arcutronix

Synchronize the Ethernet

FSP-RPX CLI

arcutronix GmbH
Deutschland

Reference Guide

Version 1.1

arcutronix

FSP-RPX16

Command Line Interface

Reference Guide

Doc-No.: 1303 00 65.cli

Version 1.1

Contacts

arcutronix GmbH
Garbsener Landstraße 10
D-30419 Hannover, Germany

Tel.: +49 (0)511 277- 2700
Fax: +49 (0)511 277- 2709
E-Mail: info@arcutronix.com
Web: http://www.arcutronix.com

Copyright Note

Document Contents

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

Trademarks

Table of Contents

1 INTRODUCTION AND OVERVIEW 10

1.1 Covered Software 10
1.2 Access to the Device 10
1.2.1 SSH Connection 10
1.3 Command Line Interface (CLI) 11
1.3.1 Introduction to the CLI 11
1.3.2 CLI Editor Features 12
1.3.2.1 Context Sensitive Help 12
1.3.2.2 Syntax Checks 12
1.3.2.3 Path and Command Completion 12
1.3.2.4 Abbreviations of Path and Command Names 12
1.3.2.5 Prompt and Path 13
1.3.2.6 Comments 13
1.3.2.7 Quoting and Escaping 13
1.3.2.8 Continuation Mode 14
1.4 The CLI Commands 14
1.4.1 The CONFIG Command 15
1.4.2 Additional CLI Commands 17

2 SPECIAL CLI CONSTRUCTS 19

2.1 Tables 19
2.2 Form Pages 23

3 OVERVIEW REFERENCE GUIDE 24

3.1 Design 24
3.2 Types of Variables 26

4 MENUS AND VARIABLES IN THE FSP-RPX CLI 28

4.1 Administration 28
4.1.1 Administration / Configuration Management 28
4.1.1.1 Administration / Configuration Management / <Config Name> 30
4.1.2 Administration / Date and Time Settings 34
4.1.2.1 Administration / Date and Time Settings / <IP Address> 36
4.1.2.2 Administration / Date and Time Settings / NTP Server Setup 39
4.1.3 Administration / Diagnostics 44
4.1.4 Administration / Firmware Update 46
4.1.5 Administration / Port and IP Configuration 50
4.1.5.1 Administration / Port and IP Configuration / <MGMT Port> 51
4.1.6 Administration / Reset System 68
4.1.7 Administration / Self-Test 71
4.1.8 Administration / User and Access Administration 71
4.1.8.1 Administration / User and Access Administration / <Server> 73
4.1.8.2 Administration / User and Access Administration / SNMP Configuration 77
4.1.8.3 Administration / User and Access Administration / SSH Access 93
4.1.8.4 Administration / User and Access Administration / Users and Passwords 99
4.1.8.5 Administration / User and Access Administration / Web Configuration 105
4.2 Alarm Management 110
4.2.1 Alarm Management / <Alarm Group> 110
4.2.1.1 Alarm Management / <Alarm Group> / Group Details 112

4.2.2 Alarm Management / Active Alarm List....118
4.2.2.1 Alarm Management / Active Alarm List / <Alarm Num>....119
4.3 General System Information....121
4.3.1 General System Information / Inventory....122
4.4 Log View....125
4.5 Remote Feeding Control....127
4.5.1 Remote Feeding Control / <RF Port No.>....127
4.5.1.1 Remote Feeding Control / <RF Port No.> / RF Port Configuration....127

5 EXAMPLES AND USE CASES....133

5.1 Configuring the Local Management Port....133
5.1.1 Enabling the Local Port....133
5.1.2 Configuring a Fixed IPv4 Address....134
5.1.3 Disabling IPv6 Support....134
5.1.4 Verifying the Network Configuration....135
5.2 Configuring the Remote Management Port....135
5.2.1 Enabling the North Port....136
5.2.2 Configuring a Fixed IPv4 Address and Default Gateway....136
5.2.3 Enabling IPv6 Support....137
5.2.4 Setting up IPv6 Automatic Address Configuration....137
5.2.5 Manually Adding IPv6 Addresses....137
5.2.6 Verifying the Network Configuration....138
5.3 Configuring the Forwarding Management Port....139
5.3.1 Enabling the South Port....139
5.3.2 Verifying the Network Configuration....139
5.4 Improving Networking Security....140
5.4.1 Restricting SNMP access to SNMPv3....140
5.4.2 Disabling ICMP for IPv4....140
5.4.3 Disabling HTTP Access....141
5.5 Adding a User and Defining a Password....143
5.5.1 Creating a new User Account....143
5.5.2 Verifying the Settings....144
5.6 Replacing the Default Admin User....145
5.6.1 Creating a new Admin User....145
5.6.2 Verifying the User Creation....145
5.6.3 Deleting the Default Admin User....146
5.7 Automatic Date/Time Setting Using NTP....146
5.7.1 Verifying the Settings....147
5.8 Manually Setting Date and Time....147
5.9 Ping Connectivity Test....148
5.10 Transferring Device Logfiles to a Storage Server....148
5.10.1 Configuring the Storage Server....148
5.10.2 Uploading the Logs to the Storage Server....149
5.10.3 Verification....150
5.11 Transferring Configuration Snapshots to a Storage Server....150
5.11.1 Configuring the Storage Server....150
5.11.2 Uploading the Snapshot to the Storage Server....151
5.11.3 Deleting old Configuration Snapshots....152
5.12 Immediate System Reset....152
5.13 Scheduled Reset....152
5.14 Reset to Factory Defaults....153
5.15 Configure Alarm Settings....154
5.15.1 Setting the Severity of a Digital Alarm....154
5.15.2 Display and Change Thresholds of an Analog Alarm....154
5.15.3 Configuring SNMP Notification for an Alarm....155

