arcutronix

Synchronize the Ethernet

SCX2e WebGUI

GS1

arcutronix GmbH
Deutschland

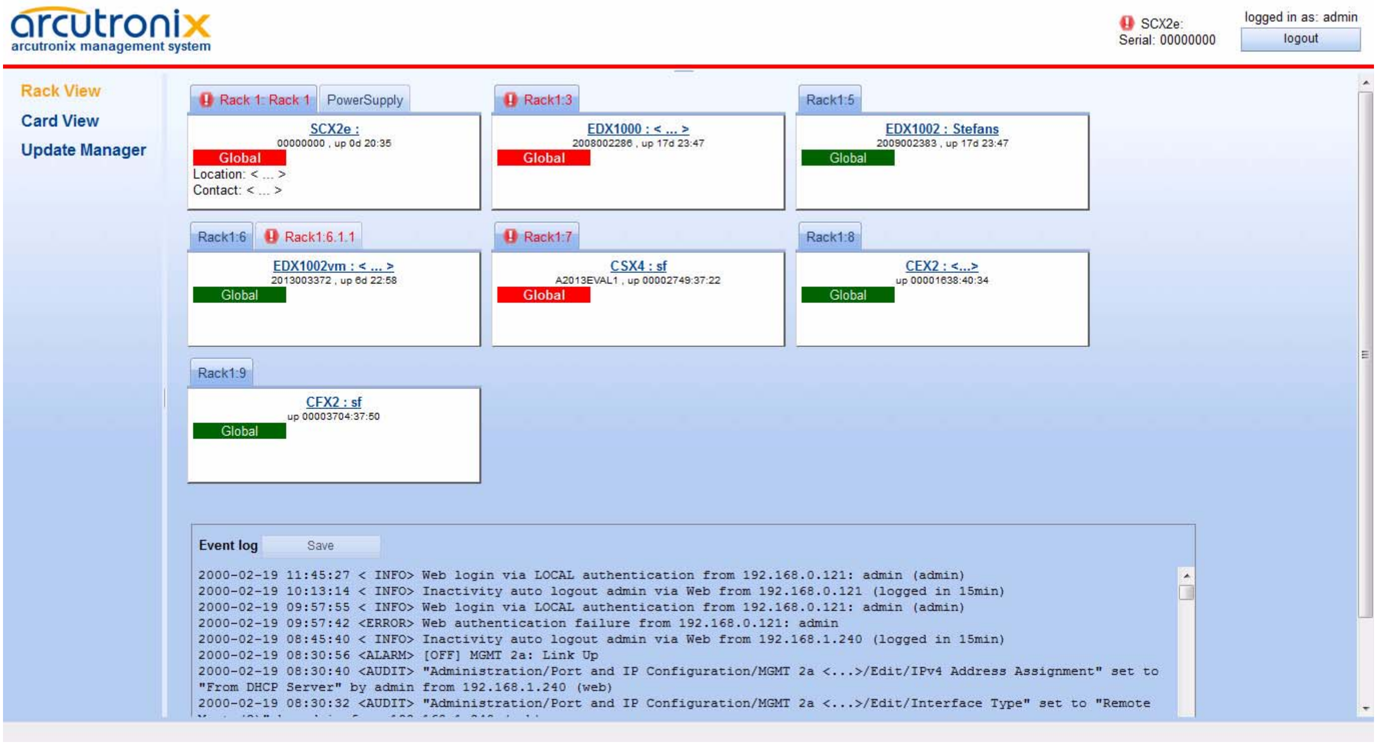
Reference Guide

Version 1.0

SCX2e

REFERENCE GUIDE

Web-GUI



```
2000-02-19 11:45:27 < INFO> Web login via LOCAL authentication from 192.168.0.121: admin (admin)
2000-02-19 10:13:14 < INFO> Inactivity auto logout admin via Web from 192.168.0.121 (logged in 15min)
2000-02-19 09:57:55 < INFO> Web login via LOCAL authentication from 192.168.0.121: admin (admin)
2000-02-19 09:57:42 <ERROR> Web authentication failure from 192.168.0.121: admin
2000-02-19 08:45:40 < INFO> Inactivity auto logout admin via Web from 192.168.1.240 (logged in 15min)
2000-02-19 08:30:56 <ALARM> [OFF] MGMT 2a: Link Up
2000-02-19 08:30:40 <AUDIT> "Administration/Port and IP Configuration/MGMT 2a <...>/Edit/IPv4 Address Assignment" set to
"From DHCP Server" by admin from 192.168.1.240 (web)
2000-02-19 08:30:32 <AUDIT> "Administration/Port and IP Configuration/MGMT 2a <...>/Edit/Interface Type" set to "Remote
```

Version 1.0

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
Web: http://www.arcutronix.com

Copyright Note

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 modifying 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

About this Reference Guide

Introduction and Overview

The SCX2e can be configured and monitored via a web-based graphical user interface (GUI). The Web-GUI offers an user-friendly access to the device by standard web browser.

This reference guide will explain how to connect to the Web-GUI and the usage of it.

Part-Number of this document:	0903 30 65.web
Version:	V 1.0

Covered Software

This Reference Guide is valid for SCX2e-SW V 2_0_01.

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

2014-09-05	Version 1.0	Editor: mjz

First issue of the SCX2e Reference Guide Web-GUI. This Reference Guide is only valid for the second HW edition of SCX2e and SCX2e-WDM. The second HW edition can be identified by the acronym GS2.

Referenced and Related Documents

[axManualSCX2e] arcutronix GmbH (2013): Manual for SCX2e: Operation, installation, Functionality.

[axRefGuideCLI_SCX2e] arcutronix GmbH (2012): SCX2e Command Line Interface, Reference Guide.

[ETSI TS 101 524] Technical Specification ETSI TS 101 524 (2003), Access transmission system on metallic access cables; Symmetric single pair high bitrate Digital Subscriber Line (SDSL).

[IEEE 802.1D] IEEE Std 802.1D™-2004: Media Access Control (MAC) Bridges.

[IEEE 802.1Q] IEEE Std 802.1Q™-2011: Media Access Control (MAC) Bridges and Virtual Bridge Local Area Networks.

[IEEE 802.3] IEEE Std 802.3™-2008: Part3: Carrier sense multiple access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.

[IETF RFC 791] IETF RFC 791 (1981), Internet Protocol (IP).

[IETF RFC 1305] IETF RFC 1305 (1992), Network Time Protocol (Version 3) Specification, Implementation and Analysis.

[IETF RFC 1901] IETF RFC 1901 (1996), Introduction to Community-based SNMPv2.

[IETF RFC 2474] IETF RFC 2474 (1998), Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.

[IETF RFC 3410] IETF RFC 3410 (2002), Introduction and Applicability Statements for Internet Standard Management Framework.

[IETF RFC 3414] IETF RFC 3414 (2002), User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).

[IETF RFC 5905] IETF RFC 5905 (2010), Network Time Protocol Version 4: Protocol and Algorithms Specification.

[ITU-T M.3010] Recommendation ITU-T M.3010 (2000), TMN and Network Maintenance: International transmission systems, telephone circuits, telegraphy, facsimile and leased circuits.

[ITU-T Y.1731] Recommendation ITU-T Y.1731 (2006), OAM functions and mechanisms for Ethernet based networks.

List of Contents

Chapter 1 SCX2e Web-GUI

List of Figures

List of Tables

Chapter 1
SCX2e Web-GUI

The SCX2e can be configured via a html-based Web-GUI (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-GUI and its usage.

NOTE: A detailed presentation of all Web-GUI variables and menus is given in [axRefGuideCLI_SCX2e].

Introduction

Access to the Device

The SCX2e Web-GUI 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.

arcutronix’ devices are proved to be used with different web-browsers:

• Internet Explorer (Microsoft):	IE 7 or higher
• Mozilla Firefox (Open Source):	Firefox 6 or higher
• Opera (Opera Software ASA):	Opera 10 or higher
• Safari (Apple):	Safari 5 or higher
• Google Chrome (Google):	Chrome 9.0 or higher

Security Issues

The Web-GUI 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 1-18, how to define the other users and how to change the user password.

Web-Menu Body

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 1-1).

The Login screen is shown in the figure below. For a first quick overview, the type, name, alarm status and the serial number of the connected device is displayed on the top-right side. This makes it easy to verify, whether one has reached the right unit (the entered URL might be wrong or mistyped) and its actual status. If all is fine, it might be no need to login and one can turn towards the next device to check and work with.

The fields user-name and passwords must be filled and after pressing the “Login”-button, the inscription is verified against the local or remote data-base. If the login is accepted, the next screen will open, otherwise the login attempt is denied and one will remain on this screen.

NOTE: A refused attempt to login to the unit is logged.

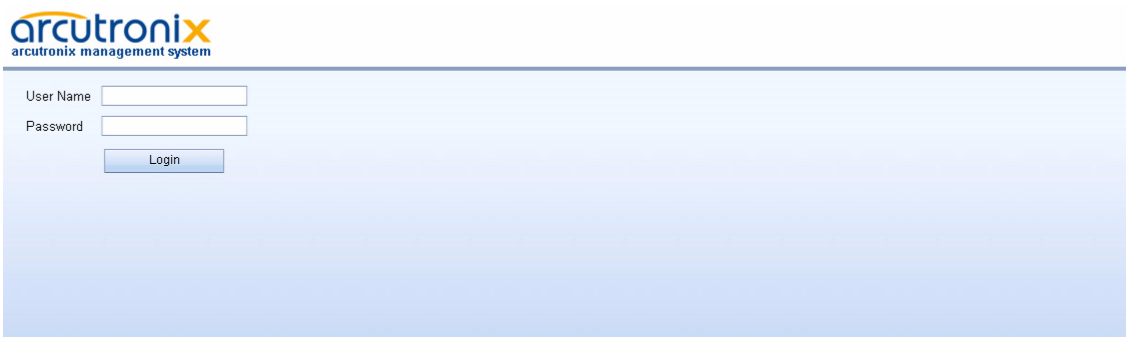


Figure 1-1 *Login Screen*

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.

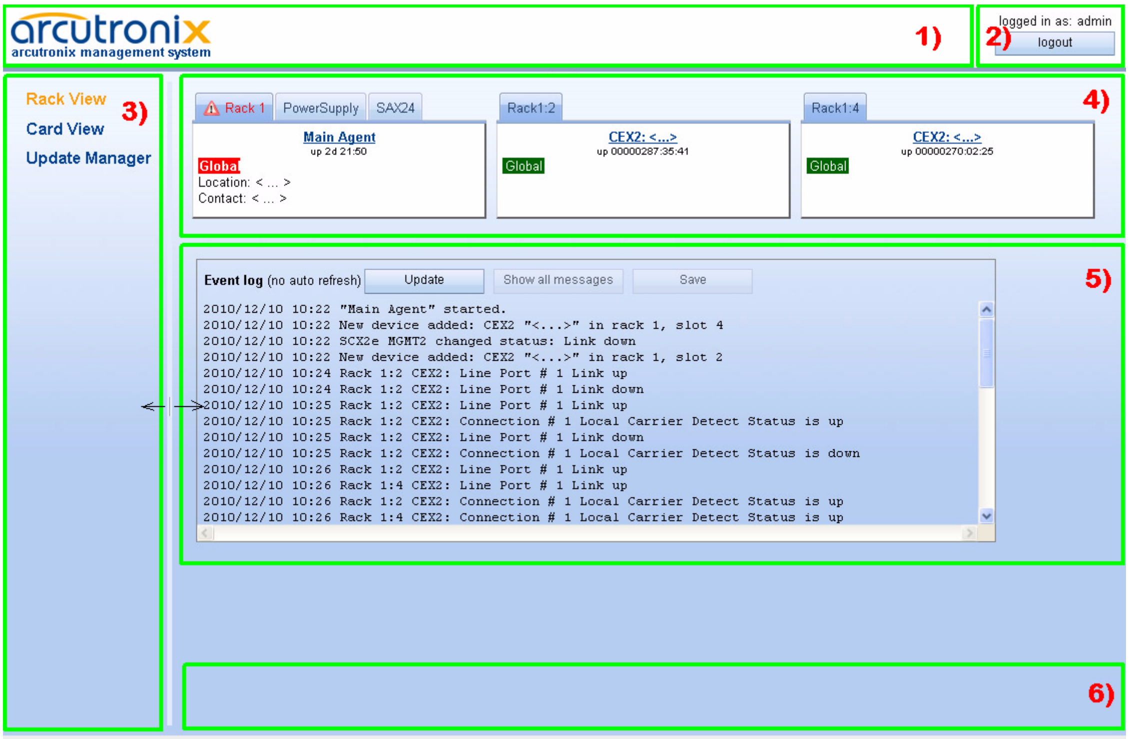
If the device is started-up the very first time, the only user ‘admin’ is defined with the password ‘private’, which should be changed immediately after login. The password is not displayed, each character is replaced by an asterisk (*). An error message will be displayed for any unsuccessful login (the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

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

Layout of Web-GUI

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

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



```
2010/12/10 10:22 "Main Agent" started.
2010/12/10 10:22 New device added: CEX2 "<...>" in rack 1, slot 4
2010/12/10 10:22 SCX2e MGMT2 changed status: Link down
2010/12/10 10:22 New device added: CEX2 "<...>" in rack 1, slot 2
2010/12/10 10:24 Rack 1:2 CEX2: Line Port # 1 Link up
2010/12/10 10:24 Rack 1:2 CEX2: Line Port # 1 Link down
2010/12/10 10:25 Rack 1:2 CEX2: Line Port # 1 Link up
2010/12/10 10:25 Rack 1:2 CEX2: Connection # 1 Local Carrier Detect Status is up
2010/12/10 10:25 Rack 1:2 CEX2: Line Port # 1 Link down
2010/12/10 10:25 Rack 1:2 CEX2: Connection # 1 Local Carrier Detect Status is down
2010/12/10 10:26 Rack 1:2 CEX2: Line Port # 1 Link up
2010/12/10 10:26 Rack 1:4 CEX2: Line Port # 1 Link up
2010/12/10 10:26 Rack 1:2 CEX2: Connection # 1 Local Carrier Detect Status is up
2010/12/10 10:26 Rack 1:4 CEX2: Connection # 1 Local Carrier Detect Status is up
```

***Figure 1-2** Web-GUI’s Appearance*

1. Logo/Family Pane.
2. Info Pane: Info about
   - device-type (here SCX2e),
   - device-name (here Demo-Device),
   - serial number,
   - and alarm status (status icon).
3. Login/Logout Pane: Info, who is logged in and a button for Logout.
4. Navigation Pane: Navigating in the Web-GUI is easy with the Navigation Pane. The settings are grouped in different categories, which can be exploded and collapsed.
5. Main Pane: This is the pane, where all the information is listed and the configuration can be changed and adopted. The next chapter will mainly handle the settings in this section.
6. Alarm-Table: Summary of all events and alarms.
7. Message Pane: Here status and error-messages are shown.

Navigation

The Web-GUI 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 Navigation Pane (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 Navigation Pane, 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 1-2).

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 logout, 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.

WARNING: If your PC/Laptop is very busy and does not reply on the devices cyclic “Hello”-messages, the web-session will be terminated after 90 seconds without reply. This auto-termination is implemented due to security reasons if you close your browser or browser-tab without logout.

Status-Symbols

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 1-1 *Status-Symbols*

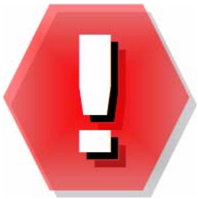
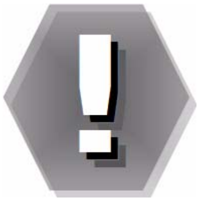
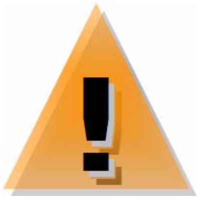
Symbol	Prio	Meaning
none (empty)	0	Everything is fine. No problems detected.
	4	Alarm-Symbol. The device has detected at least one active alarm.
	2	Alarm-Acknowledged Symbol. The device has at least one alarm, which is already acknowledged by user.
	3	Warning-Symbol. The device has detected at least one active warning.

Table 1-1 Status-Symbols (continued)

Symbol	Prio	Meaning
⚠	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.

Usage of Commit Groups

Most of the entries, which can be made via the Web-GUI, are accepted as soon as the new value for the variable is entered. No additional “Store” command is required, the new value is active as soon as it is entered.

Nevertheless, some of the variables are grouped together, as it makes only sense to make all required changes and the activate them at the end. Such groups are called “Commit Group” within this document, as the set of variables (“group”) must be committed together before it is activated and valid.

Such commit groups are:

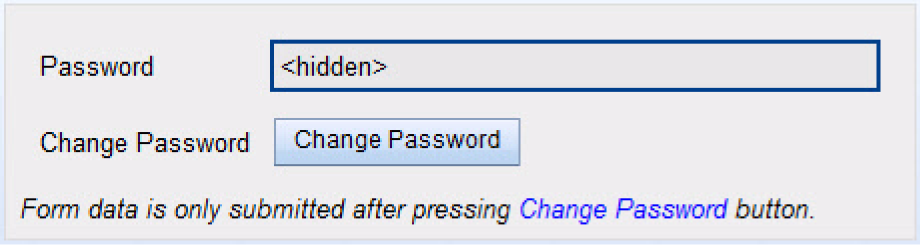
- Adding users,
- Changing passwords,
- ...

The usage of Commit Groups will be explained hereafter using the example of changing passwords. the behaviour is similar for all Commit Groups.

Display and Change of Passwords

The Web-GUI offers the possibility to enter and change passwords on several pages for very different applications. The usage of these pages are all the same and it is slightly different than other pages, as passwords need more attention to security and to prevent the user and the system from phishing (“password harvesting fishing”).

For security reason, the Web-GUI will never display passwords as clear text, but always in a hidden manner. The text <hidden> is shown:

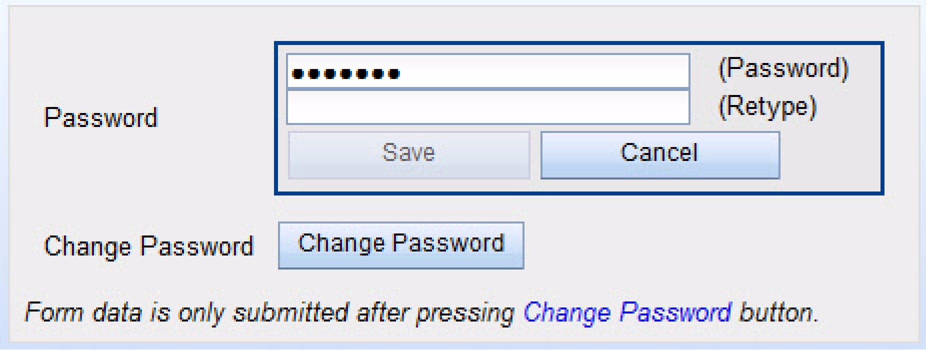

Password <hidden>

Change Password

Form data is only submitted after pressing Change Password button.

So please make sure, you note your password, as you will not have the chance to see it in the Web-GUI.

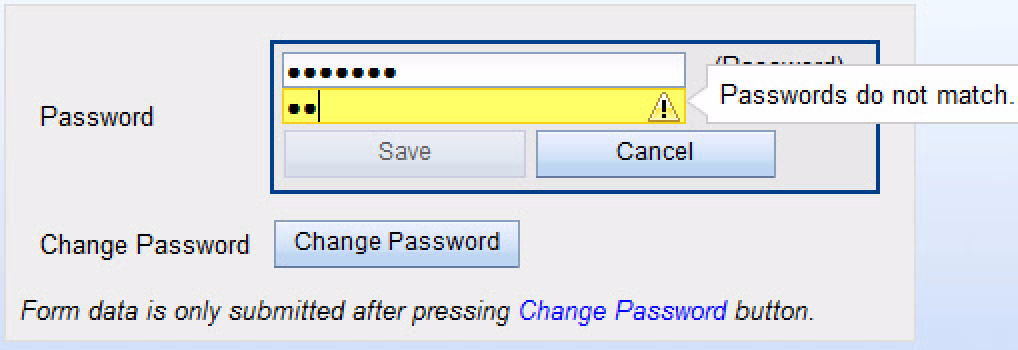
In case the password shall be changed, just click into the thick-blue bordered area and you can enter the new password. Also the entry of the new password is hidden, only dots are shown for each entered character:


Password ●●●●●●● (Password)
(Retype)

Change Password

Form data is only submitted after pressing Change Password button.

The new password has to be re-typed to be sure, no typo was entered the first time. As long as the re-typed entered password does not equal to the first entry, the field is marked yellow and a hint is shown:


Password ●●●●●●● (Password)
●●

Passwords do not match.

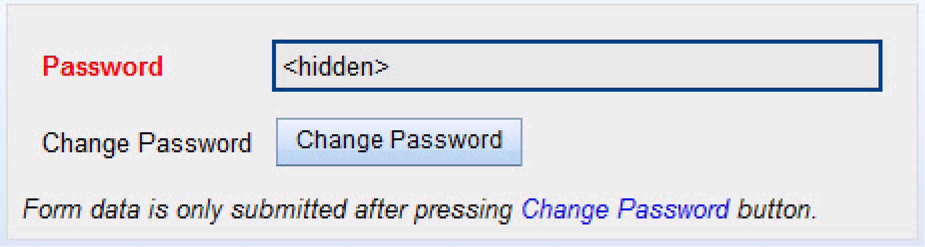
Change Password

Form data is only submitted after pressing Change Password button.

When the re-type is correct the yellow colour will disappear. Now please press “Save” to finish the entry of the new password.

NOTE: The new password is NOT stored yet for usage and NO verification is done concerning security issues up to this moment!

To make the new password active, you have to press “Change Password”. Otherwise the old password will be still valid. To indicate, that the new entered password is not active yet, the word password will be displayed in red:



Password <hidden>

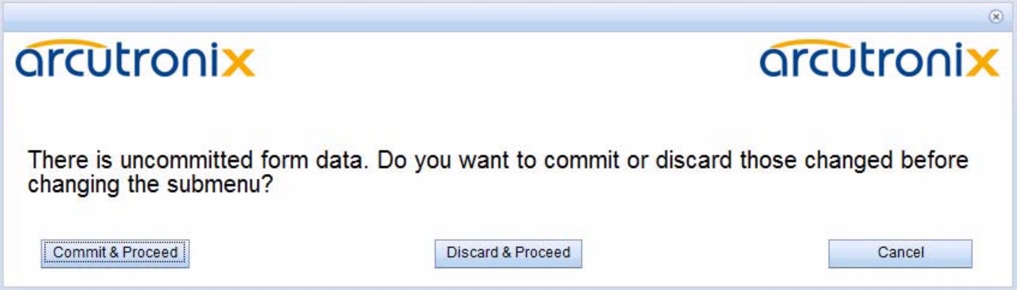
Change Password [Change Password]

Form data is only submitted after pressing Change Password button.

When pressing “Change Password”, the verification concerning security rules for passwords are done. It can now be the case, that the check will not accept the new password. For details on the security “Rules for Passwords” see below.

After successful verification of the new password, the GUI is left and the parent GUI is shown. If the check was not successful, the GUI is not left and the user has the option to enter a new (and better) password.

If the GUI is left without pressing “Change Password”, a hint is shown which indicates, that the new password is not active, yet. One can now select whether to abolish the changes, commit the changes or to stay in password GUI for more changes.



There is uncommitted form data. Do you want to commit or discard those changed before changing the submenu?

Rules for Passwords

The password given to a user or other usage must reach a certain level of “password strength” to protect the system from hackers. The strength of a password is a function of length, complexity, and unpredictably and this is verified by several security rules. If a new password does not fulfil this rules, it will be not accepted by the SCX2e. The rules are as follows:

- Minimum password length is 3 characters (, maximum password length is 32 characters),
- Character set is 7-Bit ASCII, allowed characters:
  - Capital letters: A...Z,

  - Lower case characters: a...z,
  - Digits: 0...9,
  - additional characters: 0x2D (-), 0x2E (.), 0x5F (_)
- The password may contain any of these characters.

NOTE: It is allowed to have the user-name as part of the password (forwards and backwards, not case sensitive!). BUT the system will remove this string from the password before it is verified.

  - E.g. the user-name is “weakuser”. Then a password “12weakUser!” would lead to strength-verification of “12!”. The password would be too weak and not accepted!
  - The same user-name in combination with password “12weakuser!_ButStrongPassword” would be ok, as the strength-verification is done on the reduced password “12!_ButStrongPassword” and this fulfils the requirements for a strong password.

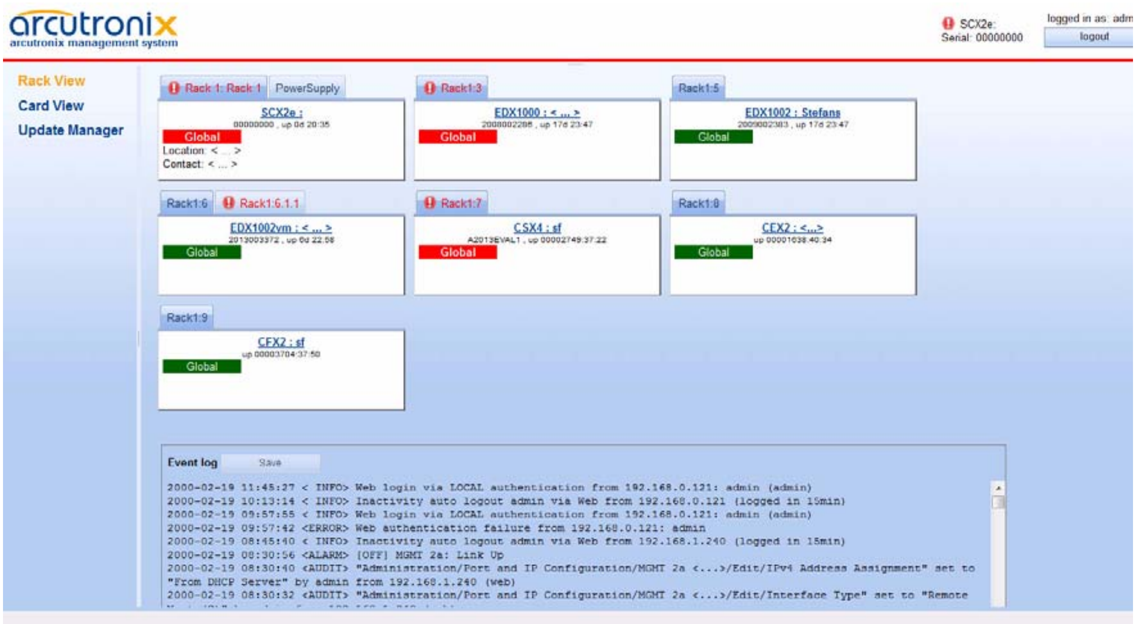
Rack View

The “Rack View” is the presentation of the information and actual status of all cards in a general overview of the ax MSP rack. All discovered cards are shown in parallel and a summery for each is given. The summery shows short information like serial number, user’s given name, slot-ID, up-time, and alarm-status.

If remote cards are detected, which can be detected and managed by the local agent, the remote cards and local card are grouped into one icon with (at least) two tabs. Each tab represents one of the discovered (line-) cards. Using this presentation, it is easy to see, which cards are physically connected.

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

On the bottom area of the “Rack-View” the logging windows is presented. The logging window shows all entries to the log-file. Details about the logging-window and the messages are given in “Logging” on page 4-26.



```
2000-02-19 11:45:27 < INFO> Web login via LOCAL authentication from 192.168.0.121: admin (admin)
2000-02-19 10:13:14 < INFO> Inactivity auto logout admin via Web from 192.168.0.121 (logged in 15min)
2000-02-19 09:57:55 < INFO> Web login via LOCAL authentication from 192.168.0.121: admin (admin)
2000-02-19 09:57:42 <ERROR> Web authentication failure from 192.168.0.121: admin
2000-02-19 08:45:40 < INFO> Inactivity auto logout admin via Web from 192.168.1.240 (logged in 15min)
2000-02-19 08:30:56 <ALARM> [OFF] MGMT 2a: Link Up
2000-02-19 08:30:40 <AUDIT> "Administration/Port and IP Configuration/MGMT 2a <...>/Edit/IPv4 Address Assignment" set to
"From DHCP Server" by admin from 192.168.1.240 (web)
2000-02-19 08:30:32 <AUDIT> "Administration/Port and IP Configuration/MGMT 2a <...>/Edit/Interface Type" set to "Remote
```

Figure 1-3 *Rack-View*

Card View

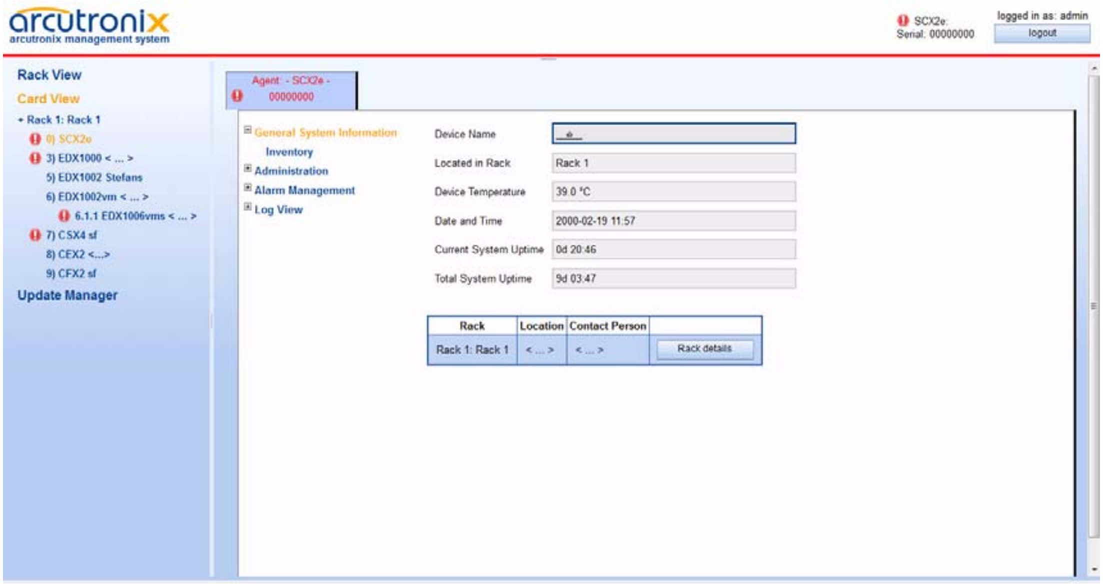
The “Card View” is the presentation of the information and actual status of all cards in a detailed form. All discovered cards can be selected and detailed configurations can be done then. While the “Rack View” is the overview section of the menu, the “Card-View” is the operating and configuration section. Only when cards a selected in the “Card View” changes in configuration can be done.

Each type of card, does have its individual card-view appearance. Though many items will be very similar on all devices, one can not present a common valid overview. New types of line-cards may have different appearances. Even new features on existing line-cards may have the result, that the appearance is different. as this document is intended to be stable, even when new line-cards, features and services are available, not all card-views of all cards can be presented here. Hereafter, only the card-view and management options for the agent itself will be presented.

Web-Menus of SCX2e

To enter the card view of the SCX2e select it in the Rack-View or in the Navigation Pane. The card’s individual menu appears. After selecting the SCX2e the main view is displayed, which provides a general overview of the menu structure.

All menu entries and the optional usage and settings are explained in detail in an extra document: [axManualSCX2e]. Please refer to this document for details.



