

arcutronix

Synchronize the Ethernet

ENX WebGUI

GS1



arcutronix GmbH
Deutschland

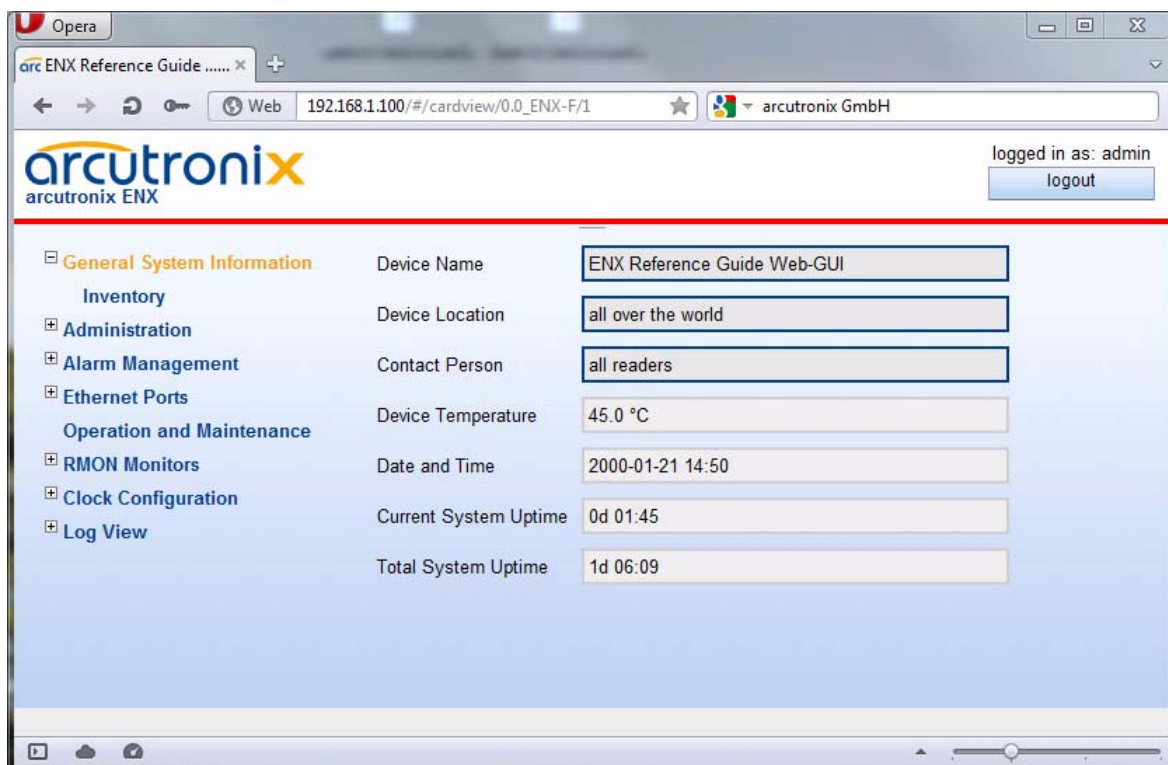
Reference Guide

Version 1.3

ENX-F

REFERENCE GUIDE

Web-GUI



Version 1.3

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

© Copyright 2013, arcutronix GmbH. All rights reserved.

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

Document Contents

This document contains the latest information available at the time of publication. The content of this document is subject to change without prior notice. arcutronix reserves the right 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

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

About this Reference Guide

Introduction and Overview

The ENX 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:
Version:

1102 00 65.man
V 1.3

Covered Software

This Reference Guide is valid for ENX-SW V 1_1_00.

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

2013-01-10 Version 1.0 Editor: mjz

First issue of the ENX Reference Guide Web-GUI. It is based on the original manual axManualENX, which became much to huge due to all the information required for web-GUI. therefore an extra document was separated.

Referenced and Related Documents

[axManualENX]	arcutronix GmbH (2012): Manual for ENX: Operation, installation, Functionality.
[axRefGuideCLI]	arcutronix GmbH (2012): ENX Command Line Interface, Reference Guide.
[IEEE 802.1AS]	IEEE Std 802.1AS™-2011: Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks.
[IEEE 802.1AX]	IEEE Std 802.1AX™-2008: Link Aggregation.
[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.
[IEEE 802.11]	IEEE Std 802.11™-2012: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
[IEEE 1588]	IEEE Std 1588™-2008: IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.
[IEEE 1901]	IEEE Std 1901™-2010: Broadband Over Power Lines PHY/MAC Working Group (COM/SC/BPLPHMAC).
[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 2544]	IETF RFC 2544 (1999), Benchmarking Methodology for Network Interconnect Devices.
[IETF RFC 2597]	IETF RFC 2597 (1999), Assured Forwarding PHB Group.
[IETF RFC 3246]	IETF RFC 3246 (2002), An Expedited Forwarding PHB (Per-Hop Behavior).
[IETF RFC 3410]	IETF RFC 3410 (2002), Introduction and Applicability Statements for Internet Standard Management Framework.

About this Reference Guide

Referenced and Related Documents

[IETF RFC 3414]	IETF RFC 3414 (2002), User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).
[ITU-T G.703]	Recommendation ITU-T G.703 (2001), Physical/electrical characteristics of hierarchical digital interfaces.
[ITU-T G.704]	Recommendation ITU-T G.704 (1998), Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels.
[ITU-T G.813]	Recommendation ITU-T G.813 (2003), Timing characteristics of SDH equipment slave clocks (SEC).
[ITU-T G.823]	Recommendation ITU-T G.823 (2000), The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy.
[ITU-T G.8261]	Recommendation ITU-T G.8261/Y.1361 (2008), Timing and synchronization aspects of packet networks.
[ITU-T G.8262]	Recommendation ITU-T G.8262/Y.1362 (2007), Timing characteristics of synchronous Ethernet equipment slave clock (EEC).
[ITU-T G.8264]	Recommendation ITU-T G.8264/Y.1364 (2008), Distribution of timing information through packet networks.
[ITU-T V.11]	Recommendation ITU-T V.11 (1996), Electrical characteristics for balanced double-current interchange circuits operating at data signalling rates up to 10 Mbit/s.
[ITU-T Y.1731]	Recommendation ITU-T Y.1731 (2006), OAM functions and mechanisms for Ethernet based networks.
[MEF 6.1]	MEF Technical Specification MEF 6.1 (2008), Ethernet Services Definitions - Phase 2
[MEF 10.2]	MEF Technical Specification MEF 10.2 (2009), Ethernet Services Attributes Phase 2
[MEF 12.1]	MEF Technical Specification MEF 12.1 (2010), Ethernet Services Layer - Base Elements
[MEF 22.1]	MEF Technical Specification MEF 22.1 (2012), Mobile Backhaul Phase 2
[SFP MSA]	Small Form-factor Pluggable (SFP) Transceiver Multi Source Agreement (MSA) (2000)

List of Contents

Introduction and Overview	about-1
Covered Software	about-1
Conventions	about-1
Release History	about-2
Referenced and Related Documents	about-3

Chapter 1 ENX Web-GUI

Introduction	1-1
Access to the Device	1-1
Security Issues	1-1
Web-Menu Body	1-2
Login Screen	1-2
Layout of Web-GUI	1-3
Navigation	1-4
Select a menu entry	1-4
Page Update	1-4
Logout	1-4
Status-Symbols (Error / Warning)	1-5
Usage of Commit Groups	1-5
Display and Change of Passwords	1-6
Rules for Passwords	1-8
Web-Menus of ENX	1-8
General System Information	1-10
Inventory	1-11
Administration	1-13
User and Access Administration	1-14
File Servers	1-17
Users and Passwords	1-20
SSH Access	1-25
SNMP Configuration	1-29
SNMP based SNMP parameter configuration	1-43
Port and IP Configuration	1-43
Edit Port Settings	1-46
Edit IP Settings	1-50
Diagnostics	1-55
Date and Time Settings	1-56
NTP Server Setup	1-59
Configuration Management	1-63
Recall Configuration Options ("Apply")	1-67
Firmware Update	1-69

Upload (http) and Download (xFTP) of new FW	1-69
Menu	1-70
Messages	1-73
Summary	1-74
Reset System	1-74
Self-Test	1-76
Alarm Management	1-77
System Alarm Group	1-78
Detailed Alarm Settings (Config)	1-80
EEC Alarm Group	1-81
Port Alarm Groups (LINE 1-2; LAN 1-4)	1-83
SFP Alarm Groups (LINE 1-2; LAN 1-4)	1-84
PTP Alarm Group	1-86
Active Alarm List	1-89
Ethernet Ports	1-89
Edit Ethernet Ports	1-91
VLAN	1-93
VLAN Unaware Mode	1-94
VLAN Aware Mode	1-95
Provider-Tagging Mode	1-99
Classification	1-102
VLAN Priority to Priority Sticker	1-104
DSCP Classification	1-105
Priority2Queue Mapping	1-107
MAC Table	1-108
MAC Settings	1-109
Policer	1-110
Ingress Limiter	1-110
Egress Shaper	1-114
Egress Queues	1-117
LACP	1-119
Port Group Details	1-120
LACP Aggregators	1-123
SFP Info	1-123
Counter	1-128
Operation and Maintenance	1-129
Ethernet First Mile	1-130
RMON Monitors	1-131
RMON Port Counters	1-132
RMON Counters History	1-133
RMON Alarms	1-134
RMON Events	1-136
Clock Configuration	1-137
Configuration of Internal TCXO and T3an	1-139
Configuration SyncE LINES	1-141

T3a/T4ab Configuration	1-143
IEEE1588 PTP Configuration	1-145
Master Port Configuration and Status	1-147
Slave Port Configuration and Status	1-149
Peer Delay Messages and notPeer Delay Messages	1-150
PTP Logging	1-150
Log View	1-152
Safe Log-Files	1-152

List of Figures

Figure 1-1	Login Screen	1-2
Figure 1-2	Web-GUI's Appearance	1-3
Figure 1-3	Web Main-menu ENX.	1-9
Figure 1-4	General System Information.	1-10
Figure 1-5	Inventory.	1-12
Figure 1-6	Administration.	1-13
Figure 1-7	User and Access Administration.	1-15
Figure 1-8	Example "Edit File Server": Firmware Store.	1-18
Figure 1-9	Users and Passwords.	1-20
Figure 1-10	Add New Account.	1-22
Figure 1-11	Modify Account.	1-24
Figure 1-12	SSH Access	1-25
Figure 1-13	SSH Password	1-27
Figure 1-14	SSH Password	1-29
Figure 1-15	SNMP Configuration, SNMP enabled.	1-30
Figure 1-16	SNMP Users and Community.	1-32
Figure 1-17	SNMPv2c Community	1-33
Figure 1-18	SNMPv3 User.	1-35
Figure 1-19	SNMPv3 Edit User Settings	1-36
Figure 1-20	SNMP Trap Configuration	1-39
Figure 1-21	Edit SNMP Trap Receiver	1-42
Figure 1-22	Port and IP Configuration	1-44
Figure 1-23	Port and IP Overview	1-45
Figure 1-24	Edit-Port-Settings, F/Q MGMT	1-47
Figure 1-25	Edit-Port-Settings, Inband MGMT	1-48
Figure 1-26	Table of LINE-Ports	1-49
Figure 1-27	Edit IP Settings (F/Q Port)	1-50
Figure 1-28	Edit IP Settings (Inband Port).	1-53
Figure 1-29	Diagnostics.	1-55
Figure 1-30	Date And Time Settings	1-56
Figure 1-31	NTP Server Setup	1-59
Figure 1-32	Edit NTP Server	1-61
Figure 1-33	Configuration Management w/o http-option	1-65
Figure 1-34	Configuration Management with http-option.	1-65

Figure 1-35	Recall Configuration	1-67
Figure 1-36	Firmware Update w/o http-option	1-70
Figure 1-37	Firmware Update with http-option	1-71
Figure 1-38	Reset System, @Specific Time	1-75
Figure 1-39	Self-Test	1-76
Figure 1-40	Alarm Management	1-77
Figure 1-41	System Alarm Group Management	1-79
Figure 1-42	Example Alarm Settings: Device Temperature	1-81
Figure 1-43	EEC Alarm Group Management	1-82
Figure 1-44	Port Alarm Group	1-84
Figure 1-45	SFP Alarm Group (LINE 1 SFP)	1-85
Figure 1-46	PTP Alarm Group Management	1-87
Figure 1-47	Active Alarm List	1-89
Figure 1-48	Ethernet Ports	1-90
Figure 1-49	Edit Ethernet Ports	1-91
Figure 1-50	VLAN Unaware Mode	1-94
Figure 1-51	VLAN Aware Mode	1-96
Figure 1-52	Edit Port VLAN Aware Settings	1-98
Figure 1-53	Provider-Tagging	1-100
Figure 1-54	Edit Port Provider-Tagging Settings	1-101
Figure 1-55	Classification	1-103
Figure 1-56	VLAN Priority to Prio Sticker	1-105
Figure 1-57	DSCP Classification	1-106
Figure 1-58	Priority2Queue Mapping	1-107
Figure 1-59	MAC Table	1-108
Figure 1-60	MAC Table	1-109
Figure 1-61	Ingress Limiter	1-110
Figure 1-62	Edit Ingress Limiter	1-111
Figure 1-63	Edit Specific Ingress Limiter	1-112
Figure 1-64	Egress Shaper	1-115
Figure 1-65	Egress Shaper Settings	1-116
Figure 1-66	Egress Queues	1-118
Figure 1-67	LACP	1-120
Figure 1-68	LACP Port Group Details	1-121
Figure 1-69	LACP Aggregators	1-123
Figure 1-70	SFP Info	1-124
Figure 1-71	SFP Details	1-125

Figure 1-72	SFP Diagnostics	1-127
Figure 1-73	Ethernet Counters	1-128
Figure 1-74	Operation and Maintenance	1-130
Figure 1-75	EFM	1-130
Figure 1-76	RMON Monitors	1-131
Figure 1-77	RMON Port Counter	1-132
Figure 1-78	RMON Counter Details	1-133
Figure 1-79	RMON Counter History	1-134
Figure 1-80	RMON Alarms	1-135
Figure 1-81	RMON Alarm Details	1-135
Figure 1-82	RMON Events	1-136
Figure 1-83	RMON Event Details	1-136
Figure 1-84	Clock Configuration	1-137
Figure 1-85	T3an Configuration	1-140
Figure 1-86	SyncE Configuration	1-142
Figure 1-87	T3an/T4ab Configuration	1-144
Figure 1-88	PTP Configuration	1-146
Figure 1-89	Master Port Configuration and Status	1-147
Figure 1-90	Slave Port Configuration and Status	1-149
Figure 1-91	PTP Logging	1-151
Figure 1-92	PTP Logging	1-151
Figure 1-93	Log View Example	1-152
Figure 1-94	Save Logfiles	1-153

List of Tables

Table 1-2	Submenus of Main-menu	1-9
Table 1-3	General System Information	1-11
Table 1-4	General System Information: Submenus	1-11
Table 1-5	Inventory	1-12
Table 1-6	Administration: Submenus	1-14
Table 1-7	User Administration	1-16
Table 1-8	Users and Passwords: Submenus	1-17
Table 1-9	Server Configuration	1-18
Table 1-10	TACACS+ Settings	1-21
Table 1-11	Users and Passwords	1-22
Table 1-12	Add Account	1-23
Table 1-13	Change Password	1-24
Table 1-14	SSH Access	1-26
Table 1-15	Submenus of SSH Access	1-26
Table 1-16	SSH User Definition	1-28
Table 1-17	SNMP Configuration	1-30
Table 1-18	SNMP Configuration: Submenus	1-31
Table 1-19	SNMPv2c Community Configuration	1-33
Table 1-20	SNMPv3 User	1-35
Table 1-21	SNMPv3 User Settings	1-36
Table 1-22	SNMPv3 Confidentiality	1-39
Table 1-23	SNMP Trap Configuration	1-40
Table 1-24	Edit SNMP Trap Receiver	1-42
Table 1-25	Port and IP-Configuration	1-44
Table 1-26	Port and IP-Configuration	1-45
Table 1-27	Port Configuration	1-47
Table 1-28	Port and IP-Configuration	1-49
Table 1-29	IP-Port Configuration	1-50
Table 1-30	IP-Port Configuration	1-53
Table 1-31	Date and Time Settings	1-57
Table 1-32	NTP Server Status	1-57
Table 1-33	NTP Server Setup	1-59
Table 1-34	Edit NTP Server	1-61
Table 1-35	Configuration Management	1-66

Table 1-36	Recall Configuration	1-68
Table 1-37	Firmware Update	1-71
Table 1-38	Reset System	1-75
Table 1-39	Alarm Management.	1-78
Table 1-40	System Alarm Group Management.	1-79
Table 1-41	EEC Alarm Group Management	1-82
Table 1-42	Port Alarm Group	1-84
Table 1-43	SFP Alarm Group	1-85
Table 1-44	PTP Alarm Group Management	1-87
Table 1-45	Ethernet Port.	1-90
Table 1-46	Edit Ethernet Port	1-91
Table 1-47	VLAN Unaware	1-95
Table 1-48	VLAN Aware	1-96
Table 1-49	VLAN Aware Overview Table	1-97
Table 1-50	Edit Port VLAN Aware Settings.	1-98
Table 1-51	Provider-Tagging.	1-100
Table 1-52	Provider Tagging Overview Table	1-100
Table 1-53	Edit Port Provider-Tagging	1-102
Table 1-54	Classification.	1-103
Table 1-55	VLAN Priority to Prio Sticker	1-105
Table 1-56	DSCP Classification	1-106
Table 1-57	VPriority2Queue Mapping	1-108
Table 1-58	MAC Table	1-109
Table 1-59	MAC Settings	1-110
Table 1-60	Edit Specific Ingress Limiter	1-112
Table 1-61	Egress Shaper	1-116
Table 1-62	Egress Queues	1-119
Table 1-63	SFP Details.	1-125
Table 1-64	SFP Diagnostics	1-127
Table 1-65	Ethernet Counters.	1-129
Table 1-66	RMON Parameters	1-132
Table 1-67	Clock Configuration.	1-138
Table 1-68	Clock Source Table.	1-139
Table 1-69	TCXO & T3an Configuration	1-140
Table 1-70	Sync-E LINE Configuration	1-142
Table 1-71	T3an/T4ab.	1-144
Table 1-72	T3an/T4ab.	1-146

Table 1-73	Master Port Configuration and Status	1-148
Table 1-74	Slave Port Configuration and Status	1-149
Table 1-75	PTP Multicast MAC Addresses	1-150
Table 1-76	Configuration of Log-Files	1-153

Chapter 1

ENX Web-GUI

The ENX 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.

Introduction

Access to the Device

The ENX Web-GUI can be accessed via the both management ports (out-of-band “F/Q” and in-band management 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 user-name and password. Any not successful attempt to login to the device is stored in the log-file and a trap can be configured to inform higher level management system about this.

Any time you connect or reconnect to the initialized ENX 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 1-14, how to define additional users and how to change the user passwords.

Web-Menu Body

Login Screen

After a management connection has been established towards the ENX, 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.



The screenshot shows the Arcutronix ENX web interface. At the top left is the Arcutronix logo with 'arcutronix ENX' below it. At the top right, there is a warning icon followed by the text 'ENX-F: ENX-F' and 'Serial: 2012010114'. Below a red horizontal line, there are two input fields: 'User Name' and 'Password'. Below the 'Password' field is a blue 'Login' button.

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 entry of strings is case-sensitive.

Layout of Web-GUI

After Login, the ENX 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 in 6 major parts, which are shown in the next figure and will be explained a little bit after this.

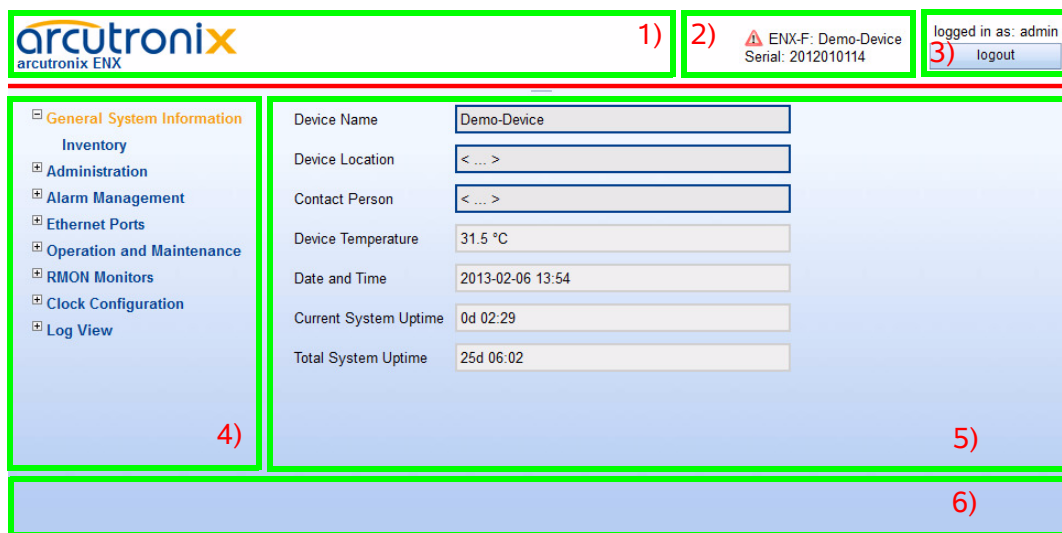


Figure 1-2 Web-GUI's Appearance



1. Logo/Family Pane.
2. Info Pane: Information about
 - device-type (here ENX-F),
 - device-name (here Demo-Device),

- serial number,
 - and alarm status (status icon, see “Status-Symbols (Error / Warning)” on page 1-5).
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. 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 terminating the session and leave the unit. Never forget to log-out, as otherwise unauthorized persons could get access to the unit and damage your services.

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





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 (Error / Warning)

On top-right of the web-GUI the status of the device is depicted. A status symbol is shown in case there is a problem detected on the device. If there is no icon to see, all is fine and the system 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.
	1	Warning-Acknowledged Symbol. The device has at least one alarm, which is already acknowledged by user.

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.

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,

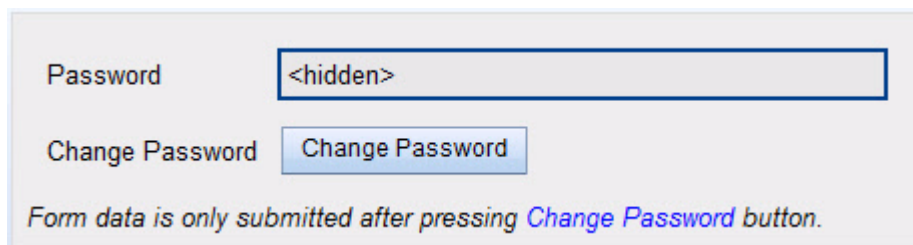
- ...

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.

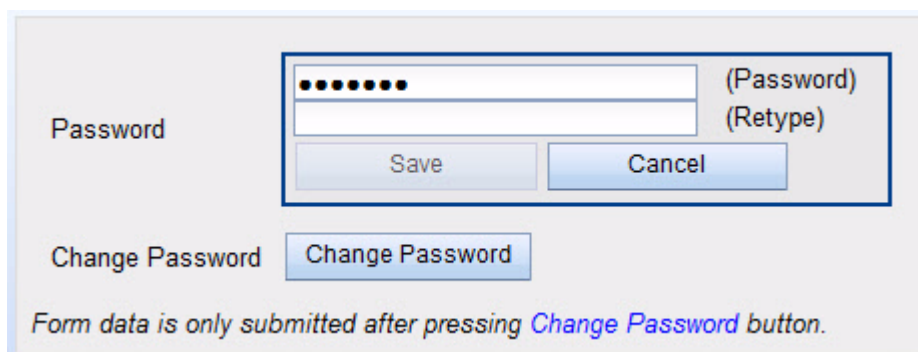
For security reason, the Web-GUI will never display passwords as clear text, but always in a hidden manner. The text <hidden> is shown:



The screenshot shows a form with a label 'Password' next to a text input field containing the text '<hidden>'. Below this is a label 'Change Password' next to a blue button labeled 'Change Password'. At the bottom of the form, there is a note: 'Form data is only submitted after pressing *Change Password* button.'

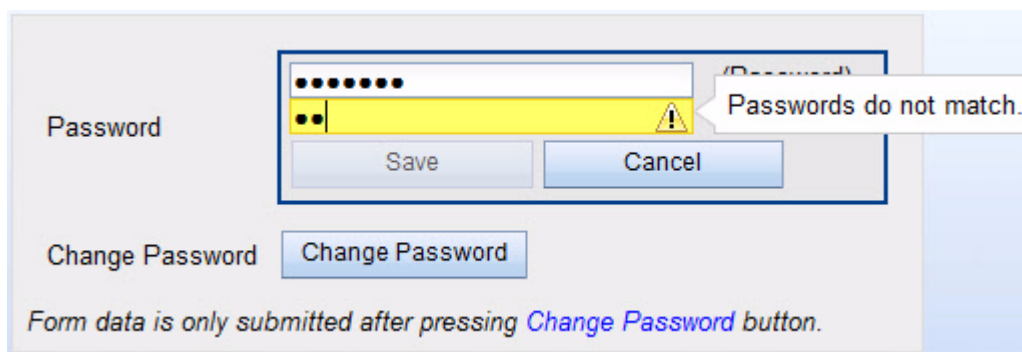
So please make sure, you note your password, as you will not have the chance to see it in the Web-GUI.

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:



The screenshot shows a form with a label 'Password' next to a text input field containing seven dots. To the right of the field are the labels '(Password)' and '(Retype)'. Below the field are two buttons: 'Save' and 'Cancel'. Below this is a label 'Change Password' next to a blue button labeled 'Change Password'. At the bottom of the form, there is a note: '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:

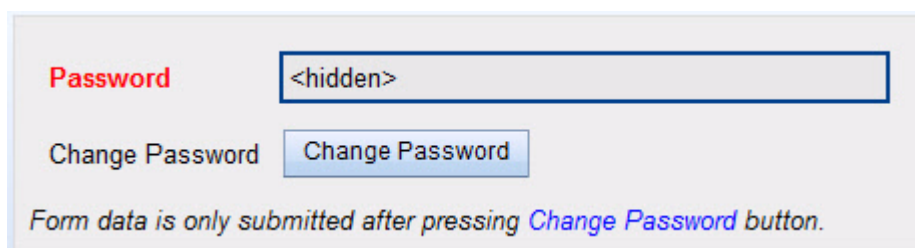


The screenshot shows a web form for changing a password. It features two password input fields, one above the other. The top field contains a series of black dots. The bottom field contains two black dots and a yellow background with a warning icon. A tooltip above the bottom field reads "Passwords do not match." Below the input fields are "Save" and "Cancel" buttons. Below these is a "Change Password" button. At the bottom of the form, it says "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:

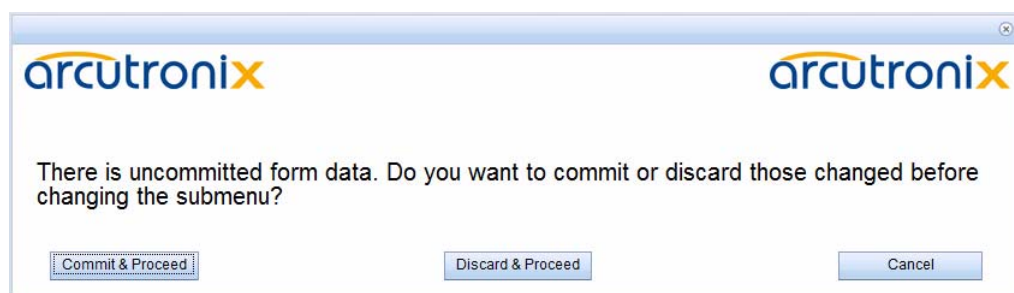


The screenshot shows the same password change form as above. The "Password" label is now in red. The input field contains the text "<hidden>". The "Change Password" button is still present. At the bottom, it says "Form data is only submitted after pressing *Change Password* button."

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.



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 unpredictability and this is verified by several security rules. If a new password does not fulfil this rules, it will be not accepted by the ENX. 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.

Web-Menus of ENX

The main view of the ENX is the top-level. From here all other (sub-)menus can be entered. It provides a general overview of the menu structure.

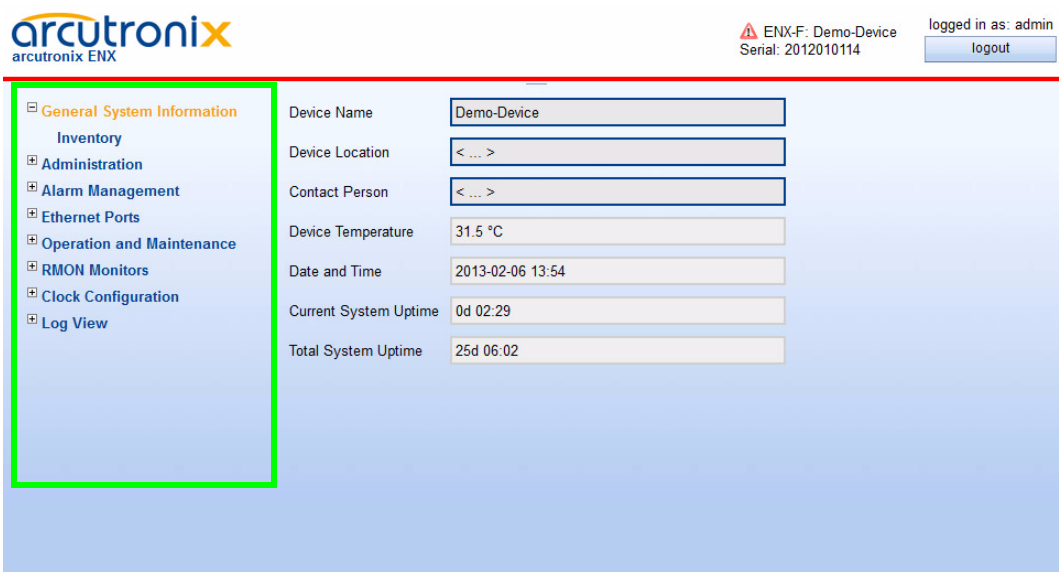


Figure 1-3 Web Main-menu ENX

Select a menu line in the Navigation Pane to open the selected submenu or to logout from the ENX' 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.
Ethernet Ports	Within this menu, all settings for the "payload"-ports (LAN- and LINE-ports) can be done. The out-of-band management port (F/Q) is not part of this menu.
Operation and Maintenance	This menu gives access to the OAM (Operation, Administration and Maintenance) settings of the device. For the time being, only EFM (Ethernet First Mile, IEEE 802.3ah) is supported.
RMON Monitors	This menu gives access to the configuration of various RMON features. All the different counters and alarms as defined in RMON-MIB.