5.15.4 Acknowledging a Single Alarm....155
5.15.5 Acknowledging all Group Alarms....155
5.15.6 Acknowledging all Alarms....156
5.15.7 View Active Alarm List....156
5.16 Adding an SNMPv3 User and Setting Authentication Parameters....156
5.16.1 Adding a New SNMPv3 User....157
5.16.2 Setting the User Name and Authentication Parameters....157
5.17 Adding an SNMPv3 Trap Receiver....158
5.17.1 Adding a new SNMP Trap Receiver....158
5.17.2 Setting Up the Trap Receiver's Configuration....158
5.17.3 Checking the Trap Receiver Setup....159
5.18 Updating the Device Firmware....159
5.18.1 Configuring the Storage Server....159
5.18.2 Downloading the Firmware Update File to the Device....160
5.18.3 Starting the Firmware Update....161
5.18.4 Verifying the Software Version....161
5.19 Enabling Remote Feeding for a Port....161
5.20 Setting Remote Feeding Current Thresholds....161
5.21 Enabling Remote Feeding Traps....162
5.21.1 Enabling the OperStatus trap....163
5.21.2 Enabling the GroundLeakage trap....163
ALPHABETICAL INDEX....164

I. History

Rev.	Date	Author(s)	Remarks
1.0	18.12.13	AFZ	Initial document.
1.1	21.5.14	SZE	Rework after minor SW changes.

1 Introduction and Overview

The FSP-RPX16 is fully configurable using a text-based Command Line Interface (CLI) which is offered over a Secure Shell (SSH) connection. Only a standard SSH client and IP connectivity are required to use the CLI.

This reference guide will explain how to connect to and use the CLI.

1.1 Covered Software

This Reference Guide is valid for RPX-SW V1_2_2.

1.2 Access to the Device

The FSP-RPX16 CLI can be accessed via

- the “Local” interface using the SSH protocol, and
- the “North” interface using the SSH protocol.

Remark: The “South” interface is intended to be used for cascading the management DCN, only. There is no management access to the device via the “South” port.

The following section will explain how to set an SSH connection up.

1.2.1 SSH Connection

SSH connections always require that the connecting user authenticates himself to the device. Several authentication options can be selected by the administrator:

- to use one of the user names/passwords from the local user database or remote authentication methods.
  - See chapter 4 of axManual_FSP-RPX.pdf for defining local users and configuring TACACS+.
  - User name and password must be supplied when establishing the SSH connection, login to the CLI happens automatically.
- to use a special “global” SSH password.
  - A single (“global”) SSH password is configured on the RPX device. The RPX only allows SSH connections for the user “cli” using the global password.
  - After the SSH connection is established, the user is asked to login to the CLI as one of the users known to the local user database or remote authentication methods.
- to use SSH key authentication, for which the keys must be stored on the RPX.
  - One of two possible behaviours can be selected for each stored key individually:
    - *Direct login key*: The key is used to establish the SSH connection as well as for CLI login.
      NOTE: The user name associated with the key must be contained in the local user database. TACACS+ users are not supported this way.
    - *Connection key*: The key is only used to establish the SSH connection. After the connection is established, the user is asked to login to the CLI as a separate step.

- See axManual_FSP-RPX.pdf information on how to install SSH keys on the device.

NOTE: All SSH passwords must follow the password security requirements defined for the device. Attempts to configure weaker passwords will be rejected with appropriate error messages.

The SSH protocol uses TCP/IP connections to port 22 by default. The port number on which the SSH server listens can be changed.

1.3 Command Line Interface (CLI)

1.3.1 Introduction to the CLI

Many devices that come with support for CLI provide a huge number of different commands to configure the various functions of the device. All of these commands come with their own syntax and parameters. The CLI of arcutronix devices follows a different and more intuitive approach.

In contrast to the devices mentioned before, the CLI of arcutronix devices provides direct access to configurable parameters and device properties, so-called variables, which can be read-only (e.g. for fixed device properties) or modifiable (for configurable parameters).

Since there is a vast number of those variables, they are organized in a hierarchical menu structure. The menu structure and the ordering of information therein is logically aligned with the device functions. Once familiar with the layout of the menu structure, which is easily comprehensible, the user quickly and intuitively navigates through the menu structure and easily manipulates the device settings as needed. The CLI supports this further by giving context-sensitive help as well as automatic command and parameter completion where ever possible.