Device Name
Located in Rack: Rack 1
Device Temperature: 39.0 °C
Date and Time: 2000-02-19 11:57
Current System Uptime: 0d 20:46
Total System Uptime: 9d 03:47

Rack	Location	Contact Person	
Rack 1: Rack 1	< ... >	< ... >	Rack details

Figure 1-4 *Card-View SCX2e*

Select a menu line in the “Navigation Pane” to open the selected submenu or to logout from the SCX2e’ Web-GUI.

The following submenus are available:

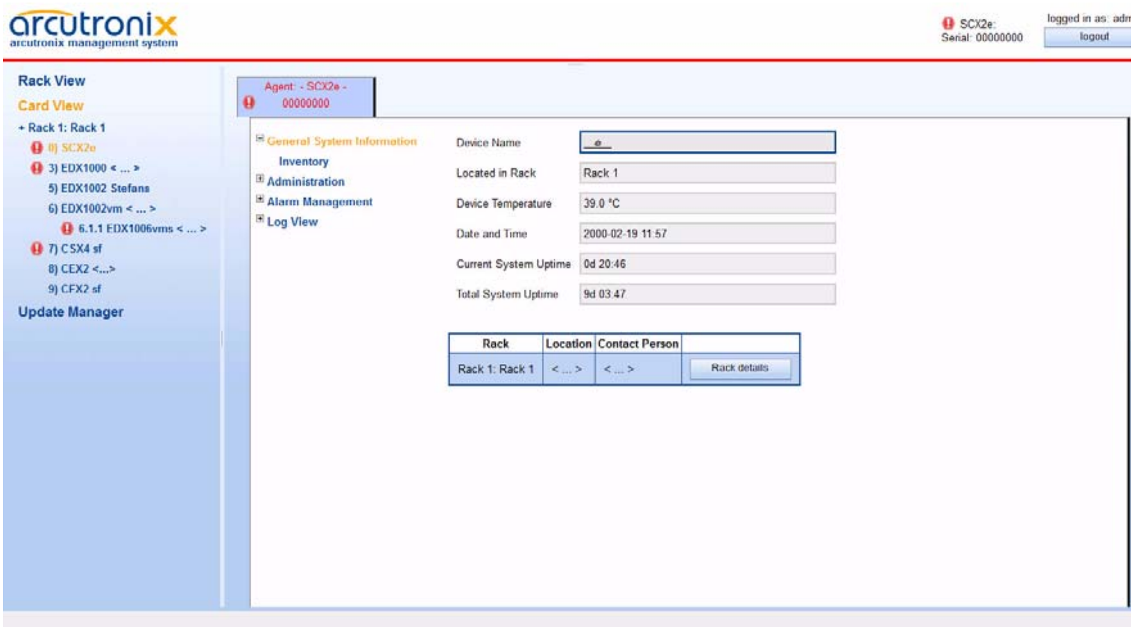
Table 1-2 *Submenus of Main-menu*

Submenu	Description
General System Information	This menu gives access to generic device information. Besides allowing administrators to assign a name and location description for the device, it shows the system runtime and detailed inventory information about the device.
Administration	This menu offers access to administrative configuration and settings of the device. admission management, time, update etc.
Alarm Management	This menu contains an overview of the current overall alarm state of the device and lists available alarm groups with their most important properties.
Log View	This menu gives access to the system’s logging entries and the storage of logging tables to a server.

In Web-GUI always one submenu will be selected. The selected submenu is highlighted in the Navigation Pane by a different colour than the other entries (orange versus blue). The default after login is the selection of submenu General System Information.

General System Information

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



Device Name: e
Located in Rack: Rack 1
Device Temperature: 39.0 °C
Date and Time: 2000-02-19 11:57
Current System Uptime: 0d 20:46
Total System Uptime: 9d 03:47

Rack	Location	Contact Person	
Rack 1: Rack 1	< ... >	< ... >	Rack details

Figure 1-5 *General System Information*

This menu contains the general system information of the SCX2e device and system. Table 1-3 provides information on the menu.

Table 1-3 *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
Device Temperature	The current device temperature in degrees Celsius.	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

Table 1-3 General System Information Menu (continued)

Parameter	Description	Format	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

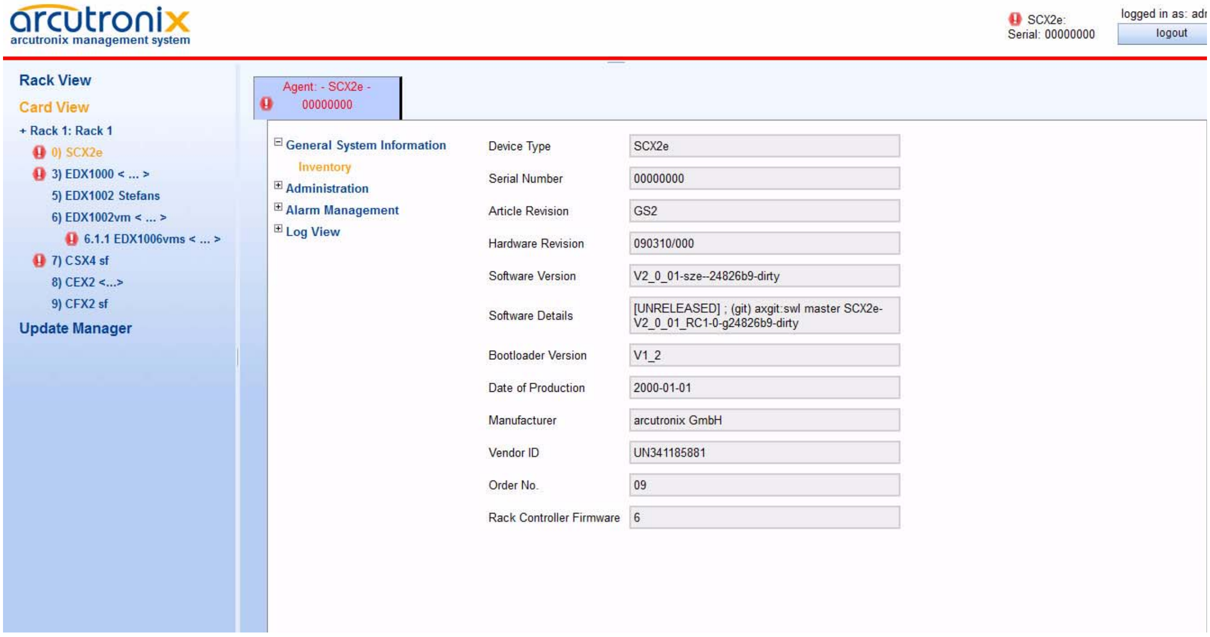
The following submenus are available:

Table 1-4 General System Information: Submenus

Submenu	Description
Inventory	This menu shows inventory details about the device. This includes device identification, software and hardware revisions as well as ordering information. All information herein are factory settings and cannot be changed.
Rack Details	Opens a new menu to enter the rack's details like location, contact person etc.

Inventory

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



Device Type	SCX2e
Serial Number	00000000
Article Revision	GS2
Hardware Revision	090310/000
Software Version	V2_0_01-sze--24826b9-dirty
Software Details	[UNRELEASED] ; (git) axgit:swl master SCX2e-V2_0_01_RC1-0-g24826b9-dirty
Bootloader Version	V1_2
Date of Production	2000-01-01
Manufacturer	arcutronix GmbH
Vendor ID	UN341185881
Order No.	09
Rack Controller Firmware	6

***Figure 1-6** Inventory*

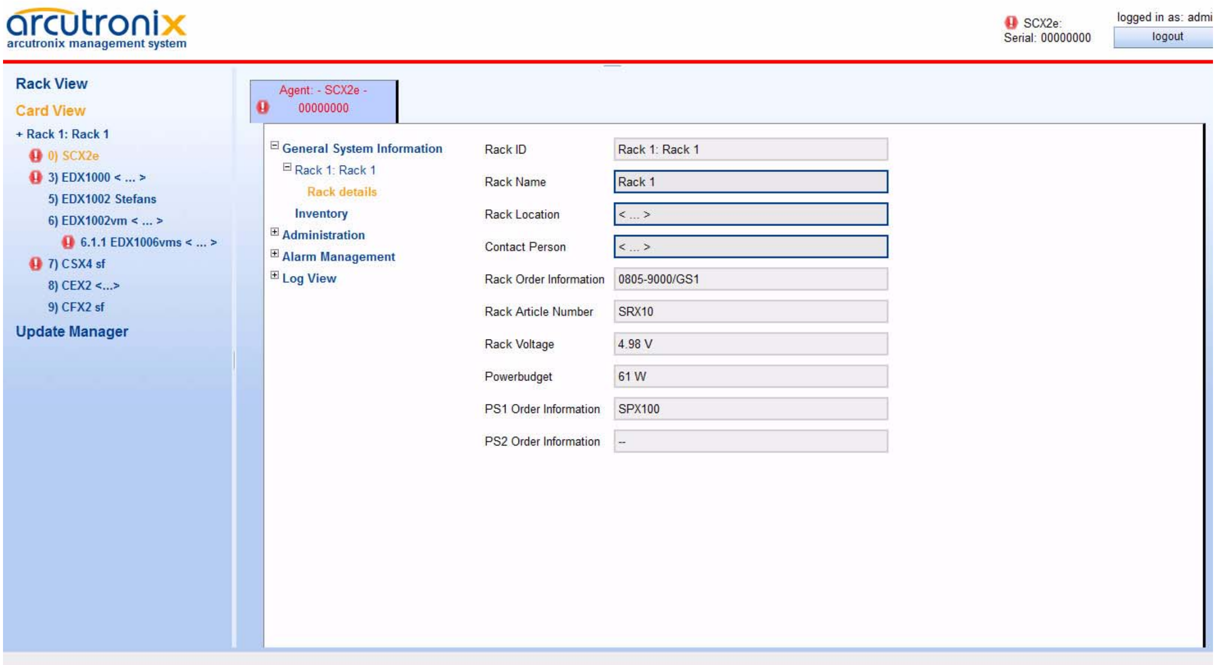
Table 1-5 provides information about the content.

Table 1-5 *Inventory*

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	The release number of the PCB-A.	Display	Depends on the factory settings
Software Version	Revision of the loaded system software.	Display	Depends on the loaded software
Bootloader Version	Revision of the loaded bootloader.	Display	Depends on the loaded software
Date of Production	Date of the device’s production.	Display	Depends on the factory settings
Manufacturer	Manufacturer of the Device (normally arcutronix GmbH).	Display	arcutronix GmbH
Vendor ID	International unique ID for arcutronix GmbH. Issuing agency is Dun & Bradstreet using D-U-N-S (R).	Display	UN341185881
Order No	Order information for the device.	Display	Depends on the device’s type. See Order Matrix (Table 1-1 of [axManualRPX]).
Rack Controller Firmware	Revision of the HW-controller for rack-details, fans and power-supply.	Display	Depends on the loaded software

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.



Rack ID: Rack 1: Rack 1
Rack Name: Rack 1
Rack Location: < ... >
Contact Person: < ... >
Rack Order Information: 0805-9000/GS1
Rack Article Number: SRX10
Rack Voltage: 4.98 V
Powerbudget: 61 W
PS1 Order Information: SPX100
PS2 Order Information: --

Figure 1-7 *Rack Details*

This menu contains the general system information of the SCX2e device and system. Table 1-3 provides information on the menu.

Table 1-6 *Rack Details Menu*

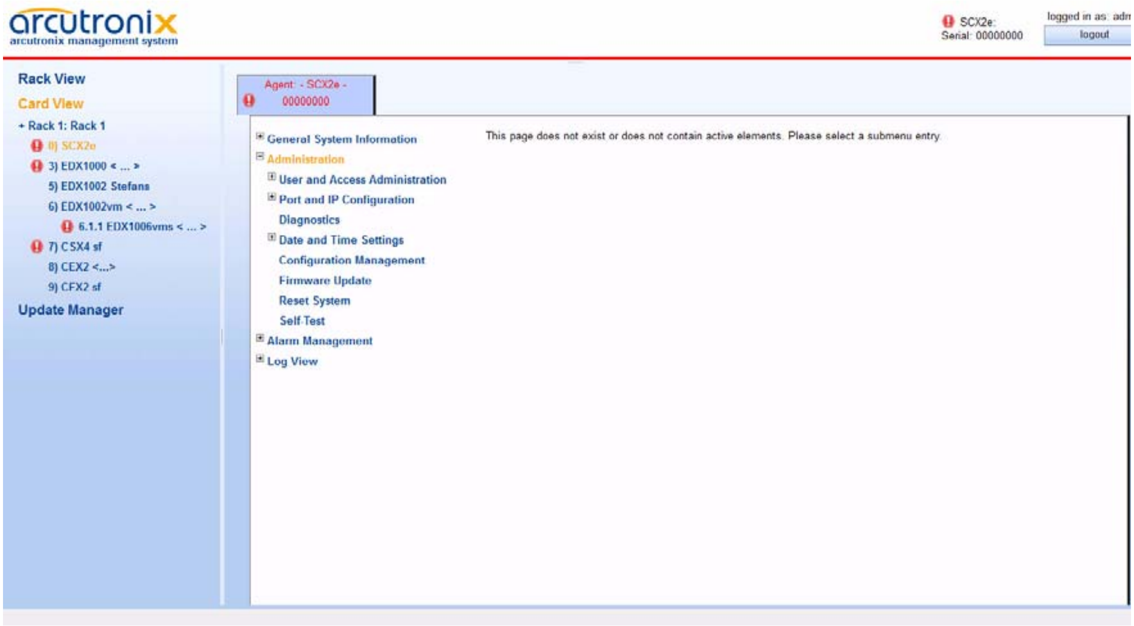
Parameter	Description	Format	Default
Rack ID	This value uniquely identifies the rack in terms of the rack number and the rack name. Each rack gets its own ID, which is computed by an internal number and the Rack Name.	Display	Rack1:Rack1
Rack Name	Description/comment of the rack.	Display/Input (up to 32 characters)	Rack1
Rack Location	Description/comment of the rack.	Display/Input (up to 32 characters)	< ... >

Table 1-6 Rack Details Menu (continued)

Parameter	Description	Format	Default
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.

Administration

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



This page does not exist or does not contain active elements. Please select a submenu entry.

Figure 1-8 *Administration*

The following submenus are available:

Table 1-7 *Administration: Submenus*

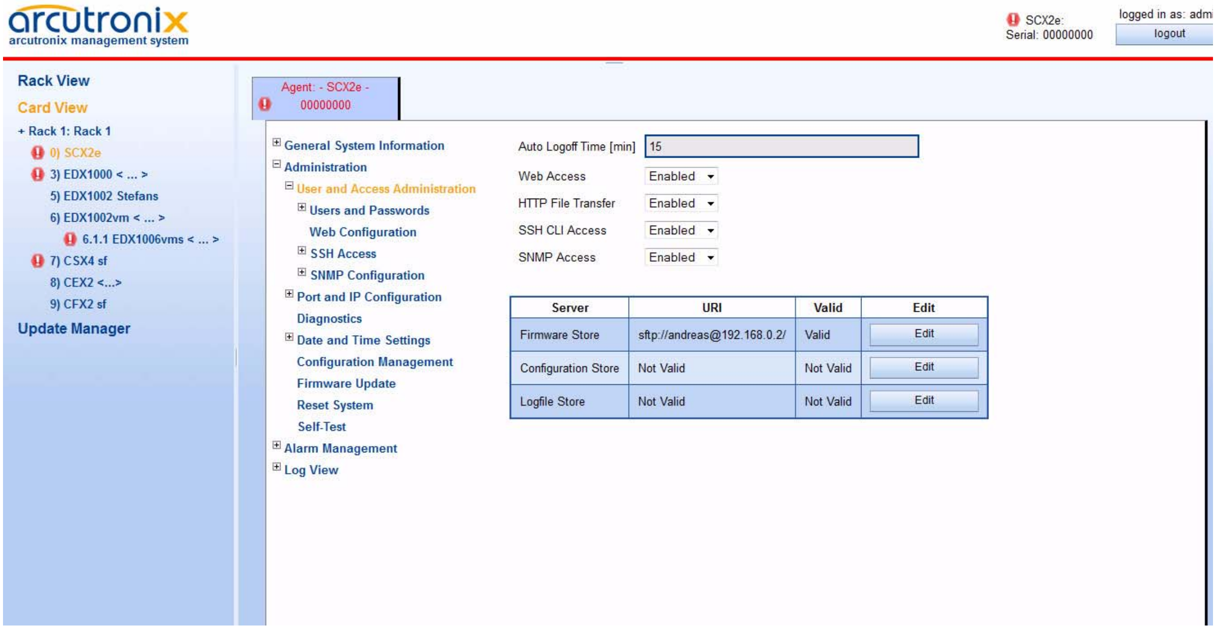
Submenu	Description
User and Access Administration	This menu gives a quick overview of various configuration options for the different ways of management access to the unit. Five variables control whether the device supports a management access method and allows them to be disabled or enabled individually.
Port and IP Configuration	This menu gives access to the configuration of IP parameters and physical port settings of the dedicated management interfaces.
Diagnostics	This submenu allows running a number of diagnostics to verify that the current management IP configuration is valid and all networking components are fully operational.
Date and Time Settings	This menu allows configuring an NTP server to use for time synchronization or to disable NTP support and set the device date/time manually.
Configuration Management	Use this menu to store a snapshot of the current configuration or reactivate one of the available configuration snapshots. The current configuration can be stored at any time and be reactivated at a later time to easily switch between different pre-built configurations. The Factory Default Configuration can be reactivated as well.

Table 1-7 *Administration: Submenus (continued)*

Submenu	Description
Firmware Update	This menu allows firmware updates (for the SCX2e only!) to be performed. Note: Firmware Updates for all the line-cards is done with the help of the Update Manager!
Reset System	This menu allows to perform an immediate system reset or to set up a time at which a reset shall be performed automatically.
Self-Test	This menu allows running a self-test and inspect the self-test results once the run is complete.

User and Access Administration

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



Auto Logoff Time [min] 15

Web Access Enabled

HTTP File Transfer Enabled

SSH CLI Access Enabled

SNMP Access Enabled

Server	URI	Valid	Edit
Firmware Store	sftp://andreas@192.168.0.2/	Valid	Edit
Configuration Store	Not Valid	Not Valid	Edit
Logfile Store	Not Valid	Not Valid	Edit

Figure 1-9 *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 management access (HTTP, HTTPS, SSH/CLI, CONS/CLI or SNMP) must be available. The last available access option can not be disabled! A window will pop up to inform that this will be prohibited.

The auto-logoff time can be specified. If auto-logoff time is defined to zero, the auto-logoff is disabled for all logins. For more details about the auto-logoff feature please refer to chapter “Auto-Logout” in [axManualSCX2e].

After the configuration options for the different accesses, the three file-servers (as depicted in chapter “File-Transfer to/from Servers and via HTTP(S)” in [axManualSCX2e]) and their actual URI (Uniform Resource Identifier) are shown.

Table 1-8 provides all information on the menu options.

Table 1-8 *User Administration*

Parameter	Description	Format	Default
Auto Logoff Time [min]	The time (in minutes) of inactivity after which an automatic logout will happen. Each login, does have its own timer. If Auto Logoff Time is zero, the auto-logoff is disabled.	Entry	15
Web Access	Enable or Disable the management access via HTTP and/or HTTPS (Web-GUI).	PullDown-Menu • Disabled • Enabled	Enabled
HTTP File Transfer	Enable or Disable the file transfer via HTTP and/or HTTPS.	PullDown-Menu • Disabled • Enabled	Disabled
SSH CLI Access	Enable or Disable the management access via SSH.	PullDown-Menu • Disabled • Enabled	Enabled
SNMP Access	Enable or Disable the management access via SNMP.	PullDown-Menu • Disabled • Enabled	Enabled
Firmware Store	SFTP or TFTP settings for firmware download server. See chapter “File Servers” on page 1-20 for details.	Menu / Display	

Table 1-8 User Administration (continued)

Parameter	Description	Format	Default
Configuration Store	SFTP or TFTP server settings for configuration up- and download. The Configuration Store is also used for SSH-key download via S/TFTP. See chapter “File Servers” on page 1-20 for details.	Menu / Display	
Logfile Store	SFTP or TFTP server settings to upload log-files. See chapter “File Servers” on page 1-20 for details.	Menu / Display	

The following submenus are available:

Table 1-9 Users and Passwords: Submenus

Submenu	Description
Users and Passwords	This menu provides possibilities to set up the local user database of the device and additional authentication methods (e.g. TACACS+).
Web Configuration	This menu offers the possibility to configure the web-access settings. HTTP and HTTPS is supported and both can be configured here. If required by the user, web-access can be disabled completely to avoid illegal access to the device. In factory default, web-access is enabled.
SSH Access	This menu offers the possibility to configure the SSH settings like passwords and keys. If required by the user, SSH access can be disabled completely to avoid illegal access to the device. In factory default, SSH access is enabled.
SNMP Configuration	This menu offers the possibility to configure the SNMP agent on the device. Things like SNMP communication details, allowed SNMPv2 communities or SNMPv3 Users and SNMP trap receivers are configured in various submenus.

File Servers

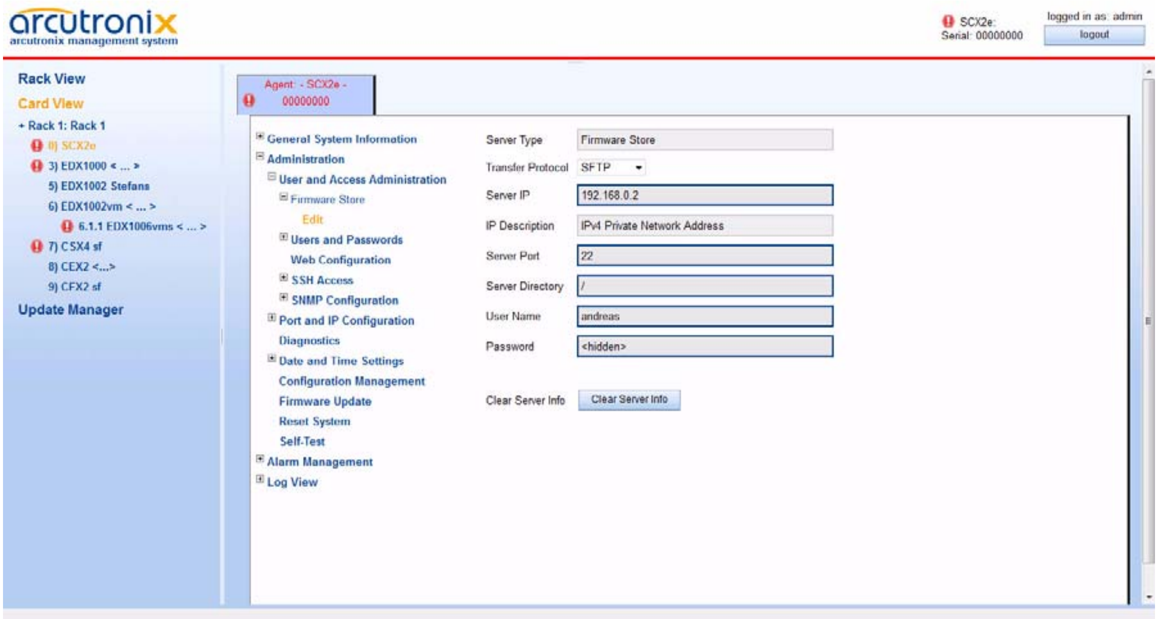
Three servers can be configured to store and load files to and from the unit via SFTP or TFTP.

- Firmware Store
- Configuration Store

- Logfile Store

Each server can be enabled or disabled and for each server the protocol can be configured independently to SFTP or TFTP. See chapter "File-Transfer to/from Servers and via HTTP(S)" in [axManualSCX2e] about details about the basics.

All three servers do have the same configuration menu, so hereafter the configuration for the Firmware store will be depicted as reference.



Server Type: Firmware Store
Transfer Protocol: SFTP
Server IP: 192.168.0.2
IP Description: IPv4 Private Network Address
Server Port: 22
Server Directory: /
User Name: andreas
Password: <hidden>
Clear Server Info

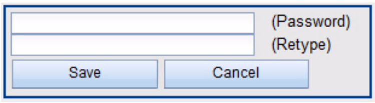
Figure 1-10 Example "Edit File Server": Firmware Store

Table 1-10 provides information about the options.

***Table 1-10** Server Configuration*

Parameter	Description	Format	Default
Server Type	Indicate the server, which is configured	Display	Firmware Store Configuration Store Logfile Store
Transfer Protocol	Selector to disable the access to the server or to select the right protocol.	PullDown Menu • Disabled • SFTP • TFTP	SFTP
Server IP	IP-address for the FTP server.	IPv4-Address IPv6-Address	0.0.0.0

Table 1-10 *Server Configuration (continued)*

Parameter	Description	Format	Default
Server Port	TCP port for the SFTP communication and/or UDP port for TFTP communication. If you enter the value “0”, the default port for the selected protocol is used.	Input	SFTP: 22 TFTP: 69
Server Directory	The file-path on the server. Keep in mind, this is the path from the server’s root-directory. [i] Note: If the path does not exist, the FTP session can not access to the file. For upload process, the FTP application will not create new paths, if the given path does not exist.	Input	/
User Name [ii]	The user name, deposed on the SFTP server.	Input	empty
Password [ii]	The password for the user’s SFTP access. The password must be entered twice for verification. Please retype it in the bottom field:  If a valid password is stored on the device, it will be shown as <hidden> to avoid phishing: 	Input	empty

[i] The file’s path has to be specified with slash (’/’), when used on a Windows based FTP-server. Otherwise the FTP-server can not locate the correct file.

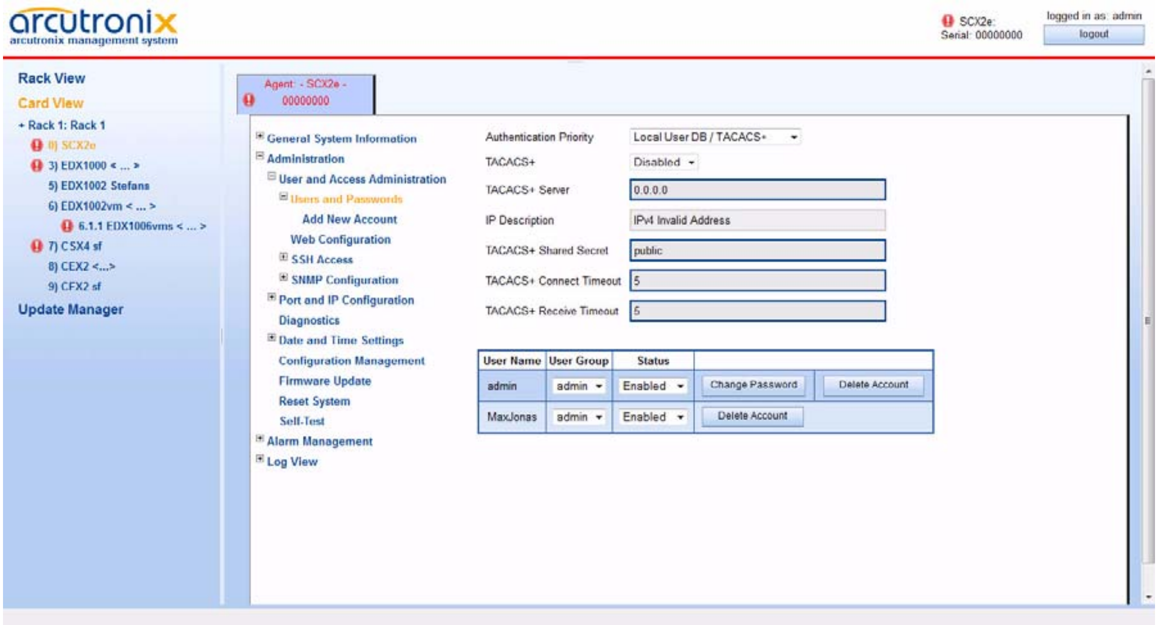
[ii] Only required for SFTP access

When all settings are compliant, the resulting URI (Uniform Resource Identifier) can be seen and the entry is signed as “Valid” in the overview menu.

To delete a server and all its settings, press “Clear Server Info”. This will remove the settings permanently.

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.



Authentication Priority	Local User DB / TACACS+
TACACS+	Disabled
TACACS+ Server	0.0.0.0
IP Description	IPv4 Invalid Address
TACACS+ Shared Secret	public
TACACS+ Connect Timeout	5
TACACS+ Receive Timeout	5

User Name	User Group	Status	
admin	admin	Enabled	Change Password Delete Account
MaxJonas	admin	Enabled	Delete Account

Figure 1-11 *Users and Passwords*

On top of the page are the settings for the TACACS+ authentication protocol (Terminal Access Controller Access-Control System). TACACS is a server based protocol and is used to define a common data-base for user/password/access-level. See chapter “TACACS+” in [axManualSCX2e] for details about TACACS+ and the settings.

Table 1-12 provides information about the options.

Table 1-11 *TACACS+ Settings*

Parameter	Description	Format	Default
Authentication Priority	The priority of the locally stored user database in relation to TACACS+ authentication. The local DB can have priority over TACACS or vice versa. When TACACS-only is selected, the local DB is ignored. When TACACS+ is disabled (see below), only the local DB will be used.	PullDown Menu • TACACS+ Authentication Only • TACACS+ / Local User DB • Local User DB / TACACS+	
TACACS+	This setting allows configuring whether authentication of logins to the Web-OPI, the CONS CLI or SSH CLI can be attempted via TACACS+. Before TACACS+ authentication can be enabled, it is required to configure the IP address of the TACACS+ server and a shared secret used to encrypt the communication with the TACACS+ server.	PullDown Menu • Disabled • Enabled	Disabled
TACACS+ Shared Secret	Enter here the “shared secret” for the secured communication with the TACACS+ server.	Text-Entry	public
TACACS+ Server	The IP-address of the TACACS+ server	IPv4-Address IPv6-Address	0.0.0.0
TACACS+ Connect Timeout	Timeout in seconds when establishing a connection to the TACACS+ server.	Entry	5
TACACS+ Receive Timeout	Timeout in seconds when waiting for a TACACS+ server response.	Entry	5

After this a list with all configured users and their read- and write-authorization is given (“users overview table“). Each user’s account can be disabled, if this is temporarily required. To delete a configured user-account and remove it from the system forever, 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”.

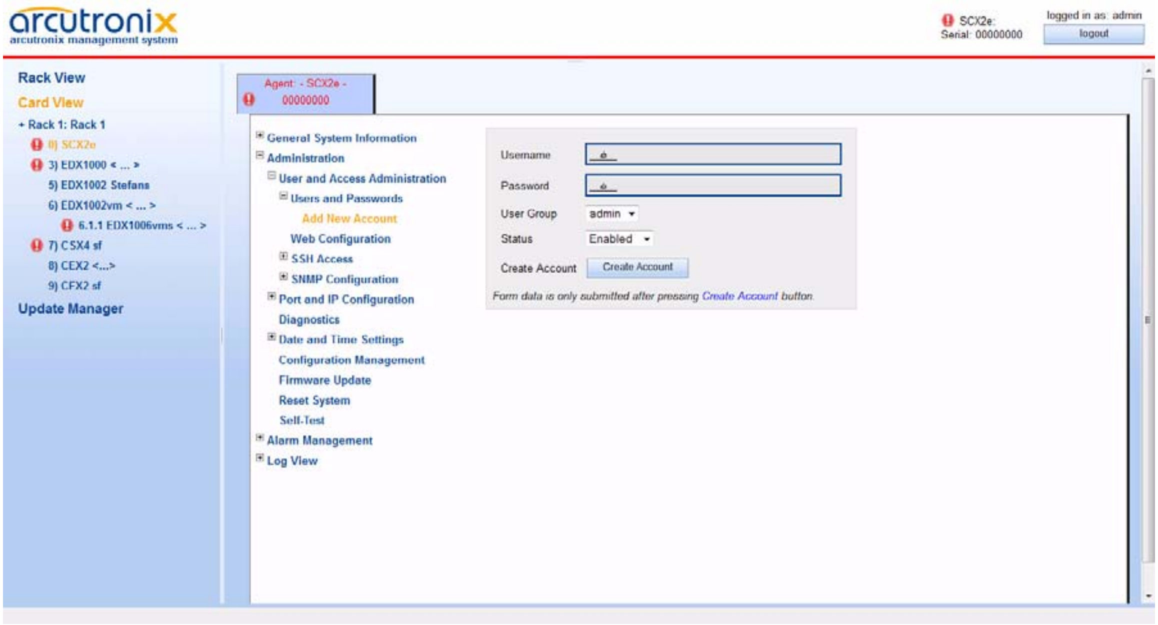
Table 1-12 provides information about the options.