Table 1-2 Submenus of Main-menu (continued)

Submenu	Description
Clock Configuration	The clock configuration menu allows the set up of the SyncE and PTP behaviour of the device. Clock sources for SyncE can be configured and the criteria for acceptance of SyncE clocks can be defined.
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 menu. The following will be displayed:

The screenshot shows the ENX Web-GUI interface. At the top left is the Arcutronix logo. At the top right, it says "ENX-F: Demo-Device Serial: 2012010114" and "logged in as: admin" with a "logout" button. The left navigation pane has several items: "General System Information" (highlighted in orange), "Inventory", "Administration", "Alarm Management", "Ethernet Ports", "Operation and Maintenance", "RMON Monitors", "Clock Configuration", and "Log View". The main content area displays the following information:

Device Name	Demo-Device
Device Location	< ... >
Contact Person	< ... >
Device Temperature	31.5 °C
Date and Time	2013-02-06 13:54
Current System Uptime	0d 02:29
Total System Uptime	25d 06:02

Figure 1-4 General System Information

This menu contains the general system information of the ENX device and system. Table 1-3 provides information about the options.

Table 1-3 General System Information

Parameter	Description	Format	Default
Device Name	Description/comment of the device.	Display/Input (up to 32 characters)	ENX-F
Device Location	Description/comment of the device.	Display/Input (up to 32 characters)	< ... >
Contact Person	Description/comment of the device.	Display/Input (up to 32 characters)	< ... >
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
Current System Uptime	The time since the last system reboot.	Display	no default
Total System Uptime	Overall sum of system up-time.	Display	no default

The following submenu is 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.

Inventory

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

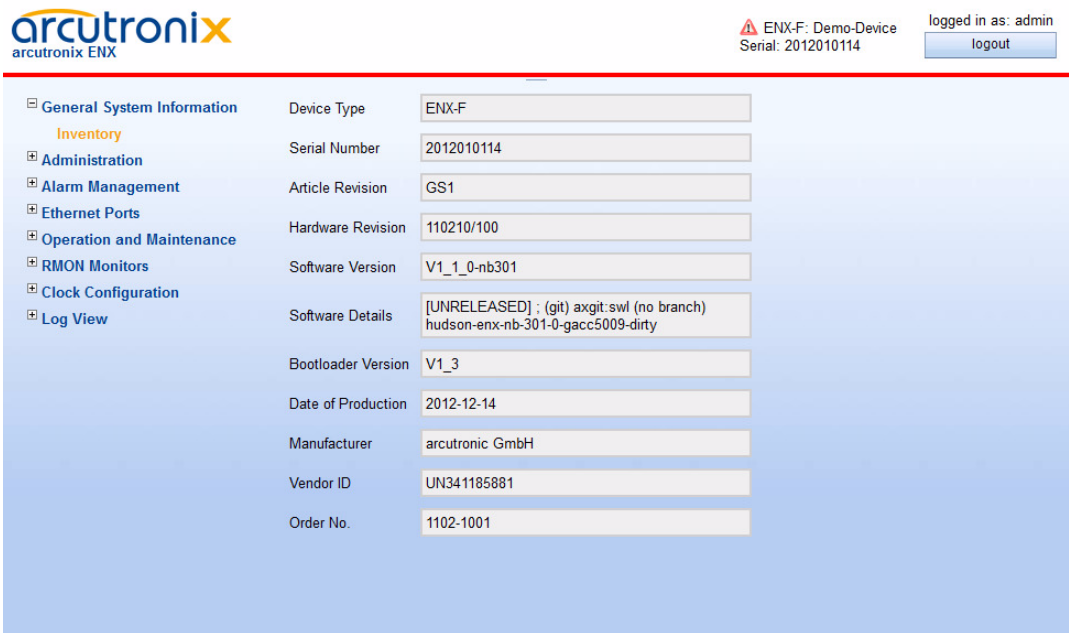


Figure 1-5 Inventory

Table 1-5 provides information about the content.

Table 1-5 Inventory

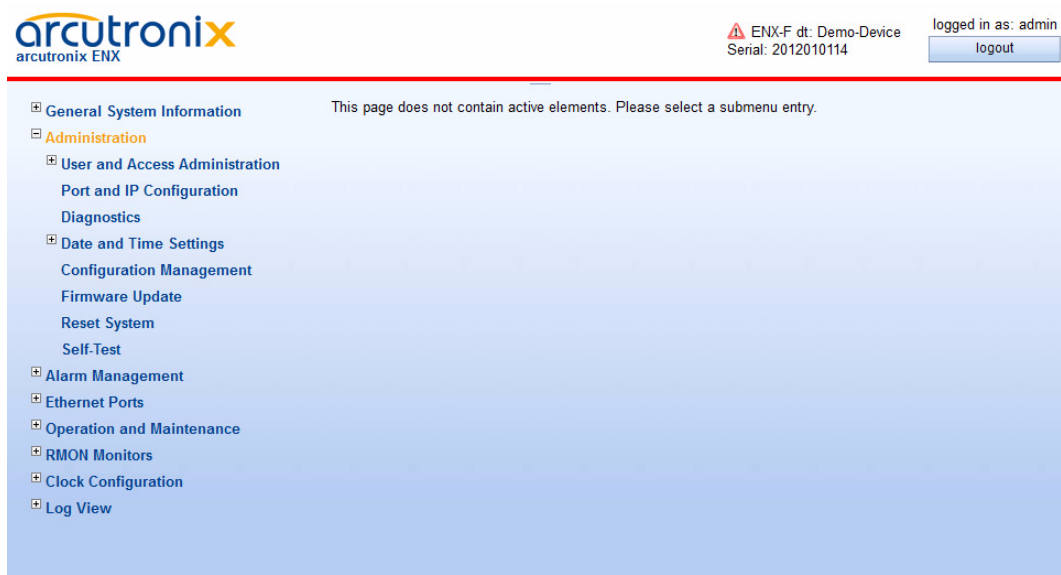
Parameter	Description	Format	Default
Device Type	Indicates the device type.	Display	ENX-F
Serial Number	Serial number of the device.	Display	Depends on the factory settings
Article Revision	The release number of the device.	Display	Depends on the factory settings
Hardware Version	The release number of 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

Table 1-5 Inventory (continued)

Parameter	Description	Format	Default
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 Number	Order information for the device.	Display	Depends on the device's type. See Order Matrix (Table 1-1 of [axManualENX]).

Administration

Select “Administration” in the Navigation Pane and the Administration menu will be displayed. This menu allows configuring the general device settings.

**Figure 1-6** Administration

The following submenus are available:

Table 1-6 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.
Firmware Update	This menu allows firmware updates to be performed.
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:

arcutronix
arcutronix ENX

ENX-F dt: Demo-Device
Serial: 2012010114

logged in as: admin
logout

General System Information
Administration
User and Access Administration
Users and Passwords
SSH Access
SNMP Configuration
Port and IP Configuration
Diagnostics
Date and Time Settings
Configuration Management
Firmware Update
Reset System
Self-Test
Alarm Management
Ethernet Ports
Operation and Maintenance
RMON Monitors
Clock Configuration
Log View

Auto Logoff Time [min] 15

HTTP Access Enabled
HTTP File Transfer Disabled
SSH CLI Access Enabled
CONS CLI Access Enabled
SNMP Access Enabled

Server	URI	Valid	Edit
Firmware Store	stfp://andreas@192.168.1.1:23/	Valid	Edit
Configuration Store	stfp://andreas@192.168.1.1/	Valid	Edit
Logfile Store	Not Valid	Not Valid	Edit

Figure 1-7 User and Access Administration

The menu gives a quick overview and configuration option for the different ways of access to the unit. Five 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, 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-log-off is disabled for all logins. For more details about the auto-logoff feature please refer to chapter “Auto-Logout” in [axManualENX].

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

Table 1-7 provides all information on the menu options.

Table 1-7 *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
HTTP Access	Enable or Disable the management access via HTTP (Web-GUI).	PullDown-Menu <ul style="list-style-type: none"> • Disabled • Enabled 	Enabled
HTTP File Transfer	Enable or Disable the file transfer via HTTP (Web-GUI).	PullDown-Menu <ul style="list-style-type: none"> • Disabled • Enabled 	Disabled
SSH CLI Access	Enable or Disable the management access via SSH.	PullDown-Menu <ul style="list-style-type: none"> • Disabled • Enabled 	Enabled
CONS CLI Access	Enable or Disable the management access CONSOLE port (115200, 8N1).	PullDown-Menu <ul style="list-style-type: none"> • Disabled • Enabled 	Enabled
SNMP Access	Enable or Disable the management access via SNMP.	PullDown-Menu <ul style="list-style-type: none"> • Disabled • Enabled 	Enabled
Firmware Store	SFTP or TFTP settings for firmware download server. See chapter "File Servers" on page 1-17 for details.	Menu / Display	

Table 1-7 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 1-17 for details.	Menu / Display	
Logfile Store	SFTP or TFTP server settings to upload log-files. See chapter “File Servers” on page 1-17 for details.	Menu / Display	

The following submenus are available:

Table 1-8 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+).
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” in [axManualENX] 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.



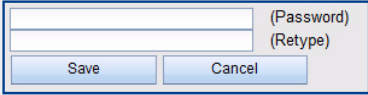

Figure 1-8 Example “Edit File Server”: Firmware Store

Table 1-9 provides information about the options.

Table 1-9 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	IPv4 address for the FTP server.	IPv4-Address	0.0.0.0

Table 1-9 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, deposited 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 ENX is 99.

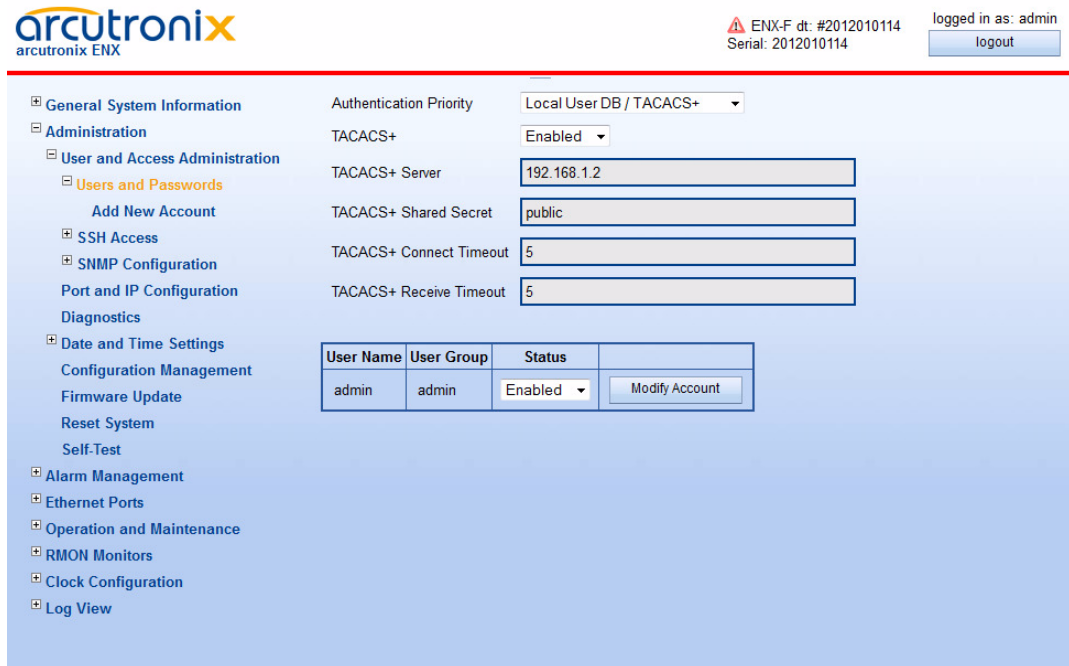


Figure 1-9 Users and Passwords

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 [axManualENX] for details about TACACS+ and the settings.

Table 1-11 provides information about the options.

Table 1-10 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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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 IPv4-address of the TACACS+ server	IPv4-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 1-11 provides information about the options.

Table 1-11 *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:

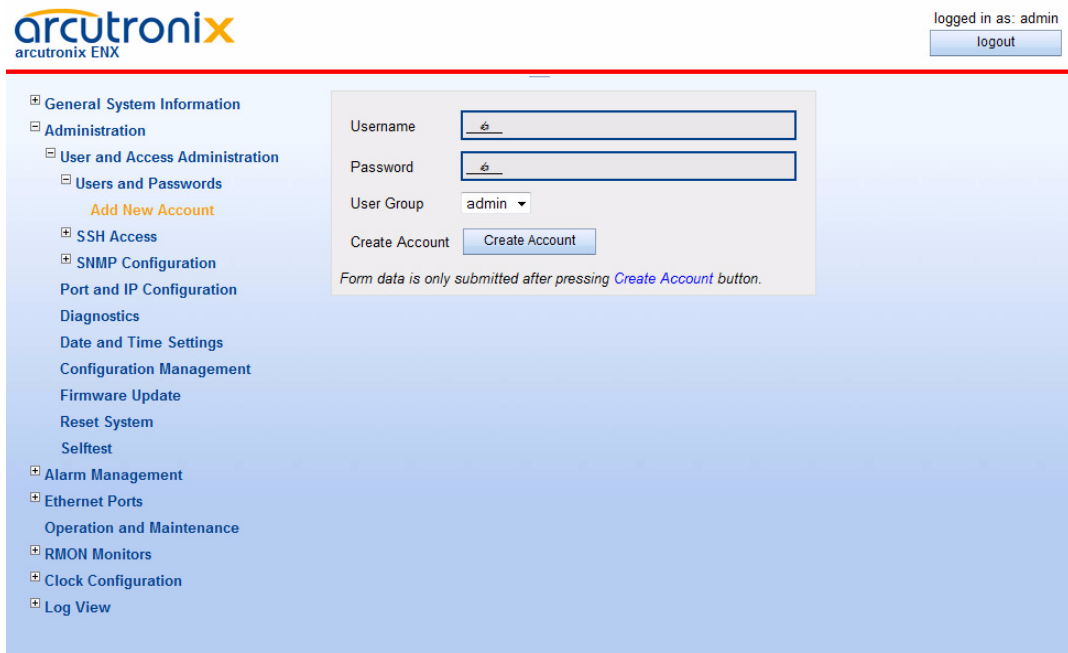
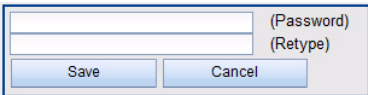
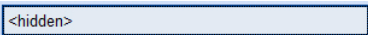


Figure 1-10 *Add New Account*

Table 1-12 provides information about the options.

Table 1-12 Add Account

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

ii. For passwords special rules are in force, which are depicted in "Rules for Passwords" of [axManualENX].

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!

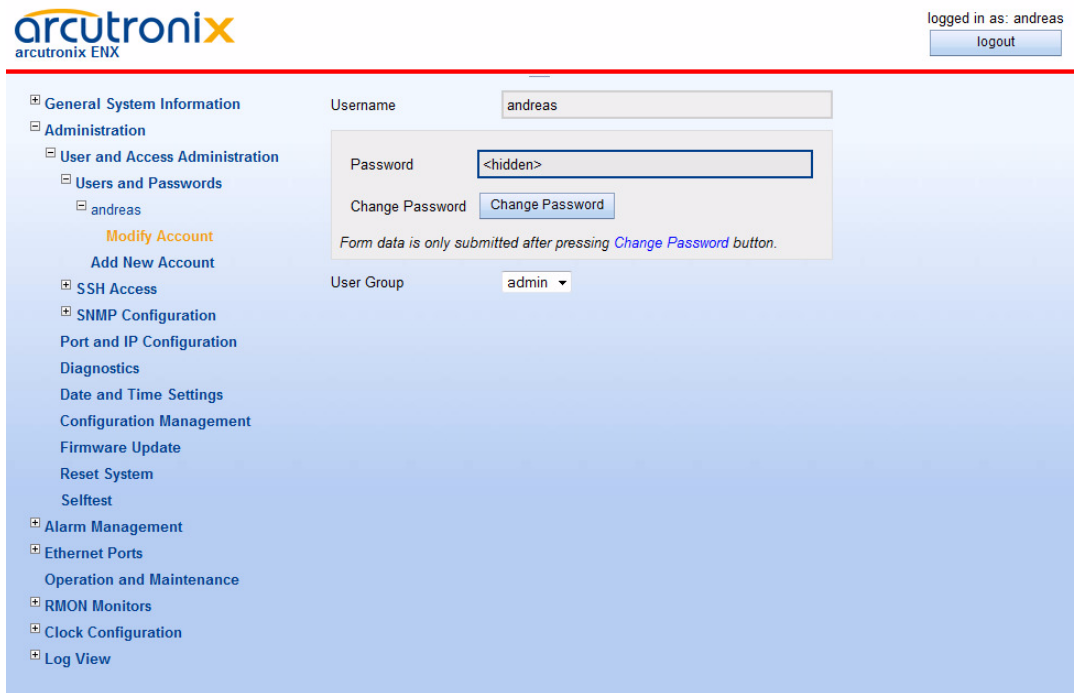
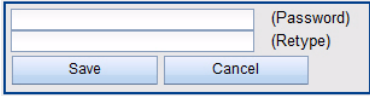



Figure 1-11 Modify Account

Table 1-13 provides information about the options.

Table 1-13 Change Password

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

- i. Only visible, if the logged-in user is the same as the selected one modifying.
- ii. Only visible, when the selected account is NOT the default ADMIN-account.

Note: 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.

SSH Access

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

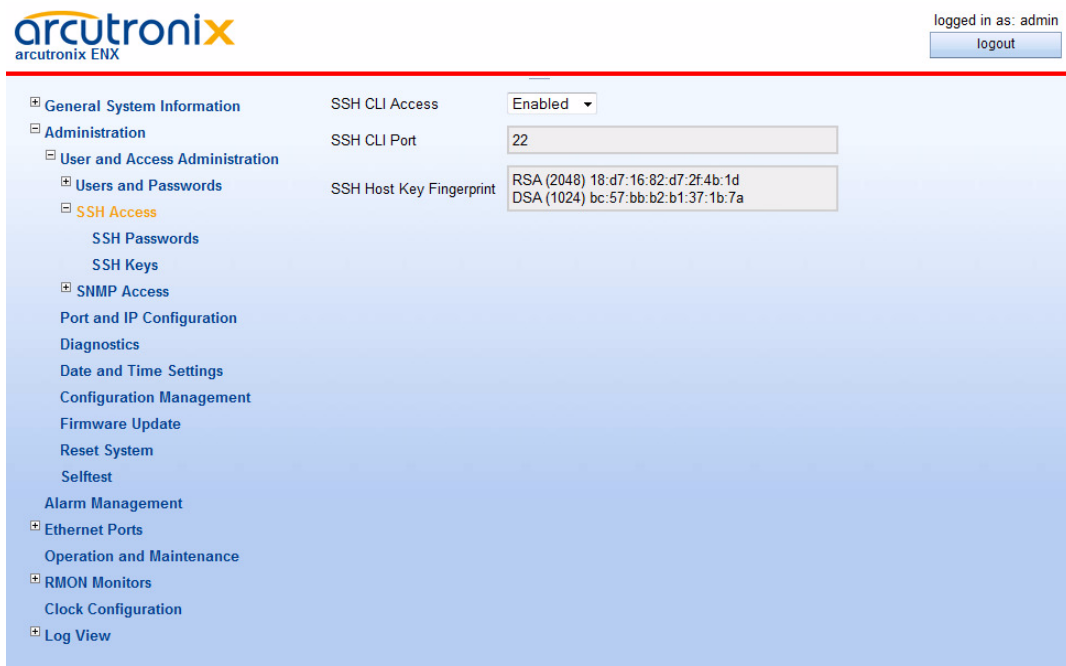


Figure 1-12 SSH Access

Table 1-15 provides information about the options.

Table 1-14 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 1-15 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 configuring 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 1-17).
- 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!

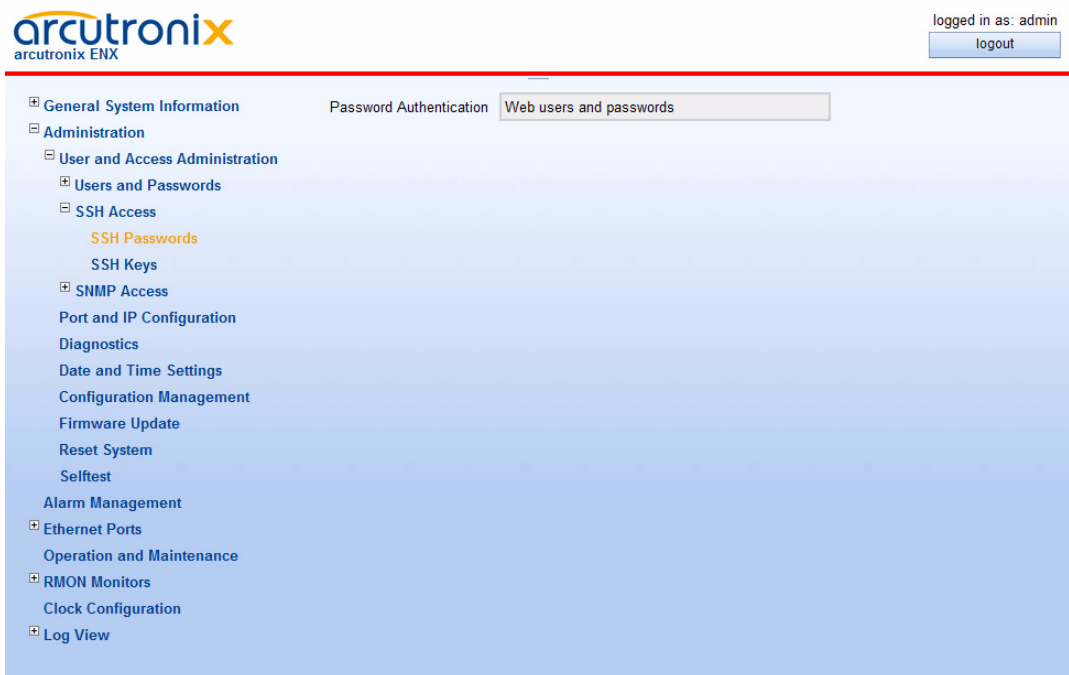
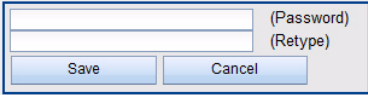



Figure 1-13 SSH Password

Table 1-16 provides information about the menu.

Table 1-16 SSH User Definition

Parameter	Description	Format	Default
Password Authentication	<p>Pulldown Menu to select the how to authenticate at the SSH server (ENX).</p> <p>For details on the possible option see [axRefGuideCLI].</p> <p>Note: The value can only be changed, when the SSH-access is disabled.</p>	<p>PullDown Menu</p> <ul style="list-style-type: none"> • "Password authentication disabled" • "Web users and passwords" • "Use global SSH connection password" 	"Web users and passwords"
Global Access Password	<p>Here one can define a global SSH-user(name) and his global SSH-password. Define this, when "Use global SSH connection password" is selected in the line above.</p> <p>The password must be entered twice for verification. Please retype it in the bottom field:</p>  <p>If a valid password is stored on the device, it will be shown as <hidden> to avoid phishing:</p> 	Input	empty

SSH Keys

This menu offers the possibility to upload a SSH key via file-transfer. The file with the SSH-key can be either 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 1-17) 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 ENX expects that the filename's extension is "*.pub".

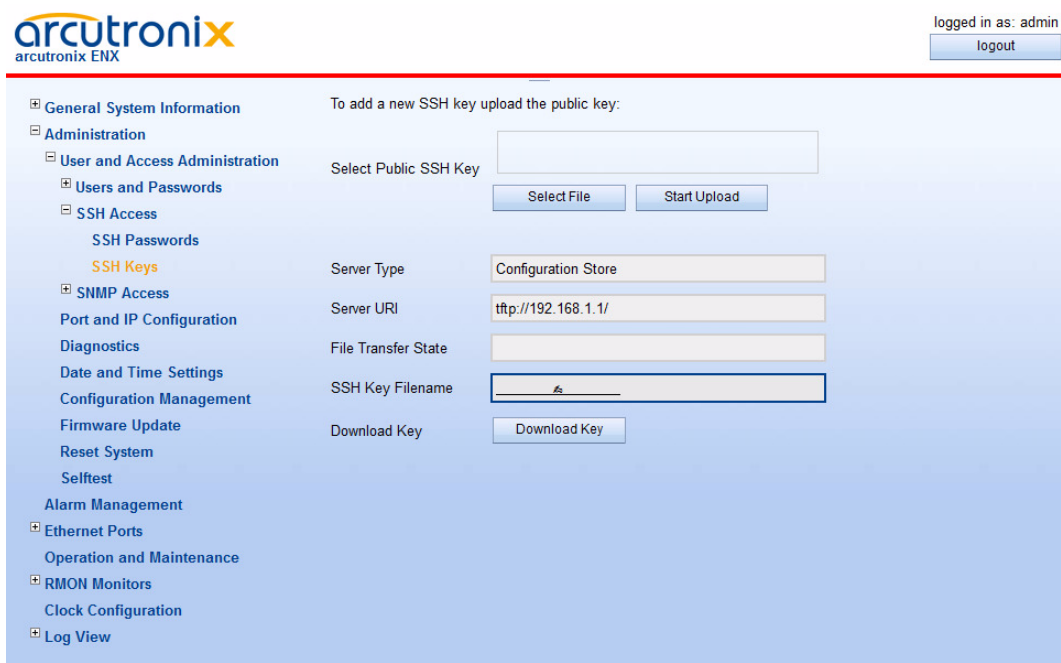


Figure 1-14 SSH Password

SNMP Configuration

This menu offers the possibility configuring 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.



Figure 1-15 SNMP Configuration, SNMP enabled

Table 1-17 provides information about the options.

Table 1-17 SNMP Configuration

Parameter	Description	Format	Default
SNMP Access	Enables or disables the SNMP access.	PullDown Menu <ul style="list-style-type: none"> • Disabled • Enabled 	Enabled
SNMP Version	Select the SNMP version to be used	PullDown Menu <ul style="list-style-type: none"> • SNMP v2c • SNMPv3 • SNMPv2c & v3 	SNMPv2c & v3
SNMP UDP Port	Enter the UDP-Port to be used for SNMP-Traps. (1-65535)	Port-Number	161
SNMP Max Message Size	Maximum numbers of data transferred within a get-bulk request.	Integer	484

Table 1-17 *SNMP Configuration (continued)*

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

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 1-18 *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 1-14).

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.

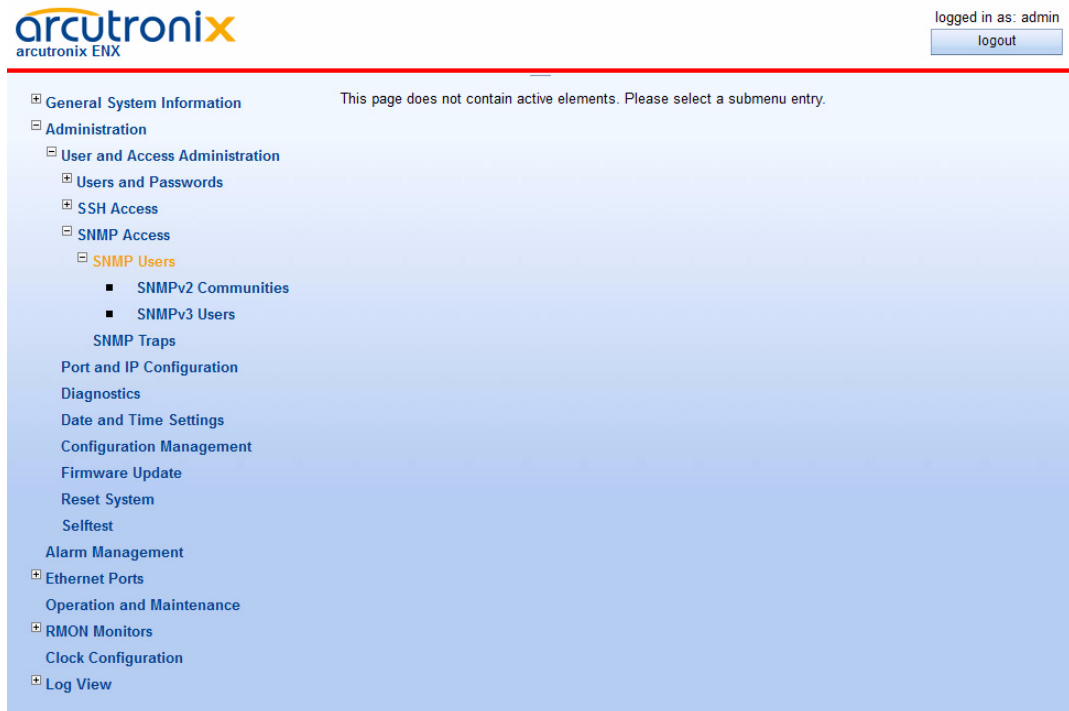


Figure 1-16 *SNMP Users and Community*

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.

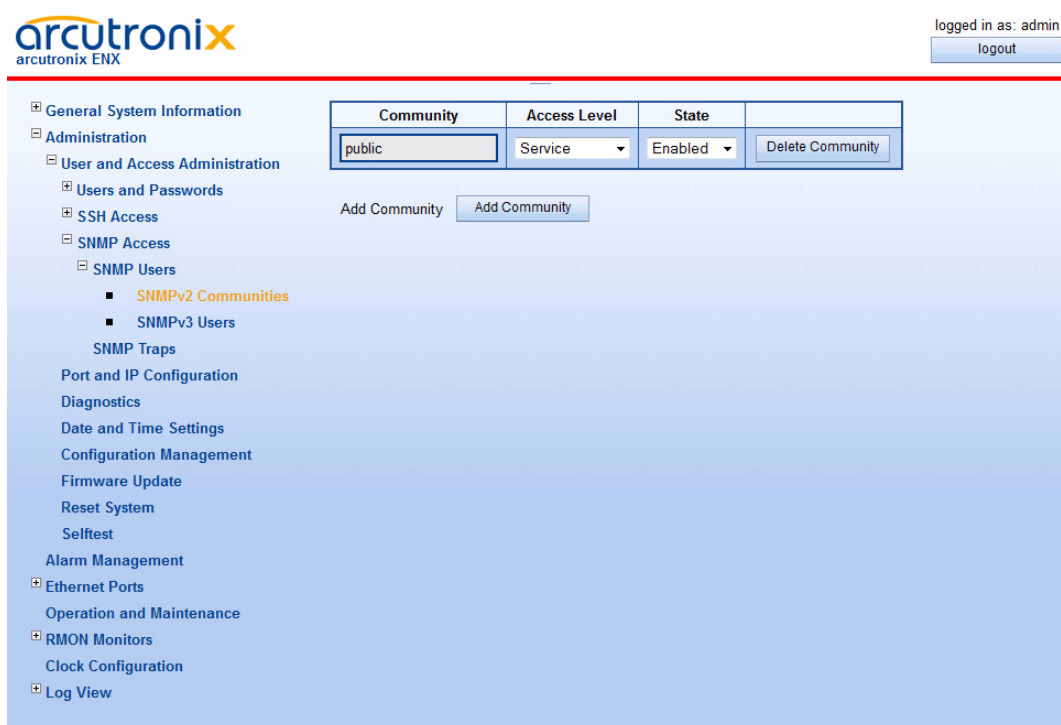


Figure 1-17 SNMPv2c Community

Table 1-19 provides information about the options.

Table 1-19 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 <ul style="list-style-type: none"> • Administrator • Service • Monitor 	Service
State	Enable / disable the community.	PullDown Menu <ul style="list-style-type: none"> • Enabled • Disabled 	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.

