2e
Number: 0805-7020, 0903-3000

to which this declaration relates conforms to the following standards, which have been described in the CE-guideline:

93/68/EEC	CE marking
2004/108/EC	Electromagnetic compatibility (EMC)
2006/95/EC	Safety of low voltage equipment (LVD)
1999/5/EC	Radio & Telecommunications Terminal Equipment (R&TTE)
2002/95/EC	Restriction of the use of certain Hazardous Substances (RoHS)
2002/96/EC	Waste Electrical and Electronic Equipment (WEEE)

The above listed products satisfy all technical regulations, applicable to the products based on following standards:

EN 55022	Electromagnetic compatibility (EMC) for Information technology equipment
EN 55024	Electromagnetic compatibility (EMC) for Information technology equipment
EN 61000-4-1	Electromagnetic compatibility (EMC) for Information technology equipment
EN 61000-4-2	Electrostatic discharge immunity test
EN 61000-4-3	Radiated, radio-frequency, electromagnetic field immunity test
EN 61000-4-4	Electrical fast transient/burst immunity test
EN 61000-4-5	Surge immunity test
EN 61000-4-6	Immunity to conducted disturbances, induced by radio-frequency fields
EN 61000-4-11	Voltage dips, short interruptions and voltage variations immunity tests
EN 61000-6-1	Generic immunity standard – Residential, commercial and light industry
EN 61000-6-2	Generic immunity standard – Industrial environment
EN 60950	Safety of Information technology equipment

Hannover, 8.3.2010

Andreas Zimmermann
TD arcutronix GmbH

arcutronix GmbH ☺ Garbsener Landstr. 10 ☺ D-30419 Hannover ☺ Germany
+49 511 277 2700 ☺ sales@arcutronix.com ☺ www.arcutronix.com

Headquarter

arcutronix GmbH
Garbsener Landstrasse 10
30419 Hannover
Germany

Phone: +49 (511) 277 2700
Fax: +49 (511) 277 2709
Email: info@arcutronix.com
Web: www.arcutronix.com