As a result, only a single command is needed to configure all aspects of the device and its functions: the “config” command explained later. It provides everything that is needed to navigate through the menu structure, to look at the information provided in submenus and to manipulate the value of configurable parameters. Each item in the menu structure (submenus, variables and possible variable values) may have helpful descriptions associated with them that can be viewed with the “config” command as well.

The navigation through the menu structure is designed to follow a principle that every computer user knows: it closely resembles the navigation though a file system. Here, menus and submenus represent directories on the hard drive, whereas configurable parameters are similar to files on the disk. The “config” command supports full path names in every place where the name of an item in the menu structure is expected. Those path names can either be relative to the current position in the menu tree, or be a path starting from the root of the menu structure. Path names are formed like file names by concatenating menu, submenu and variable names with a directory separator, for which the UNIX-style forward slash “/” was chosen. The usual name “..” for the parent menu is supported as well.

This file system similarity is also applied to more complex elements of the menu structure. For tables, which do naturally occur if there is more than one instance of an equivalent hardware component or software function present, each table row is translated into a submenu where the table columns are presented as scalar variables. Within the submenu representing the table row, editable columns can be modified as usual and further submenus of the table row become available.

Usually, the manipulation of a variable will have an immediate effect. Once the new variable value is successfully submitted, the device will make immediate use of the changed value and adjust its operation to it. Occasionally, there are cases where a group of variables needs to be consistently changed as a whole. These variable groups are also translated into submenus called “Form Pages”. Whenever the user navigates to such a form page, the CLI starts a new transaction that is automatically aborted when the user navigates away. Changes to variables within the form page will not immediately be activated but become part of the transaction data. Each form group has a BUTTON variable that fulfils the task of submitting the data and activating the changes.

1.3.2 CLI Editor Features

1.3.2.1 Context Sensitive Help

The RPX CLI offers context sensitive help which is a useful tool for new and advanced users. If, at any time, the user is in doubt about further options of a command, he may simply type a question mark (?) and terminate the line. The CLI will then show a list of possible options for the next missing parameter of the command, with <CR> standing for carriage return (to terminate the input line, e.g. the missing parameter is not required). The list that is shown depends on the input that the user has already entered.

The “help” command can be used to get a list of the available commands. When called with a command name as parameter (e.g. “help config”), a detailed list of all syntax variants of the command, their functional description and required or optional parameters is printed.

1.3.2.2 Syntax Checks

The RPX CLI carefully checks the syntax of all entered data. If a command or path is entered improperly (invalid command, invalid path, unknown option, wrong number of parameters), the CLI will inform the user and indicate where the error has occurred.

1.3.2.3 Path and Command Completion

The CLI automatically completes command names, path components and enumerated values as best as possible when the user hits the <TAB> key. This feature helps to speed up manual input of commands. If multiple matching completions are available, the CLI shows a list of all matching completions and expects the user to type in more characters to disambiguate the available options.

For example, instead of typing the `"config"` command fully, the user just has to type `"c<TAB>"` because `"config"` is the only command that begins with `"c"` and <TAB> will complete it.

1.3.2.4 Abbreviations of Path and Command Names

Commands and paths to menus or variables can be abbreviated as long as the abbreviation is not ambiguous. This is helpful when typing CLI scripts, where the auto-completion feature (using <TAB>, see above) is not available.

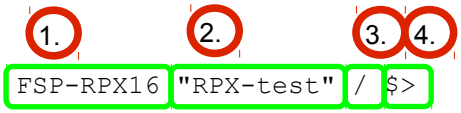
For example, the path `“/General System Information/Inventory”` can be shortened to `“/G/I”` or (as the path and command input is case-insensitive) `“/g/i”`.

1.3.2.5 Prompt and Path

The CLI prompt is composed of 4 parts, which are assembled in the following order:

1. Device Type = “FSP-RPX16”,
2. Device Name = Corresponds to the serial number by default. The device name can be changed,
3. Path = the current location within the menu tree,
4. End-Of-Prompt marker = “$>”

The current location in the menu tree is always the lop-level menu “/” directly after login:



After navigating to the “General System Information” submenu, the prompt will be:

```
FSP-RPX16 "RPX-test" /General System Information $>
```

To improve readability and avoid problems with overly long lines, the path printed in the prompt will be limited to 30 characters. If the path is longer than 30 characters, the leading characters are all replaced by three dots. So after navigating to the “Inventory” submenu, the prompt will look like this:

```
FSP-RPX16 "RPX-test" ...ystem Information/Inventory $>
```

The complete current menu path can always be retrieved with the “config path” command that prints the unshortened current menu path.

1.3.2.6 Comments

In scripts it is helpful to add comments to document the script behaviour. In order to support scripting to automate configuration and reproduce settings easily, the CLI supports comments. A comment is introduced with a hash symbol (#) and extends to the end of the input line. Any input on the left-hand side of the comment indicator is interpreted as command. Empty lines containing only white space and comments are supported as well.