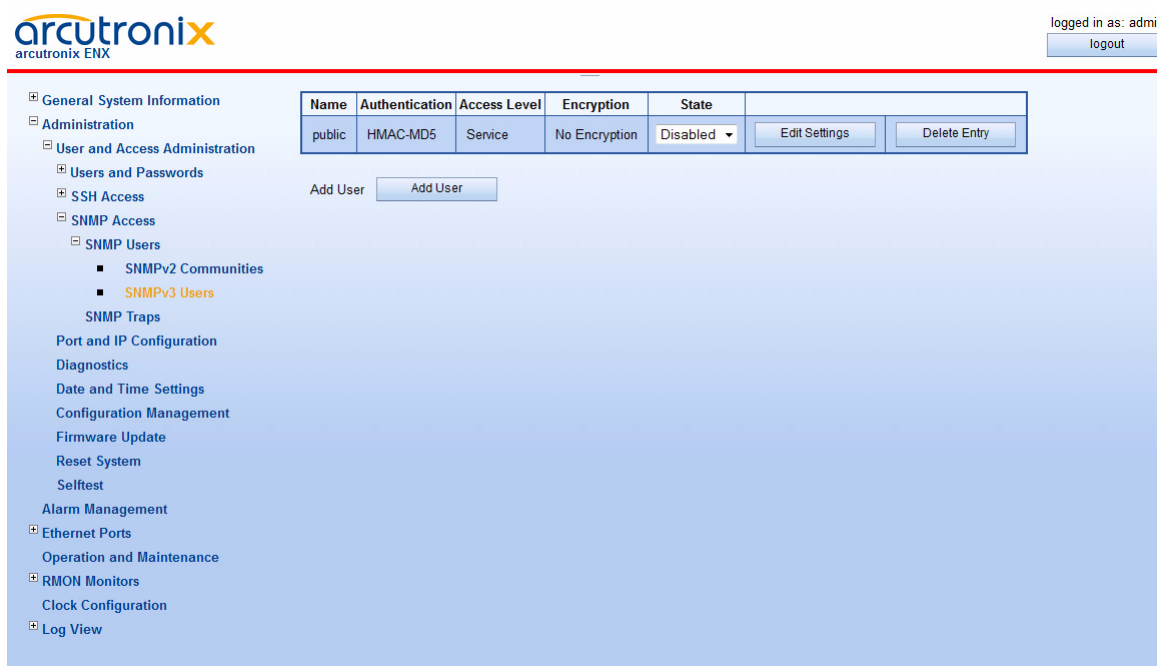


Figure 1-18 SNMPv3 User

Table 1-20 provides information about the options.

Table 1-20 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 1-21.

The screenshot shows the ENX Web-GUI interface. At the top left is the 'arcutronix' logo. At the top right, it says 'logged in as: admin' with a 'logout' button. The left sidebar contains a navigation menu with categories like 'General System Information', 'Administration', 'User and Access Administration', 'SNMP Access', 'SNMP Users', 'SNMPv2 Communities', 'SNMPv3 Users', 'SNMP Traps', 'Port and IP Configuration', 'Diagnostics', 'Date and Time Settings', 'Configuration Management', 'Firmware Update', 'Reset System', 'Selftest', 'Alarm Management', 'Ethernet Ports', 'Operation and Maintenance', 'RMON Monitors', 'Clock Configuration', and 'Log View'. The 'Edit Settings' option under 'SNMPv3 Users' is highlighted. The main content area displays a configuration form for an SNMPv3 user. The form includes the following fields: 'User Name' (text input with 'public'), 'Access Level' (dropdown menu with 'Service'), 'Authentication Type' (dropdown menu with 'No Authentication'), 'Authentication Passphrase' (password input with '<hidden>'), 'Encryption Type' (dropdown menu with 'No Encryption'), 'Encryption Passphrase' (password input with 'a'), 'Status' (dropdown menu with 'Enabled'), and an 'Apply' button. Below the form, a note reads: 'Form data is only submitted after pressing Apply button.'

Figure 1-19 SNMPv3 Edit User Settings

Table 1-21 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 <ul style="list-style-type: none"> • Administrator • Service • Monitor 	Service

Table 1-21 SNMPv3 User Settings (continued)

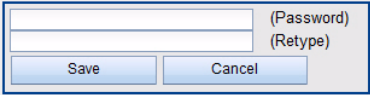

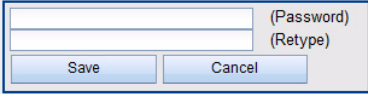

Parameter	Description	Format	Default
Authentication Type	This settings determines the authentication method to use for authenticating messages of this user. It is shown in the "Passphrase" column of the user list.	PullDown Menu <ul style="list-style-type: none"> • No Authentication • HMAC-MD5 • HMAC-SHA 	HMAC-MD5
Authentication Passphrase	<p>When the authentication method is set to "Passphrase (MD5)" or "Passphrase (SHA1)", enter the user's password here. The password will be used to generate an authentication key according to [IETF RFC 3414].</p> <p>The passphrase must be entered twice for verification. Please retype it in the bottom field:</p>  <p>If a valid passphrase is stored on the device, it will be shown as <hidden> to avoid phishing:</p> 	string	empty
Encryption Type	This setting determines whether to accept encrypted SNMP messages of this user and which encryption algorithm is in use (DES/AES).	PullDown Menu <ul style="list-style-type: none"> • No Encryption • DES Encryption • AES Encryption 	No Encryption

Table 1-21 SNMPv3 User Settings (continued)

Parameter	Description	Format	Default
Encryption Passphrase	<p>When the encryption algorithm is set to DES or AES encryption, enter the password for message decryption here. The password will be used to generate a decryption key according to [IETF RFC 3414].</p> <p>The passphrase must be entered twice for verification. Please retype it in the bottom field:</p> 	string	empty
	<p>If a valid passphrase is stored on the device, it will be shown as <hidden> to avoid phishing:</p> 		
Status	<p>When Status is set to Disabled, no messages in behalf of this user will be accepted.</p>	PullDown Menu <ul style="list-style-type: none"> • Enabled • Disabled 	Disabled
Apply	<p>The changes can be made permanent using the “Apply” button.</p> <p>If you do not want to confirm your settings, just press the “Back” button in your web browser.</p>		

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

Table 1-22 *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.

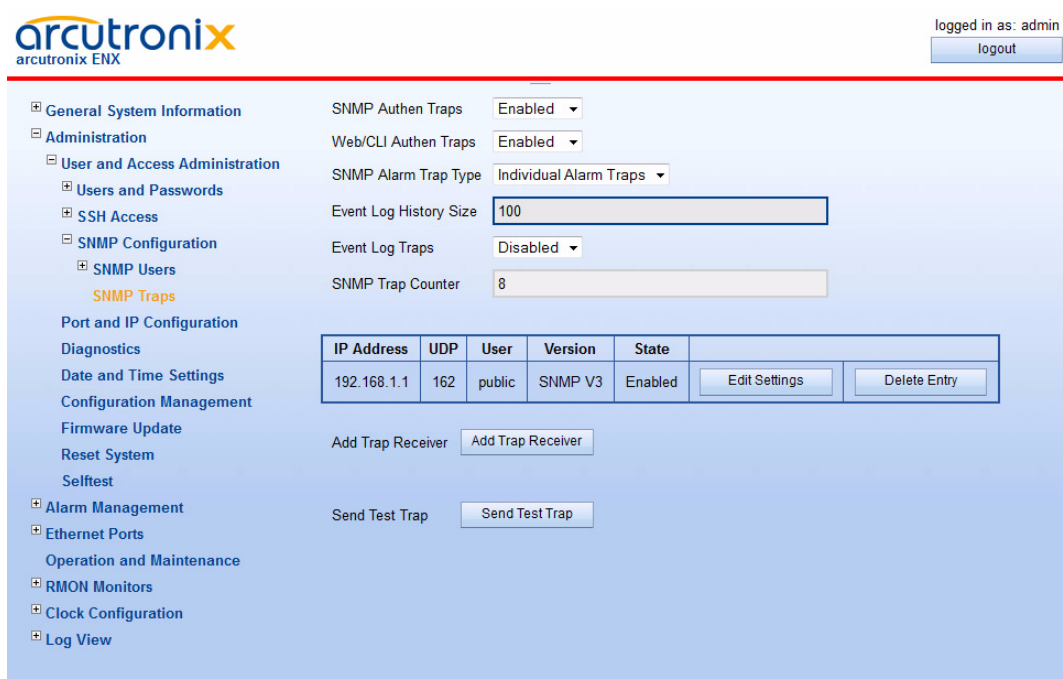


Figure 1-20 *SNMP Trap Configuration*

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 1-23):

Table 1-23 *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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • Disabled • Enabled 	Enabled
SNMP Trap Counter	Counter of all outgoing (sent) enterprise traps.	Display	0

Table 1-23 *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:

The screenshot shows the Arcutronix ENX web interface. In the top right corner, it says "logged in as: admin" with a "logout" button. The left sidebar contains a tree view of system settings, including "General System Information", "Administration", "User and Access Administration", "SSH Access", "SNMP Access", "SNMP Users", "SNMP Traps", "Port and IP Configuration", "Diagnostics", "Date and Time Settings", "Configuration Management", "Firmware Update", "Reset System", "Selftest", "Alarm Management", "Ethernet Ports", "Operation and Maintenance", "RMON Monitors", "Clock Configuration", and "Log View". Under "SNMP Traps", the IP address "192.168.1.1" is listed, and an "Edit Settings" button is visible. The main configuration area on the right has the following fields:

- IP Address: 192.168.1.1
- UDP Port: 162
- Security Name: public
- SNMP Version: SNMP V3
- Status: Enabled

Figure 1-21 Edit SNMP Trap Receiver

Table 1-24 provides information about the options.

Table 1-24 Edit SNMP Trap Receiver

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

Table 1-24 Edit SNMP Trap Receiver (continued)

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

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

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

SNMP based SNMP parameter configuration

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

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

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

for which full support is available.

Port and IP Configuration

Use this menu configuring the IP parameters and the physical settings of the two management ports:

- Out-of-band F/Q interface (called “F/Q MGMT”),
- In-band Management port (called “Inband MGMT”).

See “IP-Addressing” in [axManualENX] for details about F- and Q-interface and in-band Management port.

Figure 1-22 Port and IP Configuration

Table 1-25 provides information about the options.

Table 1-25 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)
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 (Ethernet) ports is given.

Name	AdminStatus	Link	Type	Mech.	Address	Edit	
F/Q MGMT < ... >	Enabled ▾	Link Up	Local Mgmt (F)	RJ45	Manual 192.168.1.100/24	Edit Port Settings	Edit IP Settings
Inband MGMT < ... >	Enabled ▾	Link Down	Inband Mgmt (Q)	Virtual	DHCP Unassigned Vlan 4094	Edit Port Settings	Edit IP Settings

Figure 1-23 Port and IP Overview

Table 1-25 provides information about the table rows and columns.

Table 1-26 Port and IP-Configuration

Parameter	Description	Format	Default
Name	Name of the management port.	Display	F/Q MGMT or Inband MGMT
Admin Status	The status of the port is shown. If required it can be disabled here.	Display	Enabled
Link	Indicator, whether the Ethernet link is established or not.	Display	
Type	The physical and logical type of the interface. Physique: <ul style="list-style-type: none"> • RJ45 or • Virtual. Logical: <ul style="list-style-type: none"> • Local Management in F mode, • Remote Management in Q mode or • Inband Management (always Q). The logical status of the interface can be configured in the “Edit IP Settings” submenu.	Display	
Mech.	Information about the mechanical (physical) type of the ports: <ul style="list-style-type: none"> • RJ45 = electrical 10/100BaseT, • Virtual = VLAN separated via LINE ports. 	Display	F/Q MGMT: RJ45 Inband MGMT: Virtual

Table 1-26 Port and IP-Configuration (continued)

Parameter	Description	Format	Default
Address	The host address of the interface and the setting for IP-address assignment. The address-settings of the interface can be configured in the "Edit IP Settings" submenu.	Display	-
Edit Port Settings	Press the "Edit Port Settings" to change the HW settings of a port.	Submenu	-
Edit IP Settings	Press the "Edit IP Settings" to change the IP settings of a 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 Port Settings

Use this menu to change the HW-settings and behaviour of the ports. The menus for the different ports (out-of-band and in-band) are different, as the in-band port is a virtual port, basing on ALL LINE-ports. For this reason, the options and menu can not be the same.

F/Q MGMT

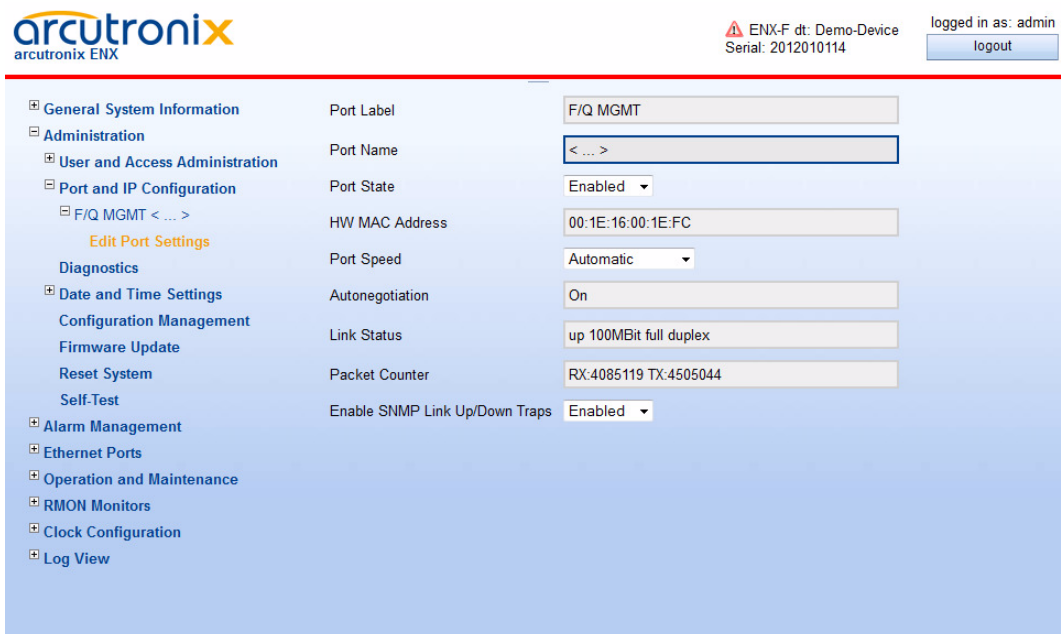


Figure 1-24 Edit-Port-Settings, F/Q MGMT

Table 1-27 provides information about the options.

Table 1-27 Port Configuration

Parameter	Description	Format	Default
Port Label	Printed text on the enclosure and front-plate.	Display	F/Q MGMT
Port Name	Name for this port. It can be free advised by user.	String	<...>
Port State	Enables or disables the local management port.	PullDown Menu <ul style="list-style-type: none"> • Enabled • Disabled 	Enabled
HW MAC Address	Displays the MAC address of the local management port.	Display	00:1E:16:aa:b b:cc
Port Speed	Configure the data transmission mode for the selected Ethernet port. ⁱ	PullDown Menu <ul style="list-style-type: none"> • Automatic • 10 Half Duplex • 10 Full duplex • 100 Half Duplex • 100 Full duplex 	Automatic

Table 1-27 Port Configuration (continued)

Parameter	Description	Format	Default
Autonegotiation	Autonegotiation handling can be invoked, even when a fixed Port Speed (see above) is selected. when Port Speed is “Automatic”, this entry is always ON.	PullDown Menu <ul style="list-style-type: none"> • On • Off 	On
Link Status	Indicates, whether the port is up, down or disabled.	Display	
Packet Counter	Counter for transmitted (TX) and received (RX) Ethernet-frames on the port.	Display	
Enable SNMP Link Up/Down Traps	Enables or disables the capability to send traps when the link state is changed.	PullDown Menu <ul style="list-style-type: none"> • Enabled • Disabled 	Enabled

i. See Table 4-7 in [axManualENX] for explanation on the settings.

Inband MGMT

The screenshot shows the 'Edit Port Settings' interface for 'Inband MGMT'. The configuration fields are as follows:

- Port Label: Inband MGMT
- Port Name: <...>
- Port State: Enabled
- HW MAC Address: 00:1e:16:00:1e:fd
- Enable SNMP Link Up/Down Traps: Enabled

Below the configuration fields is a table showing the status of two line ports:

Group	Name	Admin Status	Link Status	Type	SyncE	Edit
LINE Port Group	LINE 1 <...>	Enabled	Link Down	RJ45 (SFP) / 10/100 / 1000BaseT	Disabled	Edit
LINE Port Group	LINE 2 <...>	Enabled	Link Down	RJ45 (SFP) / 10/100 / 1000BaseT	Disabled	Edit

Figure 1-25 Edit-Port-Settings, Inband MGMT

As the in-band management port “Inband MGMT” can be used by all LINE-ports, the “Edit Port Settings” menu, does offer more submenus for all ports, which are configured as LINE. Each of these ports can have individual port settings, which can now be

adopted, when pressing the “Edit” button. The options hereafter, are the same as depicted in “Edit Ethernet Ports” on page 1-91.

The table, where all LINE-ports are summarized is a sub-set of the table, which is shown in “Ethernet Ports” on page 1-89.

Group	Name	AdminStatus		Link Status	Type		SyncE	Edit
LINE Port Group	LINE 1 <...>	Enabled	Link Down	No Link Detected	RJ45 (SFP)	10/100/1000BaseT	Disabled	<input type="button" value="Edit"/>
LINE Port Group	LINE 2 <...>	Enabled	Link Down	No Link Detected	RJ45 (SFP)	10/100/1000BaseT	Disabled	<input type="button" value="Edit"/>

Figure 1-26 Table of LINE-Ports

Table 1-25 provides information about the options.

Table 1-28 Port and IP-Configuration

Parameter	Description	Format	Default
Group	Name of the port group the ports belongs to. Here, this will always be “LINE Port Group”.	Display	LINE Port Group
Name	Name of the different LINE-ports.	Display	LINE 1 LINE 2
Admin Status	The status of the port is shown. For security reason, the interface can not be enabled or disabled here. Warning: Keep in mind, to disable the LINE will have impact to your payload traffic!	Display	Enabled
Link Status	Indicates, whether the port is up, down or disabled.	Display	
Type	Indicates the physical design of the interface (RJ45, SFP or Combo).	Display	
SyncE	Settings for the synchronous Ethernet.	Display	
Edit	Press the “Edit” to change the HW settings of a port.	Submenu	-



WARNING: When pressing the “Edit”-button, one will reach the configuration menu for the selected LINE-port. Any change of line-settings can lead to impacts on the payload traffic. Please be very careful with any changes here!

Edit IP Settings

Use this menu to change the IP settings and higher level behaviour of the ports. The menus for the different ports (out-of-band and in-band) are different.

F/Q MGMT

The out-of-band management port can be operated in different modes, which can be configured in this submenu:

- Interface-Mode: Q- or F-interface
- IP-Address assignment: Manually or via DHCP
- VLAN-Tagging: With or without VLAN tag (only in Q-mode possible)

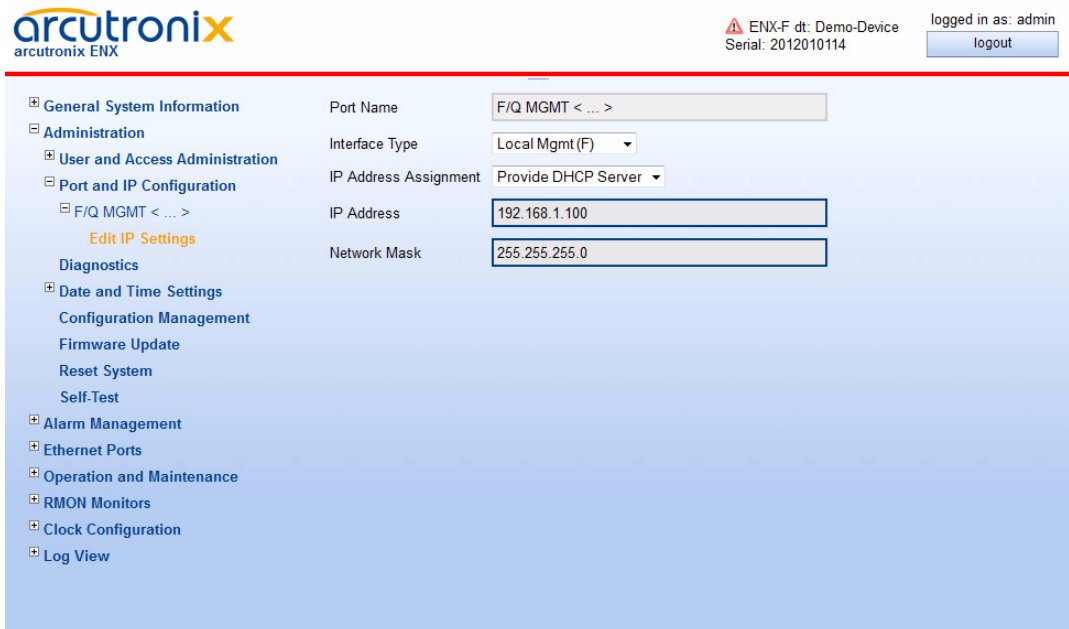


Figure 1-27 Edit IP Settings (F/Q Port)

Table 1-27 provides information about the options.

Table 1-29 IP-Port Configuration

Parameter	Description	Format	Default
Port Name	Name for this port.	Display	F/Q MGMT
Interface Type	Defines the IP behaviour of the port. Either local interface (F-interface) or remote access (Q-interface).	PullDown Menu <ul style="list-style-type: none"> • Local Mgmt (F) • Remote Mgmt (Q) 	Local

Table 1-29 IP-Port Configuration (continued)

Parameter	Description	Format	Default
IP Address Assignment	Defines the IPv4 address assignment. The Pulldown menu offers different entries, depending on the selected Interface Type (F- or Q-interface).	PullDown-Menu F-Interface: • Manual ⁱ • Provide DHCP Server Q-Interface: • Manual • From DHCP Server • From DHCP Server/ Auto IP	F-IF: Provide DHCP Server Q-IF: From DHCP Server
IP Address	Configuration of the device's IPv4 address. 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/Input	F/Q MGMT: 192.168.1.100
Network Mask	Configuration of the device's IPv4 network mask. When an IPv4 address is entered, a suggested network mask will be displayed. 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/Input	255.255.255.0
DHCP Server ⁱⁱ	IP-address of the (discovered) DHCP-server. The IP-address needs no setting.	Display	
DHCP Server State ⁱⁱ	Displays to state of connection to the DHCP-server.	Display	

Table 1-29 IP-Port Configuration (continued)

Parameter	Description	Format	Default
DHCP Default Gateway ⁱⁱ	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. The assigned Default Gateway may be overwritten by the "Overwrite Default Gateway".	Display	
Management VLAN ID Usage ⁱⁱⁱ	In Q-mode, the interface can be operated in VLAN mode. One tag may be defined for out-of-band management traffic.	PullDown Menu <ul style="list-style-type: none"> • Disable • Single Tag 	Disable
Management VLAN ID ^{iv}	Assign the VLAN ID for the in-band management traffic.	Display/Input	4094
Management VLAN Prio ^{iv}	Assign the VLAN priority field used for the in-band management traffic (0... 7).	Display/Input	3

i. "Manual" means, that there is no DHCP-server provided. The client's IP-address (PC) has to be configured manually.

ii. Only visible, when "IP Address assignment" is "From DHCP Server".

iii. Only visible, when "Interface Type" is "Remote Mgmt (Q)".

iv. Only visible, when "Management VLAN ID Usage" is "Single Tag".

Inband MGMT

The in-band management port can be operated in different modes, which can be configured in this submenu:

- IP-Address assignment: Manually or via DHCP
- VLAN-Tagging: With one or two VLAN tag(s)

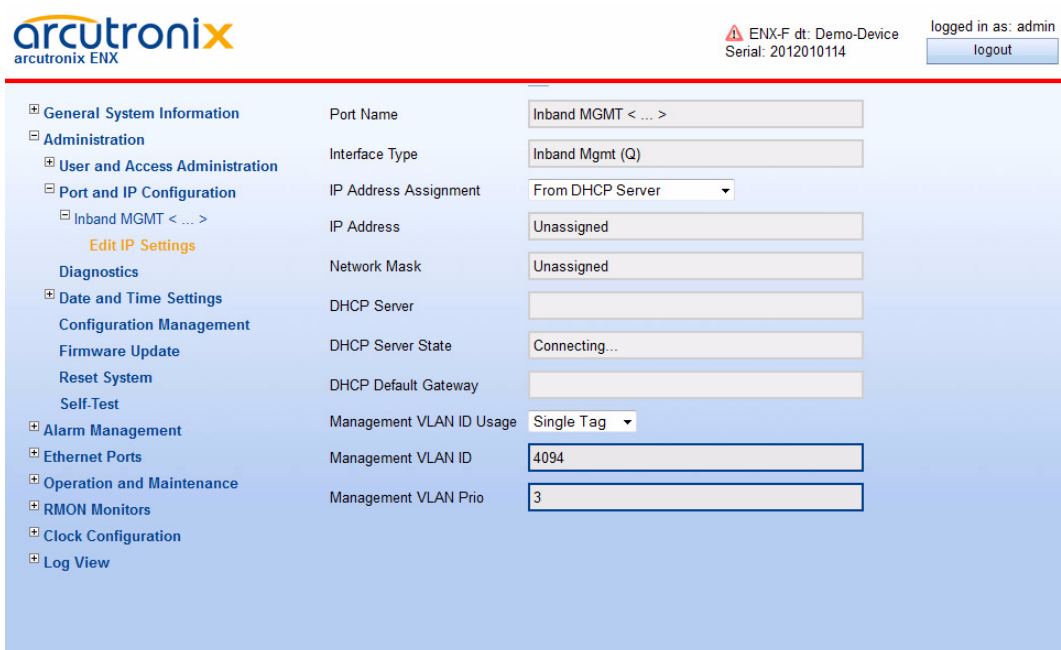


Figure 1-28 Edit IP Settings (Inband Port)

Table 1-27 provides information about the options.

Table 1-30 IP-Port Configuration

Parameter	Description	Format	Default
Port Name	Name for this port.	Display	Inband MGMT
Interface Type	Defines the IP behaviour of the port. It is always Inband MGMT (Q).	Display	Inband MGMT (Q)
IP Address Assignment	Defines the IPv4 address assignment. The Pulldown menu offers different entries, depending on the selected Interface Type (F- or Q-interface).	PullDown-Menu <ul style="list-style-type: none"> • Manual • From DHCP Server • From DHCP Server/ Auto IP 	From DHCP Server
IP Address	Configuration of the device's IPv4 address. 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/Input	unassigned

Table 1-30 IP-Port Configuration (continued)

Parameter	Description	Format	Default
Network Mask	Configuration of the device's IPv4 network mask. When an IPv4 address is entered, a suggested network mask will be displayed. 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/Input	<i>unassigned</i>
DHCP Server ⁱ	IP-address of the (discovered) DHCP-server. The IP-address needs no setting.	Display	
DHCP Server State ⁱ	Displays to state of connection to the DHCP-server.	Display	
DHCP Default Gateway ⁱ	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. The assigned Default Gateway may be overwritten by the "Overwrite Default Gateway".	Display	
Management VLAN ID Usage	The interface is operated always in VLAN mode. For more options in provider's network, the in-band management traffic may be double-tagged.	PullDown Menu • Single Tag • Double Tag	Single Tag
Management VLAN S-Tag ⁱⁱ	The S-Tag (Service Tag; Outer Tag) might have a different type than 0x8100 as standard VLAN. The default for S-Tag is 0x88A8.	Input	0x88A8
Outer Management VLAN ID ⁱⁱ	Assign the outer VLAN ID for the in-band management traffic.	Display/Input	4090
Management VLAN Prio ⁱⁱ	Assign the outer VLAN priority field used for the in-band management traffic (0... 7).	Display/Input	3

Table 1-30 IP-Port Configuration (continued)

Parameter	Description	Format	Default
Management VLAN ID	Assign the VLAN ID for the in-band management traffic.	Display/Input	4094
Management VLAN Prio	Assign the VLAN priority field used for the in-band management traffic (0... 7).	Display/Input	3

i. Only visible, when "IP Address assignment" is "From DHCP Server".

ii. Only visible, when "Management VLAN ID Usage" is "DoubleTag".



WARNING: When Provider-Tagging is enabled, the in-band access (Inband MGMT) is also expected to be double-tagged! As soon as the VLAN-mode is configured to Provider-Tagging, you will loose your in-band management connection, if the in-band is not already configured to Double-VLAN-Tagging!

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".

The screenshot displays the Arcutronix ENX web interface. On the left is a navigation tree with 'Diagnostics' selected. The main panel contains an 'IP-Address' input field, a 'Command' section with three buttons ('Ping', 'Traceroute/UDP', 'Traceroute/ICMP'), and a 'Command Output' text area. The top right corner shows the user is logged in as 'admin' with a 'logout' button.

Figure 1-29 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.

The screenshot displays the 'Date and Time Settings' page in the ENX Web-GUI. The top left shows the 'arcutronix' logo. The top right indicates the device is 'ENX-F dt: Demo-Device' with serial '2012010114' and the user is logged in as 'admin'. The left sidebar contains a navigation menu with 'Date and Time Settings' highlighted. The main content area shows configuration fields: Date (2013-02-25), Time (18:07), Time Zone (GMT+1), NTP Support (Enabled), and NTP Status (Synchronized). Below these fields is a table of NTP servers.

Server Address	Protocol Version	Admin Status	Server Status	Stratum	Reachability	Delay [ms]	Offset [ms]	Jitter [ms]
192.168.1.1	NTPv4	Enabled	Selected	6	11111111	1.130	74.277	203.856

Figure 1-30 Date And Time Settings

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

Table 1-31 provides information about the options.

Table 1-31 *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
Time Zone	Indicates the relative time deviation to GMT ⁱ , e.g. 'GMT+1' for Berlin.	PullDown Menu <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 1-32 *NTP Server Status*

Parameter	Description	Format
Server Address	The IPv4 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: <ul style="list-style-type: none"> • Enabled: May be used as reference clock. • Disabled: Never used as reference clock. 	PullDown Menu <ul style="list-style-type: none"> • Enabled • Disabled

Table 1-32 NTP Server Status (continued)

Parameter	Description	Format
Server Status	<p>The actual (communication) status between ENX and the server. Possible values are:</p> <ul style="list-style-type: none"> • 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	<p>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.</p>	Display
Reachability	<p>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:</p> <ul style="list-style-type: none"> • network communication has failed • NTP server is not synchronous to its time source. <p>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.</p> <div style="display: flex; align-items: center; margin-top: 10px;"> <div style="border: 1px solid black; padding: 5px; margin-right: 10px;"> <p style="background-color: #e0e0e0; margin: 0;">Reachability</p> <p style="margin: 0;">00011111</p> </div> <div> <p>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.</p> </div> </div>	Display
Delay [ms]	<p>This variable shows the current network round-trip time of NTP packets in milliseconds.</p>	Display
Offset [ms]	<p>This variable shows the current time difference between the selected NTP server and the local system clock in milliseconds.</p>	Display
Jitter [ms]	<p>This variable shows the amount of fluctuations between subsequent NTP date-time transactions in milliseconds.</p>	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.

Figure 1-31 NTP Server Setup

Table 1-33 provides information about the options.