Table 1-12 *Users and Passwords*

Parameter	Description	Format
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 Navigation Pane. The following menu will be displayed:



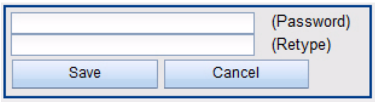
Username	
Password	
User Group	admin ▾
Status	Enabled ▾
Create Account	Create Account

Form data is only submitted after pressing Create Account button.

Figure 1-12 *Add Account*

Table 1-13 provides information about the options.

Table 1-13 *Add Account*

Parameter	Description	Format	Default
Username [i]	Enter name of new user.	Input	no default
Password [ii]	The user’s (new) password. The password must be entered twice for verification. Please retype it in the bottom field:  If a valid password is stored on the device, it will be shown as <hidden> to avoid phishing: <hidden>	Input	no default
User Group	The read/write access level is allocated.	PullDown Menu • admin • user • guest	admin
Create Account	Press button to confirm new user data. See in the bottom row, whether the creation was successful.	Confirm Button	

[i] For user names some simple rules are in force, which are depicted in “Rules for Usernames” of [axManualSCX2e].
[ii] For passwords special rules are in force, which are depicted in “Rules for Passwords” of [axManualSCX2e].

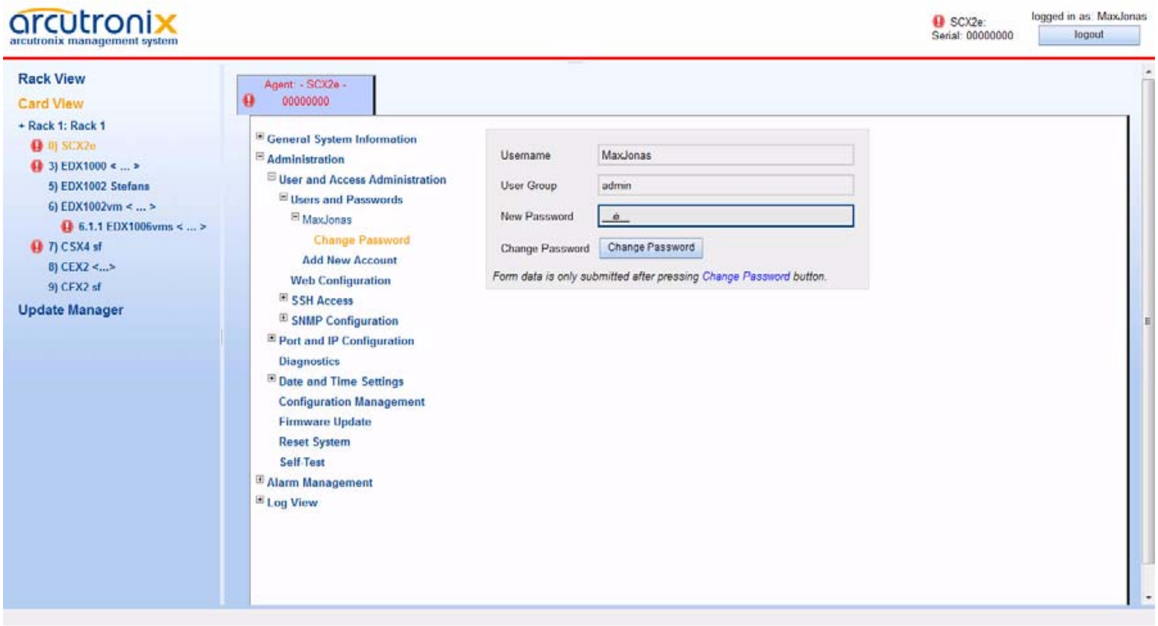
Note: The maximum number of different users is 99.

Note: After successful creating of a new user, a new entry in the “users overview table” must be visible. 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!



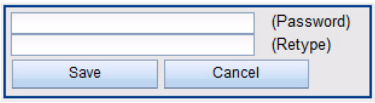
Username: MaxJonas
User Group: admin
New Password: e
Change Password

Form data is only submitted after pressing Change Password button.

__Figure 1-13__ Modify Account

Table 1-14 provides information on the menu.

__Table 1-14__ 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:  (Password) (Retype) Save Cancel If a valid password is stored on the device, it will be shown as <hidden> to avoid phishing: <hidden>	Input	no default
User Group [ii]	The new read/write access level be allocated.	PullDownMenu • admin • user • guest	old value

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: After successful changes of user-settings, the modified entry in the “users overview table” must be visible. There you can see all created users and their read- and write-permissions.

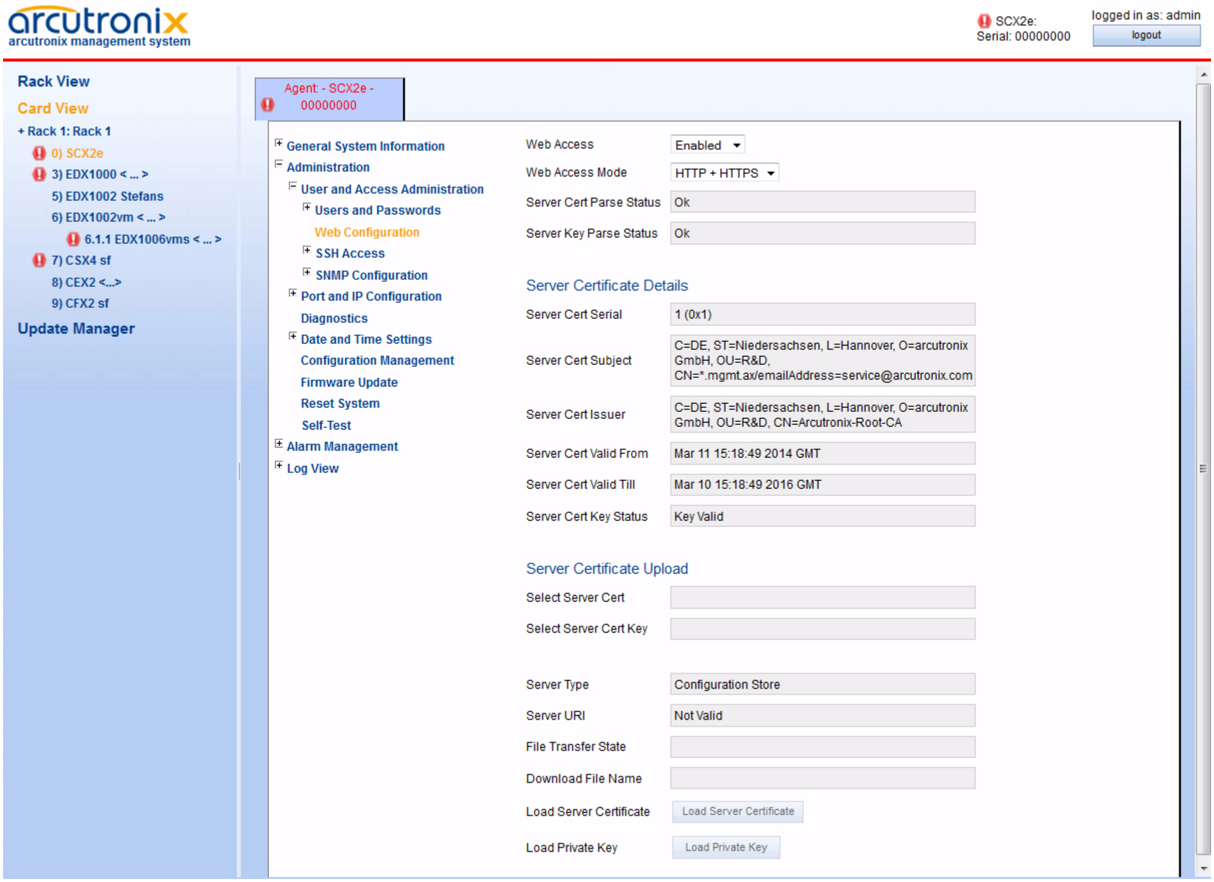
NOTE: If a user has forgotten its password, nobody can reset it to any default. In this case, the user’s account must be deleted and re-added with (new) password.

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.

Web Configuration

This menu offers the possibility to configure the web-access and managing the HTTPS settings, especially the https-certificate.The user can select, whether the web-access is enabled or not. In case it is enabled, one can choose the support of HTTP, HTTPS or both. In factory default, the web-access is enabled with both protocol options.



Web Access	Enabled
Web Access Mode	HTTP + HTTPS
Server Cert Parse Status	Ok
Server Key Parse Status	Ok

Server Certificate Details

Server Cert Serial	1 (0x1)
Server Cert Subject	C=DE, ST=Niedersachsen, L=Hannover, O=arcutronix GmbH, OU=R&D, CN=*.mgmt.ax/emailAddress=service@arcutronix.com
Server Cert Issuer	C=DE, ST=Niedersachsen, L=Hannover, O=arcutronix GmbH, OU=R&D, CN=Arcutronix-Root-CA
Server Cert Valid From	Mar 11 15:18:49 2014 GMT
Server Cert Valid Till	Mar 10 15:18:49 2016 GMT
Server Cert Key Status	Key Valid

Server Certificate Upload

Select Server Cert	
Select Server Cert Key	
Server Type	Configuration Store
Server URI	Not Valid
File Transfer State	
Download File Name	
Load Server Certificate	Load Server Certificate
Load Private Key	Load Private Key

Figure 1-14 *Web Configuration*

Table 1-15 provides information about the options.

Table 1-15 *Web Configuration*

Parameter	Description	Format
Web Access	Enables or disables the web access. The Default is Enabled.	PullDown Menu • Disabled • Enabled
Web Access Mode	Selector for the supported protocol(s), when web access is enabled. The Default is HTTP + HTTPS.	PullDown Menu • HTTP • HTTPS • HTTP + HTTPS
Server Cert Parse Status	Shows whether the server certificate could be parsed.	Display
Server Key Parse Status	Shows whether the server certificate private key could be parsed.	Display
Server Certificate Details [i]		
Server Cert Serial	Shows the serial number of the HTTPS server certificate.	Display
Server Cert Subject	Shows information about the owner of the HTTPS server certificate.	Display
Server Cert Issuer	Shows information about the issuer of the HTTPS server certificate.	Display
Server Cert Valid From	Validity start date/time of the HTTPS server certificate.	Display
Server Cert Valid Till	Validity end date/Time of the HTTPS server certificate	Display
Server Cert Key Status	Shows information about the required private key.	Display • Key Missing • No Certificate • Key Invalid • Key Mismatch • Key Valid
Server Certificate Upload [ii]		
Select Server Cert	Select a server certificate file for upload (PEM file format).	Display
Select Server Cert Key	Select a private key matching the server certificate (PEM file format, no passphrase).	Display

Table 1-15 Web Configuration (continued)

Parameter	Description	Format
Server Type	Indicate the server, which is used for S/TFTP file transfer. Always “Configuration Store”	Display
Server URI	The configuration of Configuration Store. Here one can see, whether SFTP or TFTP is selected, the IP-address etc. URI = Uniform Resource Identifier	Display
File Transfer State	Shows information about a file transfer from the configuration server.	Display
Download File Name	Name of a certificate or private key file on the configuration server.	

i. Only visible, when a certificate is available on the device.

ii. These entries are only editable, when HTTPS is disabled!

NOTE: A new certificate and or a new key can only be loaded, when HTTPS is disabled! Otherwise, the new certificate and/or key will destroy the HTTPS session, as soon as it is loaded.

As soon as all settings are set correct, the new certificate and/or new key can be uploaded by pressing the according button:

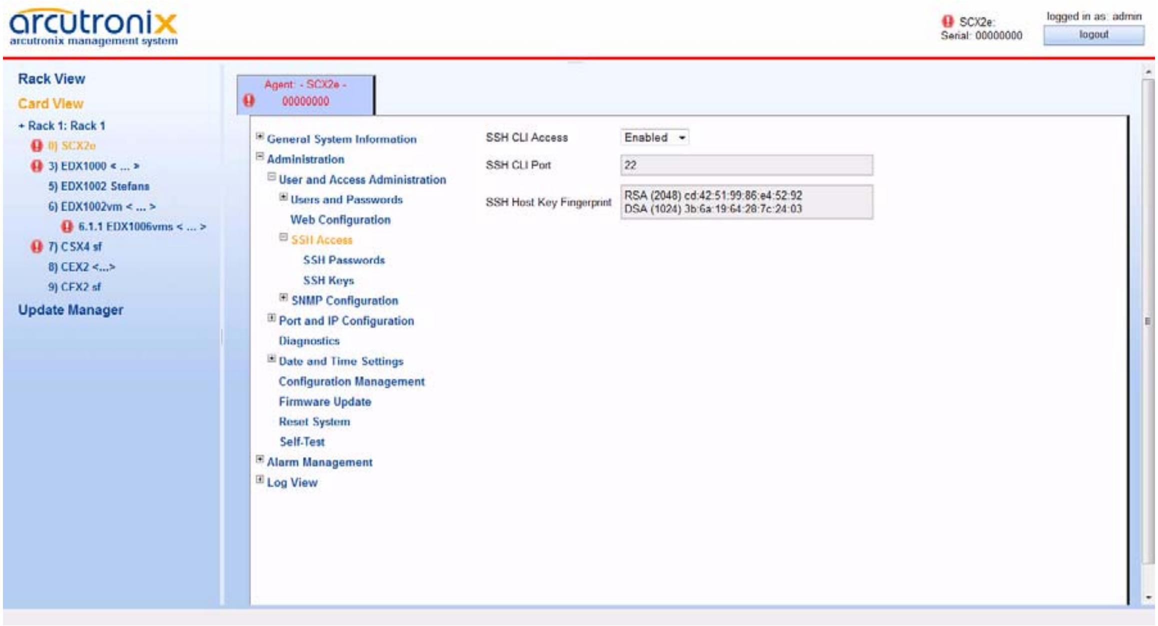
Table 1-16 Load Certificate and Key

Parameter	Description	Format
Load Server Certificate	Starts a download of the server certificate from the “Configuration Store” server.	Action
Load Private Key	Starts a download of the private key file from the “Configuration Store” server.	Action

There are no submenus available.

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.



SSH CLI Access: Enabled

SSH CLI Port: 22

SSH Host Key Fingerprint: RSA (2048) cd:42:51:99:86:e4:52:92
DSA (1024) 3b:6a:19:64:28:7c:24:03

Figure 1-15 SSH Access

Table 1-18 provides information about the options.

Table 1-17 SSH Access

Parameter	Description	Format	Default
SSH CLI Access	Enables or disables the SSH access.	PullDown Menu • Disabled • Enabled	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 [i]	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	

i. The SSH keys are very long numbers. Only the first 8 bytes are displayed.

The following submenus are available:

Table 1-18 *Submenus of SSH Access*

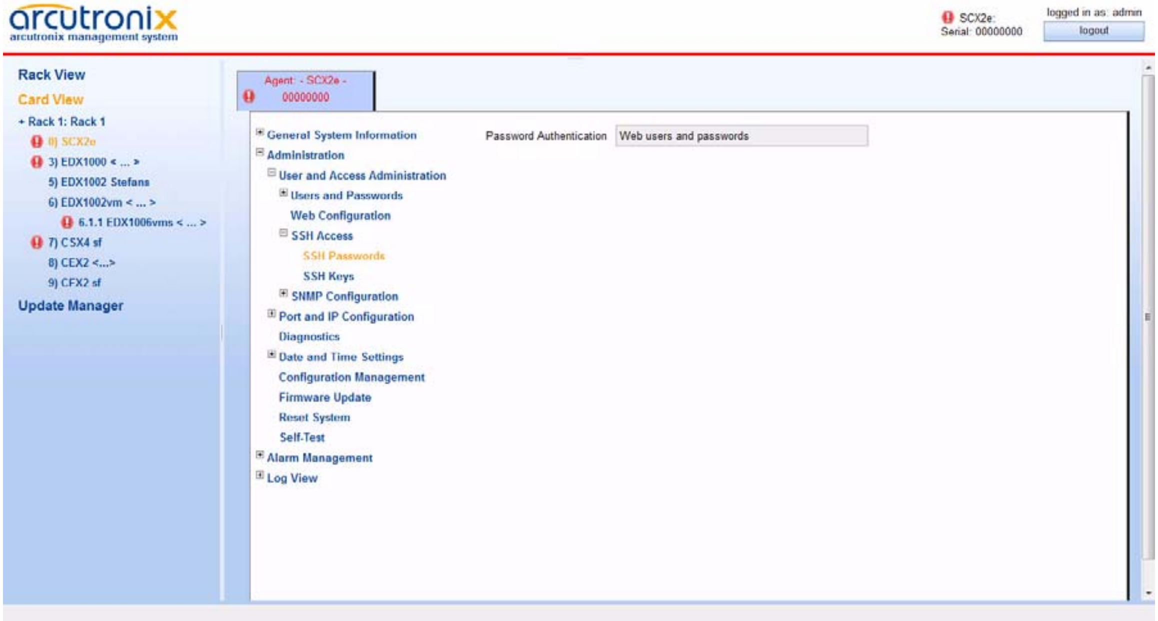
Parameter	Description
SSH Passwords	Submenu to select the way how to authenticate at the SSH server of the device.
SSH Keys	Submenu to upload a public SSH key if available.

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-GUI access (see chapter “File Servers” on page 1-20).
- Use a special global SSH-connection password, which can be configured here, when this option is selected.

NOTE: The Password Authentication can only be changed, when the CLI-access is (temporarily) disabled!

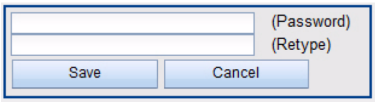


Password Authentication: Web users and passwords

Figure 1-16 *SSH Password*

Table 1-19 provides information about the menu.

Table 1-19 *SSH User Definition*

Parameter	Description	Format	Default
Password Authentication	Pulldown Menu to select the how to authenticate at the SSH server (SCX2e). For details on the possible option see [axRefGuideCLI_SCX2e]. Note: The value can only be changed, when the SSH-access is disabled.	PullDown Menu - “Password authentication disabled” - “Web users and passwords” - “Use global SSH connection password”	“Web users and passwords”
Global Access Password	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. The password must be entered twice for verification. Please retype it in the bottom field:  (Password) (Retype) Save Cancel If a valid password is stored on the device, it will be shown as <hidden> to avoid phishing: <hidden>	Input	empty

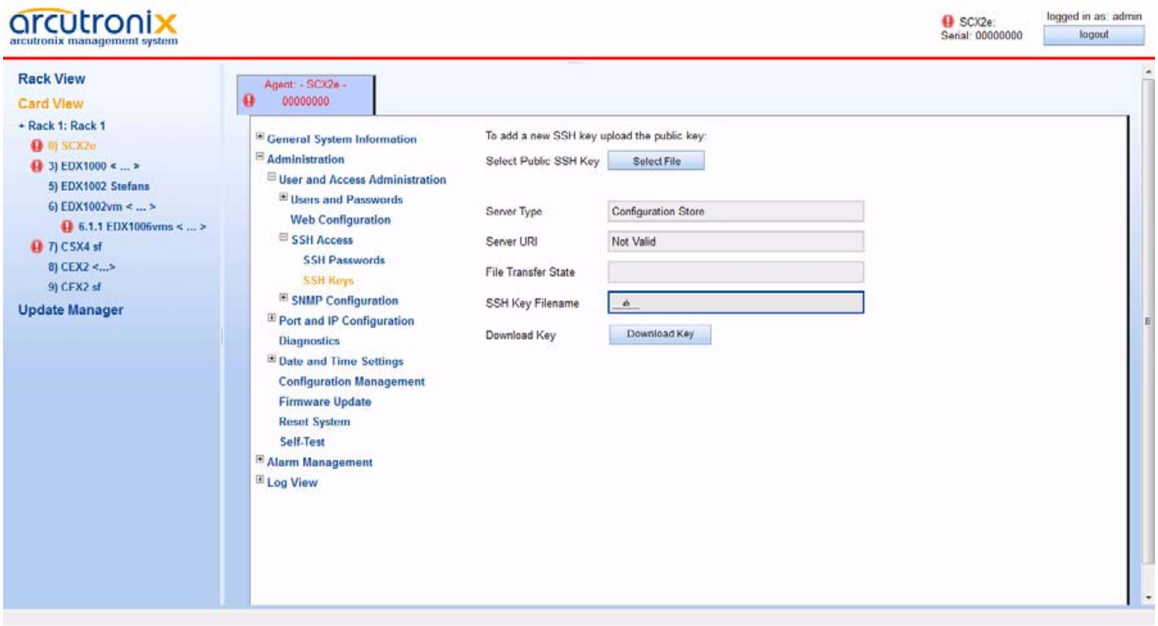
SSH Keys

This menu offers the possibility to upload a SSH key via file-transfer. The file with the SSH-key can either be uploaded via http (if enabled) or downloaded via S/TFTP.

If http-upload is enabled and selected, the file can be selected via explorer window and then uploaded to be stored on the device.

If SFTP or TFTP download shall be used, the Configuration Server (see chapter “File Servers” on page 1-20) must be properly and valid configured. Inhere, just the file-name of the SSH-key must be given and “Download Key” pressed.

NOTE: The SSH-key, which is stored on the device is a public key. The SCX2e expects that the filename’s extension is “*.pub”.



To add a new SSH key upload the public key:

Select Public SSH Key

Server Type: Configuration Store

Server URI: Not Valid

File Transfer State:

SSH Key Filename:

Download Key

Figure 1-17 SSH Password

SNMP Configuration

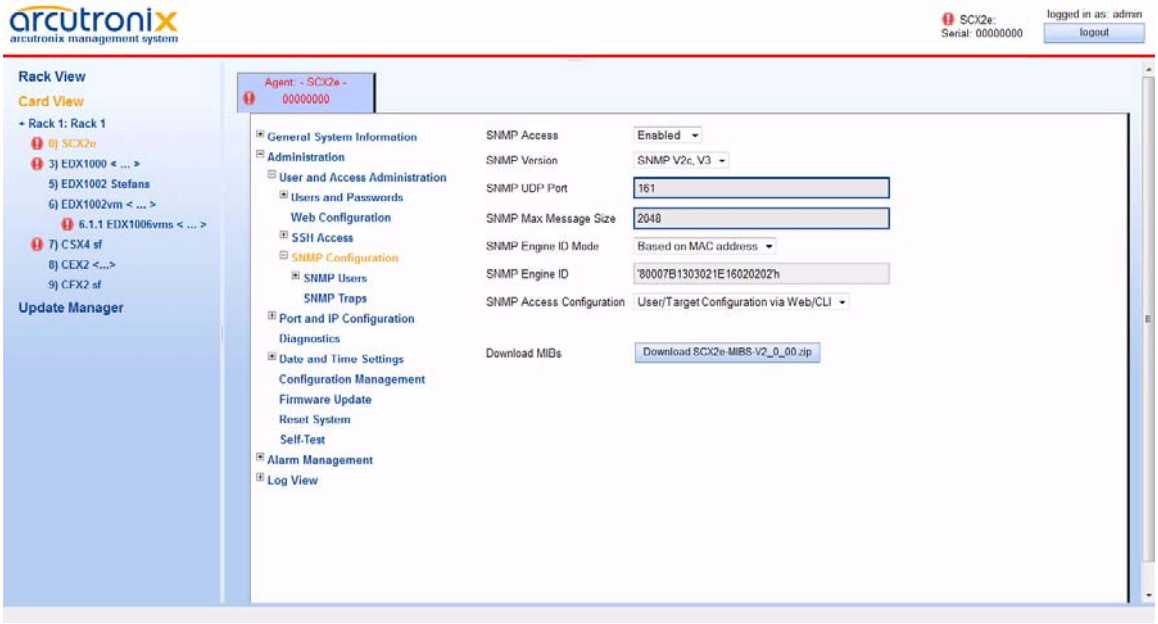
This menu offers the possibility to configure the SNMP settings, like communities and trap-receivers. If required by the user, the SNMP access can be disabled at all, to avoid illegal access to the device. In factory default, the SNMP access is enabled.

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.



SNMP Access: Enabled
SNMP Version: SNMP V2c, V3
SNMP UDP Port: 161
SNMP Max Message Size: 2048
SNMP Engine ID Mode: Based on MAC address
SNMP Engine ID: '80007B1303021E16020202'h
SNMP Access Configuration: User/Target Configuration via Web/CLI
Download MIBs: Download SCX2e-MIBS-V2_0_00.zip

Figure 1-18 SNMP Configuration, SNMP enabled

Table 1-20 provides information about the options.

Table 1-20 SNMP Configuration

Parameter	Description	Format	Default
SNMP Access	Enables or disables the SNMP access.	PullDown Menu • Disabled • Enabled	Enabled
SNMP Version	Select the SNMP version to be used	PullDown Menu • 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
SNMP Engine ID Mode	Select, how the SNMP Engine ID is assigned.	PullDown Menu • Automatically • Based on MAC Address • Bases on sysName	Based on MAC Address

Table 1-20 SNMP Configuration (continued)

Parameter	Description	Format	Default
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 • User/Target Configuration via Web/CLI • User/Target Configuration via SNMP	User/Target Configuration via Web/CLI

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

The following submenus are available:

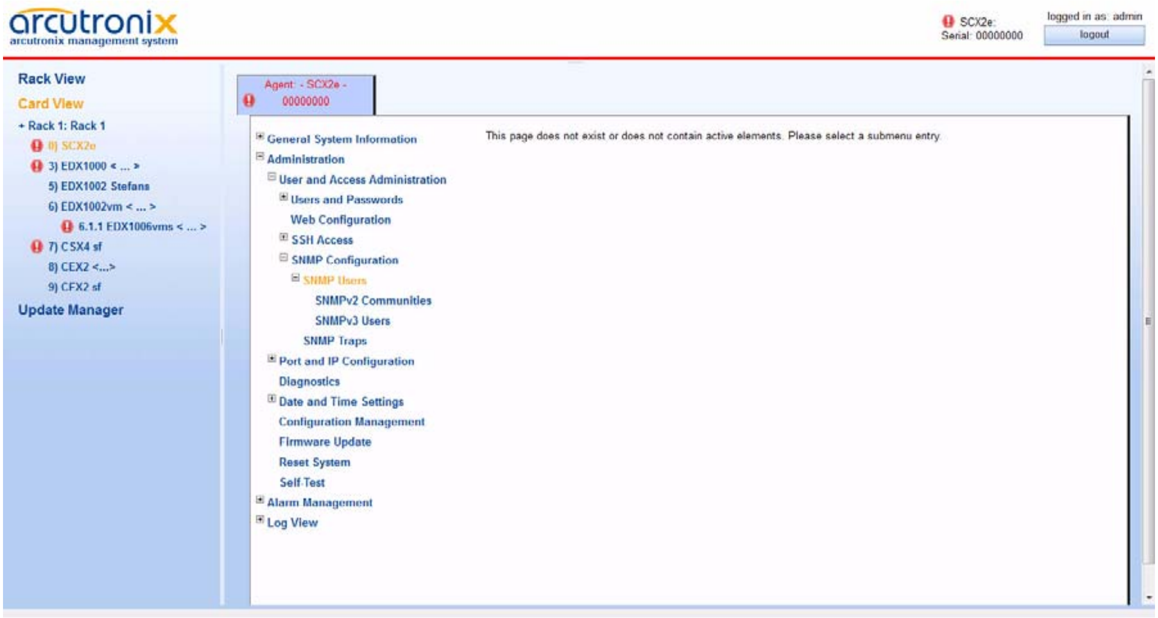
Table 1-21 SNMP Configuration: Submenus

Submenu	Description
SNMP Users	Add, change and delete the communities and the related access levels.
SNMP Traps	Add, change and delete the Trap receivers.
Download MIBs	Press Button to download a ZIP-file with all supported MIBs via HTTP. Note: This button is only visible, when “HTTP File Transfer” is enabled (see “User and Access Administration” on page 1-18).

SNMP Users and Community Configuration

This menu lists the defined SNMP community strings (SNMPv2c) or SNMP users (SNMPv3) 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 Navigation Pane. If there are not both protocols defined, only the selected one is displayed.

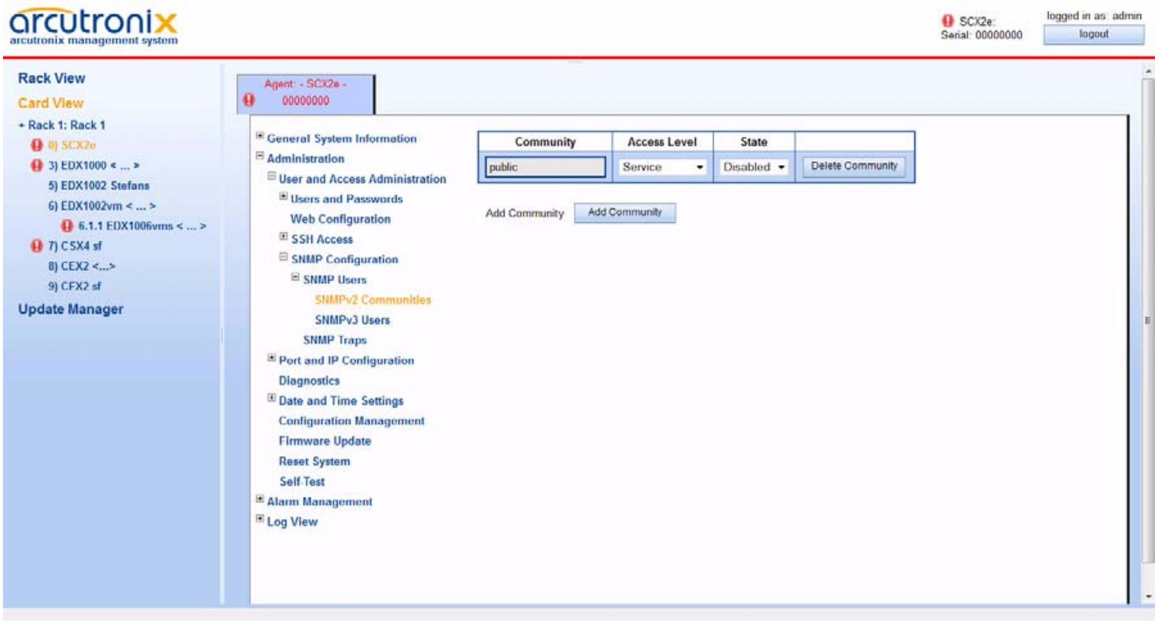


This page does not exist or does not contain active elements. Please select a submenu entry.

Figure 1-19 *SNMP Users and Community*

SNMPv2 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.