1.3.2.7 Quoting and Escaping

Some characters have a special meaning in the CLI. Examples are white space characters (which separate command arguments) and quotation indicators. When these characters are preceded by a back-slash (\), they loose their special meaning and are added to the current word instead. You may use “\\” (e.g. an escaped back-slash) to input a literal back-slash.

Those special characters also loose their special interpretation when they appear in quoted text. Quoting is introduced by a quotation indicator: either an apostrophe (') or the quotation mark ("), both of which are equivalent. Quoting ends when the same quotation indicator that was used to start the quotation is found again.

Using the back-slash to escape characters inside quoted text is possible. Flexibility is further enhanced by allowing only parts of an argument to be quoted.

Examples:

Argument Notation	Results In
`General\ System\ Information`	`General System Information`
`“General System Information”`	`General System Information`
`'General System Information'`	`General System Information`
`General' 'System' 'Information`	`General System Information`
`'I am “Superman”'`	`I am “Superman”`
`“I am \”Superman\””`	`I am “Superman”`
`I\ am\ \”Superman\”`	`I am “Superman”`
`I' 'am' “'Superman\”`	`I am “Superman”`
`c:\windows\system32`	`c:windowssystem32`
`“c:\windows\system32”`	`c:windowssystem32`
`c:\\windows\\system32`	`c:\windows\system32`
`“c:\\windows\\system32”`	`c:\windows\system32`

1.3.2.8 Continuation Mode

The CLI offers the possibility split up very long commands, so that they extend over multiple lines. Again, this is a useful feature to enhance the readability of scripts.

The end of an input line normally starts the command line interpreter. When the last character in the input line is a back-slash (\), the CLI enters the continuation mode, changes the prompt and expects more input. The continuation mode ends (and triggers the command line interpreter) when an input line is detected that does not end with a back-slash.

NOTE: The back-slash and the following newline are removed from the input before the command is interpreted.

Continuation mode is indicated by changing the prompt to:

(cont) `$>`

Some command arguments (those with embedded white space) may be quoted using either the apostrophe (') or quotation mark (") as quoting indicators. The CLI also enters continuation mode when it detects that there are unpaired quotation indicators.

NOTE: When the continuation mode was entered because of open quotations, it can only be left by either entering the missing closing quotation indicator, or by typing <CTRL>+C.

1.4 The CLI Commands

Once a CLI session is established, one can navigate within the RPX CLI menus like in a hierarchically structured directory tree. Available commands and command options vary depending on the position within this hierarchy.

To assist users in the navigation through the CLI menus, the command prompt will change to reflect the position of a user within the menu hierarchy. This allows users to easily identify where within the menu structure they are at any given moment. The context sensitive help and automatic command completion further assist the user during command input.

NOTE: Any white space inside a literal string argument must be preceded by a back-slash (\) or the string must be properly quoted. E.g.

```
$> config go "General System Information"      or
$> config go General\ System\ Information
```

Because the “Tab-by-Tab” feature is aware of required escaping and quoting, it helps a lot to always build the correct syntax.

NOTE: The CLI treats command names and paths to menus or variables case-insensitive. Other items, such as texts assigned to string variables, are case-sensitive, though.

1.4.1 The CONFIG Command

The “config” command is the most powerful command in the CLI and the one used most often. For this reason “config” gets its own chapter here in this reference guide. All the other available commands will be introduced in the following chapter 1.4.2 Additional CLI Commands.

The “config” command displays or changes configuration settings. Configuration settings are hierarchically structured in a menu tree and this command can also be used to display/change the current configuration menu. Without any argument, the “config” command displays the content of the current configuration menu. 8 syntax flavours are known for the “config” command: the table below shows a summary of each of the available variants:

Command	Syntax / Explanation
config	config
	Shows all the content of the current configuration submenu. The first character in each row indicates the type of variable that is shown: **>** for submenus, **F** for form pages, ***** for read-write variables, **!** for read-write password variables, **+** for executable commands, (blank) for read-only variables. Options: none
config path	config path
	Shows the complete path of the current configuration menu. As the CLI prompt may only show a shortened path (30 characters), it might be helpful to see the complete path displayed. Options: none.
config go	config go <PATH>
	Changes to a different configuration menu. Options: • <PATH> = root: topmost menu • <PATH> = up: go to parent menu • otherwise: go to submenu identified by <PATH>. The <PATH> may start at the present submenu or at root (/). Suitable submenus are identified by: • > regular submenu