Table 1-33 NTP Server Setup

Parameter	Description	Format
Server Address	The IPv4 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: <ul style="list-style-type: none"> Enabled: May be used as reference clock. Disabled: Never used as reference clock. 	Display

Table 1-33 NTP Server Setup (continued)

Parameter	Description	Format
Server Status	<p>The actual (communication) status between ENX and the server. Possible values are:</p> <ul style="list-style-type: none"> • 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
Reachability	<p>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:</p> <ul style="list-style-type: none"> • network communication has failed • NTP server is not synchronous to its time source. <p>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.</p> <div style="display: flex; align-items: center; margin-top: 10px;"> <div style="border: 1px solid black; padding: 5px; margin-right: 10px;"> <p style="text-align: center; margin: 0;">Reachability</p> <p style="text-align: center; margin: 0;">00011111</p> </div> <div> <p>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.</p> </div> </div>	Display
NTP Key Type	<p>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.</p>	Display
NTP Key ID	<p>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).</p>	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.



Figure 1-32 Edit NTP Server

Table 1-34 provides information about the options.

Table 1-34 Edit NTP Server

Parameter	Description	Format	Default
Server Address	The IPv4 address of the NTP-server.	IPv4-address	0.0.0.0
Protocol Version	The used version of NTP to communicate with the server.	PullDown Menu <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • Enabled • Disabled 	Enabled

Table 1-34 Edit NTP Server (continued)

Parameter	Description	Format	Default
Reachability	<p>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:</p> <ul style="list-style-type: none"> • network communication has failed • NTP server is not synchronous to its time source. <p>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.</p> <div style="display: flex; align-items: center;"> <div style="border: 1px solid black; padding: 2px; margin-right: 10px;"> <p style="margin: 0;">Reachability</p> <p style="margin: 0;">00011111</p> </div> <div> <p>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.</p> </div> </div>	Display	00000000
NTP Key Type	<p>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.</p>	PullDown Menu <ul style="list-style-type: none"> • None • MD5 • SHA1 	None

Table 1-34 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	<p>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.</p> <p>The key data can be specified in two different formats:</p> <ul style="list-style-type: none">• ASCII string, 1..20 printable characters excluding "#" and white space• HEX string, 40 characters <p>This corresponds to a key length of 160 bits.</p> <p>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".</p>	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 ENX, but externally on a server or PC. So one has the possibility to up- and download files to save them externally and/or

to use stored files as “master-config-file” for other devices. This makes it easier to put lots of units in operation with a common configuration.

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

- 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 “File Servers” on page 1-17). 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 1-14). 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”).

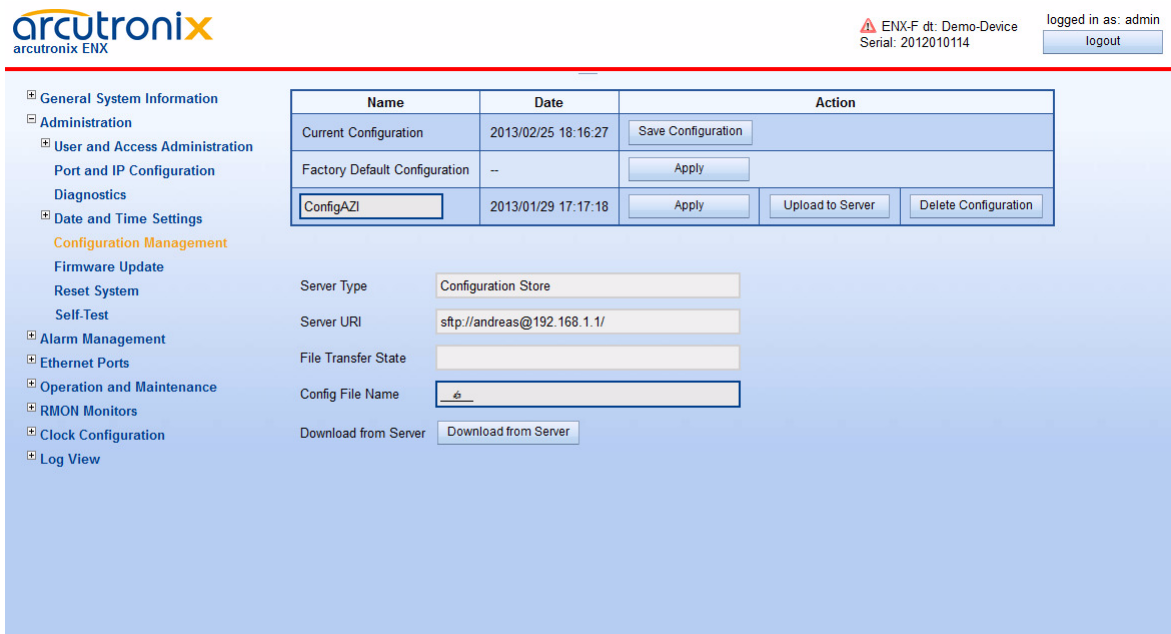


Figure 1-33 Configuration Management w/o http-option

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.

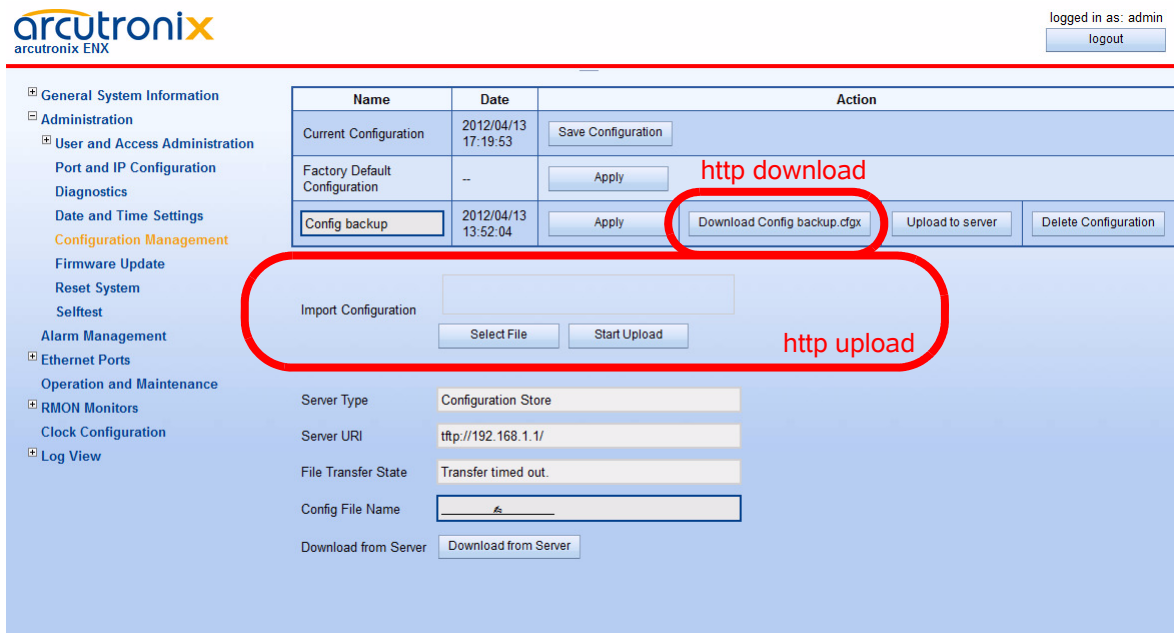


Figure 1-34 Configuration Management with http-option

Table 1-35 provides information about the options.

Table 1-35 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 1-35 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.

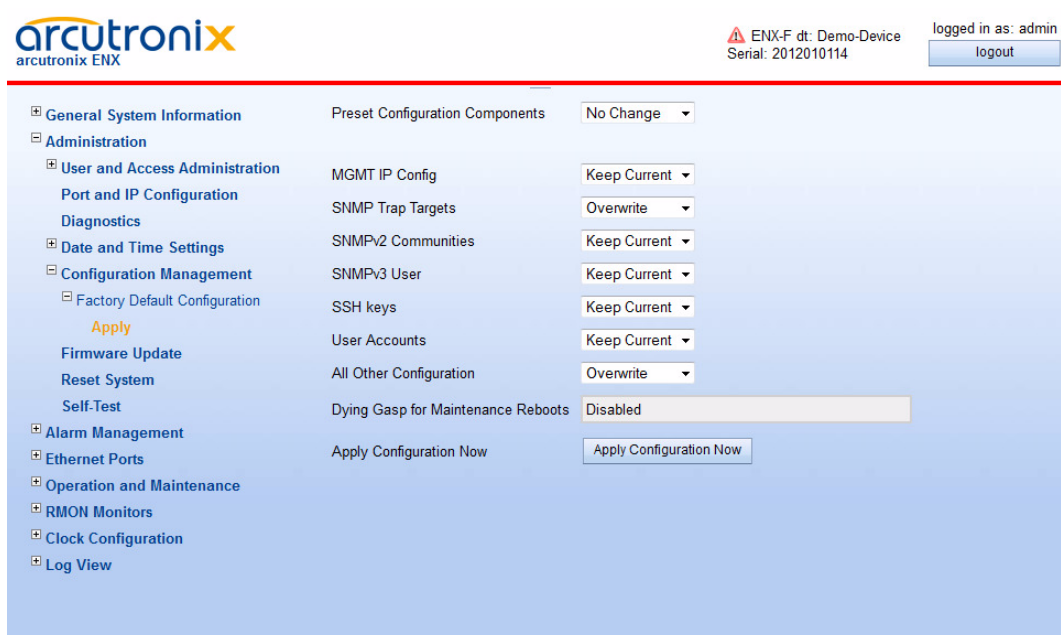


Figure 1-35 Recall Configuration

Table 1-36 provides information about the options.

Table 1-36 Recall Configuration

Parameter	Description	Format	Default
Preset Configuration Components	All settings can be configured in one-step.	PullDown-Menu <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> Overwrite Keep Current 	Keep Current
SNMP Trap Targets	The IP settings for SNMP-trap receivers.	PullDown-Menu <ul style="list-style-type: none"> Overwrite Keep Current 	Overwrite
SNMPv2 Communities		PullDown-Menu <ul style="list-style-type: none"> Overwrite Keep Current 	Overwrite
SNMPv3 Users		PullDown-Menu <ul style="list-style-type: none"> Overwrite Keep Current 	Overwrite
SSH Keys		PullDown-Menu <ul style="list-style-type: none"> Overwrite Keep Current 	Keep Current
User Accounts		PullDown-Menu <ul style="list-style-type: none"> Overwrite Keep Current 	Keep Current
All Other Configuration		PullDown-Menu <ul style="list-style-type: none"> 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 ENX. 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 ENX will reboot to finish the update process. After the reboot reconnecting to the unit is necessary.

Three different protocols are supported to update the ENX 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 1-17). 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 1-14). 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 73 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 1-78).

Menu

The screenshot shows the Arcutronix ENX web interface. At the top left is the logo 'arcutronix arcutronix ENX'. At the top right, it says 'logged in as: admin' with a 'logout' button. A navigation menu on the left lists various system settings, with 'Firmware Update' highlighted in orange. The main content area shows the following configuration options:

Dying Gasp for Maintenance Reboots	<input type="text" value="Disabled"/>
Firmware Update Status	<input type="text" value="No Update File"/>
Update Info	<input type="text"/>
Download / Update Progress	<input type="text"/>
Server Type	<input type="text" value="Firmware Store"/>
Server URI	<input type="text" value="sftp://andreas@192.168.1.1/"/>
File Name	<input type="text" value="6"/>
Start Firmware Download	<input type="button" value="Start Firmware Download"/>
Start Update	<input type="button" value="Start Update"/>

Figure 1-36 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.

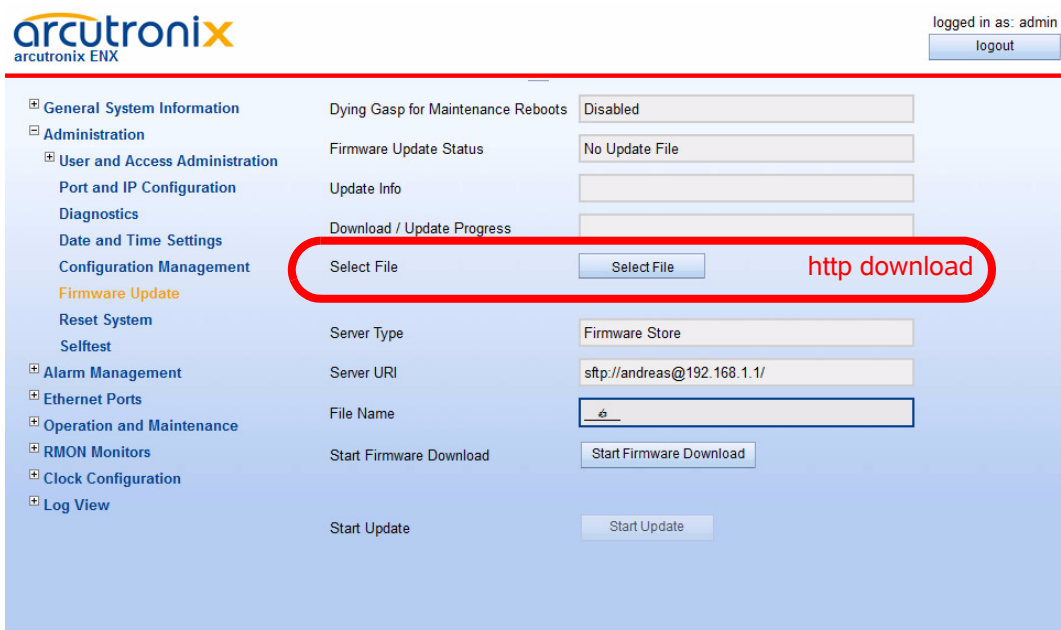


Figure 1-37 Firmware Update with http-option

Table 1-36 provides information about the options.

Table 1-37 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 1-37 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 <ul style="list-style-type: none">• IP-connection to server failed• Server was shut-down or stopped

Summary

To update the ENX 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 ENX manually immediately or at a scheduled time.

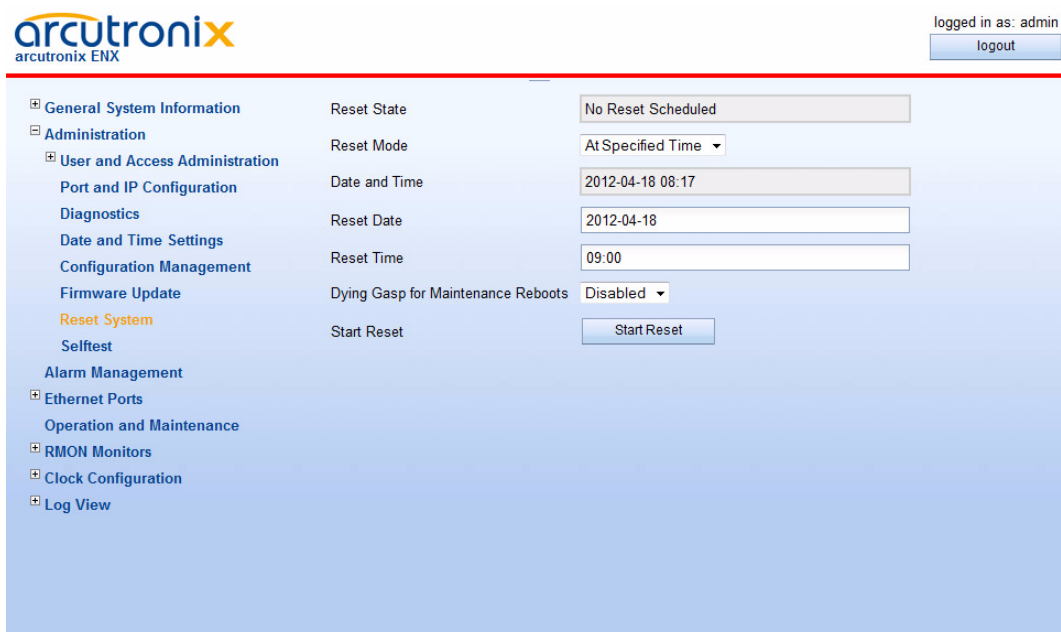


Figure 1-38 Reset System, @Specific Time

Table 1-38 provides information about the options.

Table 1-38 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 <ul style="list-style-type: none"> • 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 1-38 *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 <ul style="list-style-type: none"> • 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 Menu can be used to check, whether the unit is still working well. After starting the self-test the status and results are shown in the entries below.



Figure 1-39 *Self-Test*

Alarm Management

The Alarm Management view is designed to give a quick and detailed overview to the status of the ENX. Many details about usage of the Alarm Management is given in “Alarm Management” in [axManualENX]. Please read this chapter before using the Alarm Management.

The screenshot displays the Alarm Management interface. At the top right, it shows the device information: ENX-F dt: Demo-Device, Serial: 2012010114, and the user is logged in as admin. The main content area is divided into a summary section and a table of active alarms.

System Alarm Status Summary:

- System Alarm Status: **Error**
- Acknowledge All:
- Current Alarms: 24
- Current Warnings: 1
- Alarm Acknowledgement Policy: Unacknowledge When Raising Severity

Active Alarm List Table:

Group Name	State	Errors	Warnings	Acknowledged	Ignored	Max. Severity	Acknowledge	Details
EEC Alarms	Error	5	0	0	0	Error	<input type="button" value="Acknowledge Group Alarms"/>	<input type="button" value="Group Details"/>
LAN 1 <...> Alarms	Error	1	0	0	0	Error	<input type="button" value="Acknowledge Group Alarms"/>	<input type="button" value="Group Details"/>
LAN 1 <...> SFP Alarms	Error	1	0	0	0	Error	<input type="button" value="Acknowledge Group Alarms"/>	<input type="button" value="Group Details"/>
LAN 2 <...> Alarms	Error	1	0	0	0	Error	<input type="button" value="Acknowledge Group Alarms"/>	<input type="button" value="Group Details"/>
LAN 2 <...> SFP Alarms	Error	1	0	0	0	Error	<input type="button" value="Acknowledge Group Alarms"/>	<input type="button" value="Group Details"/>
LAN 3 <...> Alarms	Error	1	0	0	0	Error	<input type="button" value="Acknowledge Group Alarms"/>	<input type="button" value="Group Details"/>
LAN 3 <...> SFP Alarms	Error	1	0	0	0	Error	<input type="button" value="Acknowledge Group Alarms"/>	<input type="button" value="Group Details"/>
LAN 4 <...> Alarms	Error	1	0	0	0	Error	<input type="button" value="Acknowledge Group Alarms"/>	<input type="button" value="Group Details"/>
LAN 4 <...> SFP Alarms	Error	1	0	0	0	Error	<input type="button" value="Acknowledge Group Alarms"/>	<input type="button" value="Group Details"/>
LINE 1 <...> Alarms	Error	1	0	0	0	Error	<input type="button" value="Acknowledge Group Alarms"/>	<input type="button" value="Group Details"/>
LINE 1 <...> SFP Alarms	Error	1	0	0	0	Error	<input type="button" value="Acknowledge Group Alarms"/>	<input type="button" value="Group Details"/>
LINE 2 <...> Alarms	Error	1	0	0	0	Error	<input type="button" value="Acknowledge Group Alarms"/>	<input type="button" value="Group Details"/>
LINE 2 <...> SFP Alarms	Error	1	0	0	0	Error	<input type="button" value="Acknowledge Group Alarms"/>	<input type="button" value="Group Details"/>
PTP Alarms	Error	5	0	0	0	Error	<input type="button" value="Acknowledge Group Alarms"/>	<input type="button" value="Group Details"/>
System Alarms	Error	2	1	0	0	Error	<input type="button" value="Acknowledge Group Alarms"/>	<input type="button" value="Group Details"/>

Figure 1-40 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 ENX, e.g. the LED and alarm relay status are reseted.

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. EEC Alarm Group
2. Port Alarm Group, one for each LAN and LINE port
 - The F/Q interface alarms are part of the System Alarm Group.
3. SFP Alarm Groups, one for each SFP slot

4. PTP Alarm Group
5. 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 1-43 provides information about the options of the Alarm Management.

Table 1-39 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 acknowledged by administrator: Keep Acknowledged until Inactive: <ul style="list-style-type: none">• The acknowledge alarm/warning will be kept in this status, until the alarm-cause is gone. Unacknowledged when raising Severity: <ul style="list-style-type: none">• The acknowledge alarm/warning will be kept in this status, until the severity gets worse. (Default) Unacknowledged on State Change: <ul style="list-style-type: none">• 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 1-89 for details.

System Alarm Group

The System Alarm Group incorporates all the system alarms:

- Reset state of the ENX,
- Power supply alarms including DyingGasp,
- Status of interfaces F/QMGMT and Inband MGMT,

- Temperature alarms,
- Status of FW Update.

The screenshot shows the Arcutronix ENX web interface. At the top right, it displays 'ENX-F dt: #2012010114 Serial: 2012010114' and 'logged in as: admin' with a 'logout' button. The left navigation menu includes 'General System Information', 'Administration', 'Alarm Management', 'System Alarms', 'Group Details', 'Active Alarm List', 'Ethernet Ports', 'Operation and Maintenance', 'RMON Monitors', 'Clock Configuration', and 'Log View'. The main content area shows 'Alarm Group Name: System Alarms', 'Alarm Group State: Error', 'Current Alarms: 2', and 'Current Warnings: 0'. Below this is a table of active alarms.

Alarm Name	System Component	Severity	Hold Time	Config	State		Acknowledge	SNMP Notification
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
DC Power Status		Error	10 sec	Settings	Ok	DC Power Good	Acknowledge	SNMP Trap
AC Power Status		Error	10 sec	Settings	Error	AC Power Failure	Acknowledge	SNMP Trap
Link Status	F/Q MGMT <...>	Error	10 sec	Settings	Ok	Link Up	Acknowledge	SNMP Trap
Link Status	Inband MGMT <...>	Error	10 sec	Settings	Error	Link Down	Acknowledge	SNMP Trap
Device Temperature		--	10 sec	Settings	Ok	29.0 °C	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 1-41 System Alarm Group Management

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

Table 1-40 System Alarm Group Management

Parameter	Description
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!
Reset State	The “Reset State Alarm” can be raised, when a reset is scheduled. It can be configured to be used with error or warning level.
DC Power Status	The “DC Power Alarm” can be raised, when DC-input from the rear fails. It can be configured to be used with error or warning level.
AC Power Status	The “AC Power Alarm” can be raised, when AC-input from the rear fails. It can be configured to be used with error or warning level.
F/Q MGMT <name>	Status of interface F/Q MGMT. It can be configured to be used with error or warning level.

Table 1-40 System Alarm Group Management (continued)

Parameter	Description
Inband MGMT <name>	Status of interface Inband MGMT (in-band management port). 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.
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.

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°.

The screenshot shows the ENX Web-GUI interface. At the top left is the Arcutronix logo. At the top right, it displays 'ENX-F dt: #2012010114', 'Serial: 2012010114', and 'logged in as: admin' with a 'logout' button. The main content area is a settings page for 'Device Temperature'. On the left is a navigation menu with categories: General System Information, Administration, Alarm Management (expanded), System Alarms, Group Details (expanded), Device Temperature (expanded), Settings (highlighted), Active Alarm List, Ethernet Ports, Operation and Maintenance, RMON Monitors, Clock Configuration, and Log View. The settings table is as follows:

Alarm Name	Device Temperature
System Component	
Value	31.0 °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 1-42 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.

EEC Alarm Group

The EEC Alarm Group incorporates all the clock alarms which are related to the EEC-Function (Ethernet Equipment Clock) of the device:

- State of the onboard TCXO (OCXO) and PLL,
- T3 and T4 clock state and quality,
- Synchronous Ethernet clock state and quality.

The screenshot shows the 'EEC Alarms' management page. The top header includes the Arcutronix logo, the text 'ENX-F dt: #2012010114 Serial: 2012010114', and a 'logged in as: admin' status with a 'logout' button. The left navigation menu has options like 'General System Information', 'Administration', 'Alarm Management', 'EEC Alarms', 'Group Details', 'Active Alarm List', 'Ethernet Ports', 'Operation and Maintenance', 'RMON Monitors', 'Clock Configuration', and 'Log View'. The main content area contains form fields for 'Alarm Group Name' (EEC Alarms), 'Alarm Group State' (Error), 'Current Alarms' (7), 'Current Warnings' (0), and 'Max. Group Severity' (Error). Below these is a table of alarm details.

Alarm Name	System Component	Severity	Hold Time	Config	State	Acknowledge	SNMP Notification
EEC Source Status	Internal TCXO	Error	10 sec	Settings	Ok	Used for Synchronization	SNMP Trap
EEC Source Status	T3an	Error	10 sec	Settings	Link Down	Link Down	SNMP Trap
EEC Source Status	SyncE LINE 1 Optical	Error	10 sec	Settings	Link Down	Link Down	SNMP Trap
EEC Source Status	SyncE LINE 2 Optical	Error	10 sec	Settings	n.a.	SyncE Disabled at Port	SNMP Trap
EEC Source Status	SyncE LINE 1 Electrical	Error	10 sec	Settings	Link Down	Link Down	SNMP Trap
EEC Source Status	SyncE LINE 2 Electrical	Error	10 sec	Settings	n.a.	SyncE Disabled at Port	SNMP Trap
EEC Source Priority		--	10 sec	Settings	15	15	SNMP Trap
T3an Receive Level		--	10 sec	Settings	-37 dB	-37 dB	SNMP Trap
T4ab Status		Error	10 sec	Settings	Not Connected	Not Connected	SNMP Trap
T3an Status		Error	10 sec	Settings	Not Connected	Not Connected	SNMP Trap
PLL Status		Error	10 sec	Settings	Ok	Locked	SNMP Trap

Figure 1-43 EEC Alarm Group Management

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

Table 1-41 EEC Alarm Group Management

Parameter	Description
Internal TCXO	The "Internal TCXO Alarm" can be raised, when the internal XO fails. It can be configured to be used with error or warning level.
T3an	The "T3an Alarm" can be raised, when T3an is not available. It can be configured to be used with error or warning level.
SyncE LINE 1 Optical	The "SyncE LINE 1 Optical Alarm" can be raised, when clock from fibre-part of combo LINE 1 is not available. It can be configured to be used with error or warning level.
SyncE LINE 1 Electrical	The "SyncE LINE 1 Electrical Alarm" can be raised, when clock from copper-part of combo LINE 1 is not available. It can be configured to be used with error or warning level.
SyncE LINE 2 Optical	The "SyncE LINE 2 Optical Alarm" can be raised, when clock from fibre-part of combo LINE 2 is not available. It can be configured to be used with error or warning level.
SyncE LINE 2 Electrical	The "SyncE LINE 2 Electrical Alarm" can be raised, when clock from copper-part of combo LINE 2 is not available. It can be configured to be used with error or warning level.

Table 1-41 EEC Alarm Group Management (continued)

Parameter	Description
EEC Source Priority	The “EEC Source Priority Alarm” can be raised, when a clock-source is selected from priority list, which is below the given thresholds. It can be configured to be used with error or warning level.
PLL Status	The “PLL Status Alarm” can be raised, when the onboard PLL is not locked. It can be configured to be used with error or warning level.
T3an Status	The “T3an Status Alarm” can be raised, when T3an is not connected. It can be configured to be used with error or warning level.
T3an Receive Level	The “T3an Receive Level Alarm” can be raised, when the device detects a low input level on this port. 2 levels can be specified for either warning or error status.
T4ab Status	The “T4ab Status Alarm” can be raised, when T4ab is not connected. It can be configured to be used with error or warning level.

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 1-80.

Port Alarm Groups (LINE 1-2; LAN 1-4)

The Port Alarm Groups incorporates all the alarms for the 6 Ethernet ports: LINE 1, LINE 2, LAN 1, LAN 2, LAN 3 and LAN 4:

- State of the Ethernet ports,
- Autonegotiation results,
 - Autonegotiation is also required for SyncE of Copper ports. So if SyncE is enabled on Copper ports, the Autonegotiation is important!
- Loopback of the port.

The screenshot shows the ENX Web-GUI interface for configuring a Port Alarm Group. The header includes the Arcutronix logo, the text "ENX-F dt: #2012010114 Serial: 2012010114", and a "logged in as: admin" status with a "logout" button. The left navigation menu includes options like "General System Information", "Administration", "Alarm Management", "LINE 1 <.> Alarms", "Group Details", "Active Alarm List", "Ethernet Ports", "Operation and Maintenance", "RMON Monitors", "Clock Configuration", and "Log View". The main content area contains form fields for "Alarm Group Name" (set to "LINE 1 <.> Alarms"), "Alarm Group State" (set to "Error"), "Current Alarms" (set to "1"), "Current Warnings" (set to "0"), and "Max. Group Severity" (set to "Error"). Below these fields is a table with the following data:

Alarm Name	System Component	Severity	Hold Time	Config	State	Acknowledge	SNMP Notification
Performance Degrad	LINE 1 <.>	Ignore	10 sec	Settings	Ok	Performance Ok	SNMP Trap
Autoneg Failure	LINE 1 <.>	Error	10 sec	Settings	n.a.	Autoneg in Progress	SNMP Trap
Loopback Status	LINE 1 <.>	Ignore	10 sec	Settings	Ok	No Loopback	SNMP Trap
Link Status	LINE 1 <.>	Error	10 sec	Settings	Error	Link Down	SNMP Trap

Figure 1-44 Port Alarm Group

Table 1-42 provides information about the options of the Port Alarm Group.

Table 1-42 Port Alarm Group

Parameter	Description
Performance Degrad	The "Performance Degrad 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	The "Autonegotiation Alarm" can be raised, when port's autonegotiation did not succeed with peer. For copper ports, the autoneg-feature is essential, when SyncE is enabled. It can be configured to be used with error or warning level.
Loopback Status	The "Loopback Alarm" can be raised, when port's loopback status is changing. It can be configured to be used with error or warning level.
Link Status	The "Link Status Alarm" can be raised, when port's link status is changing. It can be configured to be used with error or warning level.

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 1-80.

SFP Alarm Groups (LINE 1-2; LAN 1-4)

The SFP Alarm Group incorporates all the alarms related to SFPs:

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

- SFP temperature

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

Figure 1-45 SFP Alarm Group (LINE 1 SFP)

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

Table 1-43 SFP Alarm Group

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 (dBm)	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 1-43 SFP Alarm Group (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 1-80.

PTP Alarm Group

The PTP Alarm Group incorporates all the alarms, which can be raised by the Precision Time Protocol (PTP) stack of the device:

- Connection status to PTP Grandmaster Clock (GM) and the (calculated) time offset to GM,
- PTP status of the LAN ports,
- PTP status of the LINE ports and their path delay to the GM.

ENX-F dt: #2012010114
Serial: 2012010114
logged in as: admin
logout

Alarm Group Name: PTP Alarms
Alarm Group State: Error
Current Alarms: 1
Current Warnings: 0
Max. Group Severity: Error

Alarm Name	System Component	Severity	Hold Time	Config	State	Acknowledge	SNMP Notification
PTP Path Delay Variation		--	10 sec	Settings	n.a. -- ns	Acknowledge	SNMP Trap
PTP Master Clock Connection Status		Error	10 sec	Settings	Error no slave port active	Acknowledge	SNMP Trap
Offset From Master		--	10 sec	Settings	n.a. -- ns	Acknowledge	SNMP Trap
PTP Port Status	LAN 1	Error	10 sec	Settings	n.a. Disabled	Acknowledge	SNMP Trap
PTP Port Status	LAN 2	Error	10 sec	Settings	n.a. Disabled	Acknowledge	SNMP Trap
PTP Port Status	LAN 3	Error	10 sec	Settings	n.a. Disabled	Acknowledge	SNMP Trap
PTP Port Status	LAN 4	Error	10 sec	Settings	n.a. Disabled	Acknowledge	SNMP Trap
PTP Port Status	LINE 1	Error	10 sec	Settings	n.a. Disabled	Acknowledge	SNMP Trap
PTP Port Status	LINE 2	Error	10 sec	Settings	n.a. Disabled	Acknowledge	SNMP Trap

Figure 1-46 PTP Alarm Group Management

Table 1-44 provides information about the options of the System Alarm Group Management.