Community	Access Level	State	
public	Service	Disabled	Delete Community

Add Community: Add Community

Figure 1-20 *SNMPv2c Community*

Table 1-22 provides information about the options.

***Table 1-22** SNMPv2c Community Configuration*

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 • Administrator • Service • Monitor	Service
State	Enable / disable the community.	PullDown Menu • Enabled • Disabled	Disabled
Delete SNMP 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*!

SNMPv3 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

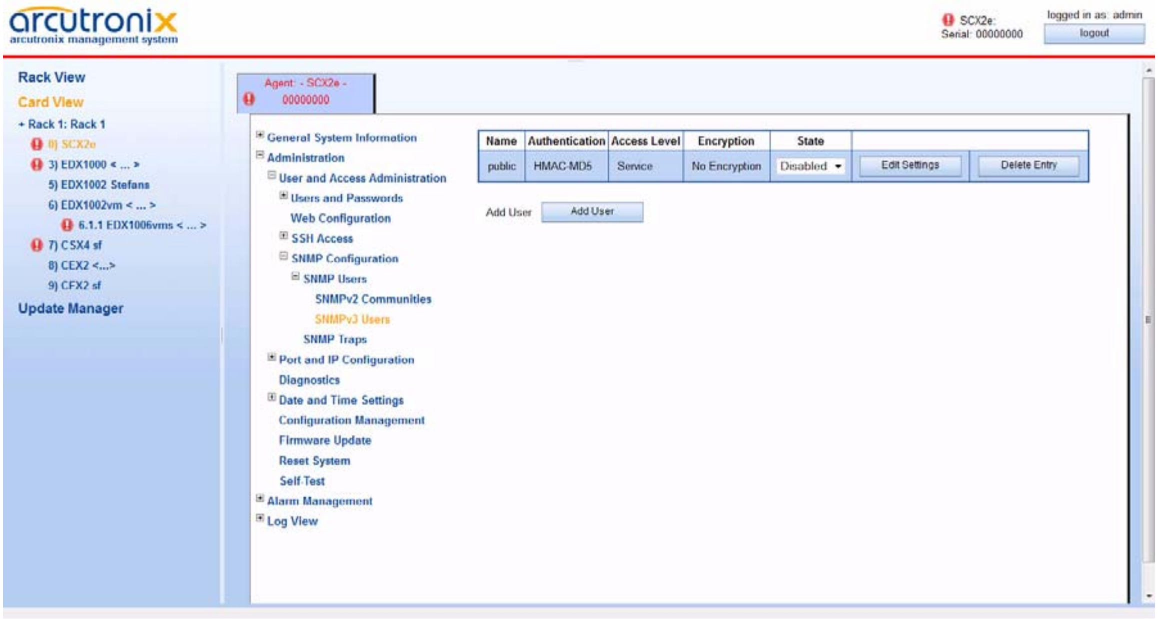
- Encryption: the encryption mode that is supported for the SNMPv3 user (DES/AES encryption with Passovers or no encryption)

- 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.



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

Figure 1-21 *SNMPv3 User*

Table 1-23 provides information about the options.

Table 1-23 *SNMPv3 User*

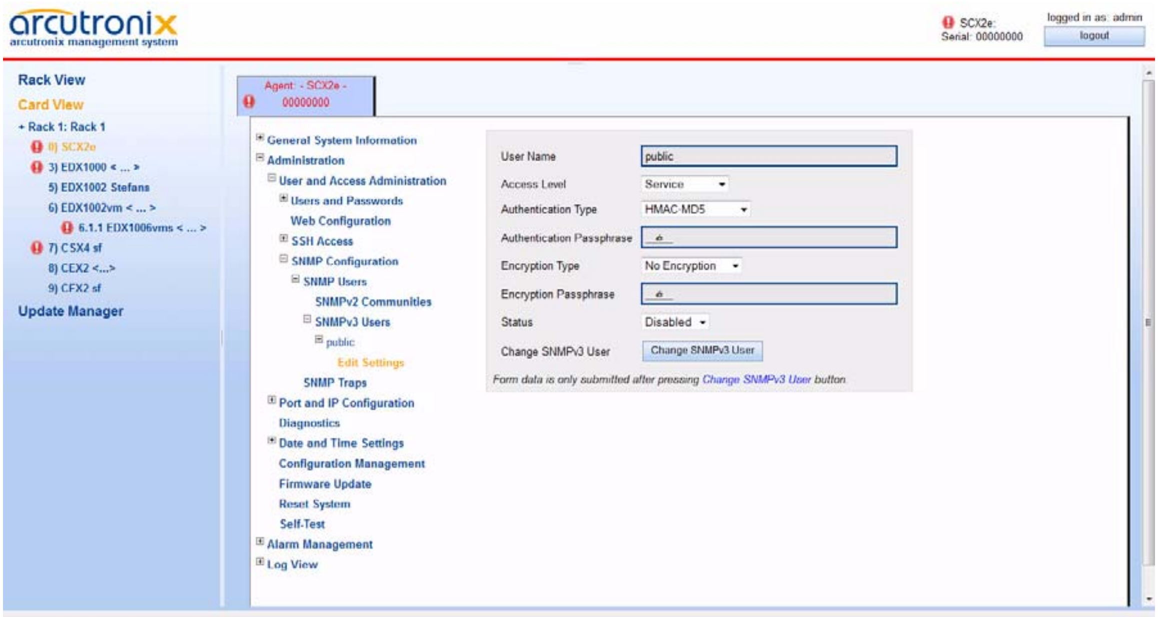
Parameter	Description	Format	Default
Edit Settings	Press Button and select an entry in the (scroll) list. After this the Edit SNMP User menu opens.	SelectList/Menu	
Delete Entry	Press Enter and select an entry in the (scroll) list. After this confirm the action.	SelectList/Confirm	
Add User	Add a new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

NOTE: When “Add SNMPv3 User” is selected, a new entry in the list above is created: “public”, with access level *User*. 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 options are shown in Table 1-24.



User Name: public
Access Level: Service
Authentication Type: HMAC-MD5
Authentication Passphrase:
Encryption Type: No Encryption
Encryption Passphrase:
Status: Disabled
Change SNMPv3 User

Form data is only submitted after pressing Change SNMPv3 User button.

Figure 1-22 *SNMPv3 Edit User Settings*

Table 1-24 *SNMPv3 User Settings*

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 • Administrator • Service • Monitor	Service

Table 1-24 SNMPv3 User Settings (continued)

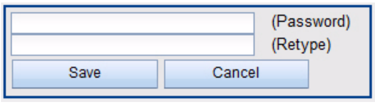
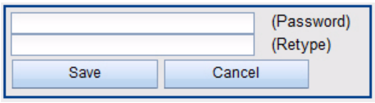
Parameter	Description	Format	Default
Authentication Type	This settings determines the authentication method to use for authenticating messages of this user. It is shown in the “Passphrase” column of the user list.	PullDown Menu • No Authentication • HMAC-MD5 • HMAC-SHA	HMAC-MD5
Authentication Passphrase	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 [IETF RFC 3414]. The passphrase must be entered twice for verification. Please retype it in the bottom field:  If a valid passphrase is stored on the device, it will be shown as <hidden> to avoid phishing: <hidden>	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 • No Encryption • DES Encryption • AES Encryption	No Encryption

Table 1-24 SNMPv3 User Settings (continued)

Parameter	Description	Format	Default
Encryption Passphrase	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 [IETF RFC 3414]. The passphrase must be entered twice for verification. Please retype it in the bottom field:  If a valid passphrase is stored on the device, it will be shown as <hidden> to avoid phishing: <hidden>	string	empty
Status	When Status is set to Disabled, no messages in behalf of this used will be accepted.	PullDown Menu • Enabled • Disabled	Disabled
Apply	The changes can be made permanent using the “Apply” button. If you do not want to confirm your settings, just press the “Back” button in your web browser.	Select Button/Confirm	

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:

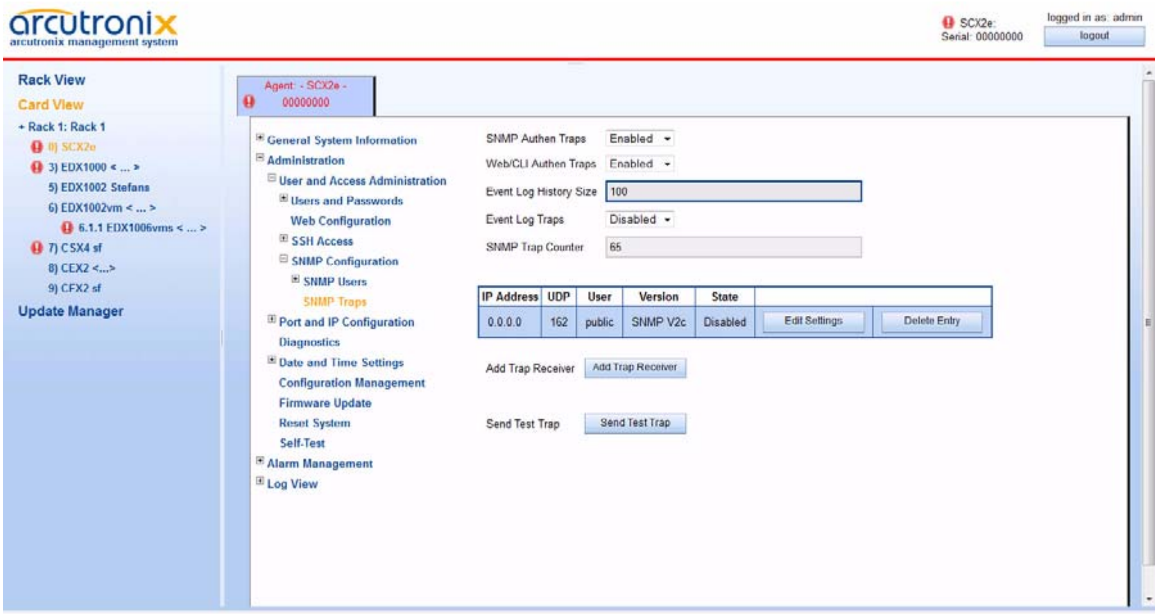
***Table 1-25** SNMPv3 Confidentiality*

Authentication	Encryption	Accepted SNMP Messages
enabled	enabled	noAuthNoPriv; authNoPriv; authPriv
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 AuthenTraps can be enabled or disabled. Furthermore, the list of currently known trap receivers (e.g. management stations) is visible.



SNMP Authen Traps: Enabled
Web/CLI Authen Traps: Enabled
Event Log History Size: 100
Event Log Traps: Disabled
SNMP Trap Counter: 65

IP Address	UDP	User	Version	State		
0.0.0.0	162	public	SNMP V2c	Disabled	Edit Settings	Delete Entry

Add Trap Receiver: Add Trap Receiver
Send Test Trap: Send Test Trap

***Figure 1-23** 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 1-26):

Table 1-26 *SNMP Trap Configuration*

Parameter	Description	Format	Default
SNMP Authen Traps	When the 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.	PullDown Menu • Disabled • Enabled	Enabled
Web/CLI Authen Traps	When the device detects an invalid login either from Web-GUI or CLI, it can send an authentication trap message. An invalid Login is either unknown user-name or wrong password.	PullDown Menu • Disabled • Enabled	Enabled
SNMP Alarm Trap Type	Determines whether an individual alarm trap is sent for each alarm or one common trap for all alarms.	PullDown Menu • Individual Alarm Traps • Common Alarm Trap	Individual Alarm Traps
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 • Disabled • Enabled	Enabled
INFO Message Traps	A trap can be enabled, at any time an INFO-event is written into the log file. [i]	PullDown Menu • Disabled • Enabled	Enabled
ERROR Message Traps	A trap can be enabled, at any time an ERROR-event is written into the log file. [i]	PullDown Menu • Disabled • Enabled	Enabled
ALARM Message Traps	A trap can be enabled, at any time an ALARM-event is written into the log file. [i]	PullDown Menu • Disabled • Enabled	Enabled
SNMP Trap Counter	Counter of all outgoing (sent) enterprise traps.	Display	0

Table 1-26 SNMP Trap Configuration (continued)

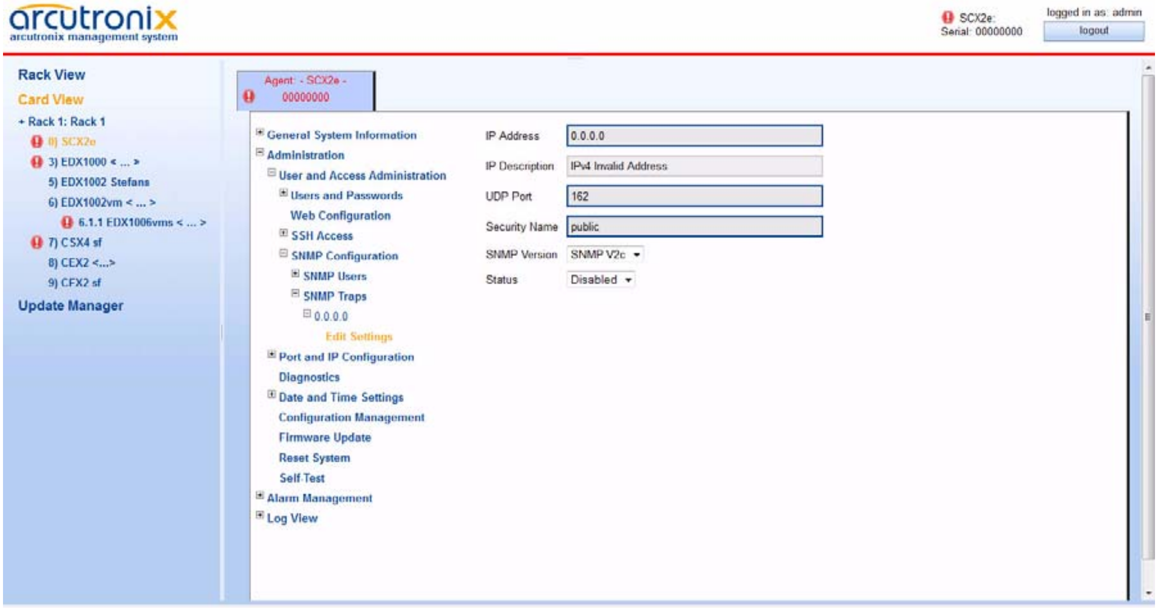
Parameter	Description	Format	Default
Edit Settings	Press Button for an entry in the list. After this the Edit SNMP Trap Receiver menu opens.	Select Button/Menu	
Delete Entry	Press Button and the related entry will be removed from the list.	Select Button/Confirm	
Add Trap Receiver	Add a new SNMP Trap Receiver. A new entry in the trap receiver list will be attached, which can be configured thereafter.	Action	
Send Test Trap	Sends a test trap (axCommonTestTrap) to all configured trap receivers to test SNMP trap settings.	Action	

i. Only visible, when "Event Log Traps" is enabled.

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:



IP Address: 0.0.0.0
IP Description: IPv4 Invalid Address
UDP Port: 162
Security Name: public
SNMP Version: SNMP V2c
Status: Disabled

Figure 1-24 Edit SNMP Trap Receiver

Table 1-27 provides information about the options.

Table 1-27 *Edit SNMP Trap Receiver*

Parameter	Description	Format	Default
IP Address	The IP-address of the management station to which the traps should be sent.	IPv4-Address IPv6-Address	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
SNMP Version	Whether to generate SNMPv2 or SNMPv3 trap messages.	PullDown Menu • SNMP v2c • SNMP v3	SNMP v2c
Status	Whether this management station will receive any traps or not.	PullDown Menu • Enabled • Disabled	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 and the physical settings of the available management ports. Depending on the given configuration, the device can have two to four independent ports. In the case there are less than four ports, some physical interfaces might be grouped to a Combo-port (Copper / fibre combination). The ports can be used in 4 different operation modes:

- Remote Mgmt (Q): Remote connection via DCN to a central NOC,
- Local Mgmt (F): Local management access via laptop for service and craft people,
- Daisy Chain: Forwarding port of remote management traffic, e.g. to a sub-ordinary SCX2e,
- Agent Communication: Agent-2-agent link for remote management.

See “IP-Addressing” in [axManualSCX2e] for details about F- and Q-interface, Daisy-Chain and Agent-Comm Management ports.

NOTE: The type “Daisy-Chain” and “Agent-Comm” can not be selected by customer, but comes with the factory configuration of the device!

Setup for SCX2e

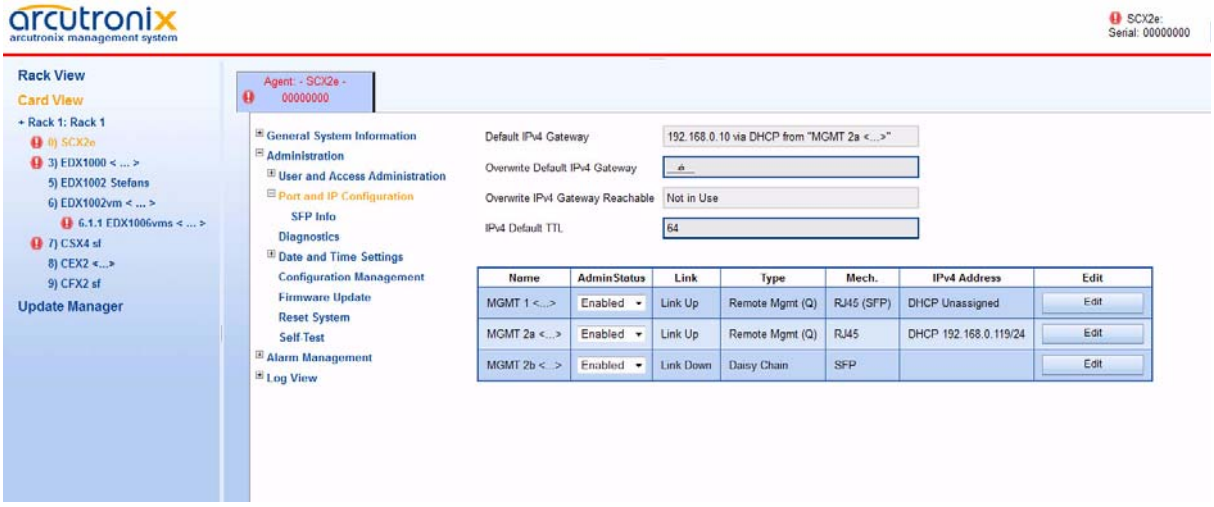
For SCX2e the following factory setup is given:

- MGMT1a/b: Combo-port in Q-mode,
- MGMT2a: Copper port in F-mode,
- MGMT2b: Fibre port for cascading the remote management traffic.

Setup for SCX2e-WDM

- MGMT1a: Copper port in F-mode,
- MGMT1b: Fibre port in Q-mode,
- MGMT2a: not equipped,
- MGMT2b: Fibre port for remote management (Agent Comm).

Menu



Default IPv4 Gateway: 192.168.0.10 via DHCP from "MGMT 2a <...>"

Overwrite Default IPv4 Gateway:

Overwrite IPv4 Gateway Reachable: Not in Use

IPv4 Default TTL: 64

Name	AdminStatus	Link	Type	Mech.	IPv4 Address	Edit
MGMT 1 <...>	Enabled	Link Up	Remote Mgmt (Q)	RJ45 (SFP)	DHCP Unassigned	Edit
MGMT 2a <...>	Enabled	Link Up	Remote Mgmt (Q)	RJ45	DHCP 192.168.0.119/24	Edit
MGMT 2b <...>	Enabled	Link Down	Daisy Chain	SFP		Edit

Figure 1-25 *Port and IP Configuration*

Table 1-28 provides information about the options.

Table 1-28 *Port and IP-Configuration*

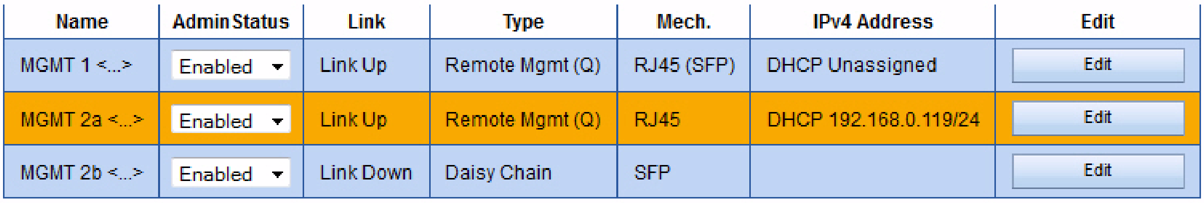
Parameter	Description	Format	Default
Default Gateway	Shows the address of the (selected) Default Gateway. The Default GW may be assigned via DHCP or manually. Note: The manual assignment (if given called Overwrite Gateway) has priority above DHCP.	IPv4	None
Overwrite Gateway Address	This variable allows to manually specify a default gateway to use by the device. Setting the Overwrite Gateway Address to address to 0.0.0.0 disables the use of the manually specified gateway.	IPv4	Not in Use (0.0.0.0)

Table 1-28 Port and IP-Configuration (continued)

Parameter	Description	Format	Default
Overwrite Gateway Reachable	Indicator, whether the Overwrite Gateway is reachable with the actual IP settings or not.	Display	
IP Default TTL	Default Time-to-Life value for all outgoing IP packets.	Integer	64

Below the above mentioned 4 entries a quick overview of all management ports is given.

NOTE: The list depends on the given configuration.



Name	Admin Status	Link	Type	Mech.	IPv4 Address	Edit
MGMT 1 <...>	Enabled	Link Up	Remote Mgmt (Q)	RJ45 (SFP)	DHCP Unassigned	Edit
MGMT 2a <...>	Enabled	Link Up	Remote Mgmt (Q)	RJ45	DHCP 192.168.0.119/24	Edit
MGMT 2b <...>	Enabled	Link Down	Daisy Chain	SFP		Edit

Figure 1-26 *Port and IP Overview*

Table 1-29 provides information about the table rows and columns.

Table 1-29 Port and IP-Configuration

Parameter	Description	Format
Name	Name of the management port.	Display
Admin Status	The status of the port is shown. If required it can be disabled here.	Display
Link	Indicator, whether the Ethernet link is established or not.	Display
Type	The physical and logical type of the port: • Local Management in F mode, • Remote Management in Q mode, • Daisy Chain or • Agent Communication.	Display
Mech.	Information about the mechanical (physical) type of the port: • RJ45 = electrical 10/100BaseT, • SFP = optical 100BaseFx, • in case of a Combo port, the inactive part of the combo is written in brackets.	Display

Table 1-29 *Port and IP-Configuration (continued)*

Parameter	Description	Format
IPv4 Address	The host address of the interface and the setting for IP-address assignment.	Display
Edit	Press the “Edit” button to change the HW (PHY) and IP settings of the port.	Submenu

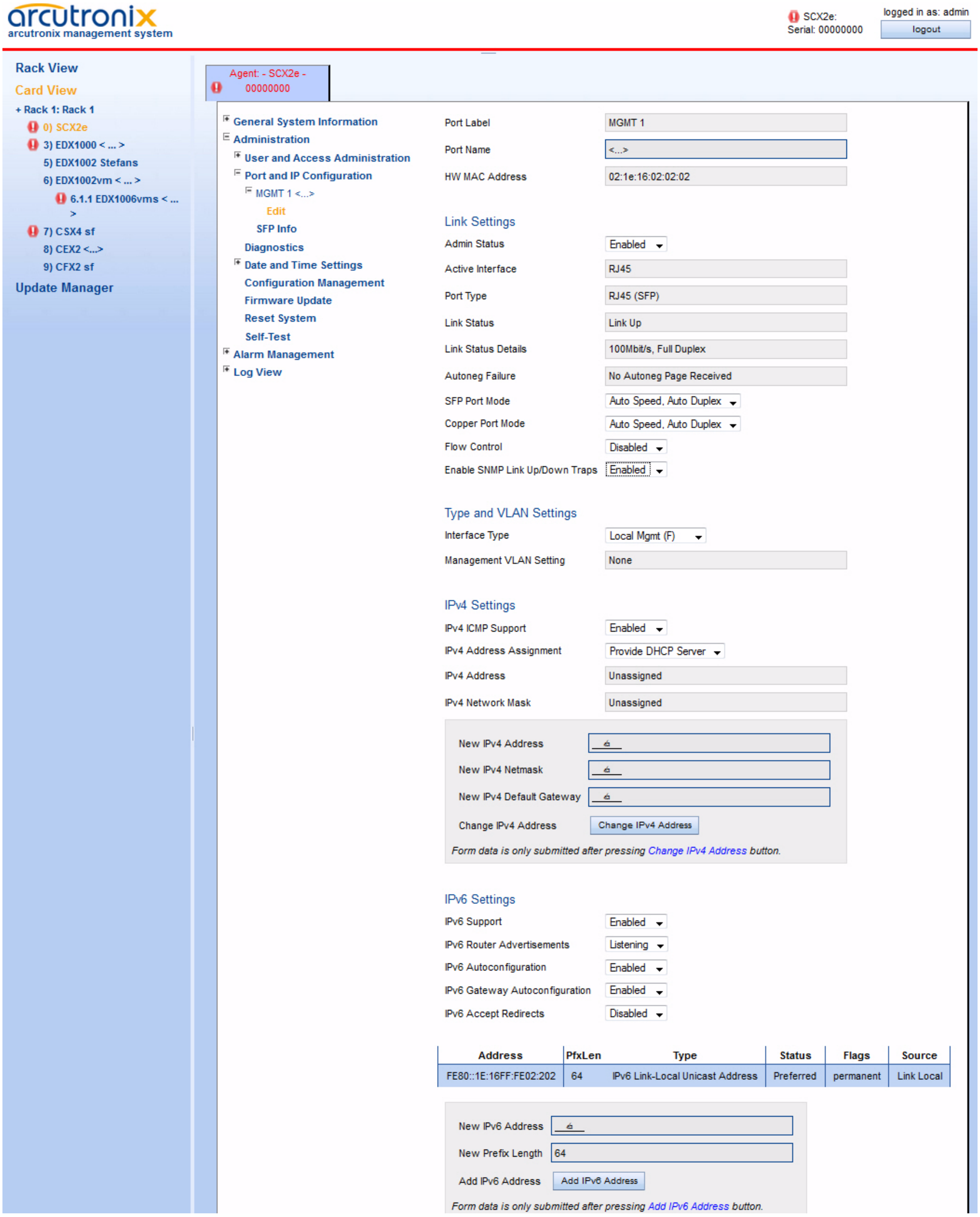
Warning: Any changes of the IP parameters may lead to contact loss with the device. Be careful when changing this attributes.
In case you made any changes a re-connection with the new IP address could be necessary.

Edit Settings

Use this menu to change the HW and IP settings and behaviour of the ports. The menu for the different ports might be different, as not all options are possible for the three types (local, remote, daisy-chain, agent-comm).

NOTE: The type “Daisy-Chain” and “Agent-Comm” can not be selected by customer, but comes with the factory configuration of the device!

Local MGMT Port (F-Interface)



Port Label	MGMT 1
Port Name	<...>
HW MAC Address	02:1e:16:02:02:02

Link Settings

Admin Status	Enabled
Active Interface	RJ45
Port Type	RJ45 (SFP)
Link Status	Link Up
Link Status Details	100Mbit/s, Full Duplex
Autoneg Failure	No Autoneg Page Received
SFP Port Mode	Auto Speed, Auto Duplex
Copper Port Mode	Auto Speed, Auto Duplex
Flow Control	Disabled
Enable SNMP Link Up/Down Traps	Enabled

Type and VLAN Settings

Interface Type	Local Mgmt (F)
Management VLAN Setting	None

IPv4 Settings

IPv4 ICMP Support	Enabled
IPv4 Address Assignment	Provide DHCP Server
IPv4 Address	Unassigned
IPv4 Network Mask	Unassigned

New IPv4 Address	
New IPv4 Netmask	
New IPv4 Default Gateway	
Change IPv4 Address	Change IPv4 Address

Form data is only submitted after pressing Change IPv4 Address button.

IPv6 Settings

IPv6 Support	Enabled
IPv6 Router Advertisements	Listening
IPv6 Autoconfiguration	Enabled
IPv6 Gateway Autoconfiguration	Enabled
IPv6 Accept Redirects	Disabled

Address	PfxLen	Type	Status	Flags	Source
FE80::1E:16FF:FE02:202	64	IPv6 Link-Local Unicast Address	Preferred	permanent	Link Local

New IPv6 Address	
New Prefix Length	64
Add IPv6 Address	Add IPv6 Address

Form data is only submitted after pressing Add IPv6 Address button.

Figure 1-27 *Edit LOCAL Port Settings*

Table 1-30 provide information about the options.