Command	Syntax / Explanation
	• F form page
config VARIABLE	config <VARIABLE>
	Display the current value of <VARIABLE>. If <VARIABLE> points to a submenu, display all content of the submenu. Options: • <VARIABLE>: path to a variable or submenu. The path may start at the present submenu or at root (/). Suitable entries are identified by: • * read-write • ! read-write password • > submenu • (blank) read-only
config help	config help <VARIABLE>
	Display help for <VARIABLE>. The help usually contains a description of the type of the variable, its purpose and allowed values. If <VARIABLE> points to a submenu, display help for the submenu. Options: • <VARIABLE>: path to variable or submenu. The path may start at the present submenu or at root (/). Allowed are all entries that the config command displays.
config set	config set <VARIABLE> <VALUE>
	Change the value of <VARIABLE> to new <VALUE>. Options: • <VARIABLE>: path to the variable which is to be modified. The path may start at the present submenu or at root (/). Allowed are variables identified by: • * read-write • ! read-write password • <VALUE>: New value of the variable. Value must match the value range defined for <VARIABLE>.
config hidden	config hidden <VARIABLE>
	Change the value of the protected (password) <VARIABLE> in a hidden mode. The password will be prompted for in a new line. The typed value will be invisible for security reasons. To protect from accidental mistyping errors, the new value has to be re-entered for confirmation. Options: • <VARIABLE>: path to the variable. The path may start at the present submenu or at root (/). Allowed are variables identified by: • ! read-write password
config do	config do <COMMAND>
	Start or execute <COMMAND>.

Command	Syntax / Explanation
	Options: • <COMMAND>: path to a command variable. The path may start at the present submenu or at root (/). A command starts a complex action. Allowed are variables identified by: • + (executable command)

1.4.2 Additional CLI Commands

While the command “config” is the most important command, there are many other helpful commands for use in the CLI. The command “config” is explained in the previous chapter (1.4.1 The CONFIG Command) and here all the other commands will be explained.

The table below shows a summary of commands and the corresponding syntax:

Command	Syntax / Explanation
help	help [COMMAND]
	The help command is available in any context and lists the possible commands in the given context. If HELP is used with a command, it shows the syntax of the command together with a short help text. Options: • COMMAND – any available command.
log	log [LINES]
	LOG shows the last entries of the device log file. The optional parameter allows to specify the number of lines to show. Options: • <LINES> - The number of lines to print at most (default: 100)
quit	quit
	Quit the current CLI session. Options: • none
save_devlog	save_devlog <FILENAME>
	Save the developer log-files onto the “Logfile Store” server. Options: • FILENAME – file name on the “Logfile Store” server. That file must not yet exist on the server!
print_devlog	print_devlog
	Print a base64-encoded version of the developer log-files to screen. If requested, please capture the output and send it to arcutronix.

Command	Syntax / Explanation
	Options: • none
show	show [<PATH>]
	Displays the settings in the selected (or current) menu in a format suitable for copying the lines back into the CLI. Changeable settings are printed as CLI commands, read-only settings are printed as comments. Each line is terminated by a semi-colon. Options: • <PATH> - Path to a menu. If omitted, the current menu path is used.
showall	showall [<PATH>]
	Displays the settings in the selected (or current) menu including all submenus in a format suitable for copying the lines back into the CLI. Changeable settings are printed as CLI commands, read-only settings are printed as comments. Each line is terminated by a semi-colon. Options: • <PATH> - Path to a menu. If omitted, the current menu path is used.

2 Special CLI Constructs

The RPX offers management access in several ways: per Web-OPI, CLI, and SNMP. The Web-OPI management access method represents a graphical user interface, CLI is command-line oriented (CLI) and SNMP is used in machine-to-machine (M2M) communication scenarios.

Web-OPI and CLI share a common design of the management plane (menu structure and variable names) that makes it very easy for users familiar with the device to switch between those interactive management access methods. Some constructs that are easily handled in a graphical user interface require more explanation when operated in the CLI: tables and form pages.

2.1 Tables

Tables are an essential part of the RPX management plane. A lot of information is ordered in tables. A table has the advantage that information can be shown very compact. Some tables are even dynamic, which means the number of rows can vary, depending on configuration settings or device states.

Though tables are a good option to present information, it is difficult for a CLI to manipulate individual table cells. The CLI does not have a mouse pointer to select one element within the table – it can only use commands to navigate the rows and columns. The following explanation shows how to navigate in tables and how to edit table cells.

The RPX CLI handles tables as a list of submenus (sub-directories). Each table row is presented in its own submenu, which can be navigated to with help of the `config go` command. The CLI calculates a unique name for each table row from the data within the table. Usually (but not always), the content of the first table column is used to index the table rows, eventually followed by a suffix to disambiguate equal row names.

Within the submenu corresponding to a table row, the table columns are displayed as variable-value pairs (where the column titles represent the variable names). The same layout is already known from regular menu pages. Editable table cells can be changed only in the row's submenu, and submenus of the table row are available there as well.