Table 1-44 PTP Alarm Group Management

Parameter	Description
Offset from Master	<p>The “Offset from Master Alarm” can be raised, when the (calculated) offset from PTP Grandmaster is too large. The offset can be positive or negative. In best case, the offset from master is equals zero, as internal controller adjust the clock to this value.</p> <p>If positive, the (local) PTP clock has to much advance against the GM. If negative the (local) PTP clock has too much backlog. The thresholds to raise warning and error can be defined individually.</p> <p>The offset from master does have a granularity of 8 ns. So values in step of 8 ns make sense for the thresholds.</p>
PTP Master Clock Connection Status	<p>The “PTP Master Clock Connection Status Alarm” can be raised, when the device can not establish PTP connection to (any) PTP Grandmaster or a previously established connection gets lost.</p>

Table 1-44 PTP Alarm Group Management (continued)

Parameter	Description
PTP Path Delay Variation	<p>The “PTP Path Delay Variation Alarm” can be raised, when the device detects large variation(s) in the path delay to the PTP Grandmaster. The thresholds for PTP Path Delay Variations can be defined. The defaults are 16 ns and 8 ns.</p> <p>A huge change in the path delay is an indication for the change of network topology.</p> <p>The variation can be positive and negative, though the threshold can only be entered as positive value. A change with negative sign will be raised as alarm or warning as well.</p>
LAN 1 PTP Port Status	<p>The “LAN 1 Port Status Alarm” can be raised, when the PTP state of LAN 1 enters a non-operable state. The possible PTP states are defined in [IEEE 1588].</p> <p>Possible values (for a PTP master port) are:</p> <ul style="list-style-type: none"> • DISABLED -> ok • INITIALIZING -> alarm cond. • FAULTY -> alarm cond. • LISTENING -> alarm cond. • PASSIVE -> alarm cond. • PRE_MASTER -> alarm cond. • MASTER -> ok
LAN 2 PTP Port Status	see LAN 1 Port Status.
LAN 3 PTP Port Status	see LAN 1 Port Status.
LAN 4 PTP Port Status	see LAN 1 Port Status.
LINE 1 PTP Port Status	<p>The “LINE 1 Port Status Alarm” can be raised, when the PTP state of LINE 1 enters a non-operable state. The possible PTP states are defined in [IEEE 1588].</p> <p>Possible values (for a PTP slave port) are:</p> <ul style="list-style-type: none"> • DISABLED -> ok • INITIALIZING -> alarm cond. • FAULTY -> alarm cond. • LISTENING -> alarm cond. • UNCALIBRATED -> alarm cond. • SLAVE -> ok
LINE 2 PTP Port Status	see LINE 1 Port Status.

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 1-80.

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.

No	Group Name	Alarm Name	System Component	State	Acknowledge
1	EEC Alarms	EEC Source Priority	--	Error 15	Acknowledge
2	EEC Alarms	EEC Source Status	SyncE LINE 1 Optical	Error Link Down	Acknowledge
3	EEC Alarms	EEC Source Status	T3an	Error Link Down	Acknowledge
4	EEC Alarms	EEC Source Status	SyncE LINE 1 Electrical	Error Link Down	Acknowledge
5	EEC Alarms	T3an Receive Level	--	Error -37 dB	Acknowledge
6	EEC Alarms	T3an Status	--	Error Not Connected	Acknowledge
7	EEC Alarms	T4ab Status	--	Error Not Connected	Acknowledge
8	LAN 1 <...> Alarms	Link Status	LAN 1 <...>	Error Link Down	Acknowledge
9	LAN 1 <...> SFP Alarms	SFP Status	LAN 1 <...>	Error No SFP present	Acknowledge
10	LINE 1 <...> Alarms	Link Status	LINE 1 <...>	Error Link Down	Acknowledge
11	LINE 1 <...> SFP Alarms	SFP Status	LINE 1 <...>	Error No SFP present	Acknowledge
12	System Alarms	AC Power Status	--	Error AC Power Failure	Acknowledge
13	PTP Alarms	PTP Master Clock Connection Status	--	Warning Acknowledged no slave port active	Acknowledge
14	System Alarms	Link Status	Inband MGMT <...>	Warning Acknowledged Link Down	Acknowledge

Figure 1-47 Active Alarm List

Ethernet Ports

The “Ethernet Ports” menu gives access to all (Ethernet-) ports, which are involved in service provisioning:

- LAN (or user-) ports
- LINE ports (or up-links).

The out-of-band management interface “F/Q” will not be listed here, as it is purely a management port. The settings for “F/Q” can be made in “Port and IP Configuration” on page 1-43.

For the service and line-ports the physical configuration can be changed and the status monitored. VLAN settings, required for service setup can be done here and for all ports a large number of counters are available to check operation and availability.

The menu gives an overview to all six Ethernet ports available on the ENX:

The screenshot shows the ENX Web-GUI interface. At the top left is the Arcutronix logo. At the top right, it displays 'ENX-F dt: #2012010114', 'Serial: 2012010114', and 'logged in as: admin' with a 'logout' button. The left navigation menu includes: General System Information, Administration, Alarm Management, Ethernet Ports (highlighted), VLAN, Classification, MAC Table, Policer, Egress Queues, LACP Configuration, SFP Info, Counter, Operation and Maintenance, RMON Monitors, Clock Configuration, and Log View. The main content area features a table with the following data:

Group	Name	AdminStatus	Link Status	Type	SyncE	Edit		
LAN Port Group	LAN 1 <.>	Enabled	Link Down	No Link detected	RJ45 (SFP)	10/100/1000BaseT	Disabled	Edit
LAN Port Group	LAN 2 <.>	Enabled	Link Down	No Link detected	RJ45 (SFP)	10/100/1000BaseT	Disabled	Edit
LAN Port Group	LAN 3 <.>	Enabled	Link Down	No Link Detected	RJ45 (SFP)	10/100/1000BaseT	Disabled	Edit
LAN Port Group	LAN 4 <.>	Enabled	Link Down	No Link Detected	RJ45 (SFP)	10/100/1000BaseT	Disabled	Edit
LINE Port Group	LINE 1 <.>	Enabled	Link Down	No Link Detected	RJ45 (SFP)	10/100/1000BaseT	Disabled	Edit
LINE Port Group	LINE 2 <.>	Enabled	Link Down	No Link Detected	RJ45 (SFP)	10/100/1000BaseT	Disabled	Edit

Figure 1-48 Ethernet Ports

Table 1-45 provides information about the options.

Table 1-45 Ethernet Port

Parameter	Description	Format	Default
Group	Name of the port group the ports belongs to.	Display	
Name	Name of the different ports.	Display	
Admin Status	The status of the port can be enabled and disabled.	PullDown Menu • Enabled • Disabled	Enabled
Link Status	Indicates, whether the port is up, down or disabled.	Display	
Type	Indicates the physical design of the interface (RJ45, SFP or Combo). Combo is shown as "RJ45 (SFP)".	Display	
SyncE	Settings for the synchronous Ethernet.	Display	
Edit	Press the "Edit" to change the HW settings of a port.	Submenu	-

Edit Ethernet Ports

This submenu gives configuration options to the HW-layer of the port.

Figure 1-49 Edit Ethernet Ports

Table 1-46 provides information about the options.

Table 1-46 Edit Ethernet Port

Parameter	Description	Format	Default
Settings for Port	This is a combination of port's label (printed on device front) and port's name (given by user).	Display	
Port Group	Defines the port's usage. A "LAN" port is dedicated for user's equipment, while a "LINE" port is connected to the PSN. For the time being only one LAN group can be selected. This might be more in the future.	PullDown Menu: <ul style="list-style-type: none"> LAN Port Group1 LINE Port Group 	
Port Name	The given name by user.	Input	<...>
Admin Status	Enables or disables the port.	PullDown Menu <ul style="list-style-type: none"> Enabled Disabled 	Enabled

Table 1-46 Edit Ethernet Port (continued)

Parameter	Description	Format	Default
Combo Port Mode	<p>Restrict combo port to use only RJ45 or SFP.</p> <p>In “Prefer SFP” mode if a SFP is plugged, combo port is always in SFP mode, otherwise RJ45 can be used.</p> <p>You can restrict combo port mode to always activate SFP or to always activate RJ45. If combo port is set to “Always RJ45” a plugged SFP will be ignored. If combo port is set to “Always SFP” RJ45 cannot be used (but as in normal operation is it still not allowed to connect a RJ45 cable when a SFP is inserted).</p>	<p>PullDown Menu</p> <ul style="list-style-type: none"> • Prefer SFP • Always RJ45 • Always SFP 	
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	<p>Indicates a failure in the auto-negotiation process between the port and its peer.</p> <p>Note: Keep in mind for Copper I/F the auto-neg procedure is very important in case SyncE is enabled.</p>	Display	
SFP Port Mode	<p>Autonegotiation settings for the SFP (fibre) part of the combo-port. ⁱ.</p> <p>To disable the fibre option of the combo-port, select “do-not-use” here. In this case, the FO link can never be established.</p>	<p>PullDown Menu</p> <ul style="list-style-type: none"> • do-not-use • Auto Speed, Auto Duplex • ... 	Auto Speed, Auto Duplex

Table 1-46 Edit Ethernet Port (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 <ul style="list-style-type: none"> do-not-use Auto Speed, Auto Duplex ... 	Auto Speed, Auto Duplex
MTU Size	The maximum transmission unit for the MAC layer can be defined in 3 steps.	PullDown Menu <ul style="list-style-type: none"> 1518 (1522) ⁱⁱ 2048 10240 	2048
Flow Control	IEEE 802.3x (PAUSE frames) can be enabled or disabled.	PullDown Menu <ul style="list-style-type: none"> Enabled Disabled 	Disabled
SyncE Mode	Synchronous Ethernet can be enabled and disabled. When configured as “Master”, the port will use internal PLL as reference for transmitting data. This is good for LAN-ports. When configured as “Slave”, the port will use incoming data as clock reference and can distribute it to internal PLL. This is good for LINE-ports.	PullDown Menu <ul style="list-style-type: none"> Disabled Master (only for LAN-ports) Slave (only for LINE-ports) 	Disabled
Loopback	Enables or disables an Ethernet loopback.	PullDown Menu <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> Enabled Disabled 	Enabled

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

ii. 1518 (1522) is max 1518 for untagged and 1522 for VLAN-tagged packets.

VLAN

The ENX supports three different modes for VLAN:

- VLAN unaware: In this mode the device does not investigate in any VLAN-tag and packet-forwarding is only based on MAC addresses.

- VLAN aware: In this mode each LAN-port can be part in one or more VLAN, which much be configured. Untagged packets may be accepted and tagged, when ingressing. Packet forwarding is based on the VLAN-tag and MAC addresses.
- Provider VLAN-Tagging: In this mode, each packet entering at a LAN-port, will get an additional tag, called the provider-tag.

the configuration of VLAN-mode is done with the help of the variable "VLAN Mode". The default mode is VLAN unaware (= VLAN mode OFF).

NOTE: The configuration of many VLANs (more than 250) may slow down the start-up of the device after reboot. The device must first configure all ports and all VLANs properly before it allows any packet forwarding. Per 250 VLANs configuring, one must calculate about 2 seconds configuring.

VLAN Unaware Mode

VLAN Unaware mode is the default mode for VLAN handling in ENX. In fact, the VLAN-handling is disabled. Arriving packets may or may not carry VLAN-tags, it will not be considered when forwarding with the exception of in-band management.

In-band management (via LINE-ports) must always carry at least one VLAN-tag to give some security to the communication. Even when VLAN mode is disabled, this is expected and only packets carrying the correct management VLAN-tag will be forwarded to the management core.

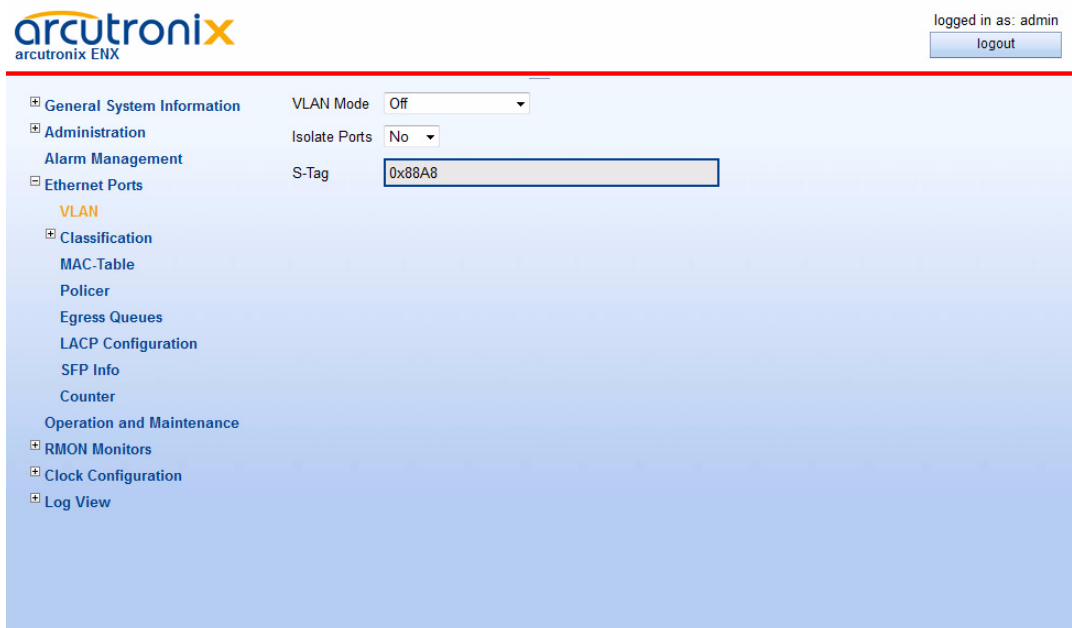


Figure 1-50 VLAN Unaware Mode

Table 1-47 provides information about the options.

Table 1-47 *VLAN Unaware*

Parameter	Description	Format	Default
VLAN Mode	The type of VLAN Policy can be set.	PullDown Menu <ul style="list-style-type: none">• Off• Aware• Provider-Tagging	Off
Isolate Ports	The LAN-ports can be isolated between each other. Isolation prohibits packet transfer between the LAN-ports. If isolation is enabled, packets from LAN-ports may only be forwarded to LINE-ports. Isolation may be switched off, when all LAN-ports are used for the same customer.	PullDown Menu <ul style="list-style-type: none">• No• Yes	Yes
S-Tag	The Ethertype for the S-Tag.	Input (>=0x8100)	00x88A8

VLAN Aware Mode

The functionality and possible settings of the VLAN Aware Mode is depicted in detail in chapter “VLAN Aware” in [axManualENX].

In VLAN-aware mode an overview to all LAN-ports is given, which shows the basic settings of the ports and give further access to detailed configuration of each LAN-port. Remember, only LAN-ports must be configured in VLAN-aware mode.

logged in as: admin
logout

VLAN Mode: Aware

Name	Def. ID	Untagged	Tagged	VLAN IDs	Egress	Edit
LAN 1 <...>	1	Discard all packets	Pass all packets	None	Pass all packets unmodified	Edit
LAN 2 <...>	2	Discard all packets	Pass all packets	None	Pass all packets unmodified	Edit
LAN 3 <...>	3	Discard all packets	Pass all packets	None	Pass all packets unmodified	Edit
LAN 4 <...>	4	Discard all packets	Pass all packets	None	Pass all packets unmodified	Edit

Global VLAN Discards:

Isolate Ports:

S-Tag:

Figure 1-51 VLAN Aware Mode

Table 1-48 provides information about the options.

Table 1-48 VLAN Aware

Parameter	Description	Format	Default
VLAN Mode	The type of VLAN Policy can be set.	PullDown Menu <ul style="list-style-type: none"> Off Aware Provider-Tagging 	Off
Global VLAN Discards	List of VLAN, which will be discarded at all LAN-ports. Note: The VLAN-ID of the in-band management (default 4094) will be discarded @ all LAN-ports and does not need to be explicitly in this list.	List of VLAN-IDs. Format: enumeration separated by comma and area specification. A mixture is possible. E.g.: 1,2, 4-8, 12, ...	None

Table 1-48 VLAN Aware (continued)

Parameter	Description	Format	Default
Isolate Ports	The LAN-ports can be isolated between each other. Isolation prohibits packet transfer between the LAN-ports. If isolation is enabled, packets from LAN-ports may only be forwarded to LINE-ports. Isolation may be switched off, when all LAN-ports are used for the same customer.	PullDown Menu <ul style="list-style-type: none"> • No • Yes 	Yes
S-Tag	The Ethertype for the S-Tag.	Input (>=0x8100)	00x88A8

Table 1-49 provides information on the overview table.

Table 1-49 VLAN Aware Overview Table

Parameter	Description	Format
Name	Name of LAN-port	Display
Def. ID	Default VLAN-ID for this port. All untagged packets may be tagged on ingress with this VID.	Display
Untagged	Setting for behaviour when untagged packets are ingressing the port.	Display
Tagged	Setting for behaviour when tagged packets are ingressing the port.	Display
VLAN IDs	List of associated VLAN IDs	Display
Egress	Setting for behaviour when packets are egressing the port.	Display
Edit	Submenu to configure the presented settings	Action

Edit Port VLAN Aware Settings

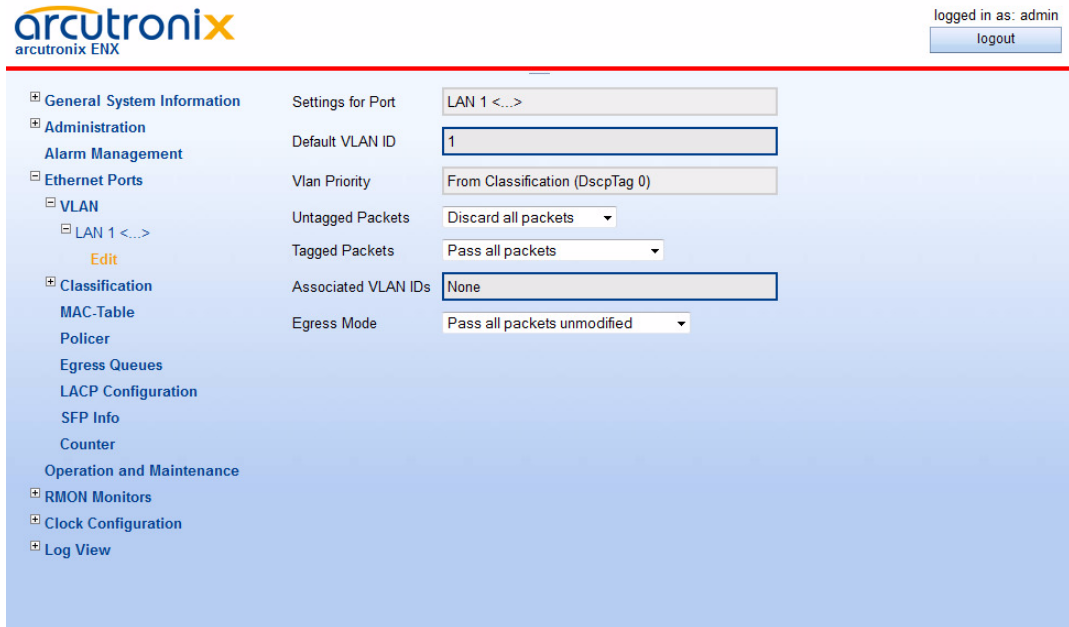


Figure 1-52 Edit Port VLAN Aware Settings

Table 1-48 provides information about the options.

Table 1-50 Edit Port VLAN Aware Settings

Parameter	Description	Format	Default
Setting for Port	Name of the port	Display	
Default VLAN ID	Default VLAN-ID for this port. All untagged packets may be tagged on ingress with this VID. Note: The VLAN-ID of the in-band management (default 4094) might be configured here as Default VID. But then the in-band Port must be changed to a different VID.	Input (1 - 4095)	LAN 1: 1 LAN 2: 2 LAN 3: 3 LAN 4: 4
Untagged Packets	Setting for behaviour when untagged packets are ingressing the port.	PullDown Menu <ul style="list-style-type: none"> Force default VLAN ID Discard all Packets 	Force Default VLAN ID

Table 1-50 Edit Port VLAN Aware Settings (continued)

Parameter	Description	Format	Default
Tagged Packets	Setting for behaviour when tagged packets are ingressing the port.	PullDown Menu <ul style="list-style-type: none">• Pass all Packets• Allow associated VLANs only• Block associated VLANs• Force default VLAN ID• Discard all Packets	Pass all Packets
Associated VLAN IDs	List of associated VLAN IDs	List of VLAN-IDs. Format: enumeration separated by comma and area specification. A mixture is possible. E.g.: 1,2, 4-8, 12, ...	None
Egress Mode	Setting for behaviour when packets are egressing the port.	PullDown Menu <ul style="list-style-type: none">• Pass all packets unmodified• Remove tag from all packets• Remove default VLAN ID only	Pass all packets unmodified.

Provider-Tagging Mode

The functionality and possible settings of the VLAN Provider-Tagging Mode is depicted in detail in chapter “Provider VLAN-Tagging” in [axManualENX].

In Provider-tagging mode an overview to all LAN-ports is given, which shows the basic settings of the ports and give further access to detailed configuration of each LAN-port. Remember, only LAN-ports must be configured in Provider-tagging mode.

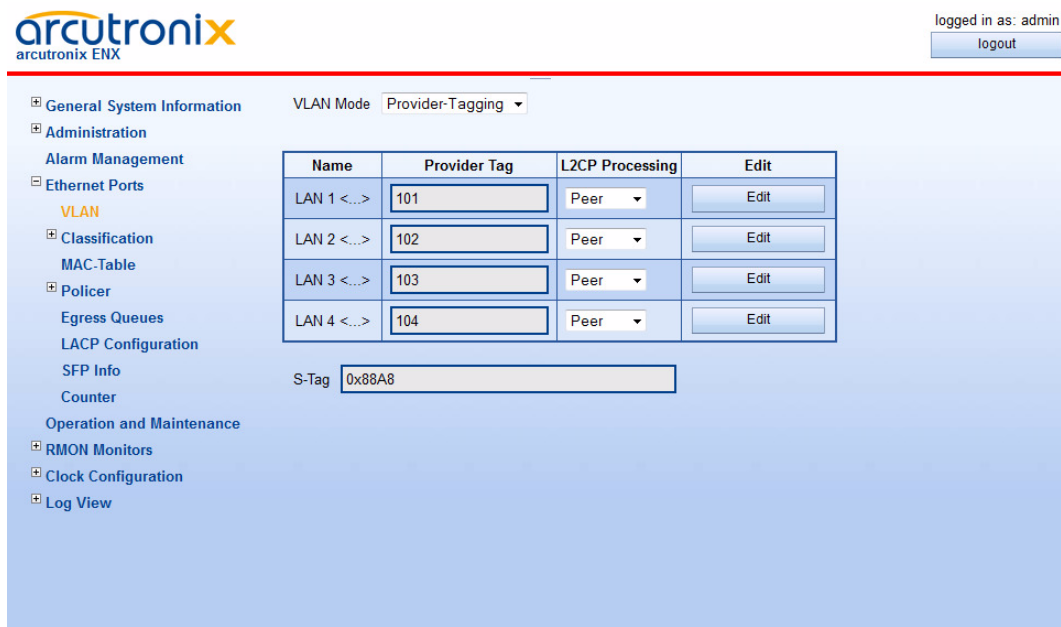


Figure 1-53 Provider-Tagging

Table 1-51 provides information about the options.

Table 1-51 Provider-Tagging

Parameter	Description	Format	Default
VLAN Mode	The type of VLAN Policy can be set.	PullDown Menu <ul style="list-style-type: none"> Off Aware Provider-Tagging 	Off
S-Tag	The Ethertype for the S-Tag.	Input (>=0x8100)	00x88A8

Table 1-52 provides information on the overview table.

Table 1-52 Provider Tagging Overview Table

Parameter	Description	Format	Default
Name	Name of LAN-port	Display	Display
Provider Tag	VLAN-ID for provider tag this port. All packets are tagged on ingress with this VID.	Input (1 - 4095)	LAN 1: 101 LAN 2: 102 LAN 3: 103 LAN 4: 104

Table 1-52 Provider Tagging Overview Table (continued)

Parameter	Description	Format	Default
L2CP Processing	<p>Set processing of L2CP frames on this port.</p> <p>Peer = Handle L2CP locally.</p> <p>Discard = Discard ingress L2CP frames, do not generate any L2CP frames.</p> <p>Tunnel = Transparently pass L2CP packets.</p> <p>See chapter “L2CP Frames Handling” of [axManualENX] and [MEF 10.2] for details.</p>	<p>PullDown Menu</p> <ul style="list-style-type: none"> • Peer • Discard • Tunnel 	Peer
Edit	Submenu to configure the presented settings	Action	Action

Edit Port Provider-Tagging Settings

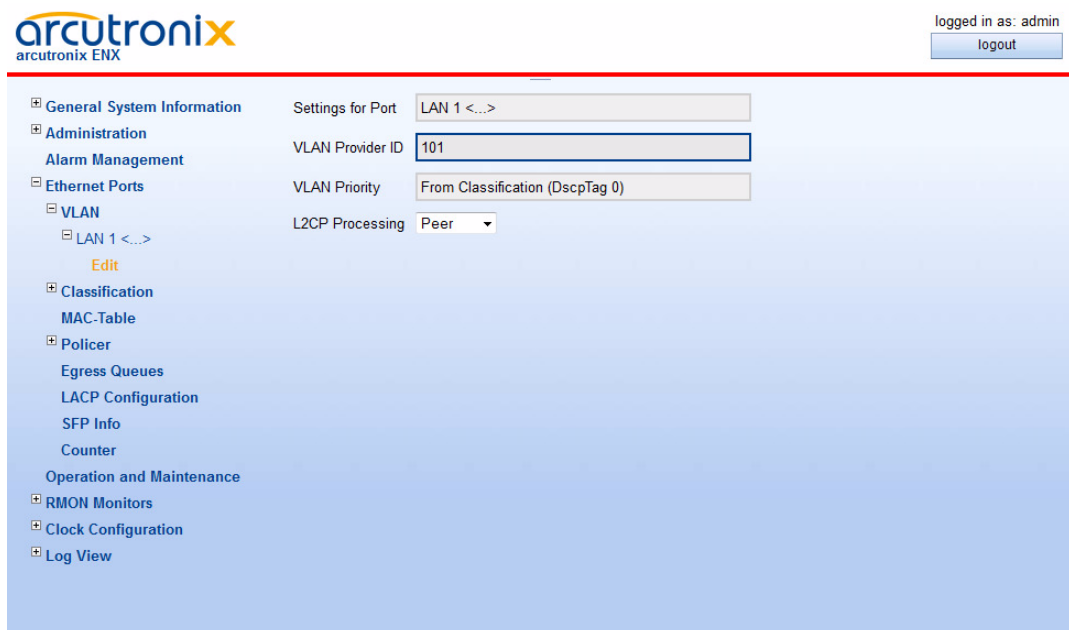


Figure 1-54 Edit Port Provider-Tagging Settings

Table 1-48 provides information about the options.

Table 1-53 Edit Port Provider-Tagging

Parameter	Description	Format	Default
Setting for Port	Name of the port	Display	
VLAN Provider ID	Provider VLAN-ID for this port. All packets are tagged on ingress with this VID.	Input (1 - 4095)	LAN 1: 101 LAN 2: 102 LAN 3: 103 LAN 4: 104
VLAN Priority	Information Field indicating the source (and value) of the VLAN Priority Field.	Display	
L2CP Processing	Setting for handling of Layer 2 Control Protocols. See chapter "L2CP Frames Handling" of [axManualENX] and [MEF 10.2] for details.	PullDown Menu <ul style="list-style-type: none"> • Peer • Discard • Tunnel 	

Classification

The classifier block of ENX is responsible assigning each packet its characterisation. The assigned character defines the further handling of the packets within the forwarding plane and allows to differentiate.

The characterisation ("Ingress Classification") can be based on different information, coming with(in) the packet:

- Layer3 (IP) DSCP field,
- Layer2 (Ethernet) VLAN priority or
- Ingress port's priority.

Layer3 (IP-DSCP) and Layer2 (VLAN) information is not available for all packets ingressing the device, while the port's priority is an attribute, which is added by the ENX and exits always for analysis. The order of evaluation of the 3 mentioned attributes can be configured per port and the first match will decide about the characterisation. The per port option gives the possibility to achieve different behaviour for different customers.

NOTE: While the classification based on VLAN priority can be configured on a per port basis, the IP-DSCP based classification is a device-wide setting. So the VLAN classification can/must be configured for each port, and the DSCP-classification can/must be configured once for all ports.

The characterisation consists out of 2 stickers, which are attached to the packets: priority-sticker and queue-sticker. Both use the same match-order of characterisation ("Ingress Classification").

The menu shows a table, which consists out of all “data-plane” Ethernet-interfaces. Each interface can get its priority-value and the order of classification. The VLAN-prio to priority-sticker mapping can be defined on a per port basis:

The screenshot shows the Arcutronix ENX Web-GUI interface. On the left is a navigation menu with categories like General System Information, Administration, Ethernet Ports, and Classification. The 'Classification' section is expanded, showing options for DSCP Classification, Priority2Queue Mapping, MAC-Table, Policer, Egress Queues, LACP Configuration, SFP Info, Counter, Operation and Maintenance, RMON Monitors, Clock Configuration, and Log View. The main content area displays a table with the following data:

Name	Default Priority	Vlan Classification	Ingress Classification
LAN 1 <...>	p0	Vlan Priority to Prio Sticker	IP-DSCP; VLAN; Default Priority
LAN 2 <...>	p0	Vlan Priority to Prio Sticker	IP-DSCP; VLAN; Default Priority
LAN 3 <...>	p0	Vlan Priority to Prio Sticker	IP-DSCP; VLAN; Default Priority
LAN 4 <...>	p0	Vlan Priority to Prio Sticker	IP-DSCP; VLAN; Default Priority
LINE 1 <...>	p0	Vlan Priority to Prio Sticker	IP-DSCP; VLAN; Default Priority
LINE 2 <...>	p0	Vlan Priority to Prio Sticker	IP-DSCP; VLAN; Default Priority

Figure 1-55 Classification

Table 1-54 provides information about the options.