Table 1-30 *LOCAL Port Configuration*

Parameter	Description	Format	Default
Port Label	Printed text on the enclosure and front-plate.	Display	
Port Name	Name for this port. It can be free advised by user.	String	<...>
HW MAC Address	Displays the MAC address of the local management port.	Display	*00:1E:16:aa:bb:cc*
Link Settings:			
Admin Status	Indicator, whether the port shall be enabled or not.	PullDown Menu • Enabled • Disabled	Enabled
Active Interface	Indicates, whether the combo-port is in copper or fibre mode. Either “RJ45” (=copper) or “SFP” (=fibre).	Display	
Port Type	Show the port's mechanical type and usage.	Display	
Link Status	Indicates, whether the port is up, down or disabled.	Display	
Link Status Details	Indicates the link status in more details.	Display	
Autoneg Failure	Indicates a failure in the auto-negotiation process between the port and its peer. Note: Keep in mind for Copper I/F the auto-neg procedure is very important in case SyncE is enabled.	Display	
SFP Port Mode	Autonegotiation settings for the SFP (fibre) part of the combo-port. [i]. To disable the fibre option of the combo-port, select “do-not-use” here. In this case, the FO link can never be established.	PullDown Menu • do-not-use • Auto Speed, Auto Duplex • ...	Auto Speed, Auto Duplex

Table 1-30 LOCAL Port Configuration (continued)

Parameter	Description	Format	Default
Copper Port Mode	Autonegotiation settings for the copper part of the combo-port. [i] To disable the copper option of the combo-port, select “do-not-use” here. In this case, the UTP-link can never be established.	PullDown Menu • do-not-use • Auto Speed, Auto Duplex • ...	Auto Speed, Auto Duplex
Flow Control	IEEE 802.3x (PAUSE frames) can be enabled or disabled.	PullDown Menu • Enabled • Disabled	Disabled
Enable SNMP Link Up/Down Traps	Enables or disables a SNMP trap, if the link for this ports is changing its status to up or down.	PullDown Menu • Enabled • Disabled	Enabled
Type and VLAN Settings			
Interface Type	Defines the IP behaviour of the port. Here one can change the behaviour • Local Mgmt (F), • Remote Mgmt Q). Note: The type “Daisy-Chain” and “Agent-Comm” can not be selected by customer, but comes with the factory configuration of the device!	Display	Local Mgmt (F)
Management VLAN Setting	Displays the VLAN settings for management traffic on this port. The LOCAL port does not support any VLAN.	Display	None
IPv4 Settings			
IPv4 ICMP Support	Indicates, whether ICMP for IPv4 is supported or not.	PullDown Menu • Enabled • Disabled	Enabled

Table 1-30 LOCAL Port Configuration (continued)

Parameter	Description	Format	Default
IPv4 Address Assignment	Defines the IP-address assignment. The Pulldown menu offers different entries, depending on the selected Interface type. • The LOCAL port is always F-interface.	PullDown-Menu • Manual [ii] • Provide DHCP Server	Provide DHCP Server
IPv4 Address	The IPv4 address of the LOCAL management port.	Display	192.168.1.100
IPv4 Network Mask	Configuration of the port’s IP-network mask. If the “IP Address Assignment” is “From DHCP Server”, the entry is read-only. As long as no assignment is carried out, the value presented is “Unassigned”	Display	255.255.255.0
Commit Group “New IPv4 Address”			
New IPv4 Address	New IPv4-address for the local port.	Input	*empty*
New IPv4 Netmask	New IPv4-netmask for the local port.	Input	*empty*
New IPv4 Default Gateway	New IPv4-default gateway for the local port.	Input	*empty*
Change IPv4 Address	Button to accept all the above new entries. This makes ALL the changes active at the same time. After pressing the button, the changes/new entries have to be confirmed. Note: Contact lost may happen after pressing this apply button.	Select Button/Confirm	
IPv6 Settings			
IPv6 Support	Selects whether IPv6 is supported on this interface.	PullDown Menu • Enabled • Disabled	Disabled

Table 1-30 LOCAL Port Configuration (continued)

Parameter	Description	Format	Default
IPv6 Router Advertisements	This variable allows to control whether the interface listens for IPv6 router advertisement messages for an automatic router detection. If this variable is set to “Ignoring”, the interface will ignore those messages and not detect IPv6 routers automatically. If this variable is set to “Listening”, the interface will listen to router advertisements.	PullDown Menu • Listening • Ignoring	Listening
IPv6 Auto-configuration	This variable allows to control whether the interface should automatically configure IPv6 addresses for prefixes learned from IPv6 router advertisements. If this variable is set to “Disabled”, the interface will never configure IPv6 addresses automatically in response to router advertisement messages.	PullDown Menu • Enabled • Disabled	Enabled
IPv6 Gateway Auto-configuration	This variable allows to configure whether default gateways learned via router advertisements shall be used. If this variable is set to “Disabled”, default gateways advertised by IPv6 routers will be ignored. If this variable is set to “Enabled”, default gateways advertised by IPv6 routers will be used.	PullDown Menu • Enabled • Disabled	Enabled

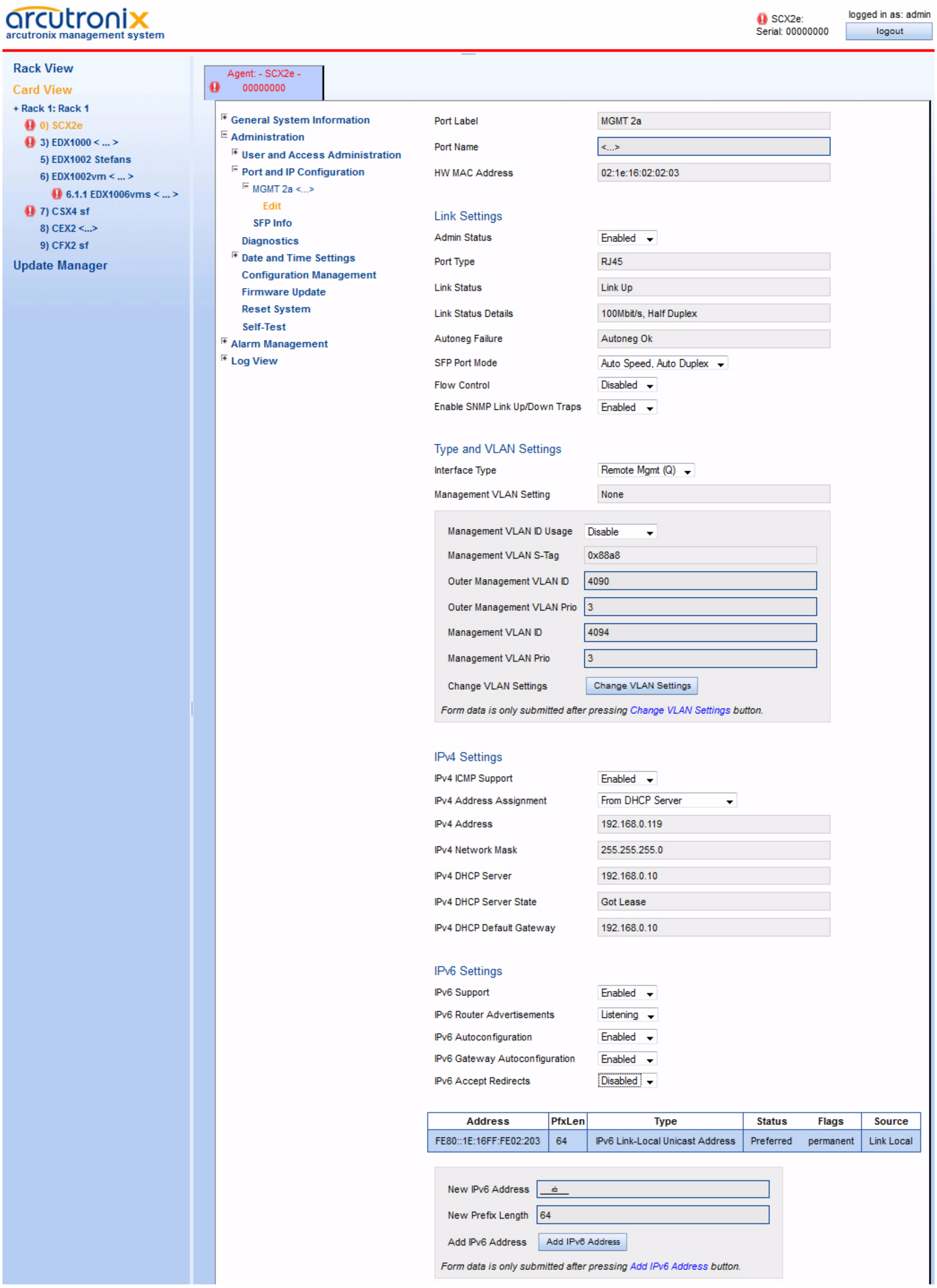
Table 1-30 LOCAL Port Configuration (continued)

Parameter	Description	Format	Default
IPv6 Accept Redirects	This variable allows to configure whether redirect messages sent from IPv6 routers shall be ignored. Redirect messages are sent by routers to inform IPv6 hosts about better routes to a destination, but it may improve network security to ignore those messages.	PullDown Menu • Enabled • Disabled	Disabled
Commit Group “New IPv6 Address”			
New IPv6 Address	New IPv6-address for the local port.	Input	*empty*
New IPv6 Prefix Length	New IPv6 prefix length for the local port.	Input	*empty*
New IPv4 Default Gateway	New IPv4-default gateway for the local port.	Input	*empty*
Add IPv6 Address	Button to accept all the above new entries. This makes ALL the changes active at the same time. After pressing the button, the changes/new entries have to be confirmed. Note: Contact lost may happen after pressing this apply button.	Select Button/Confirm	

i. See “Settings Auto-Negotiation” in [axManualSCX2e] for explanation on the settings.

ii. “Manual” means, that there is no DHCP-server provided. The client’s IP-address (PC) has to be configured manually.

REMOTE MGMT Port



Port Label	MGMT 2a
Port Name	<...>
HW MAC Address	02:1e:16:02:02:03

Link Settings

Admin Status	Enabled
Port Type	RJ45
Link Status	Link Up
Link Status Details	100Mbit/s, Half Duplex
Autoneg Failure	Autoneg Ok
SFP Port Mode	Auto Speed, Auto Duplex
Flow Control	Disabled
Enable SNMP Link Up/Down Traps	Enabled

Type and VLAN Settings

Interface Type	Remote Mgmt (Q)
Management VLAN Setting	None
Management VLAN ID Usage	Disable
Management VLAN S-Tag	0x88a8
Outer Management VLAN ID	4090
Outer Management VLAN Prio	3
Management VLAN ID	4094
Management VLAN Prio	3
Change VLAN Settings	Change VLAN Settings

Form data is only submitted after pressing Change VLAN Settings button.

IPv4 Settings

IPv4 ICMP Support	Enabled
IPv4 Address Assignment	From DHCP Server
IPv4 Address	192.168.0.119
IPv4 Network Mask	255.255.255.0
IPv4 DHCP Server	192.168.0.10
IPv4 DHCP Server State	Got Lease
IPv4 DHCP Default Gateway	192.168.0.10

IPv6 Settings

IPv6 Support	Enabled
IPv6 Router Advertisements	Listening
IPv6 Autoconfiguration	Enabled
IPv6 Gateway Autoconfiguration	Enabled
IPv6 Accept Redirects	Disabled

Address	PfxLen	Type	Status	Flags	Source
FE80::1E:16FF:FE02:203	64	IPv6 Link-Local Unicast Address	Preferred	permanent	Link Local

New IPv6 Address	
New Prefix Length	64
Add IPv6 Address	Add IPv6 Address

Form data is only submitted after pressing Add IPv6 Address button.

Figure 1-28 *Edit REMOTE Port Settings*

Table 1-31 provide information about the options.

Table 1-31 *REMOTE Port Configuration*

Parameter	Description	Format	Default
Port Label	Printed text on the enclosure and front-plate.	Display	
Port Name	Name for this port. It can be free advised by user.	String	<...>
HW MAC Address	Displays the MAC address of the remote management port.	Display	*00:1E:16:aa:bb:cc*
Link Settings:			
Admin Status	Indicator, whether the port shall be enabled or not.	PullDown Menu • Enabled • Disabled	Enabled
Active Interface	Indicates, whether the combo-port is in copper or fibre mode. Either “RJ45” (=copper) or “SFP” (=fibre).	Display	
Port Type	Show the port's mechanical type and usage.	Display	
Link Status	Indicates, whether the port is up, down or disabled.	Display	
Link Status Details	Indicates the link status in more details.	Display	
Autoneg Failure	Indicates a failure in the auto-negotiation process between the port and its peer. Note: Keep in mind for Copper I/F the auto-neg procedure is very important in case SyncE is enabled.	Display	
SFP Port Mode	Autonegotiation settings for the SFP (fibre) part of the combo-port. [i]. To disable the fibre option of the combo-port, select “do-not-use” here. In this case, the FO link can never be established.	PullDown Menu • do-not-use • Auto Speed, Auto Duplex • ...	Auto Speed, Auto Duplex

Table 1-31 REMOTE Port Configuration (continued)

Parameter	Description	Format	Default
Copper Port Mode	Autonegotiation settings for the copper part of the combo-port. [i] To disable the copper option of the combo-port, select “do-not-use” here. In this case, the UTP-link can never be established.	PullDown Menu • do-not-use • Auto Speed, Auto Duplex • ...	Auto Speed, Auto Duplex
Flow Control	IEEE 802.3x (PAUSE frames) can be enabled or disabled.	PullDown Menu • Enabled • Disabled	Disabled
Enable SNMP Link Up/Down Traps	Enables or disables a SNMP trap, if the link for this ports is changing its status to up or down.	PullDown Menu • Enabled • Disabled	Enabled
Type and VLAN Settings			
Interface Type	Defines the IP behaviour of the port. Here one can change the behaviour • Local Mgmt (F), • Remote Mgmt Q). Note: The type “Daisy-Chain” and “Agent-Comm” can not be selected by customer, but comes with the factory configuration of the device!	Display	Remote Mgmt (Q)
Management VLAN Setting	Displays the VLAN settings for management traffic on this port.	Display	None
Commit Group “Change VLAN Setting”			
Management VLAN ID Usage	The VLAN tagging mode for the NORTH interface.	PullDown Menu • Single Tag • Double Tag • Disabled	Disabled
Management VLAN S-Tag	Enter the value of the management VLAN S-tag here.	Input	*0x88a8*

Table 1-31 *REMOTE Port Configuration (continued)*

Parameter	Description	Format	Default
Outer Management VLAN ID	Enter the value of the outer management VLAN ID here.	Input	*4090*
Outer Management VLAN Prio	Enter the priority field of the outer management VLAN tag here	Input	*3*
Management VLAN ID	Enter the value of the (inner) management VLAN ID here.	Input	*4094*
Management VLAN Prio	Enter the priority field of the (inner) management VLAN tag here	Input	*3*
Change VLAN Settings	Button to accept all the above new entries. This makes ALL the changes active at the same time. After pressing the button, the changes/new entries have to be confirmed. Note: Contact lost may happen after pressing this apply button.	Select Button/Confirm	
IPv4 Settings			
IPv4 ICMP Support	Indicates, whether ICMP for IPv4 is supported or not.	PullDown Menu • Enabled • Disabled	Enabled
IPv4 Address Assignment	Defines the IP-address assignment. The Pulldown menu offers different entries, depending on the selected Interface type. • The LOCAL port is always F-interface.	PullDown-Menu • Manual [ii] • Provide DHCP Server	Provide DHCP Server
IPv4 Address	The IPv4 address of the LOCAL management port.	Display	192.168.1.100

Table 1-31 *REMOTE Port Configuration (continued)*

Parameter	Description	Format	Default
IPv4 Network Mask	Configuration of the port's IP-network mask. If the "IP Address Assignment" is "From DHCP Server", the entry is read-only. As long as no assignment is carried out, the value presented is "Unassigned"	Display	255.255.255.0
IPv4 DHCP Server	When a network address has been received via DHCP, this variable shows the DHCP server that has answered the DHCP request.	Display	
IPv4 DHCP Server State	When DHCP is enabled, this variable shows the current state of communication with the DHCP server.	Display	searching
IPv4 DHCP Default Gateway	When DHCP is enabled, this variable shows the default gateway that was suggested by the DHCP server. If no gateway address was supplied by the DHCP server, the variable is empty.	Display	empty
Commit Group "New IPv4 Address"			
New IPv4 Address	New IPv4-address for the local port.	Input	*empty*
New IPv4 Netmask	New IPv4-netmask for the local port.	Input	*empty*
New IPv4 Default Gateway	New IPv4-default gateway for the local port.	Input	*empty*
Change IPv4 Address	Button to accept all the above new entries. This makes ALL the changes active at the same time. After pressing the button, the changes/new entries have to be confirmed. Note: Contact lost may happen after pressing this apply button.	Select Button/Confirm	

Table 1-31 *REMOTE Port Configuration (continued)*

Parameter	Description	Format	Default
IPv6 Settings			
IPv6 Support	Selects whether IPv6 is supported on this interface.	PullDown Menu • Enabled • Disabled	Disabled
IPv6 Router Advertisements	This variable allows to control whether the interface listens for IPv6 router advertisement messages for an automatic router detection. If this variable is set to “Ignoring”, the interface will ignore those messages and not detect IPv6 routers automatically. If this variable is set to “Listening”, the interface will listen to router advertisements.	PullDown Menu • Listening • Ignoring	Listening
IPv6 Auto-configuration	This variable allows to control whether the interface should automatically configure IPv6 addresses for prefixes learned from IPv6 router advertisements. If this variable is set to “Disabled”, the interface will never configure IPv6 addresses automatically in response to router advertisement messages.	PullDown Menu • Enabled • Disabled	Enabled
IPv6 Gateway Auto-configuration	This variable allows to configure whether default gateways learned via router advertisements shall be used. If this variable is set to “Disabled”, default gateways advertised by IPv6 routers will be ignored. If this variable is set to “Enabled”, default gateways advertised by IPv6 routers will be used.	PullDown Menu • Enabled • Disabled	Enabled

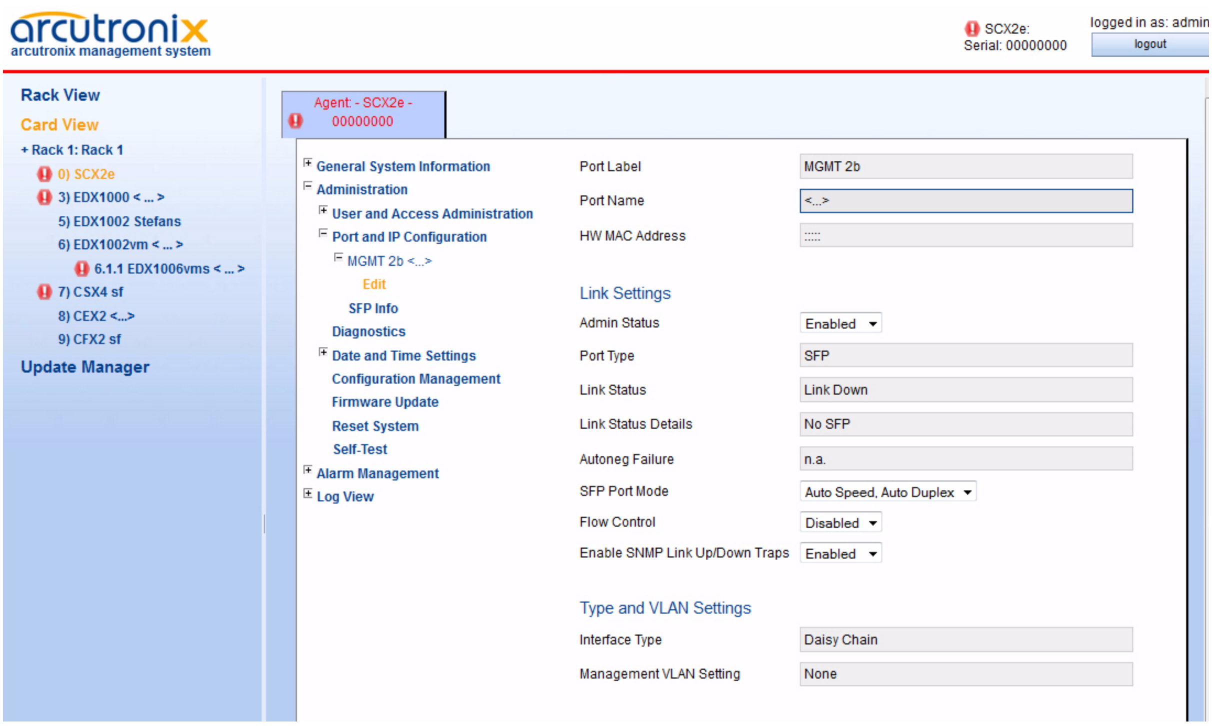
Table 1-31 REMOTE Port Configuration (continued)

Parameter	Description	Format	Default
IPv6 Accept Redirects	This variable allows to configure whether redirect messages sent from IPv6 routers shall be ignored. Redirect messages are sent by routers to inform IPv6 hosts about better routes to a destination, but it may improve network security to ignore those messages.	PullDown Menu • Enabled • Disabled	Disabled
Commit Group “New IPv6 Address”			
New IPv6 Address	New IPv6-address for the local port.	Input	*empty*
New IPv6 Prefix Length	New IPv6 prefix length for the local port.	Input	*empty*
New IPv4 Default Gateway	New IPv4-default gateway for the local port.	Input	*empty*
Add IPv6 Address	Button to accept all the above new entries. This makes ALL the changes active at the same time. After pressing the button, the changes/new entries have to be confirmed. Note: Contact lost may happen after pressing this apply button.	Select Button/Confirm	

i. See “Settings Auto-Negotiation” in [axManualSCX2e] for explanation on the settings.
ii. “Manual” means, that there is no DHCP-server provided. The client’s IP-address (PC) has to be configured manually.

Daisy-Chain MGMT Port

NOTE: The type “Daisy-Chain” can not be selected by customer, but comes with the factory configuration of the device!



Port Label: MGMT 2b
Port Name: <...>
HW MAC Address: :::::

Link Settings
Admin Status: Enabled
Port Type: SFP
Link Status: Link Down
Link Status Details: No SFP
Autoneg Failure: n.a.
SFP Port Mode: Auto Speed, Auto Duplex
Flow Control: Disabled
Enable SNMP Link Up/Down Traps: Enabled

Type and VLAN Settings
Interface Type: Daisy Chain
Management VLAN Setting: None

***Figure 1-29** Edit DAISY-CHAIN Port Settings*

Table 1-32 provide information about the options.

***Table 1-32** DAISY-CHAIN Port Configuration*

Parameter	Description	Format	Default
Port Label	Printed text on the enclosure and front-plate.	Display	
Port Name	Name for this port. It can be free advised by user.	String	<...>
HW MAC Address	A Daisy-Chain port is a forwarding port only. It does not carry an own MAC address.	Display	:::::
Link Settings:			
Admin Status	Indicator, whether the port shall be enabled or not.	PullDown Menu • Enabled • Disabled	Enabled
Active Interface	Indicates, whether the combo-port is in copper or fibre mode. Either “RJ45” (=copper) or “SFP” (=fibre).	Display	

Table 1-32 DAISY-CHAIN Port Configuration (continued)

Parameter	Description	Format	Default
Port Type	Show the port's mechanical type and usage.	Display	
Link Status	Indicates, whether the port is up, down or disabled.	Display	
Link Status Details	Indicates the link status in more details.	Display	
Autoneg Failure	Indicates a failure in the auto-negotiation process between the port and its peer. Note: Keep in mind for Copper I/F the auto-neg procedure is very important in case SyncE is enabled.	Display	
SFP Port Mode	Autonegotiation settings for the SFP (fibre) part of the combo-port. [i]. To disable the fibre option of the combo-port, select “do-not-use” here. In this case, the FO link can never be established.	PullDown Menu • do-not-use • Auto Speed, Auto Duplex • ...	Auto Speed, Auto Duplex
Copper Port Mode	Autonegotiation settings for the copper part of the combo-port. [i] To disable the copper option of the combo-port, select “do-not-use” here. In this case, the UTP-link can never be established.	PullDown Menu • do-not-use • Auto Speed, Auto Duplex • ...	Auto Speed, Auto Duplex
Flow Control	IEEE 802.3x (PAUSE frames) can be enabled or disabled.	PullDown Menu • Enabled • Disabled	Disabled
Enable SNMP Link Up/Down Traps	Enables or disables a SNMP trap, if the link for this ports is changing its status to up or down.	PullDown Menu • Enabled • Disabled	Enabled
Type and VLAN Settings			

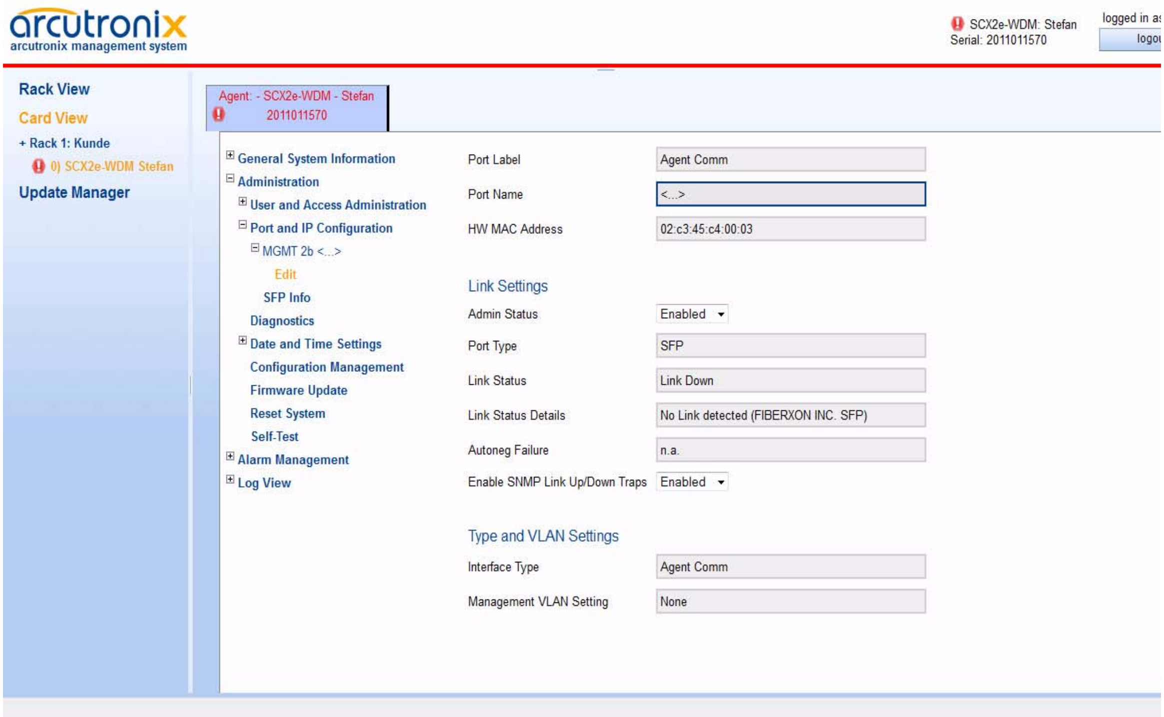
Table 1-32 DAISY-CHAIN Port Configuration (continued)

Parameter	Description	Format	Default
Interface Type	Defines the IP behaviour of the port. Here one can change the behaviour • Daisy Chain. Note: The type “Daisy-Chain” and “Agent-Comm” can not be selected by customer, but comes with the factory configuration of the device!	Display	Daisy Chain
Management VLAN Setting	Displays the VLAN settings for management traffic on this port.	Display	None

i. See “Settings Auto-Negotiation” in [axManualSCX2e] for explanation on the settings.

Agent-Comm Port

NOTE: The type “Agent-Comm” can not be selected by customer, but comes with the factory configuration of the device!



Port Label: Agent Comm
Port Name: <...>
HW MAC Address: 02:c3:45:c4:00:03

Link Settings

Admin Status: Enabled
Port Type: SFP
Link Status: Link Down
Link Status Details: No Link detected (FIBERXON INC. SFP)
Autoneg Failure: n.a.
Enable SNMP Link Up/Down Traps: Enabled

Type and VLAN Settings

Interface Type: Agent Comm
Management VLAN Setting: None

***Figure 1-30** Edit AGENT-COMM Port Settings*

Table 1-32 provide information about the options.

Table 1-33 *AGENT-COMM Port Configuration*

Parameter	Description	Format	Default
Port Label	Printed text on the enclosure and front-plate.	Display	
Port Name	Name for this port. It can be free advised by user.	String	<...>
HW MAC Address	Displays the MAC address of the remote management port.	Display	*00:1E:16:aa:bb:cc*
Link Settings:			
Admin Status	Indicator, whether the port shall be enabled or not.	PullDown Menu • Enabled • Disabled	Enabled
Active Interface	Indicates, whether the combo-port is in copper or fibre mode. Either “RJ45” (=copper) or “SFP” (=fibre).	Display	
Port Type	Show the port's mechanical type and usage.	Display	
Link Status	Indicates, whether the port is up, down or disabled.	Display	
Link Status Details	Indicates the link status in more details.	Display	
Autoneg Failure	Indicates a failure in the auto-negotiation process between the port and its peer. Note: Keep in mind for Copper I/F the auto-neg procedure is very important in case SyncE is enabled.	Display	
SFP Port Mode	Autonegotiation settings for the SFP (fibre) part of the combo-port. [i]. To disable the fibre option of the combo-port, select “do-not-use” here. In this case, the FO link can never be established.	PullDown Menu • do-not-use • Auto Speed, Auto Duplex • ...	Auto Speed, Auto Duplex

Table 1-33 AGENT-COMM Port Configuration (continued)

Parameter	Description	Format	Default
Copper Port Mode	Autonegotiation settings for the copper part of the combo-port. [i] To disable the copper option of the combo-port, select "do-not-use" here. In this case, the UTP-link can never be established.	PullDown Menu • do-not-use • Auto Speed, Auto Duplex • ...	Auto Speed, Auto Duplex
Flow Control	IEEE 802.3x (PAUSE frames) can be enabled or disabled.	PullDown Menu • Enabled • Disabled	Disabled
Enable SNMP Link Up/Down Traps	Enables or disables a SNMP trap, if the link for this ports is changing its status to up or down.	PullDown Menu • Enabled • Disabled	Enabled
Type and VLAN Settings			
Interface Type	Defines the IP behaviour of the port. Here one can change the behaviour • Daisy Chain. Note: The type "Daisy-Chain" and "Agent-Comm" can not be selected by customer, but comes with the factory configuration of the device!	Display	Daisy Chain
Management VLAN Setting	Displays the VLAN settings for management traffic on this port.	Display	None

[i] See "Settings Auto-Negotiation" in [axManualSCX2e] for explanation on the settings.

Diagnostics

The Diagnostics-menu 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 "Trace-route/ICMP". The result is given in the line below called "Command Output".

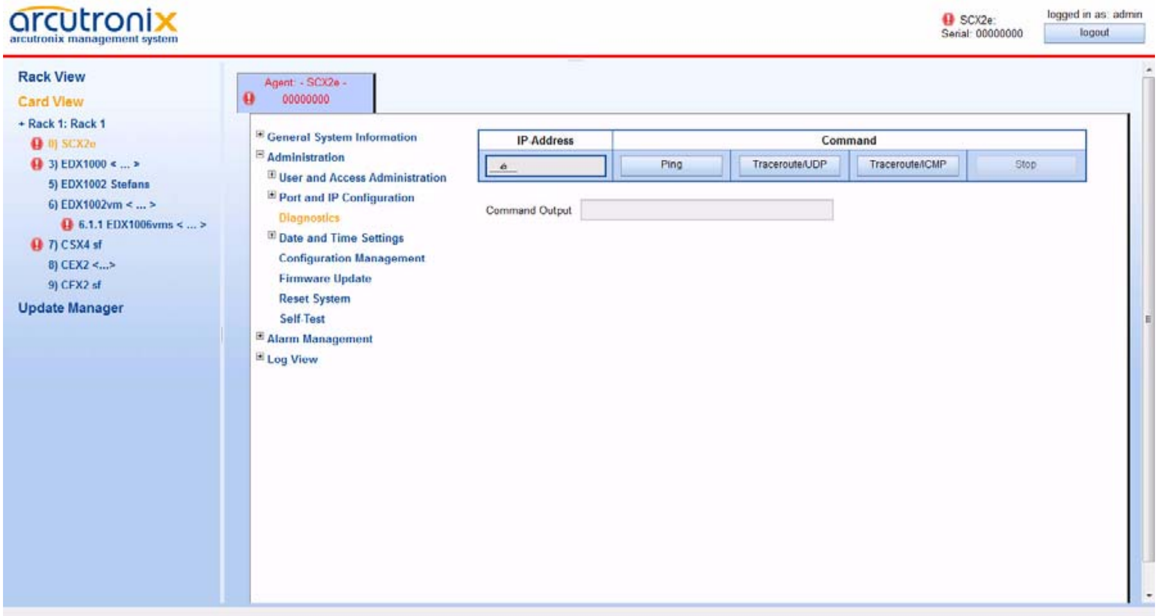


Figure 1-31 Diagnostics

Date and Time Settings

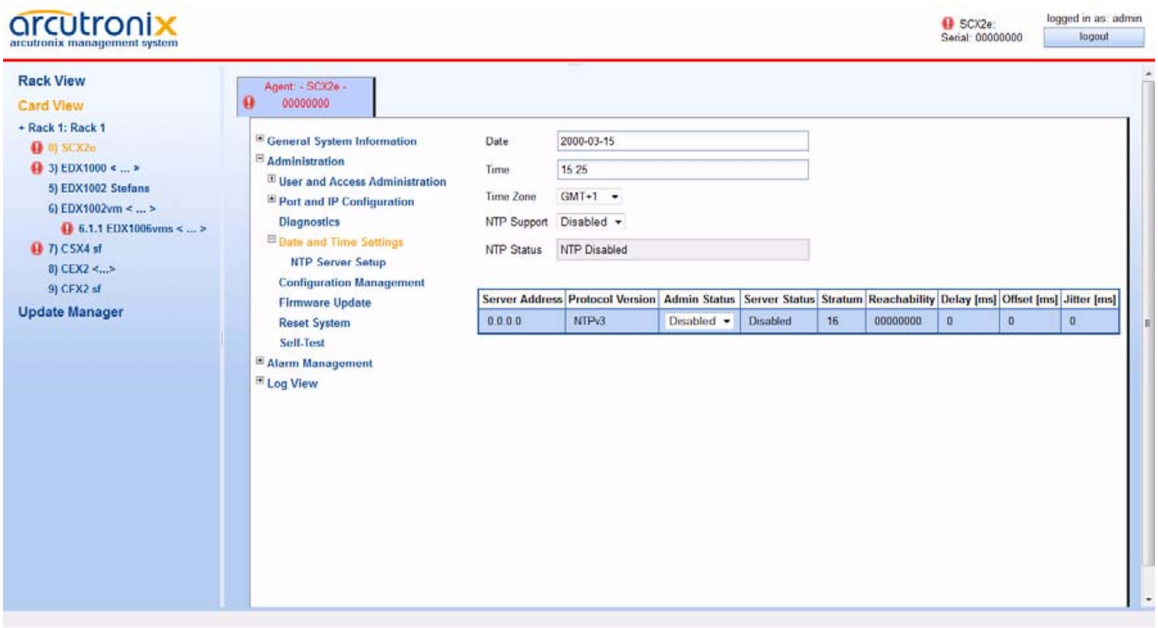
Use this menu to set the date, time, and time zone for the device. The date and time can be configured manually or via NTP [1].