An easy example is the table of 3 servers for different store and load processes. The table layout is like this:

Server	URI	Valid	Edit
Firmware Store	sftp://andreas@192.168.1.1	Valid	Edit
Configuration Store	sftp://lab6@192.168.0.6/D:\tmp\	Valid	Edit
Logfile Store	Not valid	Not valid	Edit

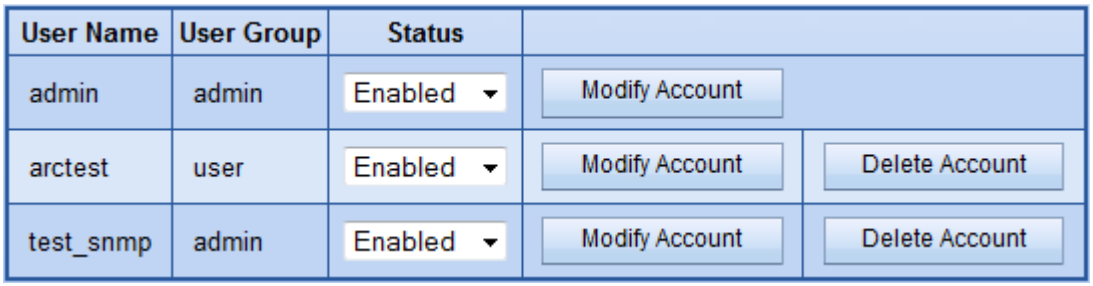
In CLI the same table looks like this:

```
                        Server              URI                                 Valid

> Firmware Store        Firmware Store      sftp://andreas@192.168.1.1          Valid

> Configuration Store   Configuration       sftp://lab6@192.168.0.6/D:\tmp\     Valid
                        Store

> Logfile Store         Logfile Store       Not valid                           Not valid
```

The first line contains the titles of the table columns. Please note that the “Edit” column was removed (these column contains links to per-table-row submenus only). The following lines (one per table row) all start with the “link” to the submenu corresponding to the table row, followed by the column data. This table uses the content of the first table column as name of the submenu, but different row indices are used by other tables.

To edit/view the settings of any table row, use the command `config go <row name>` to enter the submenu. Here, the link to the “Edit” submenu is present as well.

Another table example is the local user database. It is presented as follows in the Web-OPI:



Each row has a pull-down menu to enable/disable the entry, a “Modify Account” submenu link and a “Delete Account” command button.

The CLI offers the same information in a slightly different way:

```
                    User Name       User Group          Status

> admin             admin           admin               Enabled

> arctest           arctest         user                Enabled

> test_snmp         test_snmp       admin               Enabled
```

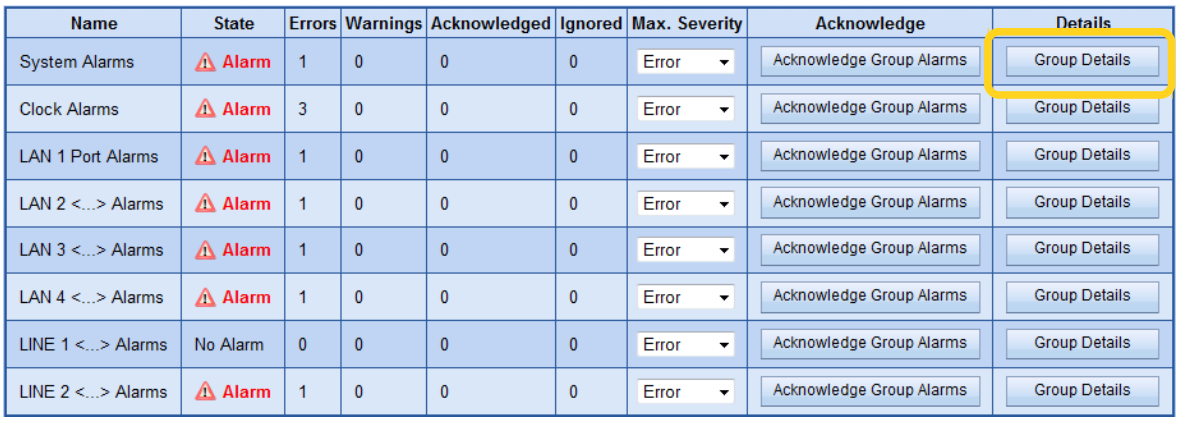
An account can be modified by entering the submenu of the corresponding table row, where the account can also be enabled, disabled or deleted:

```
…Passwords $> config go arctest
…Passwords/arctest $> config
-- Users and Passwords
  User Name: arctest
  User Group: admin
* Status: Enabled
> Modify Account
+ [Delete Account]
```

- the prompt shows the submenu name (here `arctest`),
- “User Name” and “User Group” are read-only table columns
- the “Status” column is properly converted to an ENUM variable that can be modified with the `config set Status <Enabled|Disabled>` command
- the “Modify Account” submenu is available here and can be entered with the `config go "Modify Account"` command
- the “Delete Account” command is available here and can be executed by typing `config do "Delete Account"`

Those examples highlight the full equivalence between CLI and Web-OPI, with the exception that in the CLI, each table row has an associated submenu where settings can be changed instead of just clicking into the table as in the Web-OPI.