Table 1-54 Classification

Parameter	Description	Format	Default
Name	Name of Ethernet-IF	Display	
Default Priority	The port's Default priority for classification purposes. The value range is p0 (low priority) to p7 (high priority).	PullDown Menu <ul style="list-style-type: none"> • p0 • ... • p7 	p0

Table 1-54 Classification (continued)

Parameter	Description	Format	Default
VLAN Classification	Submenu	Button	
Ingress Classification	<p>Order of the 3 sources for classification (characterisation). The 3 sources are:</p> <ul style="list-style-type: none"> • Layer3 (IP-DSCP) • Layer2 (VLAN) • Port (Default) Priority <p>One of 5 options of order can be selected per port. The order is given in the name: First occurrence = highest order to match.</p>	<p>PullDown Menu</p> <ul style="list-style-type: none"> • Default Priority • VLAN; Default Priority • VLAN; IP-DSCP; Default Priority • IP-DSCP; VLAN; Default Priority • IP-DSCP; Default Priority 	<p>IP-DSCP; VLAN; Default Priority</p>

VLAN Priority to Priority Sticker

A mapping can be defined for VLAN-prio to priority-sticker. This mapping is valid per port and is used, when in the “Ingress Classification” the VLAN is part of the characterisation order.

The 8 VLAN priorities (Prio0 to Prio7) can be freely mapped to the 8 priority-stickers (p0 to p7). It is possible assigning more than one VLAN priority to a single priority-sticker (e.g. Prio0 - Prio3 = p0; Prio4 - Prio7 = p5).

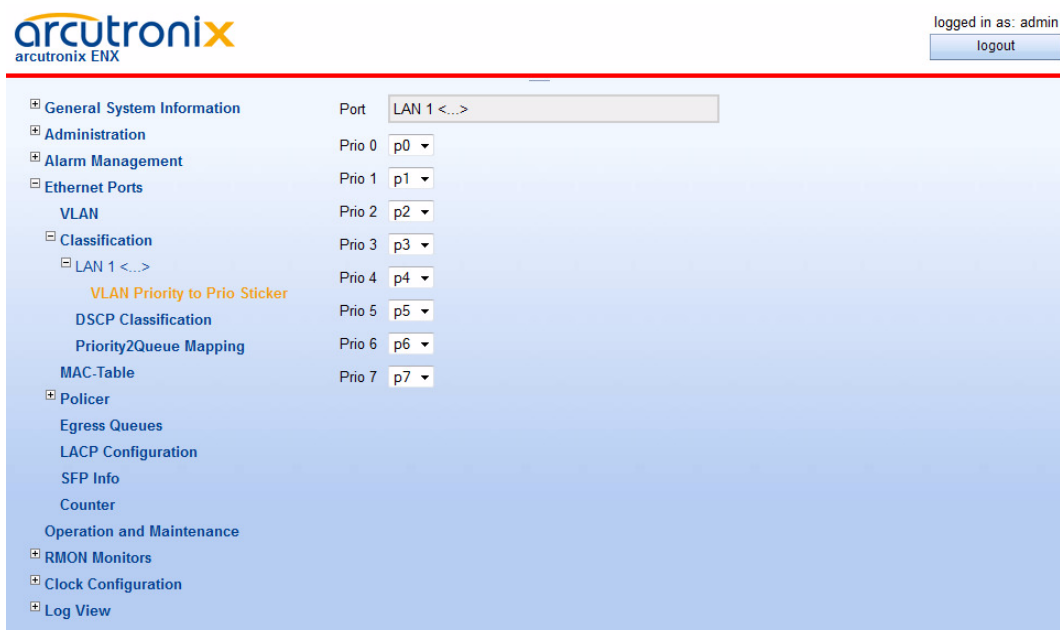


Figure 1-56 VLAN Priority to Prio Sticker

Table 1-55 provides information about the options.

Table 1-55 VLAN Priority to Prio Sticker

Parameter	Description	Format	Default
Port	Name of Ethernet-IF	Display	
Prio X	8 VLAN priority values, which need mapping to (internal) priority-sticker (p0 to p7). p0 is the lowest, p7 the highest priority.	PullDown Menu <ul style="list-style-type: none"> • p0 • ... • p7 	pX

DSCP Classification

A mapping can be defined for DSCP value to priority-sticker and queue-sticker. This mapping is valid for the whole device and is used, when in the “Ingress Classification” the IP-DSCP is part of the characterisation order.

The 64(!) DSCP-values (000000 to 111111) can be freely mapped to the 8 priority-stickers (p0 to p7) and 4 queue-stickers (Q1 to Q4). For better understanding, the table does contain the pre-defined DSCP values for Class Selector ([IETF RFC 2474]), Assured Forwarding ([IETF RFC 2597]) and Expedited Forwarding ([IETF RFC 3246]).

It is possible assigning more than one DSCP value to a single priority-sticker (e.g. 000000-000111 = p0; 001000 - 111111 = p5).

	DSCP	Priority Sticker	Queue Sticker
000000	CS0	p0	Q1
000001		p0	Q1
000010		p0	Q1
000011		p0	Q1
000100		p0	Q1
000101		p0	Q1
000110		p0	Q1
000111		p0	Q1
001000	CS1	p0	Q1
001001		p0	Q1
001010	AF11	p0	Q1
001011		p0	Q1
001100	AF12	p0	Q1
001101		p0	Q1
001110	AF13	p0	Q1
001111		p0	Q1
010000	CS2	p2	Q2
010001		p2	Q2
010010	AF21	p2	Q2
010011		p2	Q2
010100	AF22	p2	Q2
010101		p2	Q2
010110	AF23	p2	Q2
010111		p2	Q2
011000	CS3	p2	Q2
011001		p2	Q2
011010	AF31	p2	Q2

Figure 1-57 DSCP Classification

Table 1-56 provides information about the options.

Table 1-56 DSCP Classification

Parameter	Description	Format	Default
DSCP	Column for DiffServ Code Points. For better reading, the 3 pre-defined subsets (CS, AF and EF) are mentioned, too.	Display	

Table 1-56 DSCP Classification (continued)

Parameter	Description	Format	Default
Priority Sticker	64 DSCP values, which need mapping to (internal) priority-sticker (p0 to p7). p0 is the lowest, p7 the highest priority.	PullDown Menu • p0 • ... • p7	pX
Queue Sticker	64 DSCP values, which need mapping to (internal) queue-sticker (Q1 to Q4). Q1 is the lowest, Q4 the highest queue priority.	PullDown Menu • Q1 • ... • Q4	QX

Priority2Queue Mapping

A mapping can be defined between priority-sticker to queue-sticker. This mapping is valid for queue classification only.

The 8 priority-sticker (p0 to p7) can be freely mapped to the 4 queue-stickers (Q1 to Q4). It is possible assigning more than one priority-sticker to a single queue-sticker (e.g. p0 - p3 = Q1; p4 - p7 = Q3).

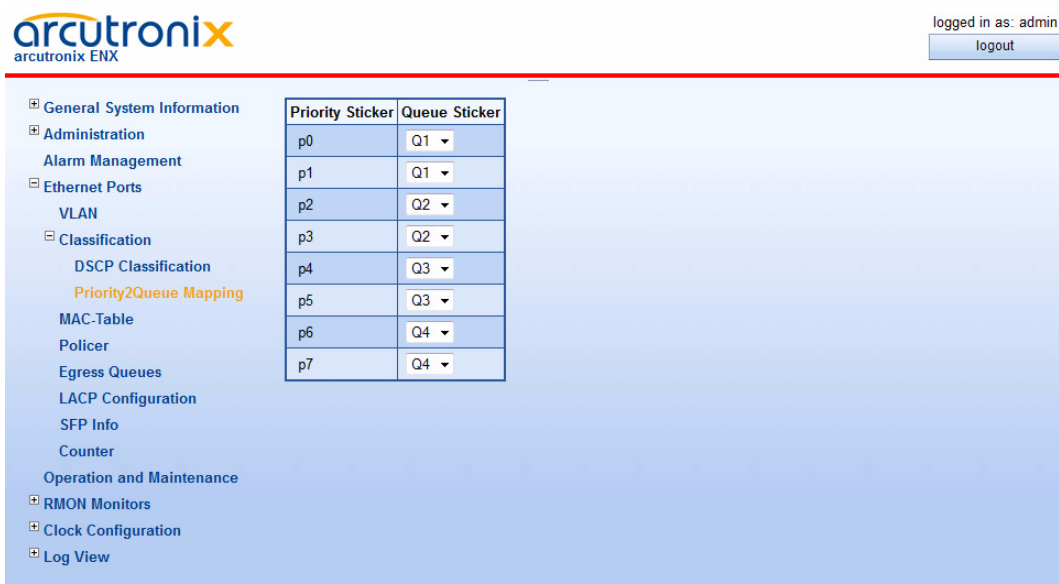


Figure 1-58 Priority2Queue Mapping

Table 1-57 provides information about the options.

Table 1-57 VPriority2Queue Mapping

Parameter	Description	Format	Default
Queue Sticker	8 priority-sticker values, which need mapping to (internal) queue-sticker (Q1 to Q4). Q1 is the lowest, Q4 the highest queue priority.	PullDown Menu <ul style="list-style-type: none"> • Q1 • ... • Q4 	QX

MAC Table

The MAC Table submenu is dedicated to clean-up the MAC table entries per port or for the whole device. If the unit shall be used in a different environment, it might be useful to delete all entries in the MAC address table to make it start from an empty list.

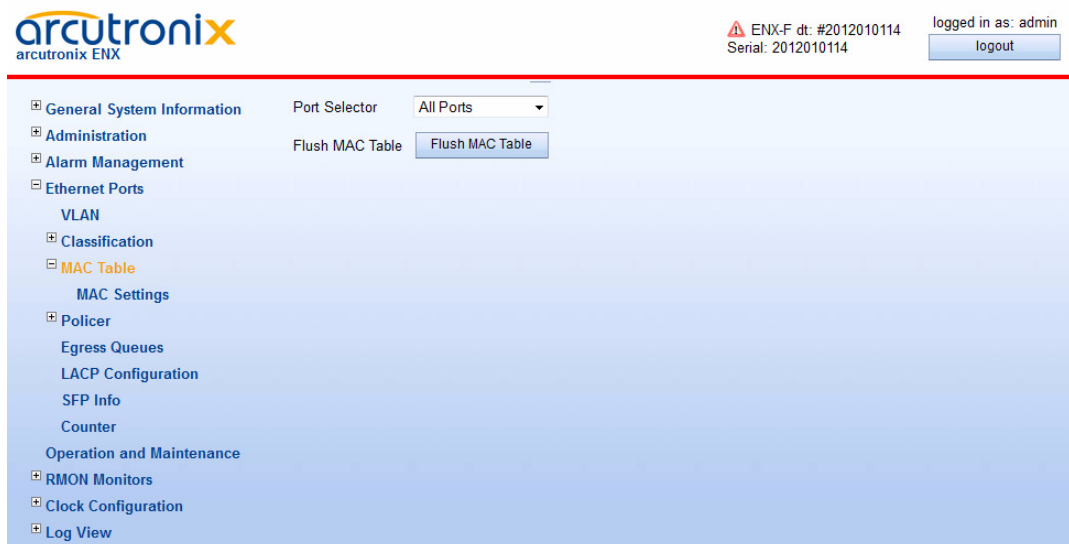


Figure 1-59 MAC Table

Table 1-59 provides information about the options.

Table 1-58 MAC Table

Parameter	Description	Format	Default
Port Selector	Choose for which port(s) MAC table command (flush) are executed.	PullDown Menu <ul style="list-style-type: none"> • All Ports • LINE 1 • LINE 2 • LAN 1 • LAN 2 • LAN 3 • LAN 4 • LINE Port Group • LAN Port Group 	All Ports
Flash MAC Table	The complete MAC Table or the entries for the selected part will be cleaned.	Action	

To define the aging time of the MAC learning instance, select the submenu MAC Settings.

MAC Settings

In MAC Settings the aging time of the MAC learning instance can be defined. It is valid for the whole device.

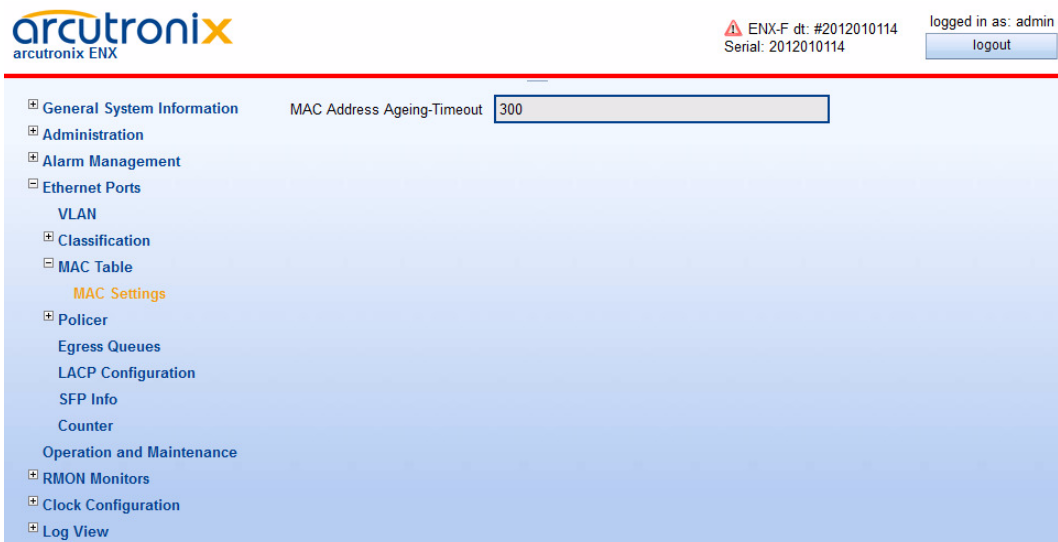


Figure 1-60 MAC Table

Table 1-59 provides information about the options.

Table 1-59 MAC Settings

Parameter	Description	Format	Default
MAC Address Ageing Timeout	The amount of time an entry (the packet source MAC address and port that packet ingresses) remain in the MAC table. The value 0 means that MAC ageing is disabled.	Input	300

Policer

The policing of packets is done in two steps:

- Ingress Packet Limiter
- Egress Stream Shaping

Ingress Limiter

The ingress is a per port tool to limit incoming traffic to the maximum of service-level-agreement (SLA). Per port up to 4 different limiter can be configured to act on different streams of frames.

The screenshot shows the Arcutronix ENX web interface. In the top right corner, it says "logged in as: admin" with a "logout" button. The left navigation menu includes: General System Information, Administration, Alarm Management, Ethernet Ports, VLAN, Classification, MAC-Table, Policer (highlighted), Ingress Limiter (highlighted), Egress Shaper, Egress Queues, LACP Configuration, SFP Info, Counter, Operation and Maintenance, RMON Monitors, Clock Configuration, and Log View. The main content area displays a table with three columns: Name, Info, and Edit. The table lists configurations for LAN 1-4 and LINE 1-2, all showing "No limiting active" and an "Edit Ingress Limiting" button.

Name	Info	Edit
LAN 1 <...>	No limiting active	Edit Ingress Limiting
LAN 2 <...>	No limiting active	Edit Ingress Limiting
LAN 3 <...>	No limiting active	Edit Ingress Limiting
LAN 4 <...>	No limiting active	Edit Ingress Limiting
LINE 1 <...>	No limiting active	Edit Ingress Limiting
LINE 2 <...>	No limiting active	Edit Ingress Limiting

Figure 1-61 Ingress Limiter

The menu gives a rough overview to the six ports and whether or not a limiter is configured to them. When pressing the “Edit Ingress Limiting”, a submenu is entered to configure the ingress limiters per port.

Edit Ingress Limiting (LAN 1-4, LINE 1-2)

This menu lists the optional 4 limiter, which are available per port. Each limiter is summarized and be configured in detail, when entering the submenu via “Edit”.



Figure 1-62 Edit Ingress Limiter



Figure 1-63 Edit Specific Ingress Limiter

The figure above shows as an example the menu for Limiter 1 of Port LAN 1.

Table 1-60 provides information about the options.

Table 1-60 Edit Specific Ingress Limiter

Parameter	Description	Format	Default
Port	Port label plus user-defined name	Display	
Limiter	Limiter's name on this port.	Display	

Table 1-60 Edit Specific Ingress Limiter (continued)

Parameter	Description	Format	Default
Limiting Mode	<p>The limiter can be disabled or it is enabled and its rate can be given in Bits-per-second (“Rate Limiting”) or frames-per-second (“Frames/s Limiting”).</p> <p>When “Limiting Mode” is equal to “Rate Limiting”, the values for “Rate Limit (CIR)” and “Rate Burst Size” are taken into account.</p> <p>When “Limiting Mode” is equal to “Frames/s Limiting”, only the value for “Frames per Second” is taken into account.</p>	PullDown Menu <ul style="list-style-type: none"> • Disabled • Rate Limiting • Frames/s Limiting 	Disabled
Frame Type	Frame-types, which are handled by this limiter.	PullDown Menu <ul style="list-style-type: none"> • All Frames • Unicast Frames • Unkown Unicast Frames • Multicast Frames • Broadcast Frames • Multicast and Broadcast Frames • TCP Frames • UDP Frames • Non-TCP/UDP Frames 	All Frames
Priorities	The Queue-priorities, sticked to the selected frame types, which are handled by this limiter.	PullDown Menu <ul style="list-style-type: none"> • Q1 Frames • Q2 Frames • Q3 Frames • Q4 Frames • Q1-Q2 Frames • Q1-Q3 Frames • Q2-Q3 Frames • Q2-Q4 Frames • Q3-Q4 Frames • All Frames 	All Frames

Table 1-60 Edit Specific Ingress Limiter (continued)

Parameter	Description	Format	Default
Rate Limit (CIR)	<p>This is the ingress Committed Information Rate.</p> <p>Enter the ingress rate limit. As a suffix kbps or Mbps is possible. If no suffix is given, the Rate Limit is in bps (bit-per-second).</p> <p>Note: The value of Rate Limit is used when "Limiting Mode" is set to "Rate limiting".</p>	Value to enter	0 kbps
Rate Burst Size	<p>Enter the ingress burst size. The ingress burst size is the accepted amount of data above the specified limiting rate, which is accepted as a burst.</p> <p>As a suffix kB or MB is possible. If no suffix is given, the Rate Burst Size is in Byte.</p> <p>Note: The value of Rate Burst size is used when "Limiting Mode" is set to "Rate limiting".</p>	Value to enter	0 kB
Frames per Second	<p>Enter the ingress rate in frames per second.</p> <p>Note: The value of Frames per Second is used when "Limiting Mode" is set to "Frames/s limiting".</p>	Value to enter	
Effective Limit	<p>The resulting limit rate, calculated on the given settings and considering the internal architecture is displayed.</p>	Display	empty

Egress Shaper

The per port egress shaper can be individually configured as a maximum egress bandwidth. The shaper menu gives an overview about the ports and the configured shaper bandwidth. Entering the submenu for each port ("Edit), one can configure the individual settings.

arcutronix
arcutronix ENX

logged in as: admin
logout

Name	Egress Limit	Edit
LAN 1 <...>	Off	Edit
LAN 2 <...>	Off	Edit
LAN 3 <...>	Off	Edit
LAN 4 <...>	Off	Edit
LINE 1 <...>	Off	Edit
LINE 2 <...>	Off	Edit

Figure 1-64 Egress Shaper

The ENX does have a granularity for the shaper, meaning not every value is possible:

Bandwidth on Port	Units for Shaper
0 - 1Mbps	64 kbps - steps
1 - 100 Mbps	1000 kbps - steps
100 - 1000 Mbps	10 Mbps - steps

If the configuration does not match the possible values, the device will step down the user's wish to the next allowed value. Both values (wish and effective) will be stored and displayed.

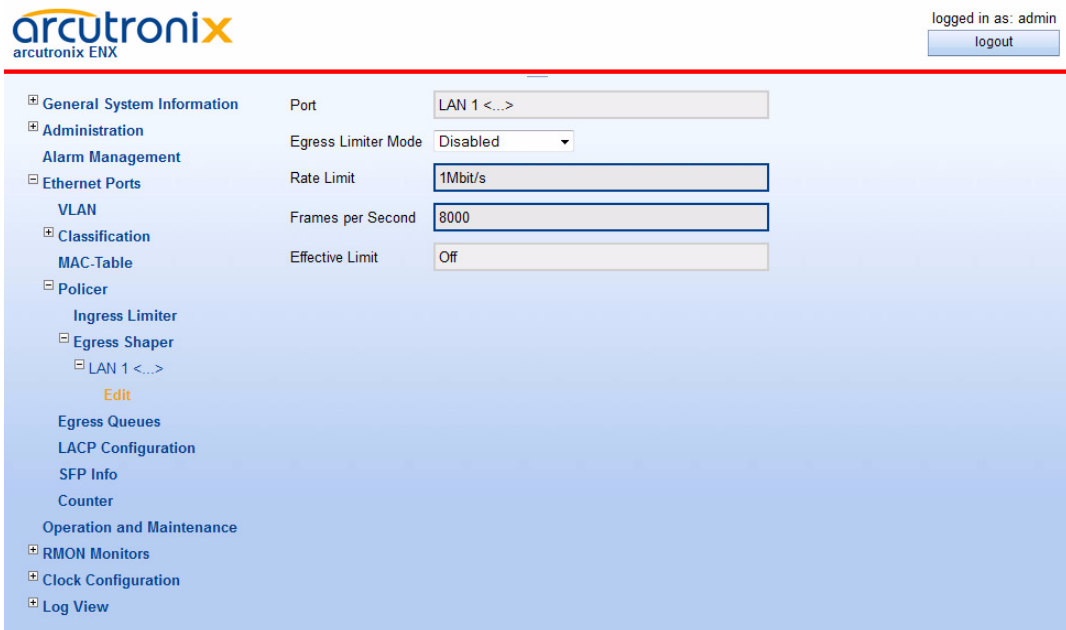


Figure 1-65 Egress Shaper Settings

Table 1-61 provides information about the options.

Table 1-61 Egress Shaper

Parameter	Description	Format	Default
Port	Port label plus user-defined name	Display	
Egress Shaping Mode	<p>The shaper can be disabled or it is enabled and its rate can be given in Bits-per-second (“Rate Limiting”) or frames-per-second (“Frames/s Limiting”).</p> <p>When “Egress Shaping Mode” is equal to “Rate Limiting”, only the value for “Rate Limit (CIR)” is taken into account.</p> <p>When “Egress Shaping Mode” is equal to “Frames/s Limiting”, only the value for “Frames per Second” is taken into account.</p>	PullDown Menu <ul style="list-style-type: none"> • Disabled • Rate Limiting • Frames/s Limiting 	Disabled

Table 1-61 Egress Shaper (continued)

Parameter	Description	Format	Default
Rate Limit (CIR)	<p>This is the egress Committed Information Rate.</p> <p>Enter the egress rate limit. As a suffix kbps or Mbps is possible. If no suffix is given, the Rate Limit is in bps (bit-per-second).</p> <p>Note: The value of Rate Limit is used when "Egress Shaping Mode" is set to "Rate Limiting".</p>	Value to enter	0 kbps
Frames per Second	<p>Enter the ingress rate in frames per second.</p> <p>Note: The value of Frames per Second is used when "Egress Shaping Mode" is set to "Frames/s Limiting".</p>	Value to enter	
Effective Limit	<p>The resulting limit rate, calculated on the given settings and considering the internal architecture is displayed.</p>	Display	empty

Egress Queues

Each port does have 4 egress queues, which represent different priorities for sending out packets. Packets from the queues with the higher priority will be sent first. Several algorithms can be selected to achieve different network behaviour. See "Queue Scheduler" of [axManualENX] for details.

The screenshot shows the Arcutronix ENX web interface. At the top left is the Arcutronix logo. At the top right, it says "logged in as: admin" with a "logout" button. The main content area has a left-hand navigation menu with categories like "General System Information", "Administration", "Ethernet Ports", "Classification", "Egress Queues" (highlighted), "LACP Configuration", "SFP Info", "Counter", "Operation and Maintenance", "RMON Monitors", "Clock Configuration", and "Log View". To the right of the menu, there is a "Fair Queuing Weights" dropdown menu currently set to "Standard (8,4,2,1)". Below this is a table with two columns: "Port" and "Queueing Mode". The table contains six rows, each representing a different port or line, all of which are configured with "Weighted Fair Queueing".

Port	Queueing Mode
LAN 1 <...>	Weighted Fair Queueing
LAN 2 <...>	Weighted Fair Queueing
LAN 3 <...>	Weighted Fair Queueing
LAN 4 <...>	Weighted Fair Queueing
LINE 1 <...>	Weighted Fair Queueing
LINE 2 <...>	Weighted Fair Queueing

Figure 1-66 Egress Queues

Table 1-62 provides information about the options.

Table 1-62 Egress Queues

Parameter	Description	Format	Default
Fair Queueing Weights	The weights for Weighted Fair Queueing can be selected between 3 modes. The 4 priority queues (prio Q4, prio Q3, prio Q2, prio Q1) will get the selected weight and have more or less precedence over the lower queues.	PullDown Menu <ul style="list-style-type: none"> Standard (8,4,2,1) Progressive (64,16,4,1) Smooth (4,3,2,1) 	Standard (8,4,2,1)
Queueing Mode	Per port one of 4 modes to read out packets from the queues can be selected: <ul style="list-style-type: none"> Weighted Fair Queueing: The queues will get shared access. Use the settings above. Queue 4strict; else...: Queue with Prio1 will get always Strict Priority over all others, the rest is WFQ. Queues 4, 3strict...: Queues with Prio1 and 2 will get always Strict Priority over all others, the rest is WFQ. Strict Priority: Higher prio-queues will get strict precedence over lower queues. 	PullDown Menu <ul style="list-style-type: none"> Weighted Fair Queueing Queue 4strict; else Weighted Fair Queueing Queues 4, 3strict; else Weighted Fair Queueing Strict Priority queueing 	Weighted Fair Queueing

LACP

Link Aggregation Control Protocol to achieve LINE-bundling for higher (virtual) throughput. LACP operates layer 2 (data link layer). Systems supporting LACP exchange link-local, multicast Ethernet frames with their link partner to negotiate their aggregation capabilities. LACP operates transparently to higher OSI layers by introducing virtual MACs (called Aggregators) that represent the aggregation.

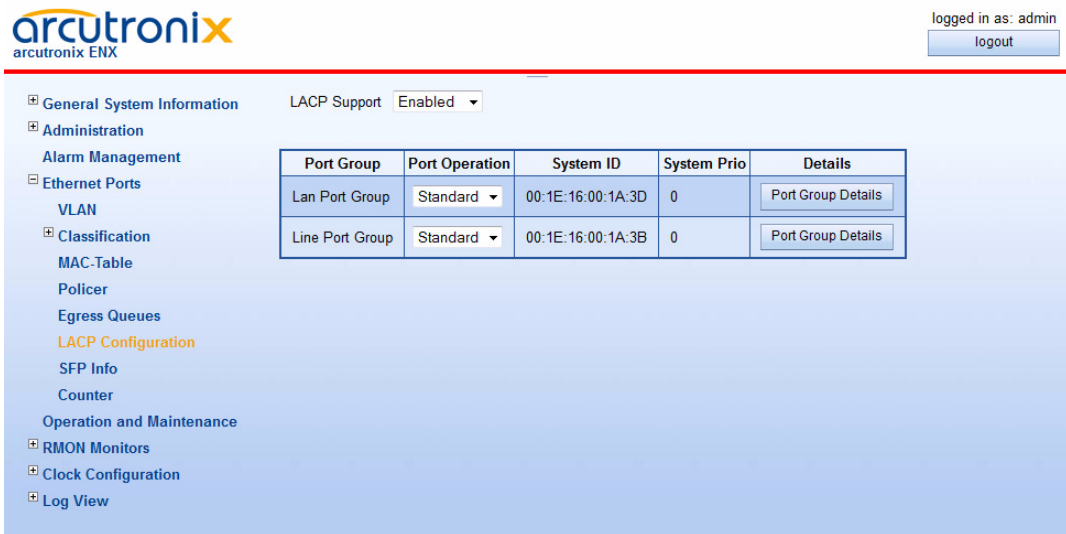


Figure 1-67 LACP

The ENX device has built-in support for LACP that can be enabled or disabled with the “LACP Support” variable. If enabled, the ENX will start to generate and respond to LACP messages on all LAN/LINE ports and show a table containing a row for each port group.

The “Port Operation” setting determines whether the ENX device allows Ethernet ports within the port group to be aggregated. If set to “Standard”, the ports will never be bonded. If set to “LACP”, the Ethernet ports within the group will automatically be bonded if possible.

The “Port Group Details” button opens a new page showing the current port aggregation status for this group and allowing configuring further LACP protocol properties.

Port Group Details

The “LACP Mode” setting determines whether the ENX does Active or Passive LACP on the ports within the port group. “Active LACP” implies a regular exchange of LACP status information between link partners, whereas “Passive LACP” reduces exchange of LACP messages to cases of LACP configuration changes.

arcutronix ENX logged in as: admin
logout

General System Information
 Administration
 Alarm Management
 Ethernet Ports
 VLAN
 Classification
 MAC-Table
 Policer
 Egress Queues
 LACP Configuration
 Line Port Group
 Port Group Details
 LACP Aggregators
 SFP Info
 Counter
 Operation and Maintenance
 RMON Monitors
 Clock Configuration
 Log View

Group name:

Port Group LACP Mode:

LACP System ID:

LACP System Priority:

LACP Mode:

LACP Transmit Interval:

Aggregation Configuration:

Port	Aggregator	Details			
LINE 1 <...>	Aggregator 5 <...>	<input type="button" value="Local Port Details"/>	<input type="button" value="Remote Port Details"/>	<input type="button" value="Remote Admin Settings"/>	<input type="button" value="LACP counters"/>
LINE 2 <...>	Aggregator 6 <...>	<input type="button" value="Local Port Details"/>	<input type="button" value="Remote Port Details"/>	<input type="button" value="Remote Admin Settings"/>	<input type="button" value="LACP counters"/>

Port Overview

Port	Link	Duplex	Port State						Partner Port	Partner Port State			
LINE 1 <...>	Down	Half	Not Aggregatable	Synchronized	Not Collecting	Not Distributing	Defaulted	Up To Date	5	Aggregatable	Not Synchronized	Collecting	Distributing
LINE 2 <...>	Down	Half	Not Aggregatable	Synchronized	Not Collecting	Not Distributing	Defaulted	Up To Date	6	Aggregatable	Not Synchronized	Collecting	Distributing

Figure 1-68 LACP Port Group Details

The “LACP Transmit Interval” determines the frequency of LACP status message exchange in case of active LACP. The setting “Long LACP Interval” requires an LACP status message exchange every 30 seconds, whereas “Short LACP Interval” reduces the communication interval to one second.

The “Aggregation Configuration” setting determines whether the port aggregation configuration on the ENX device is done automatically by the device itself or manually by the device administrator. The manual configuration mode allows maximum flexibility and allows to achieve aggregation even in the absence of LACP capable link partners, whereas the automatic mode works well with LACP capable link partners, requires no further configuration and will automatically adjust to changes in the wiring.

The first table on this page contains a row for each port in this port group.

- The “Aggregator” column shows the virtual MAC to which the port is currently bound. If several ports are bound to the same aggregator, this indicates a successful aggregation.
- The “Local Port Details” button opens a page containing information about the LACP protocol details of the ENX port. Some settings on this page can be changed in manual LACP configuration mode.
- The “Remote Port Details” button opens a page containing information about the LACP protocol details of the remote link partner port. The information on this page is read-only and shows the current operational values as determined by the LACP protocol or default values in case of missing LACP protocol information.