For manual setting, the entry for the usage of NTP must be disabled. For automatic setting, several items have to be configured properly:

- the usage of NTP must be enabled,
- at least one NTP-server must be assigned,
- at least one of the configured NTP-server must be enabled.

The GUI shows the current time and date, along with the configured time-servers and the associated status.

[1] NTP = Network Time Protocol, [IETF RFC 1305], [IETF RFC 5905]



Date: 2000-03-15

Time: 15:25

Time Zone: GMT+1

NTP Support: Disabled

NTP Status: NTP Disabled

Server Address	Protocol Version	Admin Status	Server Status	Stratum	Reachability	Delay [ms]	Offset [ms]	Jitter [ms]
0.0.0.0	NTPv3	Disabled	Disabled	16	00000000	0	0	0

***Figure 1-32** Date And Time Settings*

Table 1-34 provides information about the options.

***Table 1-34** Date and Time Settings*

Parameter	Description	Format	Default
Date	Indicates the current device's date (dd-MM-yyyy). Note: Only when NTP Support is disabled, the date can be set manually.	Display/Input	no default
Time	Indicates the current device's time (hh:mm:ss). Note: Only when NTP Support is disabled, the time can be set manually.	Display/Input	no default

Table 1-34 Date and Time Settings (continued)

Parameter	Description	Format	Default
Time Zone	Indicates the relative time deviation to GMT [i], e.g. 'GMT+1' for Berlin.	PullDown Menu • GMT-12 • ... • GMT+14	GMT+1
NTP Support	Enable and disable for the NTP-stack. Note: Only when NTP Support is disabled, the date and time can be set manually.	PullDown Menu • Enabled • Disabled	Disabled

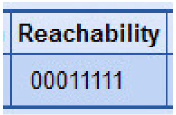
[i] GMT (Greenwich Mean Time) is synonymous with UTC (Universal Time Coordinated).

A list of all configured NTP-servers and the actual status is presented below:

Table 1-35 NTP Server Status

Parameter	Description	Format
Server Address	The IP-address of the NTP-server.	Display
Protocol Version	The used version of NTP to communicate with the server.	Display
Admin Status	Indicator, whether the server shall be used for time synchronization. Possible values are: • Enabled: May be used as reference clock. • Disabled: Never used as reference clock.	PullDown Menu • Enabled • Disabled
Server Status	The actual (communication) status between SCX2e and the server. Possible values are: • Not Used: NTP server not selected. • Bad Quality: NTP server has insufficient clock quality. • Bad DateTime: NTP server has incorrect date/time. • Usable: NTP server can be used as reference clock. • Selected: NTP server has been selected as reference clock. • Disabled: NTP server has been disabled in the configuration.	Display
Stratum	This variable shows the stratum of the selected NTP server. The stratum is a measure of how far away the NTP server is from an ideal and accurate time source.	Display

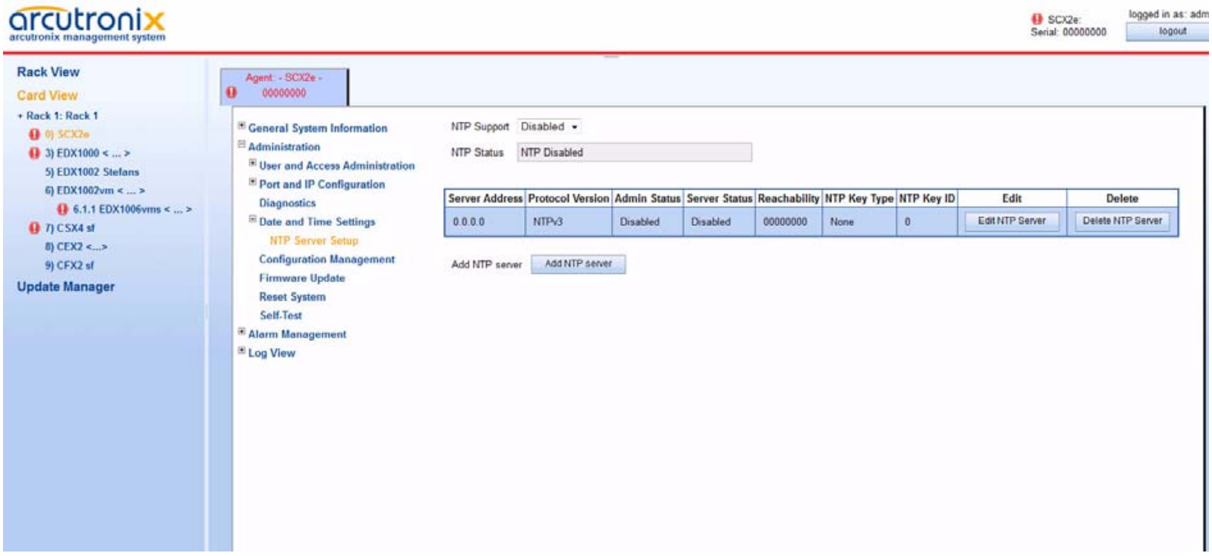
Table 1-35 NTP Server Status (continued)

Parameter	Description	Format
Reachability	This variable represents the NTP reachability register. This register is an eight bit shift register that contains the status of the last NTP transactions with the NTP server. A value of ’0’ in this bit-field indicates that a NTP transaction has failed. Possible reasons are: • network communication has failed • NTP server is not synchronous to its time source. A value of ’1’ indicates a successful transaction. New values are inserted from the right-hand side and move left with every new NTP transaction until they are pushed out at the left-hand side.  Reachability 00011111 In example on the right, one see the 5 last attempts to communicate with the server have been successful, while the 3 attempts before did fail.	Display
Delay [ms]	This variable shows the current network round-trip time of NTP packets in milliseconds.	Display
Offset [ms]	This variable shows the current time difference between the selected NTP server and the local system clock in milliseconds.	Display
Jitter [ms]	This variable shows the amount of fluctuations between subsequent NTP date-time transactions in milliseconds.	Display

To add, remove and edit the NTP-servers please select “NTP Server Setup”.

NTP Server Setup

This menu allows to manage NTP servers accessible to the device. Up to eight individual NTP servers can be configured here, identified by their IP address. A table lists all the available entries Each table row summarizes the NTP server configuration, allows to delete the server entry and gives access to a submenu allowing to modify the NTP server configuration in full detail.



NTP Support: Disabled

NTP Status: NTP Disabled

Server Address	Protocol Version	Admin Status	Server Status	Reachability	NTP Key Type	NTP Key ID	Edit	Delete
0.0.0.0	NTPv3	Disabled	Disabled	00000000	None	0	Edit NTP Server	Delete NTP Server

Add NTP server: Add NTP server

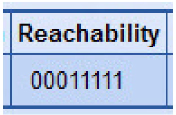
Figure 1-33 *NTP Server Setup*

Table 1-36 provides information about the options.

Table 1-36 *NTP Server Setup*

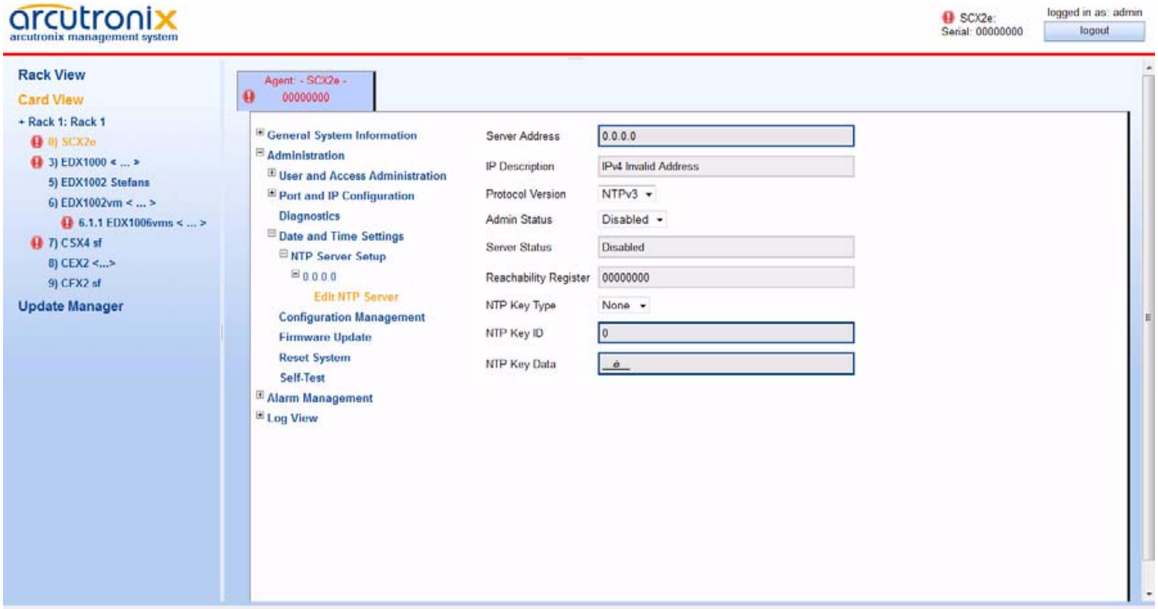
Parameter	Description	Format
Server Address	The IP-address of the NTP-server.	Display
Protocol Version	The used version of NTP to communicate with the server.	Display
Admin Status	Indicator, whether the server shall be used for time synchronization. Possible values are: • Enabled: May be used as reference clock. • Disabled: Never used as reference clock.	Display
Server Status	The actual (communication) status between SCX2e and the server. Possible values are: • Not Used: NTP server not selected. • Bad Quality: NTP server has insufficient clock quality. • Bad DateTime: NTP server has incorrect date/time. • Usable: NTP server can be used as reference clock. • Selected: NTP server has been selected as reference clock. • Disabled: NTP server has been disabled in the configuration.	Display

Table 1-36 NTP Server Setup (continued)

Parameter	Description	Format
Reachability	This variable represents the NTP reachability register. This register is an eight bit shift register that contains the status of the last NTP transactions with the NTP server. A value of '0' in this bit-field indicates that a NTP transaction has failed. Possible reasons are: • network communication has failed • NTP server is not synchronous to its time source. A value of '1' indicates a successful transaction. New values are inserted from the right-hand side and move left with every new NTP transaction until they are pushed out at the left-hand side.  Reachability 00011111 In example on the right, one see the 5 last attempts to communicate with the server have been successful, while the 3 attempts before did fail.	Display
NTP Key Type	This variable allows to configure an NTP server authentication key type for communication with the NTP server. If NTP server authentication is enabled, suitable values for Key ID and Key Data must also be supplied.	Display
NTP Key ID	This variable allows to select a NTP server authentication Key ID. The key information (Key Type, Key ID and Key Data) must be the same on the NTP server and the NTP client (NTP messages include the Key ID along with the message digest).	Display

Edit NTP Server

This menu allows to configure all NTP server properties in full detail. Beside the NTP server's IP address and protocol version, it allows to select whether the NTP server shall be used by NTP's reference clock selection algorithm and whether to use MD5 or SHA1 based NTP server security.



Server Address: 0.0.0.0
IP Description: IPv4 Invalid Address
Protocol Version: NTPv3
Admin Status: Disabled
Server Status: Disabled
Reachability Register: 00000000
NTP Key Type: None
NTP Key ID: 0
NTP Key Data:

Figure 1-34 *Edit NTP Server*

Table 1-37 provides information about the options.

Table 1-37 *Edit NTP Server*

Parameter	**Description**	**Format**	**Default**
Server Address	The IP-address of the NTP-server.	IPv4-Address IPv6-Address	0.0.0.0
Protocol Version	The used version of NTP to communicate with the server.	PullDown Menu • NTPv3 • NTPv4	NTPv3
Admin Status	This variable allows to configure whether the server is to be used for time synchronization. When set to “Enabled”, the server may be selected as reference clock for the device, depending on the quality of the time server.	PullDown Menu • Enabled • Disabled	Enabled

Table 1-37 *Edit NTP Server (continued)*

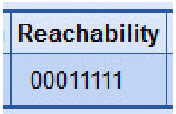
Parameter	Description	Format	Default
Reachability	This variable represents the NTP reachability register. This register is an eight bit shift register that contains the status of the last NTP transactions with the NTP server. A value of ’0’ in this bit-field indicates that a NTP transaction has failed. Possible reasons are: • network communication has failed • NTP server is not synchronous to its time source. A value of ’1’ indicates a successful transaction. New values are inserted from the right-hand side and move left with every new NTP transaction until they are pushed out at the left-hand side.  Reachability 00011111 In example on the right, one see the 5 last attempts to communicate with the server have been successful, while the 3 attempts before did fail.	Display	00000000
NTP Key Type	This variable allows to configure an NTP server authentication key type for communication with the NTP server. If NTP server authentication is enabled, suitable values for Key ID and Key Data must also be supplied.	PullDown Menu • None • MD5 • SHA1	None

Table 1-37 *Edit NTP Server (continued)*

Parameter	Description	Format	Default
NTP Key ID	This variable allows to select a NTP server authentication Key ID. The key information (Key Type, Key ID and Key Data) must be the same on the NTP server and the NTP client (NTP messages include the Key ID along with the message digest).	Input	0
NTP Key Data	This variable allows to set the NTP key data for the NTP Key ID assigned to this server. Please note that the Key Data associated with a certain Key ID must be unique, e.g. it is impossible assign different key data to the same Key ID. The key data can be specified in two different formats: • ASCII string, 1..20 printable characters excluding "#" and white space • HEX string, 40 characters This corresponds to a key length of 160 bits. Note: In order to change the Key Data for a NTP server it is required to first disable NTP authentication by setting "NTP Key Type" to "None".	Input	empty

Configuration Management

Use this menu to store and recall different configurations. The actual configuration ("Current Configuration") can be stored at any time and later recalled to switch between different settings. Also the Factory Default Configuration 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 safe 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.

Three different protocols are supported to load and store configuration files to and from the SCX2e:

- Download from Server via File-Transfer-Protocols
  - SFTP - SSH File Transfer Protocol as used for SSH-connections,
  - TFTP - Trivial File Transfer Protocol as used for IP-connections.
- Upload from (web-)client
  - HTTP - Hyper Text Transfer Protocol as used for Web-Pages. (Only available for web-sessions.)

SFTP file transfer gives most 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.

Trivial File Transfer Protocol, more commonly referred to as TFTP is a very basic and more traditional method used transferring 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 source at little to no cost, providing you with the extra funds needed to adapt the system to suit your requirements.

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 when no FTP clients are required, all your customer needs is access to a web browser and they are able to send large files.

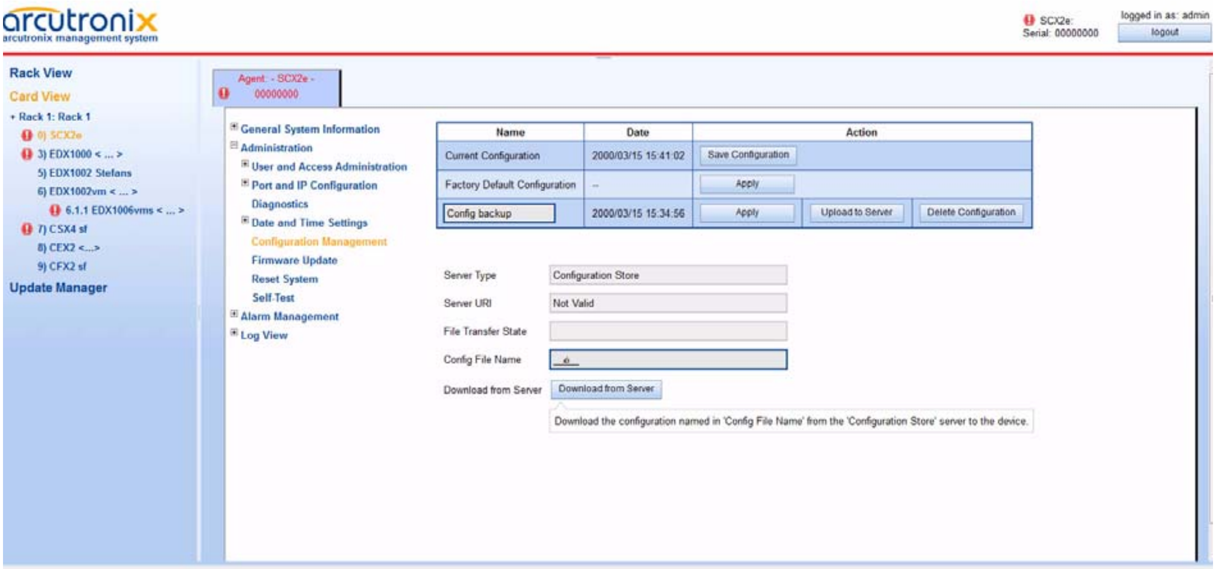
Note: The usage of HTTP file transfer can be disabled in the “User and Access Administration”-menu.

Note: If the access to the device is others then Web-GUI, the http option is not available, too!

For the server-based download via SFTP or TFTP the so-called “Configuration Store”-server is used (see “Users and Passwords” on page 1-23). The “Configuration Store” has to be configured properly to make use of it. During the configuration of the “Configuration Store”, one can select, whether SFTP or TFTP is used for communication.

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 menu of the configuration-management changes, depending of the setting “HTTP File Transfer” (see “User and Access Administration” on page 1-18). If http file-transfer is disabled, only the download option are presented (see “Firmware Update w/o http-option”), otherwise the upload option via http are visible, too (see “Firmware Update with http-option”).



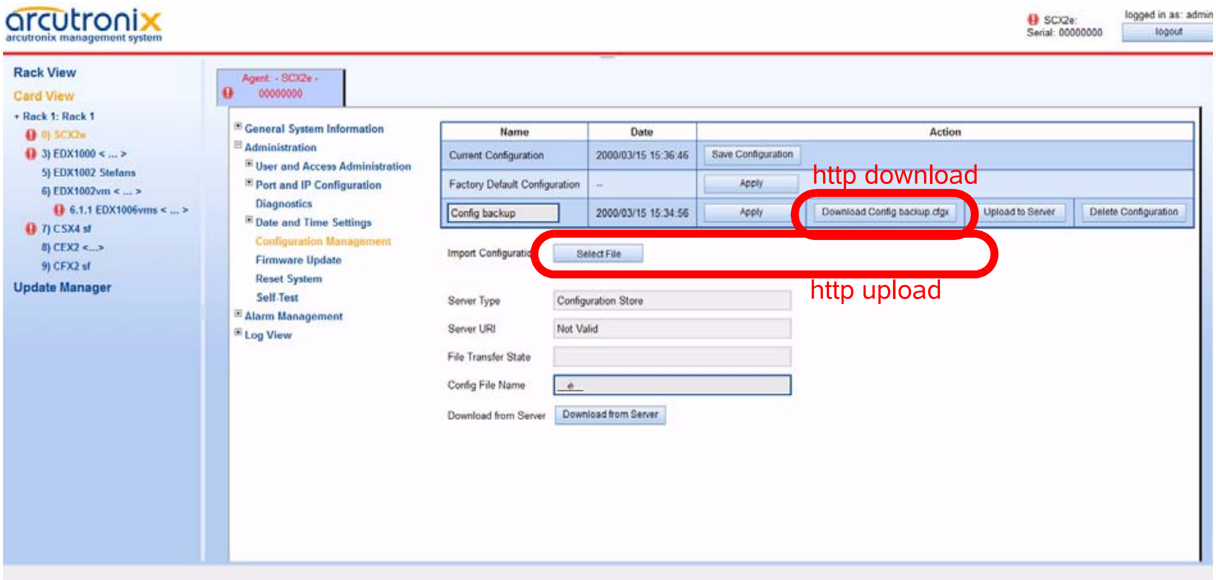
Name	Date	Action		
Current Configuration	2000/03/15 15:41:02	Save Configuration		
Factory Default Configuration	--	Apply		
Config backup	2000/03/15 15:34:56	Apply	Upload to Server	Delete Configuration

Server Type: Configuration Store
Server URI: Not Valid
File Transfer State:
Config File Name: _e_
Download from Server: Download from Server

Download the configuration named in 'Config File Name' from the 'Configuration Store' server to the device.

Figure 1-35 Configuration Management

The above picture shows the Configuration Management menu when http file transfer is disabled, while below the menu is presented, when http file transfer is enabled.



Name	Date	Action			
Current Configuration	2000/03/15 15:36:46	Save Configuration			
Factory Default Configuration	--	Apply			
Config backup	2000/03/15 15:34:56	Apply	Download Config backup.cfgx	Upload to Server	Delete Configuration

Import Configuratio: Select File

Server Type: Configuration Store
Server URI: Not Valid
File Transfer State:
Config File Name: _e_
Download from Server: Download from Server

Figure 1-36 Configuration Management with http-option

Table 1-38 provides information about the options.

Table 1-38 *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 [i]	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
Upload to Server	Upload the configuration called "xxx" via SFTP or TFTP to the "Configuration Store". 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 [i]	Select File button to open browsers window to file explorer, when http-file transfer is enabled.	Action
Start Upload [i]	To start the http file transfer.	Action
Server Type	Indicate the server, which is used for S/TFTP file transfer. Always "Configuration Store"	Display
Server URI	The configuration of Configuration Store. Here one can see, whether SFTP or TFTP is selected, the IP-address etc. URI = Uniform Resource Identifier	Display
File Transfer State	Shows information about a file transfer to/from the configuration server.	Display

Table 1-38 Configuration Management (continued)

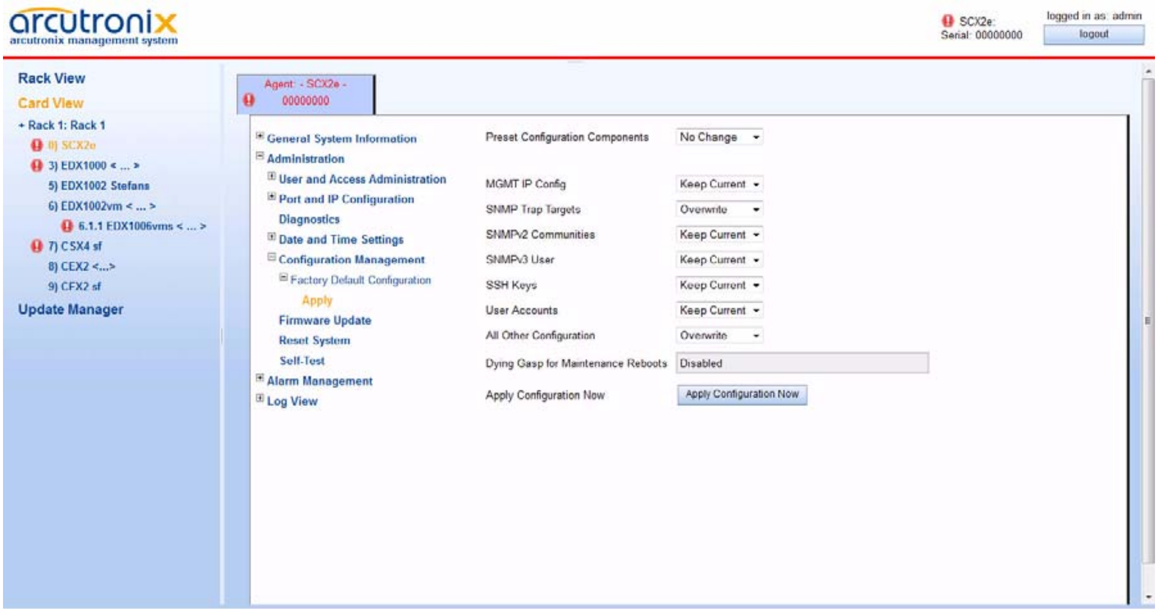
Parameter	Description	Format
Config File Name	Filename on the server. The (root-) path on the server is stored in the settings for Configuration Server. Format: *.cfgx	Input
Download from Server	Download the named configuration from the configuration server to the device.	Action

i. Only visible, in Web-GUI and when http-file-transfer is enabled!

Recall Configuration Options (“Apply”)

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

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.



Preset Configuration Components	No Change
MGMT IP Config	Keep Current
SNMP Trap Targets	Overwrite
SNMPv2 Communities	Keep Current
SNMPv3 User	Keep Current
SSH Keys	Keep Current
User Accounts	Keep Current
All Other Configuration	Overwrite
Dying Gasp for Maintenance Reboots	Disabled
Apply Configuration Now	Apply Configuration Now

Figure 1-37 Recall Configuration

Table 1-39 provides information about the options.

Table 1-39 *Recall Configuration*

Parameter	Description	Format	Default
Preset Configuration Components	All settings can be configured in one-step.	PullDown-Menu • No Change • Overwrite • Keep Current	No Change
MGMT IP Config	The IP- (and VLAN-) settings for out-of-band and in-band management.	PullDown-Menu • Overwrite • Keep Current	Keep Current
SNMP Trap Targets	The IP settings for SNMP-trap receivers.	PullDown-Menu • Overwrite • Keep Current	Overwrite
SNMPv2 Communities		PullDown-Menu • Overwrite • Keep Current	Overwrite
SNMPv3 Users		PullDown-Menu • Overwrite • Keep Current	Overwrite
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
Dying Gasp for Maintenance Reboots	Information field to show, whether the device is configured to raise a Dying-Gasp alarm, when the configuration is updated and the (maintenance-) reboot is invoked	Display	Disabled
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

Firmware Update

Upload (http) and Download (xFTP) of new FW

Use this menu to update the firmware of the SCX2e. The protocol, update-file-name and the update-time must be specified. The update itself is done in two steps:

1. Load the update file to the device (Upload or download process). A firmware update-file does always use the extension *.upx and carries some internal check-words to make sure that no illegal firmware can be installed on the unit.
2. Update the device with the new firmware. The update process stores the file into the flash and will start an automatic reset after finishing the flash-process. The time, which can be specified in this menu, is the update time, not the moment of loading the new firmware.

Note: After successful installation of the new FW, the SCX2e will reboot to finish the update process. After the reboot reconnecting to the unit is necessary.

Three different protocols are supported to update the SCX2e Firmware:

- Download from Server via File-Transfer-Protocols
  - SFTP - SSH File Transfer Protocol as used for SSH-connections.
  - TFTP - Trivial File Transfer Protocol as used for IP-connections.
- Upload from (web-)client
  - HTTP - Hyper Text Transfer Protocol as used for Web-Pages,

SFTP file transfer gives most 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.

Trivial File Transfer Protocol, more commonly referred to as TFTP is a very basic and more traditional method used transferring 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 source at little to no cost, providing you with the extra funds needed to adapt the system to suit your requirements.

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.

Note: The usage of HTTP file transfer can be disabled in the “User and Access Administration”-menu.

Note: If the access to the device is others then Web-GUI, the http option is not available, too!

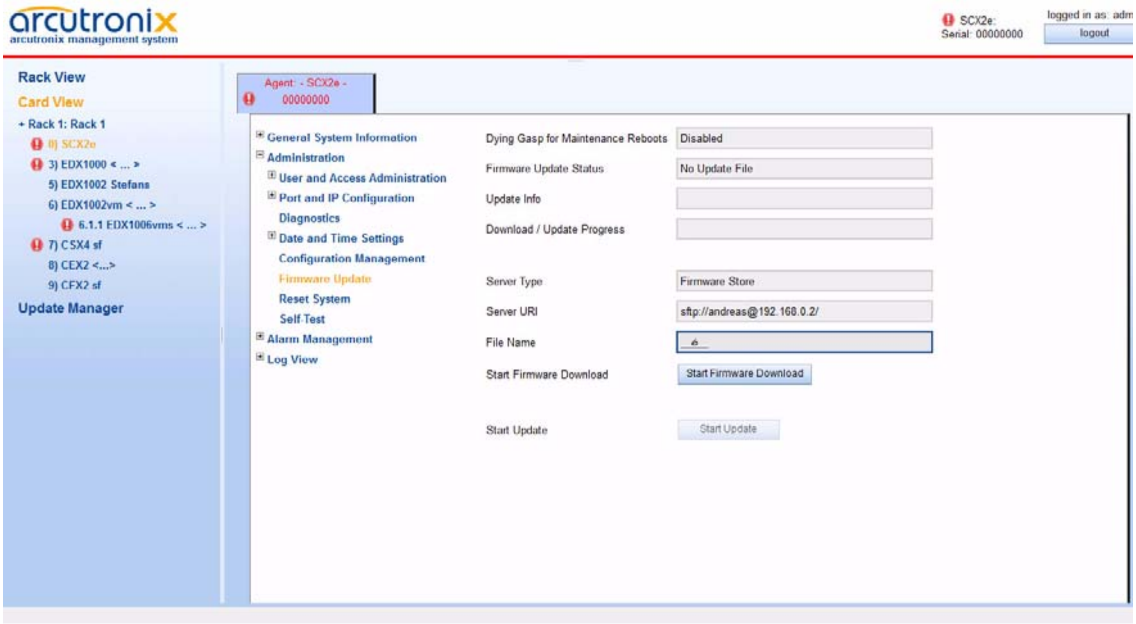
For the server-based download via SFTP or TFTP the so-called “Firmware Store”-server is used (see “File Servers” on page 1-20). The “Firmware Store” has to be configured properly to make use of it. During the configuration of the “Firmware Store”, one can select, whether SFTP or TFTP is used for communication.

The menu of the firmware-update changes, depending of the setting “HTTP File Transfer” (see “User and Access Administration” on page 1-18). If http file-transfer is disabled, only the download option are presented (see “Firmware Update w/o http-option”), otherwise the upload option via http are visible, too (see “Firmware Update with http-option”).

During load- and update process problems and errors may occur. These problems are listed in the field “Firmware Update State” and “Update Info”. See below in “Messages” on page 87 for details.

If any error occurs an alarm is raised, which can be configured in the system alarm menu (see “System Alarm Group” on page 1-92).