Nesting of tables is also possible in the RPX management approach. Each row of a “parent” table can contain one or more “child” tables. There is nothing special to consider when using such nested tables in the CLI. Each table row is a submenu and if tables are part of a submenu of a parent table, its just more submenu levels that appear. As an example, the nested tables of the Alarm Management are shown here:



Name	State	Errors	Warnings	Acknowledged	Ignored	Max. Severity	Acknowledge	Details
System Alarms	Alarm	1	0	0	0	Error	Acknowledge Group Alarms	Group Details
Clock Alarms	Alarm	3	0	0	0	Error	Acknowledge Group Alarms	Group Details
LAN 1 Port Alarms	Alarm	1	0	0	0	Error	Acknowledge Group Alarms	Group Details
LAN 2 <...> Alarms	Alarm	1	0	0	0	Error	Acknowledge Group Alarms	Group Details
LAN 3 <...> Alarms	Alarm	1	0	0	0	Error	Acknowledge Group Alarms	Group Details
LAN 4 <...> Alarms	Alarm	1	0	0	0	Error	Acknowledge Group Alarms	Group Details
LINE 1 <...> Alarms	No Alarm	0	0	0	0	Error	Acknowledge Group Alarms	Group Details
LINE 2 <...> Alarms	Alarm	1	0	0	0	Error	Acknowledge Group Alarms	Group Details

The “Group Details” of the “System Alarms” is another table:

Name	Config	State		Acknowledge	SNMP Notification
Dying Gasp Indication	Error	n.a.	Normal Operation	Acknowledge	No Notification
Reset State	Ignore	n.a.	No Reset Scheduled	Acknowledge	No Notification
DC Power Status	Error	Ok	DC Power Good	Acknowledge	SNMP Trap
AC Power Status	Error	Error	AC Power Failure	Acknowledge	SNMP Trap
Over Temperature Shutdown	Error	Ok	Normal Operation	Acknowledge	SNMP Trap
MGMT1 <...>	Error	Ok	Link Up	Acknowledge	No Notification
MGMT2 <...>	Ignore	Ok	Link Up	Acknowledge	SNMP Trap
Device Temperature	Thresholds	Ok	31.5 °C	Acknowledge	SNMP Trap
Firmware Update Status	Error	n.a.	No Update File	Acknowledge	SNMP Trap

The CLI offers the same information in the following way:

```
                  Name                State    Errors Warnings Acknowledged Ignored Max.
Severity
> System Alarms:        System Alarms       Alarm    1      0        0           0       Error
> Clock Alarms:         Clock Alarms        Alarm    3      0        0           0       Error
> LAN 1 Port Alarms:    LAN 1 Port Alarms   Alarm    1      0        0           0       Error
> LAN 2 <...> Alarms:   LAN 2 <...> Alarms  Alarm    1      0        0           0       Error
> LAN 3 <...> Alarms:   LAN 3 <...> Alarms  Alarm    1      0        0           0       Error
> LAN 4 <...> Alarms:   LAN 4 <...> Alarms  Alarm    1      0        0           0       Error
> LINE 1 <...> Alarms: LINE 1 <...> Alarms No Alarm 0      0        0           0       Error
> LINE 2 <...> Alarms: LINE 2 <...> Alarms Alarm    1      0        0           0       Error
```

The “Group Details” submenu of the “System Alarms” table row can easily be entered by typing

```
… $> config go “System Alarms/Group Details”
```

where the child table becomes visible:

```
                          Name                      Config State                      SNMP
Notification
> Dying Gasp Indication:      Dying Gasp Indication     Error  n.a. | Normal Operation   No
Notification
> Reset State:                Reset State               Ignore n.a. | No Reset Scheduled No
Notification
> DC Power Status:            DC Power Status           Error  Ok | DC Power Good        SNMP Trap
> AC Power Status:            AC Power Status           Error  Error | AC Power Failure  SNMP Trap
> Over Temperature Shutdown: Over Temperature Shutdown Error  Ok | Normal Operation     SNMP Trap
> MGMT1 <...>:                MGMT1 <...>               Error  Ok | Link Up              No
Notification
> MGMT2 <...>:                MGMT2 <...>               Ignore Ok | Link Up              SNMP Trap
> Device Temperature:         Device Temperature               Ok | 31.5 Â°C            SNMP Trap
> Firmware Update Status:     Firmware Update Status    Error  n.a. | No Update File     SNMP Trap
```

Each row can now be entered for further configuration.

2.2 Form Pages

Sometimes a number of related variables has to be changed simultaneously. The CLI offers the “config” command that allows to change one variable at a time and, usually, the changes are committed and activated immediately.

A form page is a special submenu that contains variables to be changed simultaneously. They are used in different locations in the menu hierarchy. A form page shows the special behaviour that it does not submit variable changes immediately, but collects them and waits for the user to submit the changes. The form page shows transactional behaviour: either all variables are submitted as a whole, or none at all. If one of the new variable values in the form page fails validation, all other variable changes are also rejected.

A form page always contains a BUTTON variable that submits changed values.

Due to the transactional behaviour of a form page, the CLI imposes some restrictions on the use of form page content. Variables in form pages cannot be addresses by a full path name – it is always required to enter the form page with the “config go” command and use the variable name without any path elements. Furthermore, the CLI requires an explicit confirmation when navigating away from a form page with uncommitted variable changes.