- Those administrative default values for the remote port can be changed in manual configuration mode on the page that is opened by the “Remote Admin Settings” button.
- The “LACP Counters” button opens a page showing packet counters for LACP protocol frames.

The second table on this page gives a quick overview of the current LACP state of each port in the port group.

- The “Link” column shows whether the link is up or down.
- The “Duplex” column shows whether the port is operated in half duplex or full duplex mode. Half duplex links can never aggregate.
- The “Port State” column lists a number of LACP status flags that describe the current LACP state of the ENX port:
 - Aggregatable / Not Aggregatable: whether ENX allows this port to be bonded
 - Synchronized / Not Synchronized: whether the ENX information about the remote system is correct.
 - Collecting / Not Collecting: whether the ENX is forwarding data frames originating from the remote system.
 - Distributing / Not Distributing: whether the ENX is forwarding data frames towards the remote system.
 - Defaulted / Not Defaulted: whether the ENX is using “Remote Admin Settings” or current LACP protocol information to configure aggregation.
 - Expired / Up To Data: if “Not Defaulted”, whether the last LACP message was received in time.
- The “Partner Port” column shows the port number of the remote system to which the ENX port is connected. This information is exchanged via LACP.
- The “Partner Port State” column lists a number of LACP status flags that describes the current LACP state of the remote system port:
 - Aggregatable / Not Aggregatable: whether the remote system allows this port to be bonded (set to “Not Aggregatable” in case of half-duplex operation).
 - Synchronized / Not Synchronized: whether the remote system's information about the ENX is correct.
 - Collecting / Not Collecting: whether the remote system is forwarding data frames originating from the ENX.
 - Distributing / Not Distributing: whether the remote system is forwarding data frames towards the ENX.

LACP Aggregators

arcutronix
arcutronix ENX

logged in as: admin
logout

General System Information
Administration
Alarm Management
Ethernet Ports
VLAN
Classification
MAC-Table
Policer
Egress Queues
LACP Configuration
Line Port Group
Port Group Details
LACP Aggregators
SFP Info
Counter
Operation and Maintenance
RMON Monitors
Clock Configuration
Log View

Group name: Line Port Group
Port Group LACP Mode: LACP Disabled
LACP System ID: 00:1E:16:00:1A:3B
LACP System Priority: 0

Aggregator	Oper. Key	Ports	Partner System ID	Status	Details
Aggregator 5	< ... >	5	00:00:00:00:00:00	Not Receiving / Not Transmitting	Aggregator Details
Aggregator 6	< ... >	6	00:00:00:00:00:00	Not Receiving / Not Transmitting	Aggregator Details

Figure 1-69 LACP Aggregators

This page shows a table containing the aggregators (virtual MACs) defined for this port group. The number of aggregators is the same as the number of ports in this group to have sufficient resources available in case links cannot be aggregated:

- The “Ports” column shows the ports currently bound to the aggregator.
- The “Status” column shows whether data transfer is currently operational on the Aggregator.
 - Receiving / Not Receiving: whether the aggregator is forwarding data frames originating from the remote system.
 - Transmitting / Not Transmitting: whether the aggregator is forwarding data frames towards the remote system.
- The “Aggregator Details” shows extended information about the aggregator and allows configuring whether logical link state changes shall generate an SNMP linkUp/linkDown trap.

SFP Info

The SFP-Info submenu gives information about inventory and power of the plugged SFPs.

arcutronix
arcutronix ENX

logged in as: a
logout

SFP Thresholds Source: Read thresholds from SFP when inserted

Port	SFP	Vendor	SerialNo	Tx/Rx (dBm)		Diagnostics	Details
				Tx	Rx		
LAN 3 <...>	Gigabit Ethernet SFP	FINISAR CORP.	PAM25NB	-4.915	< -40	Diagnostics	Details
LINE 1 <...>	Gigabit Ethernet SFP	FINISAR CORP.	P11JTQQ	-6.290	-31.585	Diagnostics	Details

Figure 1-70 SFP Info

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

Some SFP do have limits for alarming stored on the device itself. If such SFPs are plugged, you can decide, whether to use these limits or not.

More inventory details about the SFP can be found, when entering the submenu “Details”.

Some SFPs do support DMI = Diagnostic Monitoring Interface. DMI is a multi-vendor agreement to provide link management assistance for network operators. If DMI is supported by a plugged SFP, the “Diagnostics” submenu shows the results.

SFP Details

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



Figure 1-71 SFP Details

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

Table 1-63 provides information about the options.

Table 1-63 SFP Details

Parameter	Description	Format
SFP Info for Port	Presents the name of the elected SFP.	Display
Detected Type	The Detected Type specifies the physical device plus the service purpose.	Display
Vendor Name	The vendor name is a 16 character field. The vendor name is the full name of the corporation, a commonly accepted abbreviation of the name of the corporation, the SCSI company code for the corporation, or the stock exchange code for the corporation.	Display
Serial No	The vendor serial number (vendor SN) is a 16 character field. A value of all zero in the 16-byte field indicates that the vendor SN is unspecified	Display

Table 1-63 SFP Details (continued)

Parameter	Description	Format
Part Number	The vendor part number (vendor PN) is a 16-byte field, defining the vendor part number or product name. A value of all zero in the 16-byte field indicates that the vendor PN is unspecified.	Display
Connector Type	The connector value indicates the external optical cable connector provided as the media interface.	Display
Optical Type	These are the optical interface(s) that is (are) supported by the transceiver.	Display
Line Coding	The encoding value indicates the serial encoding mechanism that is the nominal design target of the particular transceiver.	Display
Nominal Bit Rate	The nominal bit (signalling) rate (BR, nominal) is specified in units of 100 MBd, rounded off to the nearest 100 MBd. A value of 0 indicates that the bit rate is not specified and must be determined from the transceiver technology.	Display
Link Length	This value specifies link length that is supported. The given link length is valid for the optical cable specified in quote signs.	Display
Date Code	The date code is an 8-byte field that contains the vendor's date code in ASCII characters. The date code is mandatory.	Display
Wave Length	Denotes nominal transmitter output wavelength at room temperature.	Display

SFP Diagnostics

More detailed information about the inventory data of a plugged SFP can be found [here](#).

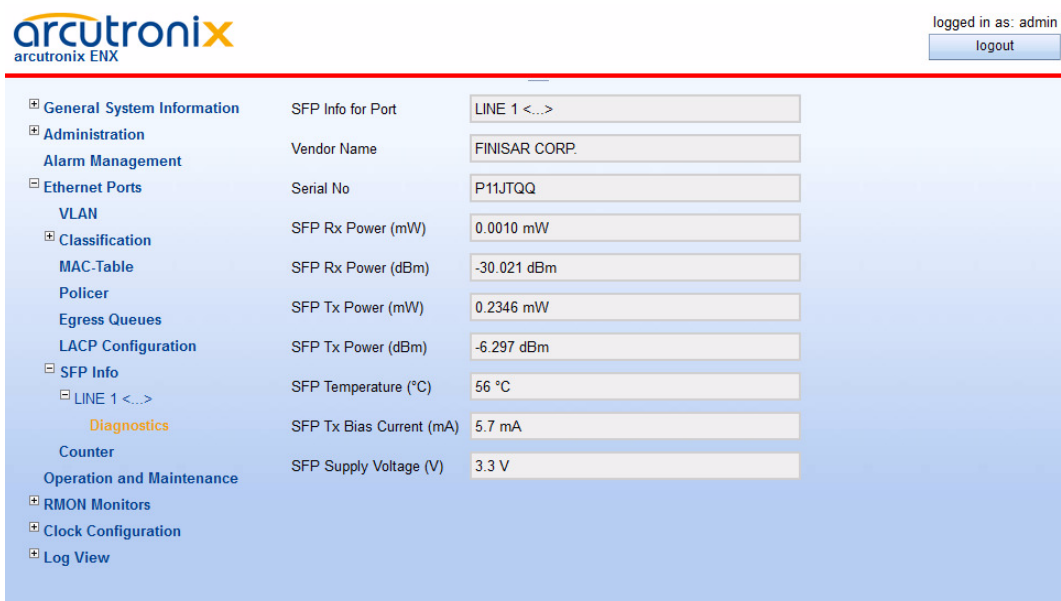


Figure 1-72 SFP Diagnostics

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

Table 1-64 provides information about the options.

Table 1-64 SFP Diagnostics

Parameter	Description	Format
SFP Info for Port	Presents the name of the elected SFP.	Display
Vendor Name	The vendor name is a 16 character field. The vendor name is the full name of the corporation, a commonly accepted abbreviation of the name of the corporation, the SCSI company code for the corporation, or the stock exchange code for the corporation.	Display
Serial No	The vendor serial number (vendor SN) is a 16 character field. A value of all zero in the 16-byte field indicates that the vendor SN is unspecified	Display
SFP Rx Power (mW)	Measured RX received optical power in mW. Value can represent either average received power or OMA.	Display
SFP Rx Power (dBm)	Measured RX received optical power in dBm. Value can represent either average received power or OMA.	Display

Table 1-64 SFP Diagnostics (continued)

Parameter	Description	Format
SFP Tx Power (mW)	Measured TX output power in mW. Data is not valid when the transmitter is disabled.	Display
SFP Tx Power (dBm)	Measured TX output power in dBm. Data is not valid when the transmitter is disabled.	Display
SFP Temperature (°C)	Internally measured transceiver temperature.	Display
SFP Tx Bias Current (mA)	Measured TX bias current in mA. Accuracy is vendor specific but must be better than $\pm 10\%$ of the manufacturer's nominal value over specified operating temperature and voltage.	Display
SFP Supply Voltage (V)	Internally measured transceiver supply voltage. Note that in some transceivers, transmitter supply voltage and receiver supply voltage are isolated. In that case, only one supply is monitored. Refer to the device specification for more detail.	Display

Counter

This submenu shows an overview of all ports and the main counters:

The screenshot shows the ENX Web-GUI interface. At the top left is the Arcutronix logo. At the top right, it says "logged in as: admin" with a "logout" button. On the left is a navigation menu with items like "General System Information", "Administration", "Ethernet Ports", "Classification", "Counter", etc. The "Counter" item is highlighted. The main content area displays a table of Ethernet ports with columns for Name, Status, InGoodOctets, InUnicasts, InBroadcasts, InMulticasts, OutGoodOctets, OutUnicasts, OutBroadcasts, and OutMulticasts. Below the table are two "Flush All Counter" buttons.

Name	Status	InGoodOctets	InUnicasts	InBroadcasts	InMulticasts	OutGoodOctets	OutUnicasts	OutBroadcasts	OutMulticasts
LAN 1 <...>	Link Down	0	0	0	0	0	0	0	0
LAN 2 <...>	Link Down	0	0	0	0	0	0	0	0
LAN 3 <...>	Link Down	0	0	0	0	0	0	0	0
LAN 4 <...>	Link Down	0	0	0	0	0	0	0	0
LINE 1 <...>	Link Down	0	0	0	0	0	0	0	0
LINE 2 <...>	Port Disabled	0	0	0	0	0	0	0	0

Figure 1-73 Ethernet Counters

Table 1-65 provides information about the options.

Table 1-65 Ethernet Counters

Parameter	Description	Format
inGoodOctets	Total data octets received in frames with a valid FCS. Undersize or oversize frames are included. The count includes the FCS but not the preamble.	Display
inUnicasts	Total valid ⁱ frames received with an unicast destination address.	Display
inBroadcast	Total valid frames received with a destination address equal to FF:FF:FF:FF:FF:FF.	Display
inMulticast	Total valid frames received with a multicast destination address that are not counted in 'inBroadcast' or 'inPause'.	Display
outGoodOctets	Total data octets transmitted from frames counted above. The count includes the FCS but not the preamble.	Display
outUnicasts	Total frames transmitted with an unicast destination address.	Display
outBroadcast	Total frames transmitted with a destination address equal to FF:FF:FF:FF:FF:FF.	Display
outMulticast	Total frames transmitted with a multicast destination address that are not counted in 'outBroadcast' or 'outPause'.	Display

i. A valid frame is one with a good FCS and whose size is 64 octets to MTU-Size octets inclusive.

More detailed counters for Ethernet ports are collected for the RMON MIB. See "RMON Monitors" on page 1-131.

Operation and Maintenance

This menu is configuring and enable the OAM protocols of ENX. For the time being this is IEEE 802.3ah, only.

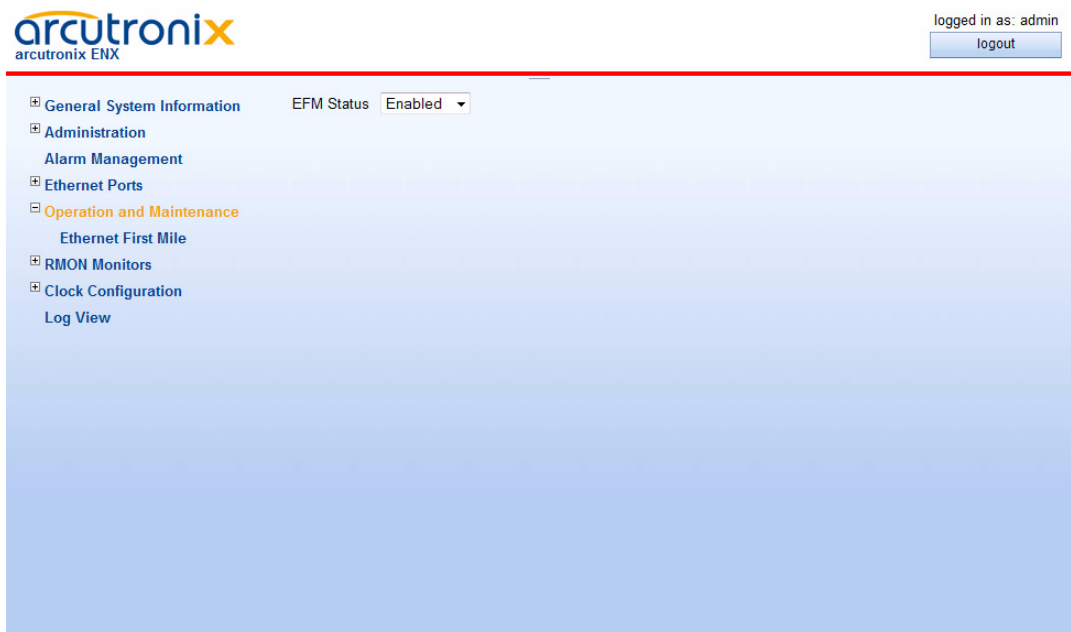


Figure 1-74 Operation and Maintenance

When EFM is enabled, the submenu “Ethernet First Mile” is visible.

Ethernet First Mile

When EFM is enabled, this submenu is visible. For each port, EFM in passive mode can be enabled or disabled.

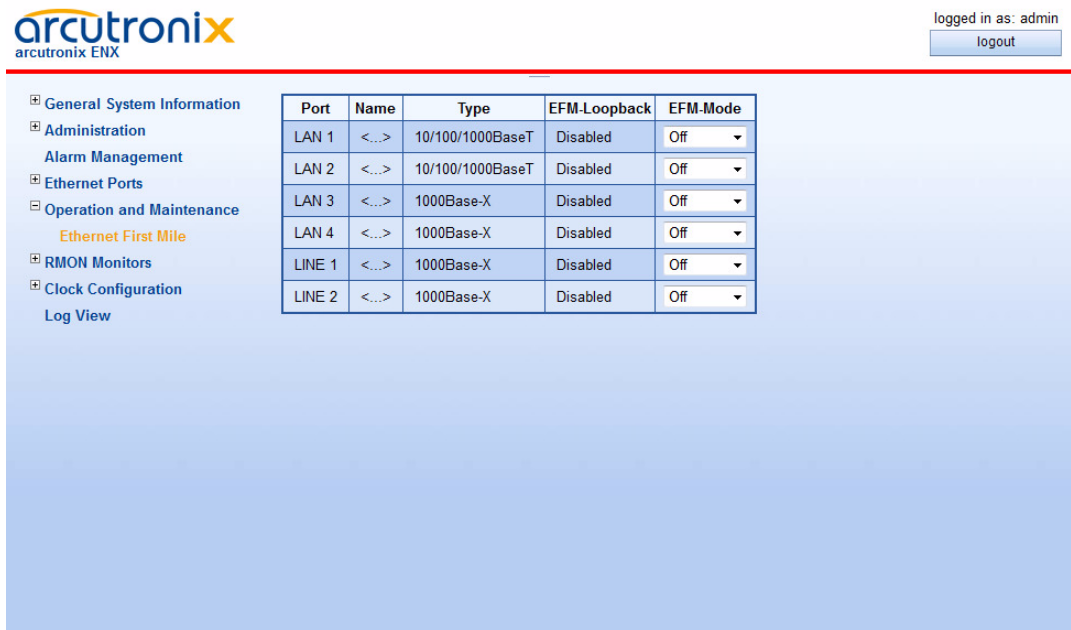


Figure 1-75 EFM

When EFM passive mode is enabled a EFM loopback can be invoked from the master-side. If this EFM loopback is invoked, it will be shown here.

RMON Monitors

The Remote Monitoring (RMON) was developed by IETF to support monitoring and protocol analysis of LANs. RMON implementation is slightly different than standard SNMP. For this reason, the RMON menu is outside the pure SNMP settings. In short, RMON is designed for “flow-based” monitoring, while SNMP is often used for “device-based” management.

A lot of variables to be monitored by RMON are predefined. But RMON opens the possibility to add any management variable to the RMON process and monitor them also. The only assumption is made, that the variable is defined in one of the device’s supported MIB. It could be a standard MIB or a vendor’s private MIB.

The Remote Monitoring is a mighty tool inside the SNMP community. With RMON many counters are defined, which can be read via SNMP and give so standard access to all devices, which support this MIB. Hereafter some global settings for RMON counters can be defined.

The screenshot shows the ENX Web-GUI interface. At the top left is the 'arcutronix' logo. At the top right, it says 'logged in as: admin' with a 'logout' button. The main content area has a sidebar menu on the left with the following items: General System Information, Administration (with sub-item Alarm Management), Ethernet Ports, Operation and Maintenance, RMON Monitors (highlighted in orange), RMON Port Counters, RMON Counter History, RMON Alarms, RMON Events, Clock Configuration, and Log View. The main content area shows two configuration fields: 'Max. Logs / Event' with a value of 250, and 'Max. Entries / History' with a value of 250.

Figure 1-76 RMON Monitors

Table 1-66 provides information about the options.

Table 1-66 *RMON Parameters*

Parameter	Description	Format	Default
Max. Logs / Event	The number of logging entries per RMON event. Be careful, this can be a huge number.	Input	250
Max. Entries / History	Maximum number of requested entries for RMON port counter histories.	Input	250

RMON Port Counters

The RMON port counters collect a huge number of statistics. If required new entries can be defined beside the predefined (automatically created) entries. A new entry will get an “owner”, making this entry easier to find.

The screenshot shows the ENX Web-GUI interface. At the top left is the Arcutronix logo. At the top right, it says "logged in as: admin" with a "logout" button. On the left is a navigation menu with categories like "General System Information", "Administration", "Alarm Management", "Ethernet Ports", "Operation and Maintenance", "RMON Monitors", "Clock Configuration", and "Log View". Under "RMON Monitors", "RMON Port Counters" is selected. The main content area displays a table of RMON Port Counters:

Port	Owner	Status	Octets	Packets	Details
LAN 1 <...>	automatically created	Active	0	0	View Details Delete Entry
LAN 2 <...>	automatically created	Active	0	0	View Details Delete Entry
LAN 3 <...>	automatically created	Active	0	0	View Details Delete Entry
LAN 4 <...>	automatically created	Active	0	0	View Details Delete Entry
LINE 1 <...>	automatically created	Active	0	0	View Details Delete Entry
LINE 2 <...>	automatically created	Active	0	0	View Details Delete Entry

Below the table, there is a "New Stats Entry" button.

Figure 1-77 *RMON Port Counter*

Entries can be deleted if it is not longer required. The details of each entry is a long list, which will not be depicted but just shown for the sake of completeness.

The screenshot shows the ENX Web-GUI interface. At the top left is the Arcutronix logo. At the top right, it says "logged in as: admin" with a "logout" button. The left navigation menu includes: General System Information, Administration, Alarm Management, Ethernet Ports, Operation and Maintenance, RMON Monitors (expanded), RMON Port Counters (expanded), LAN 1 <...> (selected), View Details, RMON Counter History, RMON Alarms, RMON Events, Clock Configuration, and Log View. The main content area displays the following settings for LAN 1:

Ethernet Port	LAN 1 <...>
Entry Owner	automatically created
Entry Status	Active ▾
Drop Events	0
Number of Octets	0
Number of Packets	0
Broadcast Packets	0
Multicast Packets	0
CRC/Align Errors	0
Undersized Packets	0
Oversized Packets	0
Fragments	0
Jabber Events	0
Detected Collisions	0
64 Byte Packets	0
Packets up to 127 Bytes	0
Packets up to 255 Bytes	0
Packets up to 511 Bytes	0
Packets up to 1023 Bytes	0
Max. Size Packets	0

Figure 1-78 RMON Counter Details

Changing the “Entry Status” from “Edit” to “Active” brings the (new) counter into action. As long as it keeps on “Edit”, it will not work properly.

NOTE: All entries, which are on status “Edit” will be deleted when system reboots!

RMON Counters History

The RMON Counter History is a list of history for each port counter in different sampling intervals. Twelve History Counters are automatically created, two for each port:

- one for 30 sec intervals
- one for 30 min intervals

More history entries for different intervals may be defined as needed.

arcutronix
arcutronix ENX

logged in as: admin
logout

- General System Information
- Administration
 - Alarm Management
- Ethernet Ports
- Operation and Maintenance
- RMON Monitors
 - RMON Port Counters
 - RMON Counter History**
 - RMON Alarms
 - RMON Events
- Clock Configuration
- Log View

Port	Owner	Status	Sampling Interval	Max. Entries	Available Entries	Details	
LAN 1 <...>	automatically created	Active	30	50	50	View Details	Delete Entry
LAN 1 <...>	automatically created	Active	1800	50	0	View Details	Delete Entry
LAN 2 <...>	automatically created	Active	30	50	50	View Details	Delete Entry
LAN 2 <...>	automatically created	Active	1800	50	0	View Details	Delete Entry
LAN 3 <...>	automatically created	Active	30	50	50	View Details	Delete Entry
LAN 3 <...>	automatically created	Active	1800	50	0	View Details	Delete Entry
LAN 4 <...>	automatically created	Active	30	50	50	View Details	Delete Entry
LAN 4 <...>	automatically created	Active	1800	50	0	View Details	Delete Entry
LINE 1 <...>	automatically created	Active	30	50	50	View Details	Delete Entry
LINE 1 <...>	automatically created	Active	1800	50	0	View Details	Delete Entry
LINE 2 <...>	automatically created	Active	30	50	50	View Details	Delete Entry
LINE 2 <...>	automatically created	Active	1800	50	0	View Details	Delete Entry

New History Entry

Figure 1-79 RMON Counter History

The details of each counter history shows the last N intervals for this counter. The number N can be configured. The default is N = 50 entries.

For example for N = 50 the “30 sec” history is a period of the last 25 minutes. The “30 min” history covers a period of 25 hours.

Changing the “Entry Status” from “Edit” to “Active” brings the (new) counter into action. As long as it keeps on “Edit”, it will not work properly.

NOTE: All entries, which are on status “Edit” will be deleted when system reboots!

RMON Alarms

NOTE: RMON Alarms is only visible when SNMP is enabled.

arcutronix
arcutronix ENX

logged in as: admin
logout

- General System Information
- Administration
 - Alarm Management
- Ethernet Ports
- Operation and Maintenance
 - RMON Monitors
 - RMON Port Counters
 - RMON Counter History
 - RMON Alarms
 - RMON Events
 - Clock Configuration
 - Log View

Variable	Owner	Type	Falling Threshold	Rising Threshold	Status	Details
ifOperStatus.1	andreas	Absolute Value	0	0	Edit	View Details Delete Entry

New Alarm Entry

Figure 1-80 RMON Alarms

The RMON ALarms gives the user the capability to define an alarm for each management variable, defined in supported MIBs. The monitored variable must be selected in the MIB and the correct value written in “Monitored Variable”. Sampling interval and the required thresholds can be configured. If the alarm raises and falls, one of the configured events (see chapter RMON Events below) can be triggered. The event decides then, whether to alarm change is logged or a trap is sent.

arcutronix
arcutronix ENX

logged in as: admin
logout

- General System Information
- Administration
 - Alarm Management
- Ethernet Ports
- Operation and Maintenance
 - RMON Monitors
 - RMON Port Counters
 - RMON Counter History
 - RMON Alarms
 - ifOperStatus.1
 - View Details
 - RMON Events
 - Clock Configuration
 - Log View

Entry Owner: andreas

Monitored Variable: ifOperStatus.1

Sampling Interval (sec): 60

Sampling Type: Absolute Value

Startup Behaviour: Check Rising or Falling Alarm

Falling Threshold: 0

Falling Alarm Event: No Event

Rising Threshold: 0

Rising Alarm Event: No Event

Last Alarm Value: 0

Last Alarm Condition: Alarm Inactive

Entry Status: Edit

Figure 1-81 RMON Alarm Details

Changing the “Entry Status” from “Edit” to “Active” brings the (new) counter into action. As long as it keeps on “Edit”, it will not work properly.

NOTE: All entries, which are on status “Edit” will be deleted when system reboots!

RMON Events

RMON events are objects, which can be linked to RMON alarms and define the system's reaction, when the alarm raises or falls.

RMON events can trigger just an entry in the logging, a SNMP trap or both.

All defined RMON events are presented in a list:

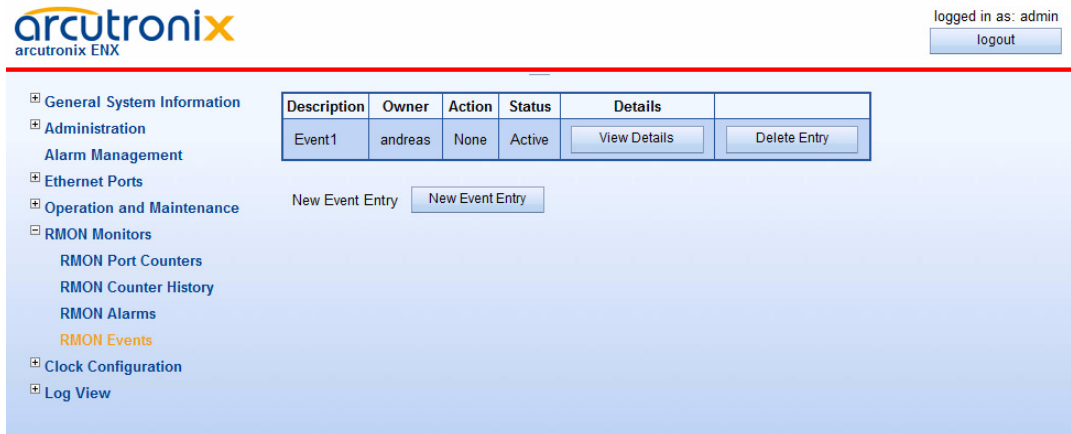


Figure 1-82 RMON Events

New RMON Events can easily created and configured, when entering the “View Details” submenu.

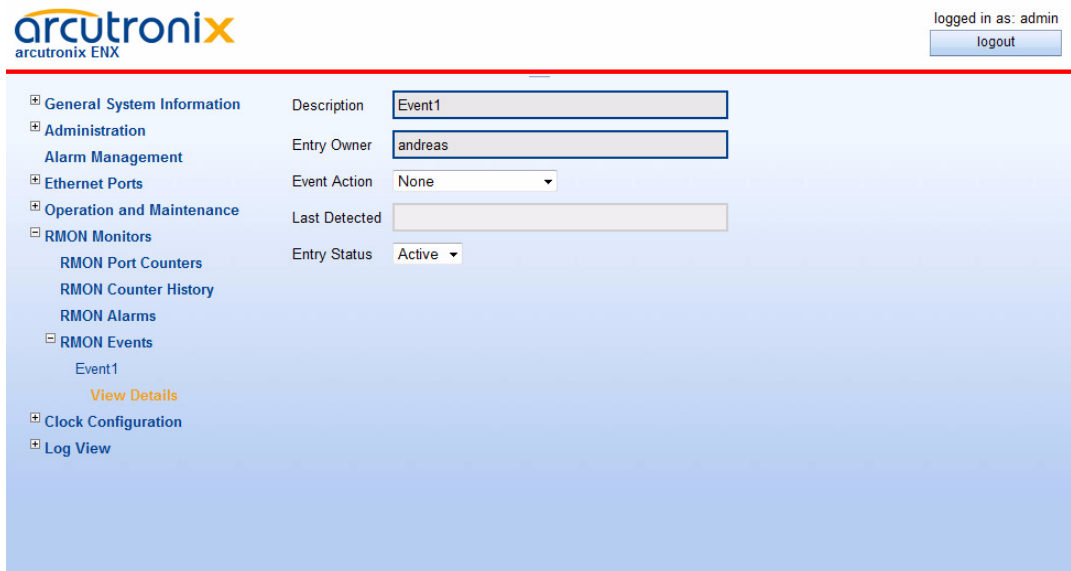


Figure 1-83 RMON Event Details

Each RMON event can get a description to make it easier to use and an owner for better filter. The action, when the event is called, can be defined:

- Log
- SNMP Trap

- Log and SNMP Trap

The last detected entry shows whether and when this event was called the last time.

Do not forget to change the status from “Edit” to “Active” after configuration. Otherwise the new event is not applicable.

Changing the “Entry Status” from “Edit” to “Active” brings the (new) counter into action. As long as it keeps on “Edit”, it will not work properly.

NOTE: All entries, which are on status “Edit” will be deleted when system reboots!

Clock Configuration

The options of the “Clock Configuration” submenu are widely declared in “Clocking and Synchronization” of [axManualENX]. All the details will not be repeated here, but the menu options.

logged in as: admin
logout

arcutronix
arcutronix ENX

- General System Information
- Administration
- Alarm Management
- Ethernet Ports
- Operation and Maintenance
- RMON Monitors
- Clock Configuration**
 - T3an/T4ab Configuration
 - IEEE1588 PTP Configuration
- Log View

PLL Status: Locked

Effective Clock Quality: SSM_QL_EEC1

Synchronization Clock Source: Internal TCXO

Sync Source Clock Quality: SSM_QL_EEC1

Overwrite Clock Quality: Disabled

Selected Overwrite Clock Quality: SSM_QL_DNU

Revertive Mode: Revertive

Device Oscillator Type (XO): TCXO (MaxD 4.6ppm)

Clock Source	Priority	Status	MDvXO	MDvXO Limit	Clock configuration
Internal TCXO	15	Used for Synchronization	0.0 ppm	1.0 ppm	Configuration
T3an	1	Bad Quality / Not Available	> 160 ppm	9.2 ppm	Configuration
SyncE LINE 1 Optical	5	Bad Quality / Not Available	> 160 ppm	9.2 ppm	Configuration
SyncE LINE 2 Optical	5	Bad Quality / Not Available	> 160 ppm	9.2 ppm	Configuration
SyncE LINE 1 Electrical	6	Bad Quality / Not Available	> 160 ppm	9.2 ppm	Configuration
SyncE LINE 2 Electrical	6	Bad Quality / Not Available	> 160 ppm	9.2 ppm	Configuration

Figure 1-84 Clock Configuration

Table 1-67 provides information about the options.