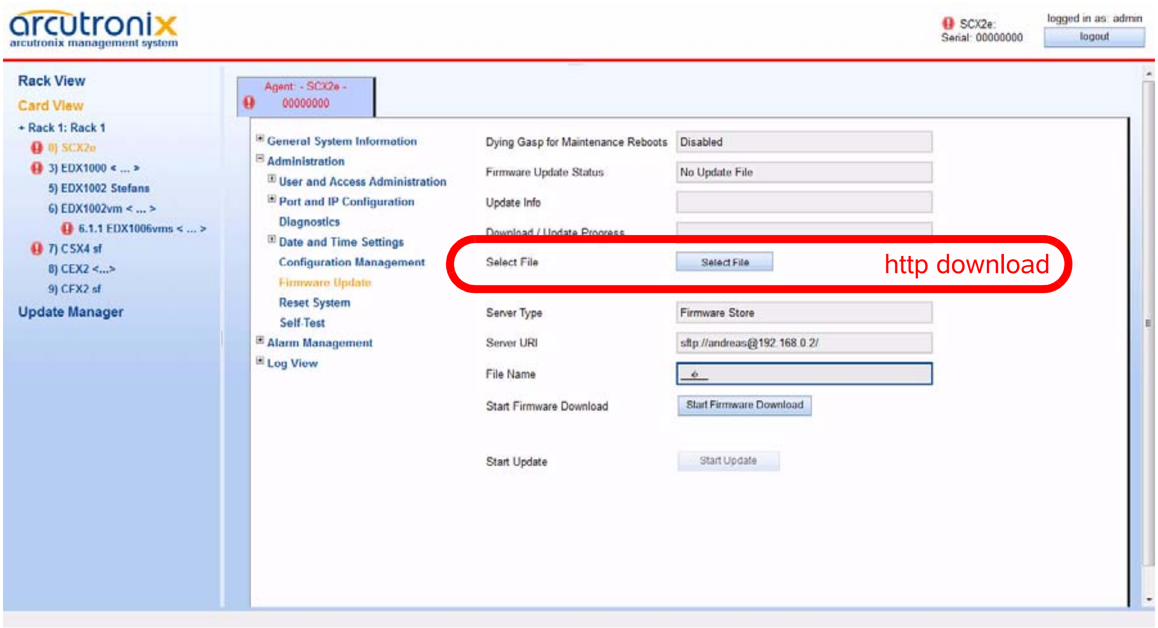
Menu



Dying Gasp for Maintenance Reboots	Disabled
Firmware Update Status	No Update File
Update Info	
Download / Update Progress	
Server Type	Firmware Store
Server URI	sftp://andreas@192.168.0.2/
File Name	
Start Firmware Download	Start Firmware Download
Start Update	Start Update

Figure 1-38 *Firmware Update w/o http-option*

The above picture shows the firmware update menu when http file transfer is disabled, while below the menu is presented, when http file transfer is enabled.



Dying Gasp for Maintenance Reboots: Disabled
Firmware Update Status: No Update File
Update Info:
Download / Update Progress:
Select File
Server Type: Firmware Store
Server URI: sftp://andreas@192.168.0.2/
File Name:
Start Firmware Download
Start Update

Figure 1-39 *Firmware Update with http-option*

Table 1-39 provides information about the options.

Table 1-40 *Firmware Update*

Parameter	Description	Format	Default
Dying Gasp for Maintenance Reboots	Information field to show, whether the device is configured to raise a Dying-Gasp alarm, when the SW is updated and the (maintenance-) reboot is invoked	Display	Disabled
Firmware Update State	Indicates the current of update state (No Update File |Update File Received | Firmware Download Active | Update Error Occurred | Update Active).	Display	No Update File
Update Info	Progress information about the update. If a update is loaded already, the name (and version) is visible here. Error messages are displayed in case of problems.	Display	empty

Table 1-40 Firmware Update (continued)

Parameter	Description	Format	Default
Download / Update Progress	Progress indicator for firmware download process and update process.	Display	empty
Select File [i]	Select File button to open browsers window to file explorer, when http-file transfer is enabled. Right after the file is selected, the upload to the device will be started.	Action	
Server Type	Indicate the server, which is used for S/TFTP file transfer.	Display	Firmware Store
Server URI	The configuration of Firmware Store for firmware download. Here one can see, whether SFTP or TFTP is selected, the IP-address etc. URI = Uniform Resource Identifier	Display	empty
File Name	Filename on the server. The (root-) path on the server is stored in the settings for Configuration Server. Format: *.upx	Input	empty
Start Firmware Download	To start the FTP file transfer.	Action	
SFTP User Name	The user name, deposed on the SFTP server.	Input	empty
SFTP Password	The password for the user’s SFTP access. Retype it for verification.	Input	empty
Start Firmware Download	After successful configuration, the download can be started.	Action	
Start Update	After successful download, the update process can be started.	Action	

[i] Only visible, in Web-GUI and when http-file-transfer is enabled!

Messages

When the download or the update process did not terminate successful, an error will be displayed and an alarm is raised. 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.

FW Update Status	Update info	Description
No Update File	<empty>	No update file is available at the moment. Since the last SW-update no action has be taken, which could cause error-messages or problems.
No Update File	Upload was aborted	Upload was interrupted: web page was reloaded, upload progress window closed or TCP connection closed or file size was too large (in this case an additional dialogue “File size is too large” is displayed)
Firmware Download Active	Connecting to server …	The download-process is trying to establish a connection to the server.
	Transferring data …	The download-process did successfully establish a connection to the server and the file transfer is now active.
Update File Received	Update package has version Vx_y_z	Ok, you can continue to start update.
Update Active	Update package has version Vx_y_z	The SW update process is ongoing. The SW update file has version Vx_y_z.
Update Error Occurred	The software is inappropriate for the device (invalid hardware).	Invalid hardware; Hardware revision is too old.
Update Error Occurred	The software is inappropriate for the device: Device Type mismatch.	Update file is not appropriate for this type of device.
Update Error Occurred	The software is inappropriate for the device: Hardware Revision mismatch.	Invalid hardware; Hardware revision of device does not match required version for update file.

FW Update Status	Update info	Description
Update Error Occurred	Invalid update file	File is no arcutronix update file or file was damaged.
Update Error Occurred	Could not open file on SFTP server: failure	The device was able to connect to the given server, but it was not able to open the specified file at the given path. Check file name and path on server.
Update Error Occurred	Error reading from input file: closed	During the file transfer from the server a problem did occur. This might be • IP-connection to server failed • Server was shut-down or stopped

Summary

To update the SCX2e software always 3 steps must be done:

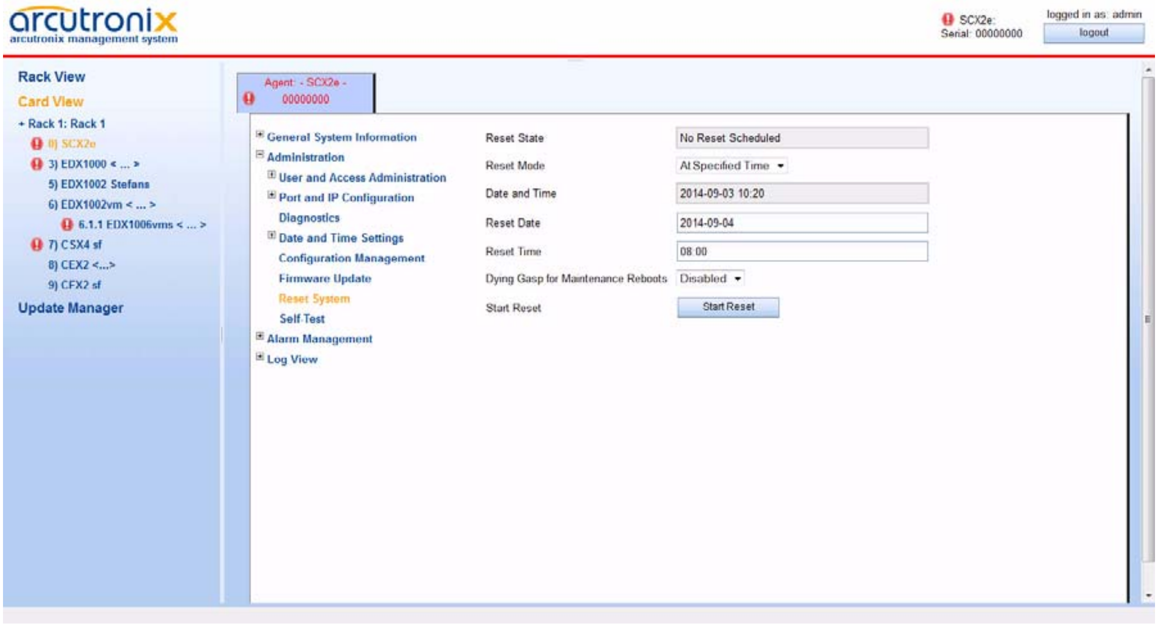
1. First select the update file (and path)
2. Then do “Start Upload” to begin with the file-transfer. The progress can be followed in the “Update Info” field (or the progress bar in the web-GUI).

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-load, the update process can be started, at any time, whenever it is required. Just do “Start Update” and it begins immediately or at the specified time. The progress is shown in the field “Update Progress”.

Reset System

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



Reset State: No Reset Scheduled
Reset Mode: At Specified Time
Date and Time: 2014-09-03 10:20
Reset Date: 2014-09-04
Reset Time: 08:00
Dying Gasp for Maintenance Reboots: Disabled
Start Reset

Figure 1-40 *Reset System, @Specific Time*

Table 1-41 provides information about the options.

Table 1-41 *Reset System*

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.	PullDown Menu • At Specified Time • Immediate Reset	Immediate Reset
Date and Time [i]	Indicates the current device's date and time (yyyy-mm-dd hh:mm).	Display	no default
Reset Date [i]	Enter the date for restart (yyyy-mm-dd).	Display/Input	no default
Reset Time [i]	Enter the time for restart (hh:mm).	Display/Input	no default

Table 1-41 Reset System (continued)

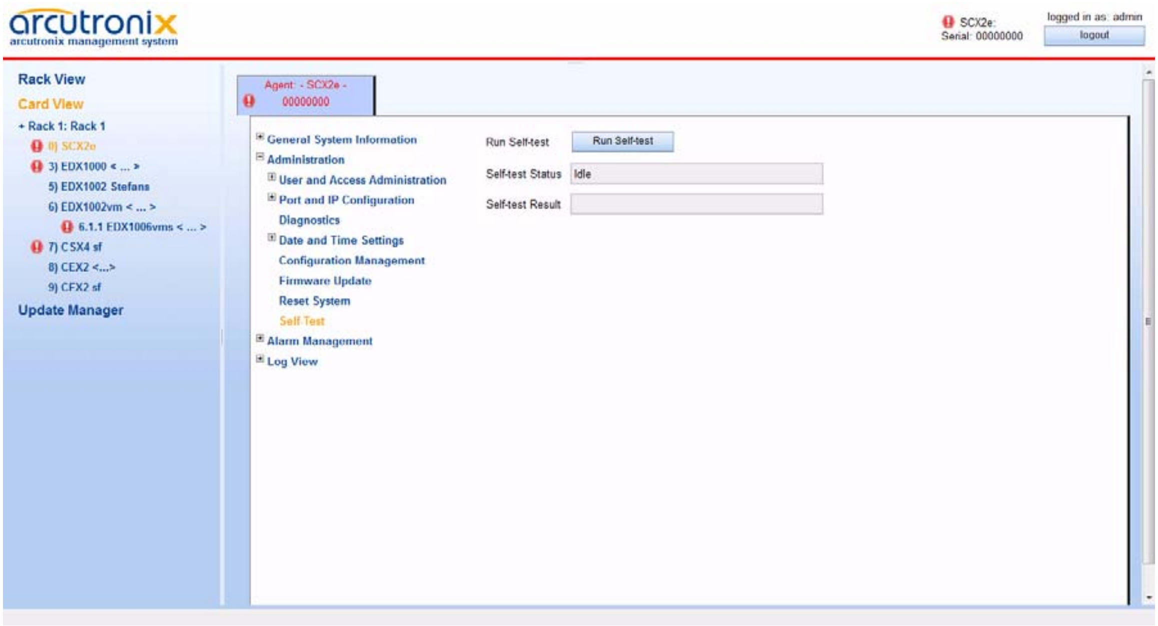
Parameter	Description	Format	Default
Dying Gasp for Maintenance Reboots	This variable decides, whether a Dying Gasp-Alarm is generated when a maintenance reboot like “Reset System” or “Reset after SW-Update” is raised.	PullDown Menu • Enabled • Disabled	Disabled
Reset System	Press Enter to confirm the settings.	Action	
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”.

NOTE: A reset can be scheduled in maximum 1 month ahead!

Self-Test

The Self-Test 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.

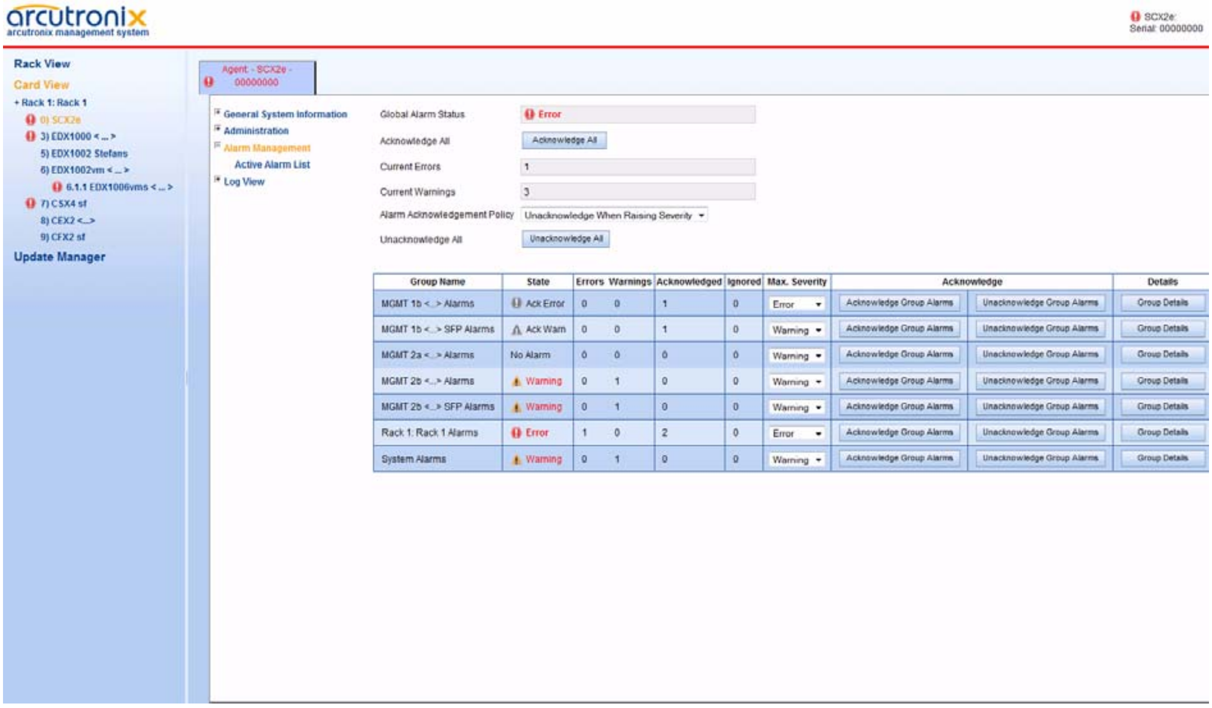


Run Self-test [Run Self-test]
Self-test Status Idle
Self-test Result

Figure 1-41 Self-Test

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 4-17 in [axManualSCX2e]. Please read this chapter before using the Alarm Management.



Global Alarm Status: Error

Acknowledge All: Acknowledge All

Current Errors: 1

Current Warnings: 3

Alarm Acknowledgement Policy: Unacknowledge When Raising Severity

Unacknowledge All: Unacknowledge All

Group Name	State	Errors	Warnings	Acknowledged	Ignored	Max. Severity	Acknowledge		Details
MGMT 1b <...> Alarms	Ack Error	0	0	1	0	Error	Acknowledge Group Alarms	Unacknowledge Group Alarms	Group Details
MGMT 1b <...> SFP Alarms	Ack Warn	0	0	1	0	Warning	Acknowledge Group Alarms	Unacknowledge Group Alarms	Group Details
MGMT 2a <...> Alarms	No Alarm	0	0	0	0	Warning	Acknowledge Group Alarms	Unacknowledge Group Alarms	Group Details
MGMT 2b <...> Alarms	Warning	0	1	0	0	Warning	Acknowledge Group Alarms	Unacknowledge Group Alarms	Group Details
MGMT 2b <...> SFP Alarms	Warning	0	1	0	0	Warning	Acknowledge Group Alarms	Unacknowledge Group Alarms	Group Details
Rack 1: Rack 1 Alarms	Error	1	0	2	0	Error	Acknowledge Group Alarms	Unacknowledge Group Alarms	Group Details
System Alarms	Warning	0	1	0	0	Warning	Acknowledge Group Alarms	Unacknowledge Group Alarms	Group Details

***Figure 1-42** Alarm Management*

On the top of the menu the summary of errors and warnings is presented. If there is any active error 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 error/warning condition of the SCX2e, e.g. the LED and alarm relay status are reset.

As there are many different alarms, several alarm-groups were defined to achieve better overview. All active alarms, can be seen in the sub-menu “Active Alarm List”.

1. MGMT 1b Alarm Group
2. MGMT 1b SFP Alarm Group
3. MGMT 2a Alarm Group
4. MGMT 2b Alarm Group
5. MGMT 2b SFP Alarm Group
6. Rack Alarm Group
7. System Alarm Group

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 1-42 provides information on the menu of the Alarm Management.

Table 1-42 *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.
Current Warnings	Summary (number) of all active warnings.
Alarm Acknowledgement Policy	What shall be done, when an alarm/warning has been acknowledge by administrator: Keep Acknowledged until Inactive: • The acknowledge alarm/warning will be kept in this status, until the alarm-cause is gone. Unacknowledged when raising Severity: • The acknowledge alarm/warning will be kept in this status, until the severity gets worse. (Default) Unacknowledged on State Change: • The acknowledge alarm/warning will be kept in this status, until the alarm-cause changes its state.

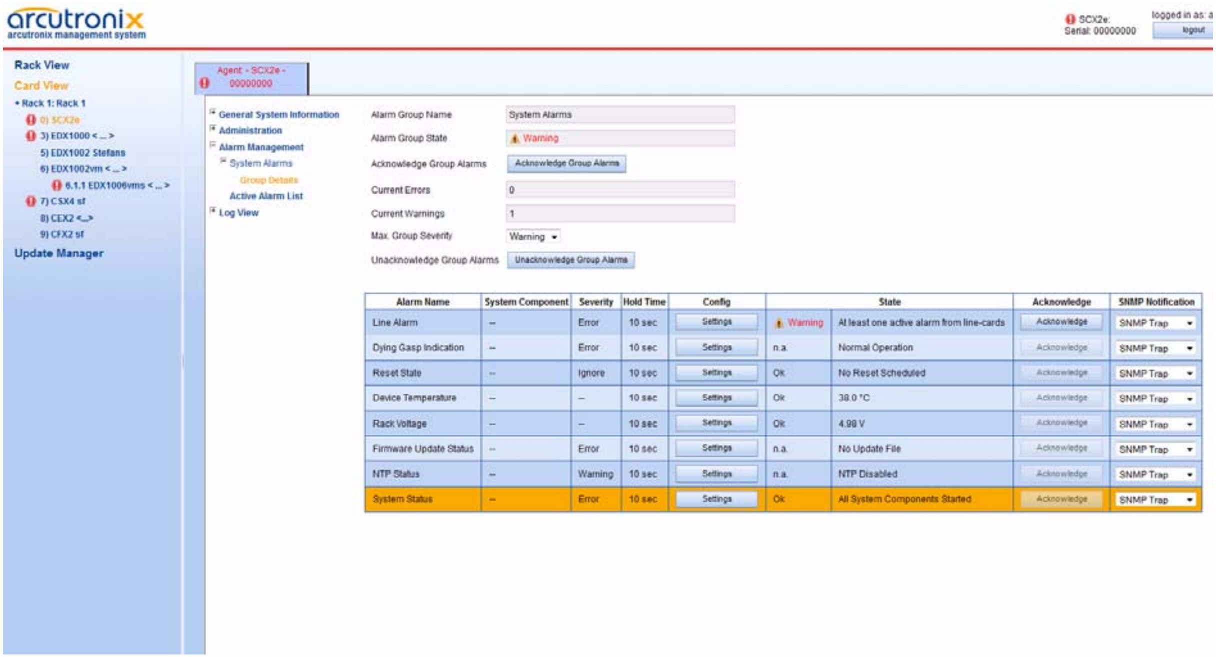
The sub-menu “Active Alarm List” shows all active alarms. This dynamic list will add remove alarms according the status of the device. See chapter “Active Alarm List” on page 1-100 for details.

System Alarm Group

The System Alarm Group incorporates all the alarms related to the system and its components like power supply, fans etc. Depending on the given configuration, alarms can be created by the device.The System Alarm Group incorporates all the system alarms:

- Collected alarm from the line-cards,
- Reset state of the SCX2e,
- Status of management interfaces,
- Device temperature and Rack voltage,

- Status of FW Update.



Alarm Group Name: System Alarms

Alarm Group State: Warning

Acknowledge Group Alarms: Acknowledge Group Alarms

Current Errors: 0

Current Warnings: 1

Max. Group Severity: Warning

Unacknowledge Group Alarms: Unacknowledge Group Alarms

Alarm Name	System Component	Severity	Hold Time	Config	State		Acknowledge	SNMP Notification
Line Alarm	--	Error	10 sec	Settings	Warning	At least one active alarm from line-cards	Acknowledge	SNMP Trap
Dying Gasp Indication	--	Error	10 sec	Settings	n.a.	Normal Operation	Acknowledge	SNMP Trap
Reset State	--	Ignore	10 sec	Settings	Ok	No Reset Scheduled	Acknowledge	SNMP Trap
Device Temperature	--	--	10 sec	Settings	Ok	38.0 °C	Acknowledge	SNMP Trap
Rack Voltage	--	--	10 sec	Settings	Ok	4.98 V	Acknowledge	SNMP Trap
Firmware Update Status	--	Error	10 sec	Settings	n.a.	No Update File	Acknowledge	SNMP Trap
NTP Status	--	Warning	10 sec	Settings	n.a.	NTP Disabled	Acknowledge	SNMP Trap
System Status	--	Error	10 sec	Settings	Ok	All System Components Started	Acknowledge	SNMP Trap

***Figure 1-43** System Alarm Group Management*

Table 1-43 provides information about the options of the System Alarm Group Management.

***Table 1-43** 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 [i]	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 its status. If an alarm is raised, the LC will announce this to the SCX2e on an accumulative signal, which is presented here.
Dying Gasp Indication	The “DyingGasp Alarm“ can be raised, when the power-supply falls under a minimum level. It can be configured to be used with error or warning level. The Dying Gasp-Trap can be enabled here!

Table 1-43 System Alarm Group Management (continued)

Parameter	Description
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.
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 [i]	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 [i]	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.
Firmware Update Status	This alarm raises, when an error occurred during firmware update. E.g. file transfer was corrupted or the flashing of the memory did not work successfully. It can be configured to be used with error or warning level.
NTP Status	This alarm raises, when an error occurred related to the NTP client. E.g. none of the defined server is reachable or the given time information is determined to be usable. It can be configured to be used with error or warning level. When the usage of NTP is disable, this alarm will be switched off.
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 (Config)

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 pre defined settings, which can be normally left untouched.

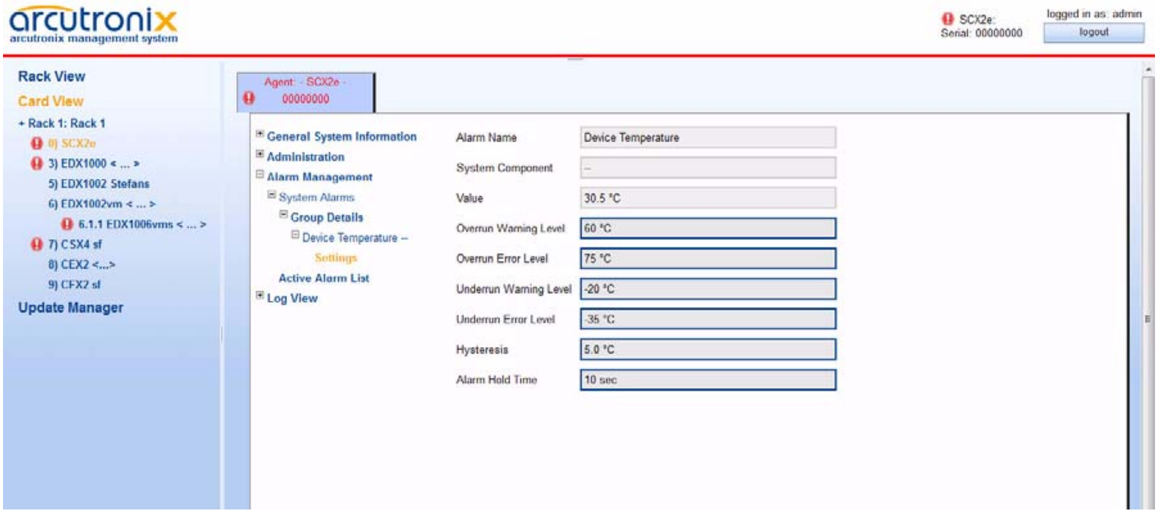
The severity defines whether the alarm

- 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 (High Temp.) = 50°C; Error (High Temp.) = 60°C
Warning (Low Temp.) = -20 °C; Error (Low Temp.) = -30 °C

To make sure, that at the threshold the alarm is not toggling all time, a hysteresis should be declared. In the example below the hysteresis is 5°.



Alarm Name: Device Temperature
System Component: --
Value: 30.5 °C
Overrun Warning Level: 60 °C
Overrun Error Level: 75 °C
Underrun Warning Level: -20 °C
Underrun Error Level: -35 °C
Hysteresis: 5.0 °C
Alarm Hold Time: 10 sec

Figure 1-44 *Example Alarm Settings: Device Temperature*

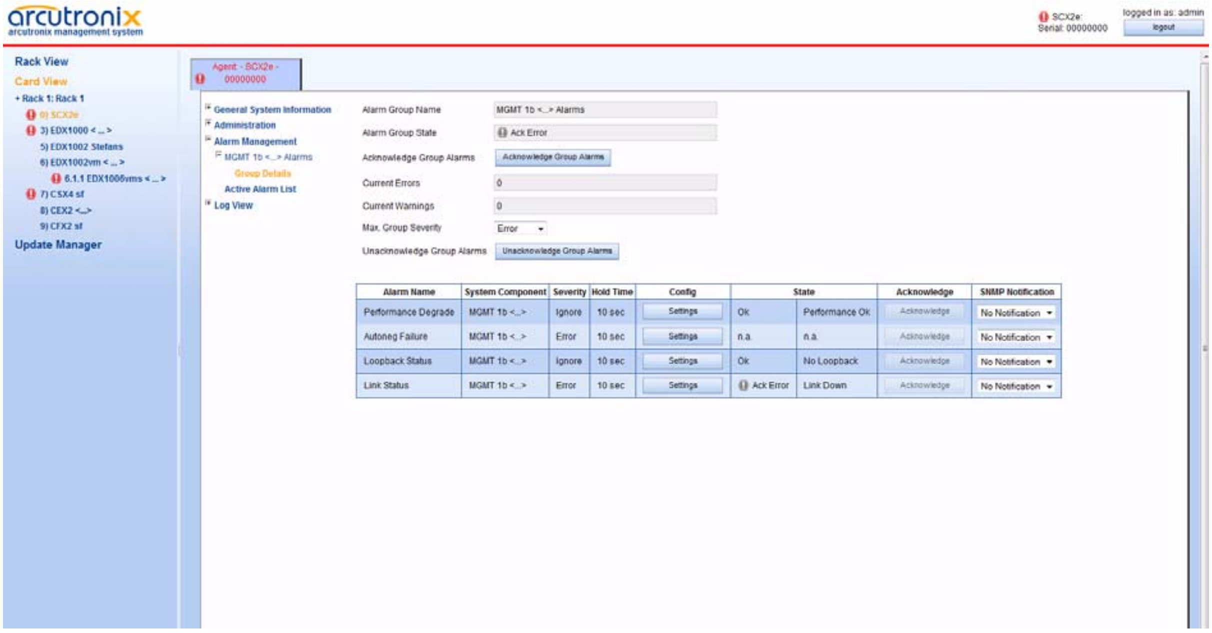
NOTE: For analogue alarms it is possible to define the warning level at a higher value than the error level. E.g. for the temperature it is possible to define the warning @60°C and the error @55°C. This is not forbidden by the system, as there might be customer’s reason to do so.

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.

MGMT Alarm Groups

The MGMT Alarm Groups incorporates all the alarms related to the management interfaces. Depending on the selected configuration, one to four independent management interfaces can be created by the device. Each of these interfaces has it “own” alarm group.

- Performance,
- Auto Negotiation (Copper & Fibre!),
- Loopback and Link Status.



Alarm Group Name: MGMT 1b <...> Alarms

Alarm Group State: Ack Error

Acknowledge Group Alarms: Acknowledge Group Alarms

Current Errors: 0

Current Warnings: 0

Max. Group Severity: Error

Unacknowledge Group Alarms: Unacknowledge Group Alarms

Alarm Name	System Component	Severity	Hold Time	Config	State		Acknowledge	SNMP Notification
Performance Degrade	MGMT 1b <...>	Ignore	10 sec	Settings	Ok	Performance Ok	Acknowledge	No Notification
Autoneg Failure	MGMT 1b <...>	Error	10 sec	Settings	n.a.	n.a.	Acknowledge	No Notification
Loopback Status	MGMT 1b <...>	Ignore	10 sec	Settings	Ok	No Loopback	Acknowledge	No Notification
Link Status	MGMT 1b <...>	Error	10 sec	Settings	Ack Error	Link Down	Acknowledge	No Notification

Figure 1-45 *MGMT Alarm Groups*

Table 1-45 provides information on the menu of the MGMT Alarm Groups.

Table 1-44 *MGMT Alarm Groups*

Parameter	Description
Performance Degrade	The 'Performance Degrade Alarm' can be raised, when problems are detected by the PHY. It can be bad input signal due to disturbance, bad cable or other reasons. It can be configured to be used with error or warning level.
Autoneg Failure	This variable shows whether auto negotiation of link parameters with the link partner was successful or not. If auto negotiation has been enabled for the selected interface, the variable will show “No Autoneg Page Received” as long as the cable/fibre is not fitted correctly on both ends of the link. A corresponding alarm can be raised when the Autoneg Failure status of the port changes. The alarm can be configured to be ignored or to be of error / warning severity.