Table 1-67 Clock Configuration

Parameter	Description	Format	Default
PLL State	Status of the internal PLL. In normal state it should be locked (to one of the available sources).	Display	
Effective Clock Quality	Shows the actual SSM level.	Display	
Synchronization Clock Source	Shows the actual source for the internal PLL.	Display	
Sync Source Clock Quality	Shows the SSM level of the selected clock. This might be different to the "Effective Clock Quality".	Display	
Overwrite Clock Quality	To change the "Effective Clock Quality" others than the "Sync Source Clock Quality", this must be changed to "enable". If disabled, the "Effective Clock Quality" is the same as the sync source.	PullDown Menu <ul style="list-style-type: none"> • Enabled • Disabled 	Disabled
Select Overwrite Clock Quality	A new clock quality for the device can be defined manually here. This is only consequence, when "Overwrite Clock Quality" is enabled.	PullDown Menu <ul style="list-style-type: none"> • SSM_QL_INV0 • ... • SSM_QL_DNU 	SSM_QL_DNU
Revertive Mode	In revertive mode, system automatically switches to the available clock source with highest priority even if the currently selected clock source is still available. In none revertive mode, clock source is only changed if the currently selected one becomes unavailable.	PullDown Menu <ul style="list-style-type: none"> • Revertive • None revertive 	Revertive
Device Oscillator Type (XO)	Shows which kind of oscillator is equipped on the device. Different option can be ordered.	Display	

The table at the end of the menu gives an overview to the 4 possible clock sources and a quick access to the most interesting settings:

- Priority of the clock (1 is the highest, 10 the lowest)
- (Mean) Deviation versus internal oscillator and hence a bench mark for quality.

the columns of the table have the following meanings:

Table 1-68 Clock Source Table

Parameter	Description
Clock Source	Name of the 4 available clock sources.
Priority	PullDown menu to select the clock's priority from 1 (high) to 10 (low).
Status	Description of the actual status of the interface and whether the (derived) clock is used as source for synchronisation or not.
MDvXO	Mean deviation versus the internal oscillator.
MDvXO Limit	Maximum for deviation before the clock is called "bad quality". The value can be entered directly here or in the configuration submenu.
Configuration	Button to enter the detailed configuration and status menu of the clock.

The four available clock-sources can be configured in more detail in the "Configuration" submenu.

Configuration of Internal TCXO and T3an

The configuration of internal TCXO and T3-clock is simple and shows only the same entries as in the Clock Configuration table above already mentioned.

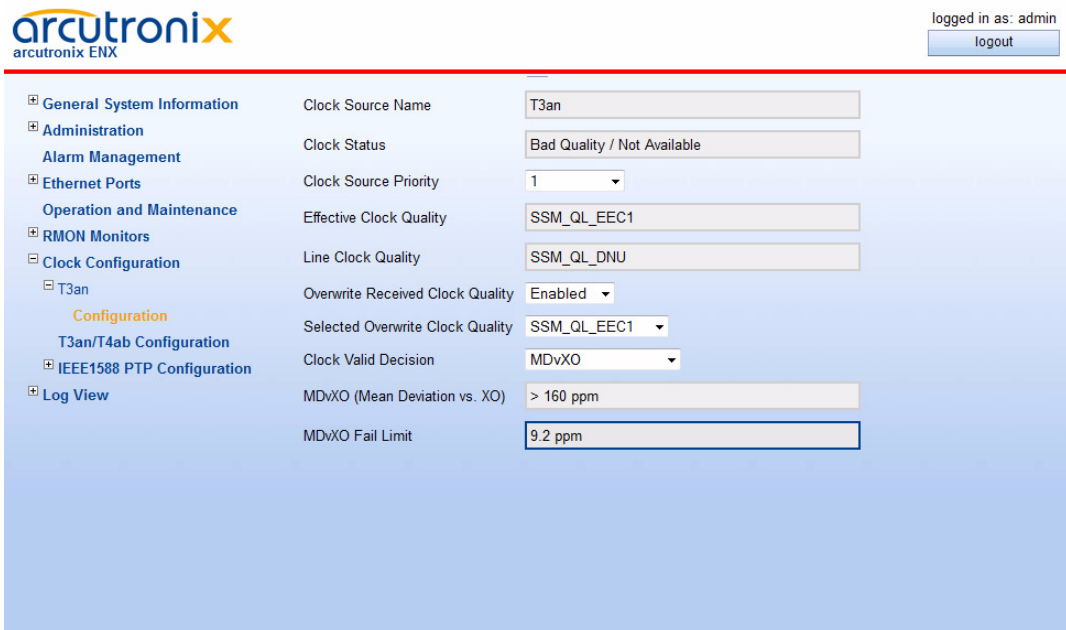


Figure 1-85 T3an Configuration

Table 1-69 provides information about the options.

Table 1-69 TCXO & T3an Configuration

Parameter	Description	Format	Default
Clock Source Name	The name of the selected clock source.	Display	
Clock Status	Shows the actual quality and whether this clock is selected for synchronisation.	Display	
Clock Source Priority	The priority level for this clock source. do-not-use = lowest level ⁱ 15 = second lowest level 1 = highest priority level	PullDown Menu <ul style="list-style-type: none"> • do-not-use • 1 • .. • 15 	1
Effective Clock Quality	The effective clock quality.	Display	
Line Clock Quality	The received SSM-level over ESMC. As TCXO and T3an do not support ESMC, this value will always be DNU ⁱ .	Display	SSM_QL_DNU

Table 1-69 TCXO & T3an Configuration (continued)

Parameter	Description	Format	Default
Overwrite Received Clock Quality	The received SSM-level may be over-written by the device with any possible value.	PullDown Menu <ul style="list-style-type: none"> enabled disabled 	enabled
Selected Overwrite Received Clock Quality	This is the new value of SSM-level in case the Overwrite Mode is enabled (see row above).	PullDown Menu <ul style="list-style-type: none"> all possible SSM-values 	EEC1
Clock Valid Decision	Decides which information shall be used to accept clock as valid: Either just the mean-deviation from internal oscillator or the deviation plus the incoming SSM-level. Note: Note: As the T3an is only in T12-mode available, no SSM-messages can be received, so in fact only single value is possible.	PullDown Menu <ul style="list-style-type: none"> MDvXO MDvXO / SSM-Level 	MDvXO
MDvXO (Mean Deviation vs. XO)	This is the mean deviation versus the internal TCXO (or OCXO) in ppm.	Display	
MDvXO Fail Limit	The offset-value of the MDvXO, which decides the clock to be bad and it will not be used any longer as reference.	Entry	9.2ppm

i. "do-not-use" is to be taken literally. A clock source, which priority is DNU, will not be considered to be used.

Configuration SyncE LINES

The configuration of a SyncE line port offers beside the above already mentioned options the possibility to overwrite the clock quality level for each line port individually. Furthermore the decision, whether the recovered clock is "good" or "bad", can be based on the deviation against internal XO only or together with the SSM messages received from the SyncE-master.

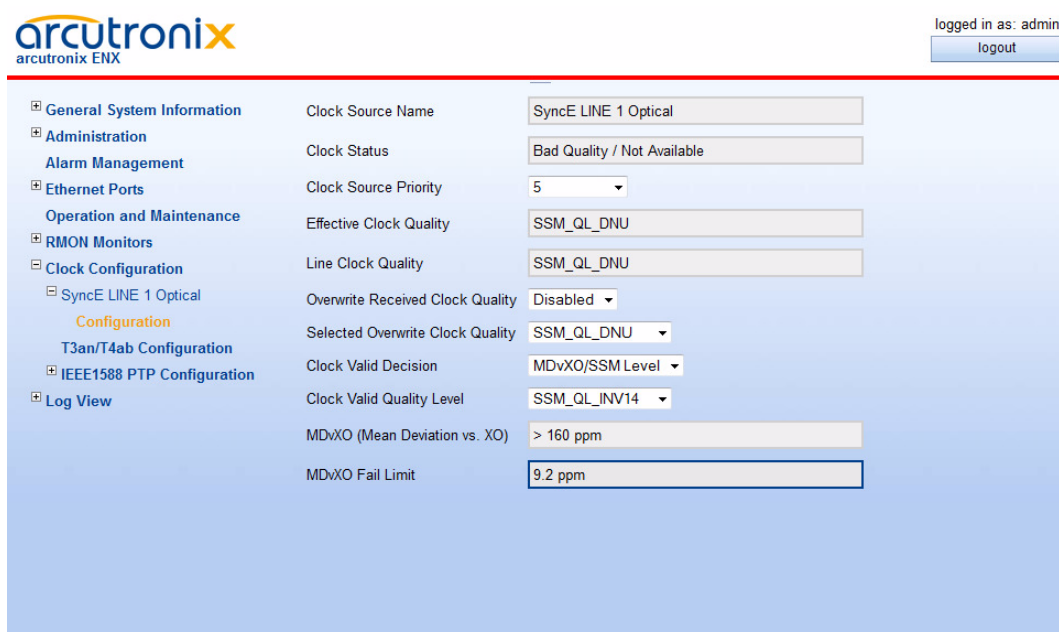


Figure 1-86 SyncE Configuration

Table 1-70 provides information about the options.

Table 1-70 Sync-E LINE Configuration

Parameter	Description	Format	Default
Clock Source Name	The name of the selected clock source.	Display	
Clock Status	Shows the actual quality and whether this clock is selected for synchronisation.	Display	
Clock Source Priority	The priority level for this clock source. do-not-use = lowest level ⁱ 15 = second lowest level 1 = highest priority level	PullDown Menu • do-not-use • 1 • .. • 15	5
Effective Clock Quality	The effective clock quality.	Display	
Line Clock Quality	The received SSM-level over ESMC. As TCXO and T3an do not support ESMC, this value is always set to DNU ⁱ .	Display	SSM_QL_DNU

Table 1-70 Sync-E LINE Configuration (continued)

Parameter	Description	Format	Default
Overwrite Received Clock Quality	The received SSM-level may be over-written by the device with any possible value.	PullDown Menu <ul style="list-style-type: none"> enabled disabled 	enabled
Selected Overwrite Received Clock Quality	This is the new value of SSM-level in case the Overwrite Mode is enabled (see row above).	PullDown Menu <ul style="list-style-type: none"> all possible SSM-values 	EEC1
Clock Valid Decision	Decides which information shall be used to accept clock as valid: Either just the mean-deviation from internal oscillator or the deviation plus the incoming SSM-level.	PullDown Menu <ul style="list-style-type: none"> MDvXO MDvXO / SSM-Level 	MDvXO / SSM-Level
Clock Valid Quality Level	The selected SSM-level is the minimum to be received via ESMC, otherwise the clock will not be used as reference.	PullDown Menu <ul style="list-style-type: none"> all possible SSM-values 	SSM_QL_INV14
MDvXO (Mean Deviation vs. XO)	This is the mean deviation versus the internal TCXO (or OCXO) in ppm.	Display	
MDvXO Fail Limit	The offset-value of the MDvXO, which decides the clock to be bad and it will not be used any longer as reference.	Entry	9.2ppm

i. "do-not-use" is to be taken literally. A clock source, which priority is DNU, will not be considered to be used.

T3an/T4ab Configuration

This menu offers the capability to enable or disable the two clock ports. While T3an is always operated in [ITU-T G.703] T12-mode (2,048MHz input), the T4ab port can be operated in two different modes:

- [ITU-T G.703] T12-mode (2,048MHz),
- [ITU-T G.703] E12-mode (2,048Mbps, HDB3) plus [ITU-T G.704] MF format with CRC4.

The status of the two ports can be checked. Both ports do have the capability to verify, whether a peer is connected, based only on the electrical sensing.

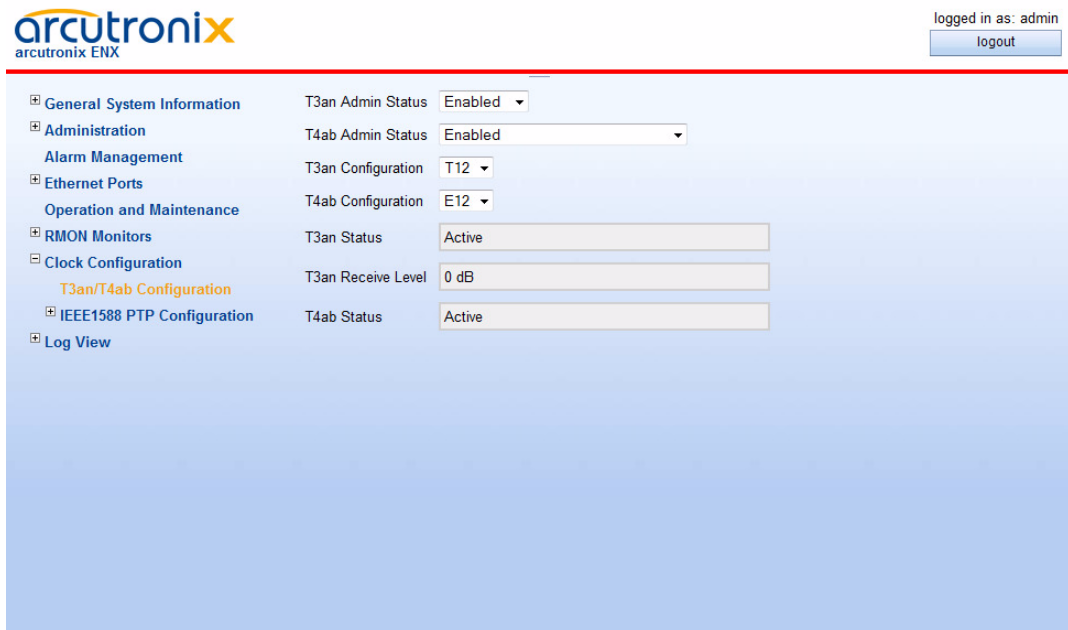


Figure 1-87 T3an/T4ab Configuration

NOTE: When T4ab is configured to T12-mode (2.048MHz), the interface can not detect any shorties or unconnected cables. This is only possible in E12-mode!

Table 1-71 provides information about the options.

Table 1-71 T3an/T4ab

Parameter	Description	Format	Default
T3an Admin Status	Admin status of T3an.	PullDown Menu <ul style="list-style-type: none"> • Disabled • Enabled 	Enabled
T4ab Admin Status	Admin status of T4ab. This variable allows configuring whether the T4ab port on the device is enabled or disabled. If it is enabled, it can be selected, whether it should be turned off, in case T3an is selected as sync-source. This is to avoid clock-loops.	PullDown Menu <ul style="list-style-type: none"> • Disabled • Enabled • Enabled, if T3an is not Sync-Source 	Enabled
Effective Clock Quality	The effective clock quality.	Display	

Table 1-71 T3an/T4ab (continued)

Parameter	Description	Format	Default
T4ab Minimum Quality Level	Configure the minimum “Effective Clock Quality“ (SSM Level) to enable T4ab.	PullDown Menu <ul style="list-style-type: none"> • SSM_QL_DNU • SSM_QL_INV0 • .. • SSM_QL_INV14 	
T3an Configuration	Interface mode of T3an.	PullDown Menu <ul style="list-style-type: none"> • T12 	T12
T4ab Configuration	Interface mode of T4ab.	PullDown Menu <ul style="list-style-type: none"> • E12 • T12 	E12
T3an State	Connection State of T3an.	Display	
T3an Receive Level ⁱ	The level of electrical signal power received at the T3an port.	Display	
T4ab State	Connection State of T4ab.	Display	

i. Only visible, when a signal is detected at T3an.

IEEE1588 PTP Configuration

The PTP configuration submenu gives access to the PTP settings and the status of PTP engine and all ports, which are enabled for PTP time-stamping.

The PTP engine and the 1PPS-Interface can be enabled or disabled.

When PTP is enabled, the unit is searching for a PTP-Grandmaster (GM), as the reference for its internal clock. When a GM is found and connection to it is established, the Master Clock ID is shown. Also the (calculated) path-delay and the clock-offset between GM and the unit (BC- or OC-mode) is shown.

PTP-master interfaces (normally LAN ports) the interval for sending Sync-messages (“SyncInt”) and Announce-messages (“AnnInt”) can be configured as a global attribute. All master ports will use the same settings.

arcutronix
arcutronix ENX

ENX-F: Demo-Device
Serial: 2012010114

logged in as: admin
logout

- General System Information
- Administration
- Alarm Management
- Ethernet Ports
- Operation and Maintenance
- RMON Monitors
- Clock Configuration
 - T3an/T4ab Configuration
 - IEEE1588 PTP Configuration
 - IEEE1588 PTP Logging
- Log View

PTP Admin Status: Enabled

PTP Mode: Boundary Clock

PTP Transport: Ethernet Multicast

Clock ID: 001E16FFFE001EFD

Master Clock ID: n.a.

Offset From Master: -- ns

PTP Path Delay: -- ns

1PPS Admin Status: Enabled

Master Port configuration and status

Port	Link Status	PTP Status	Synclnt	AnnInt	PD MAC	notPD MAC	Configuration
LAN 1	Link Down	Disabled	250ms	1s	01-80-C2-00-00-0E	01-1B-19-00-00-00	Disabled
LAN 2	Link Down	Disabled	250ms	1s	01-80-C2-00-00-0E	01-1B-19-00-00-00	Disabled
LAN 3	Link Down	Disabled	250ms	1s	01-80-C2-00-00-0E	01-1B-19-00-00-00	Disabled
LAN 4	Link Down	Disabled	250ms	1s	01-80-C2-00-00-0E	01-1B-19-00-00-00	Disabled

Slave Port configuration and status

Port	Link Status	PTP Status	Master Clock Sync Interval	PD MAC	notPD MAC	Configuration
LINE 1	Link Down	Disabled	n.a.	01-80-C2-00-00-0E	01-1B-19-00-00-00	Disabled
LINE 2	Link Down	Disabled	n.a.	01-80-C2-00-00-0E	01-1B-19-00-00-00	Disabled

Figure 1-88 PTP Configuration

Table 1-72 provides information about the options.

Table 1-72 T3an/T4ab

Parameter	Description	Format	Default
PTP Admin Status	Admin status of PTP engine.	PullDown Menu <ul style="list-style-type: none"> disabled enabled 	Disabled
PTP Mode ⁱ	The mode of the PTP engine. For the time being this is always Boundary Clock (BC).	Display	Boundary Clock
PTP Transport ⁱ	The transport mode of the PTP engine. For the time being this is always Layer2 Multicast.	Display	Ethernet Multicast
Clock ID ⁱ	The PTP clock ID of the ENX, which is provided to the PTP Ordinary Clocks (slaves).	Display	

Table 1-72 T3an/T4ab (continued)

Parameter	Description	Format	Default
Master Clock ID ⁱ	The ID of the PTP Grandmaster (GM), which is selected as reference.	Display	
Offset from Master ⁱ	Calculated time offset from PTP (Grand-)Master.	Display	
PTP Path Delay ⁱ	Calculated path delay to PTP (Grand-)Master.	Display	
1PPS Admin Status	Admin status of 1PPS.	PullDown Menu <ul style="list-style-type: none"> • disabled • enabled 	Disabled

i. Only visible, when PTP is enabled via PTP Admin Status.

When PTP is enabled, each LINE-port can be configured to be PTP slave-port towards a Grandmaster clock. By default, all LINE-ports are disabled and do not act as PTP boundary-clock slave.

NOTE: For the time being the PTP engine can not work with multiple Grandmasters, which are distributed to different MANs.

Master Port Configuration and Status

When PTP is enabled, each LAN-port can be configured to be PTP master-port towards subsequent devices. By default, all LAN-ports are disabled and do not act as PTP boundary-clock master. The table "Master Port Configuration and Status" is dedicated to overview and configure to the PTP-master ports.

Master Port configuration and status

Port	Link Status	PTP Status	Synclnt	AnnInt	PD MAC	notPD MAC	Configuration
LAN 1	Link Down	Passive	62.5ms ▾	250ms ▾	01-80-C2-00-00-0E ▾	01-1B-19-00-00-00 ▾	BC_master ▾
LAN 2	Link Down	Passive	250ms ▾	1s ▾	01-80-C2-00-00-0E ▾	01-1B-19-00-00-00 ▾	BC_master ▾
LAN 3	Link Down	Passive	1s ▾	4s ▾	01-80-C2-00-00-0E ▾	01-1B-19-00-00-00 ▾	BC_master ▾
LAN 4	Link Down	Passive	4s ▾	16s ▾	01-80-C2-00-00-0E ▾	01-1B-19-00-00-00 ▾	BC_master ▾

Figure 1-89 Master Port Configuration and Status

Table 1-73 provides information about the options.

Table 1-73 Master Port Configuration and Status

Parameter	Description	Format	Default
Port	Name indicator of the possible PTP master ports. LAN1 ... LAN4	Display	
Link Status	Indicates, whether the port is up, down or disabled.	Display	
PTP Status	The status of the PTP engine, running on this port.	Display	
SyncInt	Time between PTP Sync messages. For each PTP master interface the interval for sending Sync messages can be freely configured between 62.5msec and 4sec. Each Sync packet is followed by a Follow_up packet, containing the time when the Sync packet was send (two-step clock).	PullDown Menu <ul style="list-style-type: none"> • 62.5ms • 125ms • 250ms • 500ms • 1s • 2s • 4s 	250ms
AnnInt	Time between PTP Annotation messages. The announceInterval specifies the mean time interval between successive Announce messages, which are send on the depending port in Master mode.	PullDown Menu <ul style="list-style-type: none"> • 250ms • 500ms • 1s • 2s • 4s • 8s • 16s 	1s
PD MAC	MAC-address of Peer delay (PD) mechanism messages.	PullDown Menu <ul style="list-style-type: none"> • 01-1B-19-00-00-00 • 01-80-C2-00-00-0E 	01-80-C2-00-00-0E
notPD MAC	MAC-address of all other messages (not Peer Delay).	PullDown Menu <ul style="list-style-type: none"> • 01-1B-19-00-00-00 • 01-80-C2-00-00-0E 	01-1B-19-00-00-00
Configuration	Set the PTP port operation mode.	PullDown Menu <ul style="list-style-type: none"> • Disabled • BC_master 	Disabled

Slave Port Configuration and Status

When PTP is enabled, one(!) LINE-port can be configured to be the PTP slave-port towards the PTP GrandMaster. By default, all LINE-ports are disabled and do not act as PTP boundary-clock slave. The table “Slave Port Configuration and Status” is dedicated to overview and configure to the PTP-slave ports.

Slave Port configuration and status

Port	Link Status	PTP Status	Master Clock Sync Interval	PD MAC	notPD MAC	Configuration
LINE 1	Link Down	Listening	n.a.	01-80-C2-00-00-0E ▾	01-1B-19-00-00-00 ▾	Slave_only ▾
LINE 2	Link Down	Disabled	n.a.	01-80-C2-00-00-0E ▾	01-1B-19-00-00-00 ▾	Disabled ▾

Figure 1-90 Slave Port Configuration and Status

Table 1-74 provides information about the options.

Table 1-74 Slave Port Configuration and Status

Parameter	Description	Format	Default
Port	Name indicator of the possible PTP master ports. LINE1 ... LINE2	Display	
Link Status	Indicates, whether the port is up, down or disabled.	Display	
PTP Status	The status of the PTP engine, running on this port.	Display	
Master Clock SyncInt	The (measured) time interval of the GrandMasters PTP Sync messages. This is just an indicator for the master's settings.	Display	
PD MAC	MAC-address of Peer delay (PD) mechanism messages.	PullDown Menu • 01-1B-19-00-00-00 • 01-80-C2-00-00-0E	01-80-C2-00-00-0E
notPD MAC	MAC-address of all other messages (not Peer Delay).	PullDown Menu • 01-1B-19-00-00-00 • 01-80-C2-00-00-0E	01-1B-19-00-00-00
Configuration	Set the PTP port operation mode.	PullDown Menu • Disabled • Slave_only	Disabled

Peer Delay Messages and notPeer Delay Messages

The communication with the other PTP clock in the network uses several different types of packets.

- Peer delay (PD) mechanism messages
- All except peer delay (nonPD) mechanism messages

IEEE and ITU-T do recommend slightly different usage of MAC addresses. For this reason, ENX can be widely configured. The default is the IEEE recommendation.

Table 1-75 PTP Multicast MAC Addresses

Name	Abbr.	MAC Header	
		IEEE	ITU-T
Peer delay (PD) mechanism messages	PD	01-80-C2-00-00-0E	01-80-C2-00-00-0E
All except peer delay (notPD) mechanism messages	notPD	01-1B-19-00-00-00	01-80-C2-00-00-0E

PTP Logging

The PTP Logging is a tool to file the most important results of the PTP engine like Path-Delay and Clock-Offset compared to the PTP Grandmaster clock. The results are stored at certain moments. The interval between this points in time can be configured in this submenu. The longer the interval is, the longer is the possible maximum observed time-frame (Maximum Log Time), as the memory allocated for the PTP logging is limited. To see, the remaining log-time, refer to the value of “Estimated Remaining Log Time”.

The start of the logging plus the actual time of the device is displayed for completeness and better reading of the entries.

arcutronix
arcutronix ENX

logged in as: admin
logout

General System Information PTP Log Interval 12h

Administration Maximum Log Time 0564d 23:10

Alarm Management Estimated Remaining Log Time 0564d 12:00

Ethernet Ports Log Start Time 2012-07-20 11:08:11

Operation and Maintenance Date and Time 2012-07-20 11:07

RMON Monitors Clear PTP Logs Clear PTP Logs

Clock Configuration

T3an/T4ab Configuration

IEEE1588 PTP Configuration

IEEE1588 PTP Logging

Save Logfiles

Log View

Figure 1-91 PTP Logging

NOTE: When the PTP Log Interval is changed to a new value, the PTP-logging is restarted. Old loggings are deleted, when a new PTP-logging is started. Please store your logging in the submenu “Save Logfiles”.

To download or upload the PTP Logging select the Save Logfiles submenu.

Save Logfiles

The Save Logfiles menu offers the possibility to download the archive(s) via HTTP or upload them via (S/T)FTP. The HTTP option is only visible, when HTTP file transfer is enabled in the “User and Access Administration” menu (see page 1-14).

The SFTP or TFTP storage onto a server requires the proper setting of the “Logfile Server” (see “File Servers” on page 1-17).

arcutronix
arcutronix ENX

logged in as: admin
logout

General System Information Download the PTP performance logfile Download ptp_performance_log.csv

Administration Server Type Logfile Store

Alarm Management Server URI tftp://192.168.0.7/tftpboot

Ethernet Ports File Transfer State

Operation and Maintenance Log File Suffix

RMON Monitors Upload to 'Logfile Store' Upload to 'Logfile Store'

Clock Configuration

T3an/T4ab Configuration

IEEE1588 PTP Configuration

IEEE1588 PTP Logging

Save Logfiles

Log View

Figure 1-92 PTP Logging

The usage and handling of storage to the Logfile Server is depicted in “Safe Log-Files” on page 1-152.

Log View

The Log View shows all events. There are many predefined events as link-up and link-down, but one can define more events, if required. The definition of additional events is done in the submenu “RMON Events” on page 1-136.

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

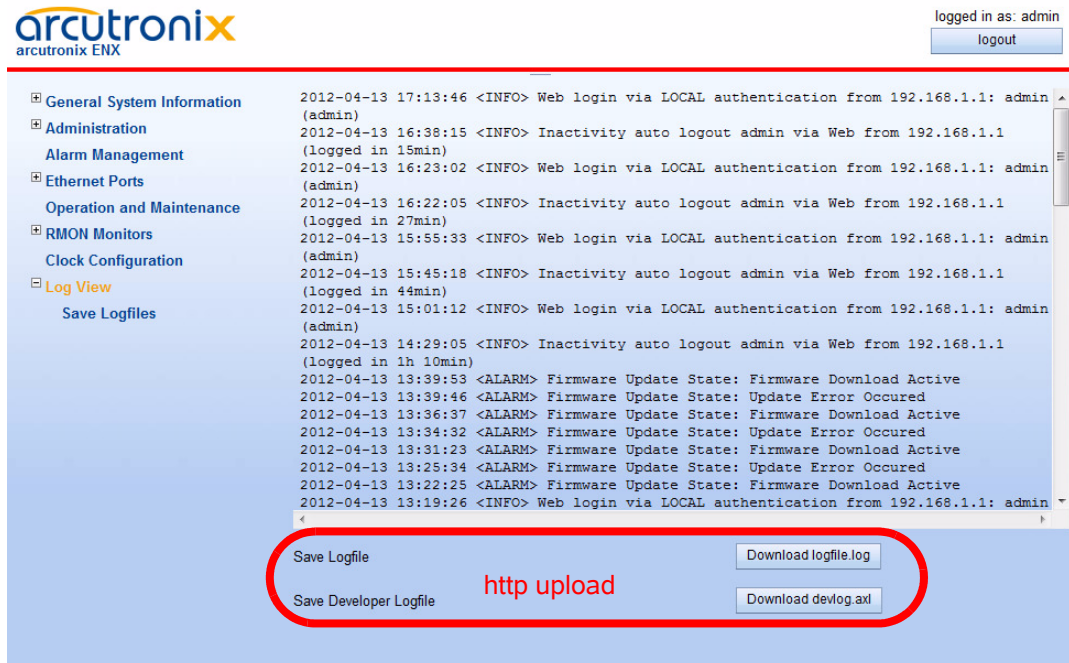


Figure 1-93 Log View Example

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 1-14).

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 1-17). 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!)

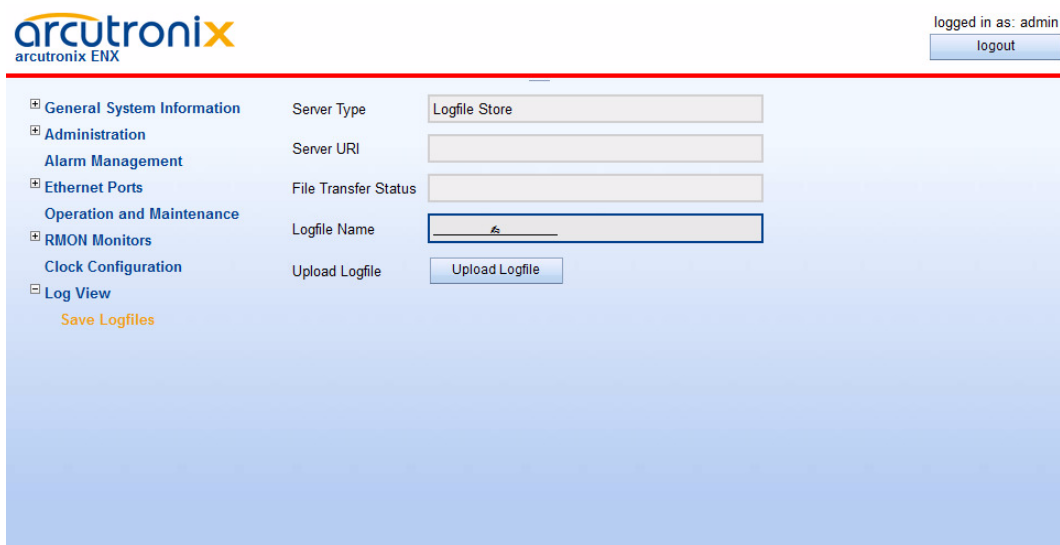


Figure 1-94 Save Logfiles

Table 1-35 provides information about the options.

Table 1-76 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: ../enx*.cfgx

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