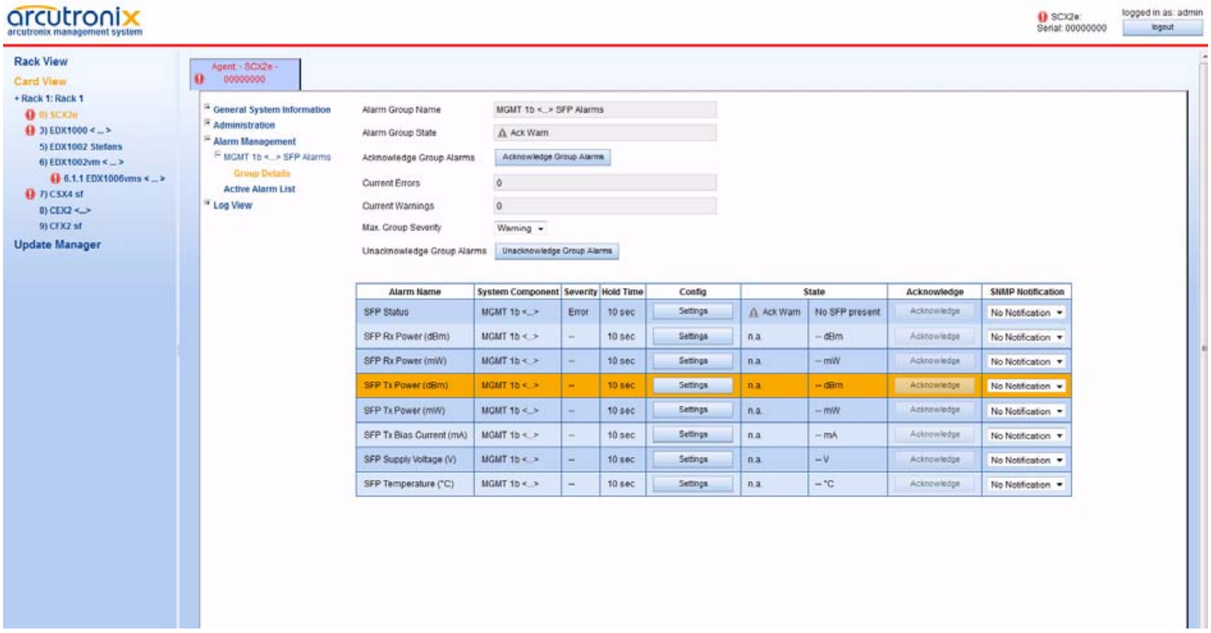
Table 1-44 *MGMT Alarm Groups*

Parameter	Description
Loopback Status	This variable holds the loopback status of the selected interface. A corresponding alarm can be raised when the Loopback Status of the port changes. The alarm can be configured to be ignored or to be of error / warning severity.
Link Status	This variable shows the link status of the selected port. A corresponding alarm can be raised when the Link Status of the port changes. The alarm can be configured to be ignored or to be of error / warning severity. “Hardware Error detected” is shown if during device initialization the port could not be initialized. The port is disabled automatically in this case. All other configuration options belonging to the failed port may not be initalized/displayed correctly depending on the type of failure.

SFP Alarm Groups (MGMT1b; MGMT2b)

The SFP Alarm Groups incorporates all the alarms related to both SFPs:

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



Alarm Group Name: MGMT 1b <...> SFP Alarms

Alarm Group State: ⚠ Ack Warn

Acknowledge Group Alarms: Acknowledge Group Alarms

Current Errors: 0

Current Warnings: 0

Max. Group Severity: Warning

Unacknowledge Group Alarms: Unacknowledge Group Alarms

Alarm Name	System Component	Severity	Hold Time	Config	State		Acknowledge	SNMP Notification
SFP Status	MGMT 1b <...>	Error	10 sec	Settings	⚠ Ack Warn	No SFP present	Acknowledge	No Notification
SFP Rx Power (dBm)	MGMT 1b <...>	--	10 sec	Settings	n.a.	-- dBm	Acknowledge	No Notification
SFP Rx Power (mW)	MGMT 1b <...>	--	10 sec	Settings	n.a.	-- mW	Acknowledge	No Notification
SFP Tx Power (dBm)	MGMT 1b <...>	--	10 sec	Settings	n.a.	-- dBm	Acknowledge	No Notification
SFP Tx Power (mW)	MGMT 1b <...>	--	10 sec	Settings	n.a.	-- mW	Acknowledge	No Notification
SFP Tx Bias Current (mA)	MGMT 1b <...>	--	10 sec	Settings	n.a.	-- mA	Acknowledge	No Notification
SFP Supply Voltage (V)	MGMT 1b <...>	--	10 sec	Settings	n.a.	-- V	Acknowledge	No Notification
SFP Temperature (°C)	MGMT 1b <...>	--	10 sec	Settings	n.a.	-- °C	Acknowledge	No Notification

Figure 1-46 *SFP Alarm Groups*

Table 1-45 provides information on the menu of the SFP Alarm Groups.

Table 1-45 *SFP Alarm Groups*

Parameter	Description
SFP Status	The “SFP Status Alarm” can be raised, when the SFP is removed or any other change of the SFP is detected. It can be configured to be used with error or warning level.
SFP Rx Power [i] (mBm)	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. Here all values are used in dBm units.
SFP Rx Power [i] (mW)	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. Here all values are used in mW units.
SFP Tx Power [i] (dBm)	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. Here all values are used in dBm units.

Table 1-45 *SFP Alarm Groups (continued)*

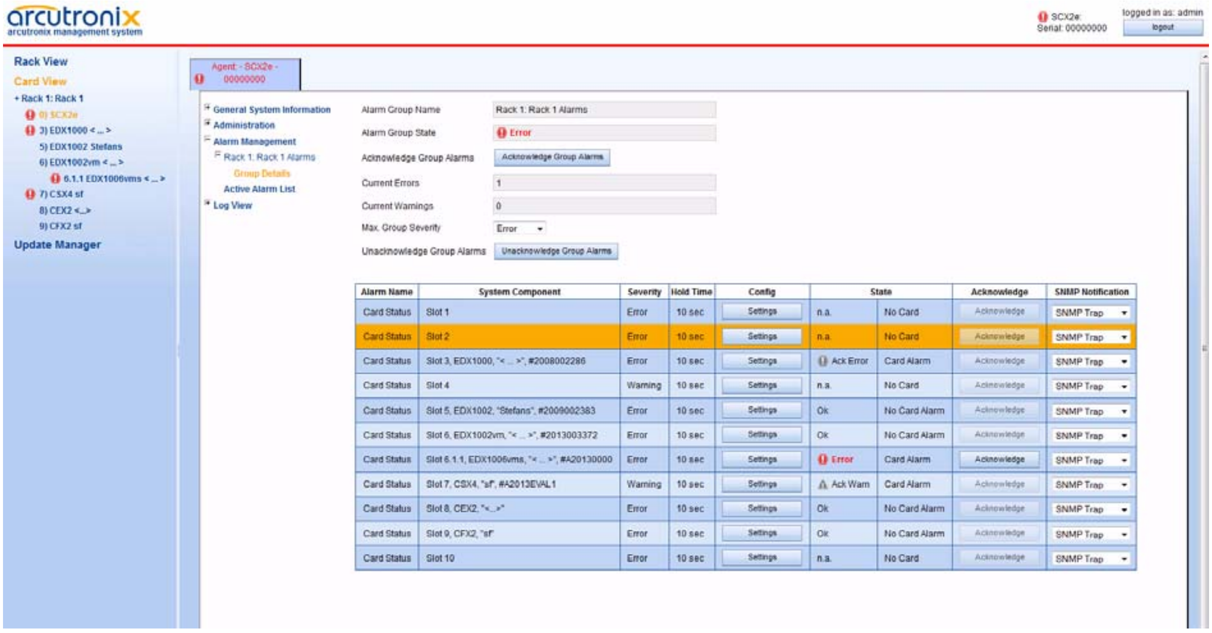
Parameter	Description
SFP Tx Power [i] (mW)	The “SFP TX Power Alarm” can be raised, when the SFP’s TX power is below a configurable value (Thresholds). The warning and alarm level can be configured separately. The allowed value depends on the used SFP. Here all values are used in mW units.
SFP TX Bias Current [i] (mA)	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.
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 (Config)” on page 1-94.

Rack Alarm Group

The Rack Alarm Group displays the alarms of the (plugged) line-cards. Each slot can rise one “line-card alarm”. The more racks are discovered, the more Rack Alarm Groups are created.



Alarm Group Name: Rack 1: Rack 1 Alarms

Alarm Group State: Error

Acknowledge Group Alarms: Acknowledge Group Alarms

Current Errors: 1

Current Warnings: 0

Max. Group Severity: Error

Unacknowledge Group Alarms: Unacknowledge Group Alarms

Alarm Name	System Component	Severity	Hold Time	Config	State		Acknowledge	SNMP Notification
Card Status	Slot 1	Error	10 sec	Settings	n.a.	No Card	Acknowledge	SNMP Trap
Card Status	Slot 2	Error	10 sec	Settings	n.a.	No Card	Acknowledge	SNMP Trap
Card Status	Slot 3, EDX1000, "< ... >", #2008002286	Error	10 sec	Settings	Ack Error	Card Alarm	Acknowledge	SNMP Trap
Card Status	Slot 4	Warning	10 sec	Settings	n.a.	No Card	Acknowledge	SNMP Trap
Card Status	Slot 5, EDX1002, "Stefans", #2009002383	Error	10 sec	Settings	Ok	No Card Alarm	Acknowledge	SNMP Trap
Card Status	Slot 6, EDX1002vm, "< ... >", #2013003372	Error	10 sec	Settings	Ok	No Card Alarm	Acknowledge	SNMP Trap
Card Status	Slot 6.1.1, EDX1006vms, "< ... >", #A20130000	Error	10 sec	Settings	Error	Card Alarm	Acknowledge	SNMP Trap
Card Status	Slot 7, CSX4, "sf", #A2013EVAL1	Warning	10 sec	Settings	Ack Warn	Card Alarm	Acknowledge	SNMP Trap
Card Status	Slot 8, CEX2, "<...>"	Error	10 sec	Settings	Ok	No Card Alarm	Acknowledge	SNMP Trap
Card Status	Slot 9, CFX2, "sf"	Error	10 sec	Settings	Ok	No Card Alarm	Acknowledge	SNMP Trap
Card Status	Slot 10	Error	10 sec	Settings	n.a.	No Card	Acknowledge	SNMP Trap

***Figure 1-47** Rack Alarm Group*

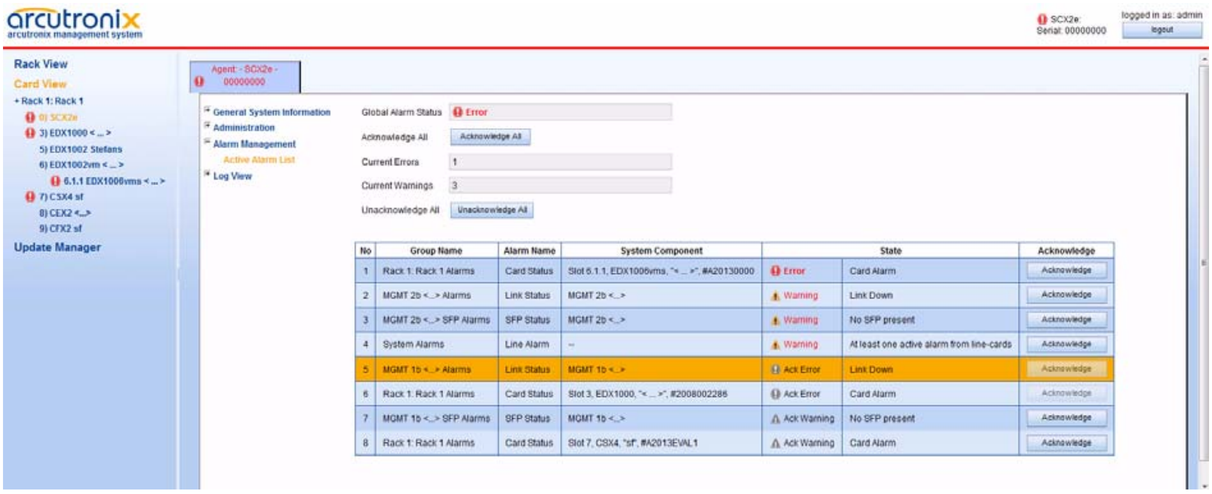
Table 1-45 provides information on the menu of the Rack Alarm Group.

***Table 1-46** Rack Alarm Group*

Parameter	Description
Card Status	The Card Status for each available slot can be source for an alarm. In the corresponding line the settings can be defined.

Active Alarm List

The Active Alarm List shows all currently active alarms in “Error”, “Warning” and “Acknowledged” state. For better location of the alarm and for further tuning of it, the group name and the alarm’s name is given together with its status.



Global Alarm Status: Error

Acknowledge All

Current Errors: 1

Current Warnings: 3

Unacknowledge All

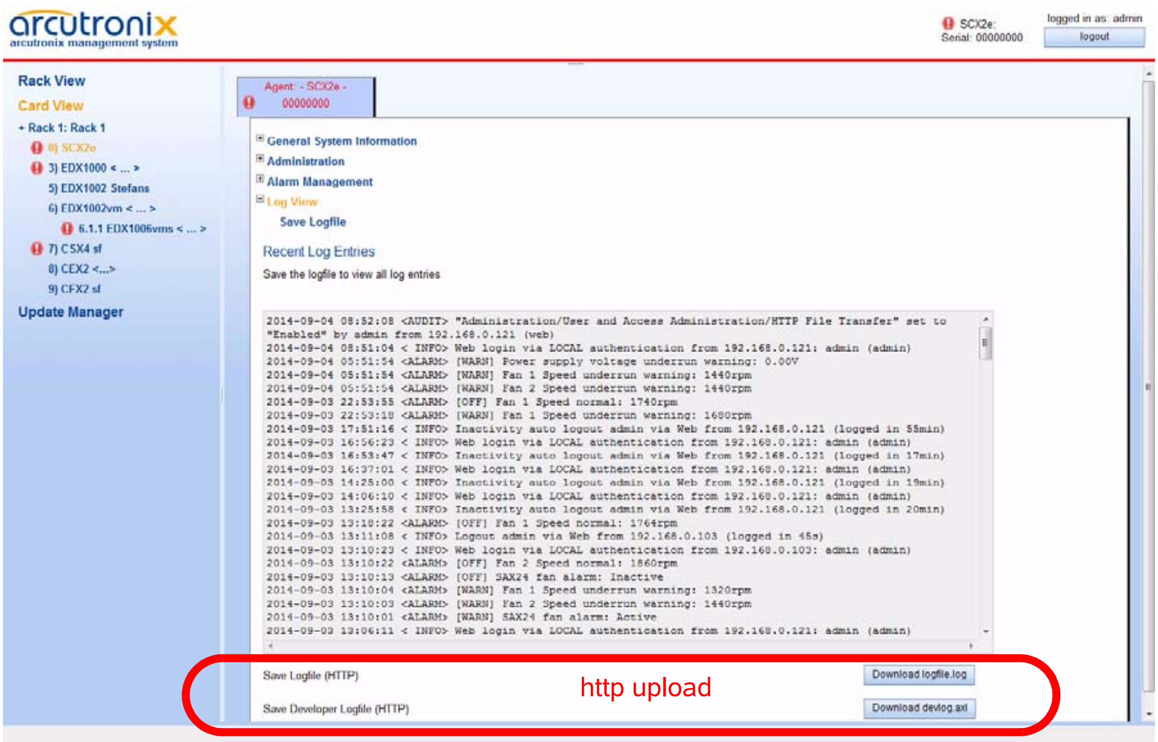
No	Group Name	Alarm Name	System Component	State		Acknowledge
1	Rack 1: Rack 1 Alarms	Card Status	Slot 6.1.1, EDX1006vms, "< ... >", #A20130000	Error	Card Alarm	Acknowledge
2	MGMT 2b <...> Alarms	Link Status	MGMT 2b <...>	Warning	Link Down	Acknowledge
3	MGMT 2b <...> SFP Alarms	SFP Status	MGMT 2b <...>	Warning	No SFP present	Acknowledge
4	System Alarms	Line Alarm	--	Warning	At least one active alarm from line-cards	Acknowledge
5	MGMT 1b <...> Alarms	Link Status	MGMT 1b <...>	Ack Error	Link Down	Acknowledge
6	Rack 1: Rack 1 Alarms	Card Status	Slot 3, EDX1000, "< ... >", #2008002286	Ack Error	Card Alarm	Acknowledge
7	MGMT 1b <...> SFP Alarms	SFP Status	MGMT 1b <...>	Ack Warning	No SFP present	Acknowledge
8	Rack 1: Rack 1 Alarms	Card Status	Slot 7, CSX4, "sf", #A2013EVAL1	Ack Warning	Card Alarm	Acknowledge

Figure 1-48 *Active Alarm List*

Log View

The Log View shows all events. There are many pre defined events as link-up and link-down, but one can define more events, if required.

The number of entries in the Log View is 999 entries.



Save the logfile to view all log entries

```
2014-09-04 08:52:08 <AUDIT> "Administration/User and Access Administration/HTTP File Transfer" set to
"Enabled" by admin from 192.168.0.121 (web)
2014-09-04 08:51:04 < INFO> Web login via LOCAL authentication from 192.168.0.121: admin (admin)
2014-09-04 05:51:54 <ALARM> [WARN] Power supply voltage underrun warning: 0.00V
2014-09-04 05:51:54 <ALARM> [WARN] Fan 1 Speed underrun warning: 1440rpm
2014-09-04 05:51:54 <ALARM> [WARN] Fan 2 Speed underrun warning: 1440rpm
2014-09-03 22:53:55 <ALARM> [OFF] Fan 1 Speed normal: 1740rpm
2014-09-03 22:53:18 <ALARM> [WARN] Fan 1 Speed underrun warning: 1680rpm
2014-09-03 17:51:16 < INFO> Inactivity auto logout admin via Web from 192.168.0.121 (logged in 55min)
2014-09-03 16:56:23 < INFO> Web login via LOCAL authentication from 192.168.0.121: admin (admin)
2014-09-03 16:53:47 < INFO> Inactivity auto logout admin via Web from 192.168.0.121 (logged in 17min)
2014-09-03 16:37:01 < INFO> Web login via LOCAL authentication from 192.168.0.121: admin (admin)
2014-09-03 14:25:00 < INFO> Inactivity auto logout admin via Web from 192.168.0.121 (logged in 19min)
2014-09-03 14:06:10 < INFO> Web login via LOCAL authentication from 192.168.0.121: admin (admin)
2014-09-03 13:25:58 < INFO> Inactivity auto logout admin via Web from 192.168.0.121 (logged in 20min)
2014-09-03 13:18:22 <ALARM> [OFF] Fan 1 Speed normal: 1764rpm
2014-09-03 13:11:08 < INFO> Logout admin via Web from 192.168.0.103 (logged in 45s)
2014-09-03 13:10:23 < INFO> Web login via LOCAL authentication from 192.168.0.103: admin (admin)
2014-09-03 13:10:22 <ALARM> [OFF] Fan 2 Speed normal: 1860rpm
2014-09-03 13:10:13 <ALARM> [OFF] SAX24 fan alarm: Inactive
2014-09-03 13:10:04 <ALARM> [WARN] Fan 1 Speed underrun warning: 1320rpm
2014-09-03 13:10:03 <ALARM> [WARN] Fan 2 Speed underrun warning: 1440rpm
2014-09-03 13:10:01 <ALARM> [WARN] SAX24 fan alarm: Active
2014-09-03 13:06:11 < INFO> Web login via LOCAL authentication from 192.168.0.121: admin (admin)
```

Save Logfile (HTTP) Download logfile.log

Save Developer Logfile (HTTP) Download devlog.axl

http upload

Figure 1-49 *Log View Example*

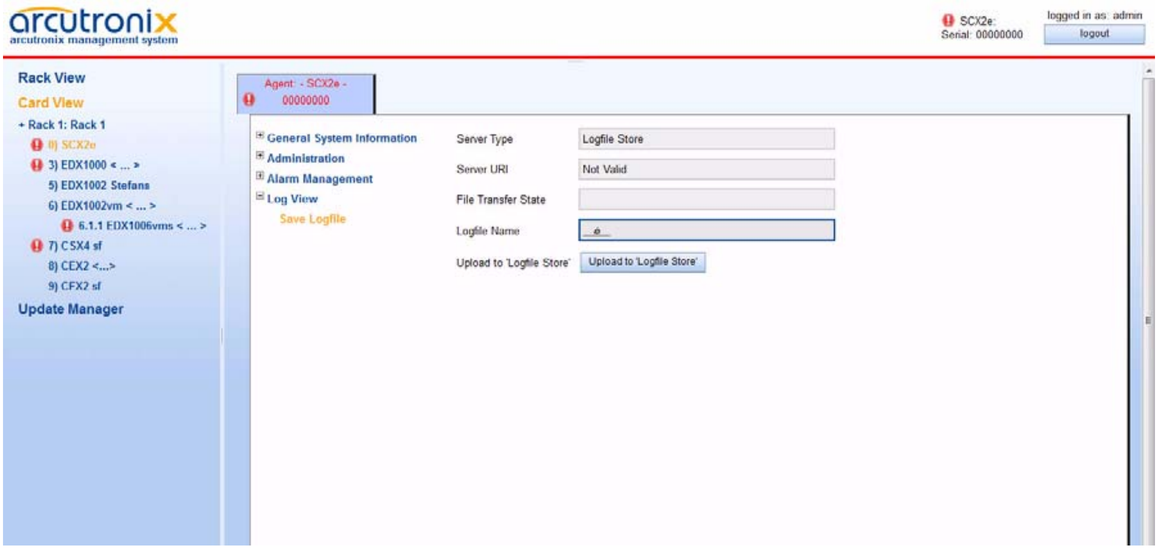
The log-files can be stored either via FTP (SFTP or TFTP) or HTTP. HTTP is only available during a web-session and when “http-file-transfer” is enabled (see “User and Access Administration” on page 1-18).

A SFTP- or TFTP-file upload is done onto the “Logfile Store”. This server is dedicated to store log-files only and the access to it can be configured in the File Server’s menu (see “File Servers” on page 1-20). To do upload via SFTP or TFTP, the submenu “Save Logfiles” must be opened.

Safe Log-Files

The file transfer to upload log-files to the “Logfile Server” needs two steps:

1. Proper configuration of “Logfile Server”
2. Filename on the server. The (root-) path on the server is stored in the settings for Configuration Server.
   Format: * (the device will store log-files always as *.log on the server!)



Server Type: Logfile Store
Server URI: Not Valid
File Transfer State:
Logfile Name:
Upload to 'Logfile Store'

Figure 1-50 Save Logfiles

Table 1-38 provides information about the options.

***Table 1-47** Configuration of Log-Files*

Parameter	Description	Format
Server Type	Indicate the server, which is used for S/TFTP file transfer. Always “Logfile Store”	Display
Server URI	The configuration of Configuration Store. Here one can see, whether SFTP or TFTP is selected, the IP-address etc. URI = Uniform Resource Identifier	Display
File Transfer State	Shows information about a file transfer to/from the configuration server.	Display
Logfile Name	(Path) and file-name on the server. Keep in mind, the path is calculated from the user’s root-directory. [i]	Input
Upload to Server	Upload the named log-file from the device to the “Logfile server”.	Action

[i] The update-file’s path has to be specified with slash (‘/’), when used on a Windows based FTP-server. Otherwise the FTP-server can not locate the correct file.
Format: /../SCX2e*.cfgx

Update Manager

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

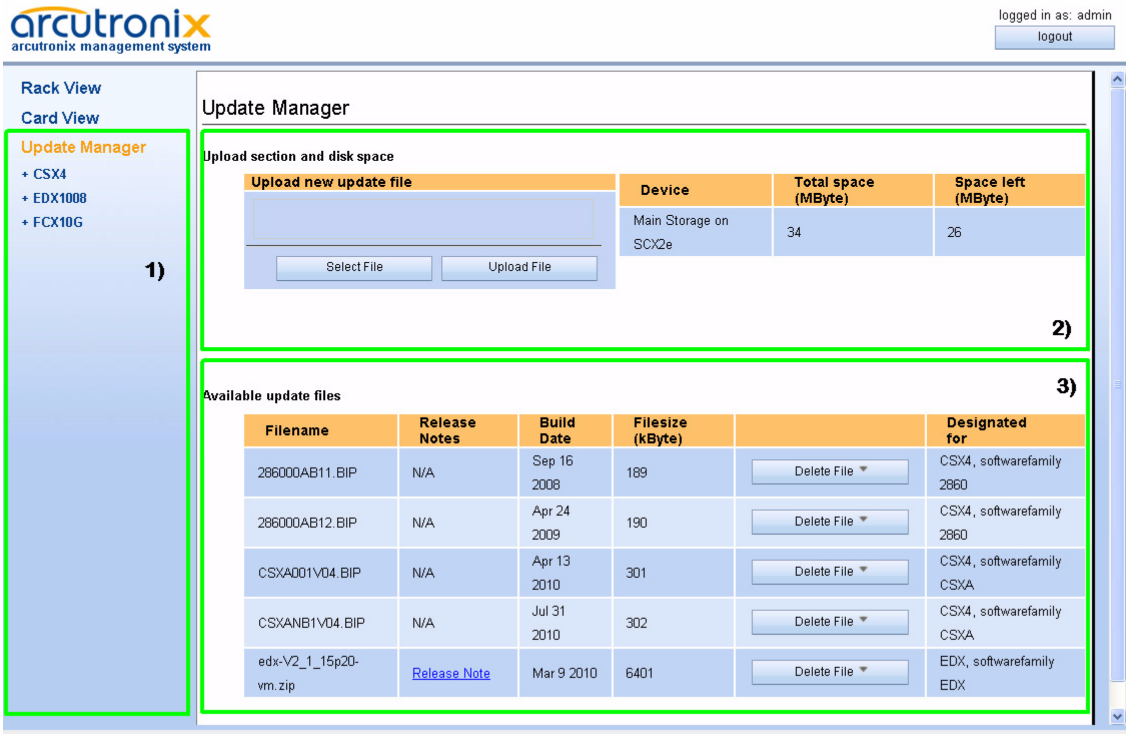
NOTE: The Update Manager is only used for the line-cards. For updating the SW of the SCX2e, please use the “Firmware Update” as written in “Firmware Update” on page 1-83.

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

The menu “Update Manager” is used to update the software of (plugged) line-cards. To update the firmware of SCX2e - System Controller use the menu entry “Firmware Update” on page 1-83.



Update Manager

Upload section and disk space

Upload new update file	Device	Total space (MByte)	Space left (MByte)
	Main Storage on SCX2e	34	26

Available update files

Filename	Release Notes	Build Date	Filesize (kByte)		Designated for
286000AB11.BIP	N/A	Sep 16 2008	189	Delete File ▾	CSX4, softwarefamily 2860
286000AB12.BIP	N/A	Apr 24 2009	190	Delete File ▾	CSX4, softwarefamily 2860
CSXA001V04.BIP	N/A	Apr 13 2010	301	Delete File ▾	CSX4, softwarefamily CSXA
CSXANB1V04.BIP	N/A	Jul 31 2010	302	Delete File ▾	CSX4, softwarefamily CSXA
edx-V2_1_15p20-vm.zip	Release Note	Mar 9 2010	6401	Delete File ▾	EDX, softwarefamily EDX

Figure 1-51 *Update Manager*

The Update Manager is divided in 3 sections:

1. On the left side is the Navigation Pane.
   The Navigation Pane shows all plugged device-types, grouped together according their nature of software. See below for a list of available device-groups.

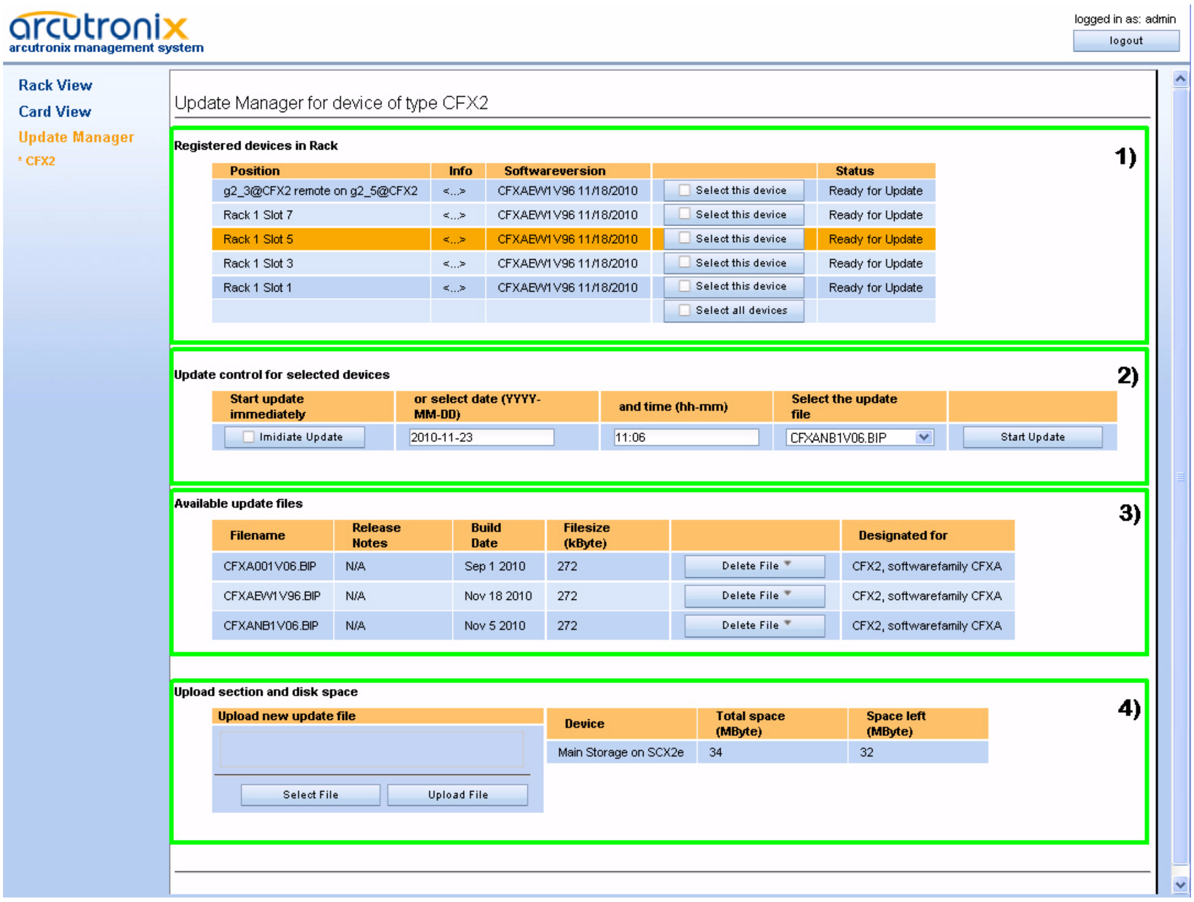
   The right side is divided in two parts, the Upload Section and the File Section:

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 Navigation Pane is shown. When selecting one entry here, the device-specific 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.



Update Manager for device of type CFX2

Registered devices in Rack

Position	Info	Softwareversion		Status
g2_3@CFX2 remote on g2_5@CFX2	<...>	CFXAEW1V96 11/18/2010	☐ Select this device	Ready for Update
Rack 1 Slot 7	<...>	CFXAEW1V96 11/18/2010	☐ Select this device	Ready for Update
Rack 1 Slot 5	<...>	CFXAEW1V96 11/18/2010	☐ Select this device	Ready for Update
Rack 1 Slot 3	<...>	CFXAEW1V96 11/18/2010	☐ Select this device	Ready for Update
Rack 1 Slot 1	<...>	CFXAEW1V96 11/18/2010	☐ Select this device	Ready for Update
			☐ Select all devices	

Update control for selected devices

Start update immediately	or select date (YYYY-MM-DD)	and time (hh-mm)	Select the update file	
☐ Imidiate Update	2010-11-23	11:06	CFXANB1V06.BIP	Start Update

Available update files

Filename	Release Notes	Build Date	Filesize (kByte)		Designated for
CFXA001V06.BIP	N/A	Sep 1 2010	272	Delete File	CFX2, softwarefamily CFXA
CFXAEW1V96.BIP	N/A	Nov 18 2010	272	Delete File	CFX2, softwarefamily CFXA
CFXANB1V06.BIP	N/A	Nov 5 2010	272	Delete File	CFX2, softwarefamily CFXA

Upload section and disk space

Upload new update file

Device	Total space (MByte)	Space left (MByte)
Main Storage on SCX2e	34	32

Figure 1-52 *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.

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