Form pages can be distinguished from regular submenus by is “entry type” in the parent menu: a form page is indicated by an “F”, while regular submenus are indicated by “>”:

```
F sub-page1      – a form page with transactional behaviour
> sub-page2      – regular menu where individual changes are submitted immediately
```

A good example for a form page is the “Create Account” submenu to add a new user. The user name, password and access level must all be known before the user can be added. So, with the help of form pages, all required data can be entered and the actual creation of the user in the local database is done when the data is committed using the “Create Account” command. An example for this is given in the use case chapter at the end of the document.

3 Overview Reference Guide

3.1 Design

Each variable available in the CLI is presented in a small table showing all available information about the variable. The table and its entries are explained in this paragraph.

Below is an example of the information about a variable as displayed throughout the document:

1 **EFM-Mode**	2 config go “/Operation and Maintenance/Ethernet First Mile/<Interface>” config set “EFM Mode” <value>			
3 Enable (passive/active) or disable (off) the EFM support on this port.				a RW RO RO b ENUM c P d Off
4 Values	Off	EFM off		
	Passive	EFM passive mode (1)		
	Active	EFM active mode (2)		
5 Constraints	**EFM Status** is "Disabled"		→	-- -- --
	Type is "100FX"		→	RO RO RO

The table can be read as this:

1 This is the name of the variable being explained.

2 Short example of CLI commands to use the variable. The first command (“config go”) indicates the variable’s location (submenu), while the second command shows how to read or change the variable.

If the path to a variable contains indices like “<Interface>”, these indices and their possible values

are explained in the introduction of the chapter that covers this menu path. In the case of the variable “EFM-Mode” used here, the explanation of <Interface> is found in the chapter on “Operation and Maintenance / Ethernet First Mile / <Interface>”.

3 This is the description of the variable. The same description is also printed in the CLI, when

```
config help <variable>
```

is entered.

More important information is summarized at the right-hand side of the description:

a Access Levels for the three possible user groups (Admin, User and Guest) from left to right. Possible access levels are
RW (read-write),
RO (read-only) and
-- (invisible / not-accessible).

In the given example, Admin users (left-hand side) have Read-Write permissions, while User (center) and Guest (right-hand side) have Read-Only permissions.

b The type of variable (see chapter 3.2 Types of Variables).

c The type of persistence: Persistent (P), Temporary (T) or Factory-Setting (F).

A persistent variable is stored in non-volatile memory and is remembered over system resets and power failures.
A temporary variable is not persistently stored and will be recalculated (or reset to a default value) when the device restarts. The current time/date is an example for a temporary variable.
A factory setting is read from the electronic type label after reset and cannot be changed by the operator.

d Default Value of this variable after Factory Reset.

4 In case the variable type is ENUM (see b) the available enumerations are given here. The values are listed one by one and are briefly explained. If there is dependency for some values, this is indicated by a number in parentheses.
NOTE: This section will not be displayed if the variable is not of ENUM type.

5 Constraints to the accessibility of the variable are shown last. These access restrictions may occur due to configuration settings or inherent device properties. The constraints section, if present, lists conditions that cause variable access to be restricted and, for each of the conditions, the resulting new access permissions for each access level.

In the given example, EFM-Mode

a) is inaccessible if “EFM Status” is "Disabled", and

b) the value cannot be changed if the interface type is "100FX".

3.2 Types of Variables

The management variables of RPX devices are of different types. The type of a variable defines the acceptable data format, value range and other constraints. The different variable types and their properties are listed in the overview below:

ENUM	The ENUM type consists of a set of named values called elements. For ENUM types the possible elements are listed in the (allowed) Values field of the variable. Other values than the listed ones are not allowed and will be refused.
STRING	A STRING is a sequence of symbols. The maximum length for STRING is 255 symbols. The allowed symbols are: • Letters, lower case and upper case • Digits • Special Characters UTF-8 characters sometimes cause problems when displayed. It is recommended not to use UTF-8 characters.
INTEGER	All positive INTEGER values (0…65535).
INTEGER (range)	All positive INTEGER values in the given range. The range can be given in the form • (val1 – val2): val1 is included in the range of allowed values as well as val2 and all integers in between. • (max. val3): all integers between 0 and val3 (including) are allowed.
COUNTER	The COUNTER type is a monotonic counter up to 2^64-1. A COUNTER wraps around after reaching 2^64-1 and starts at 0 again.

TIME	TIME variables require the value to be given as: hh:mm Seconds do not need to be specified.
DATE	The DATE variable requires the value to be given as: yyyy-mm-dd

IPADDR	The IPADDR must be in accordance to IPv4 rules in the so-called “Dotted Decimal” format: Each byte of the 4 byte-address is written in decimal, separated by a dot. E.g. 192.168.1.100 or 255.255.255.0. Where IPv6 is supported, IPv6 addresses must be given in the usual notation: 4-digit hex blocks separated by colons, e.g. 2001::1a1a:1b1b

FILENAME	The FILENAME is a string used to uniquely identify a file stored on a file system. Restrictions on length and allowed characters of file names depend on the system where the file shall be stored to or loaded from. The arcutronix device does not assume any restrictions. A FILENAME consists of (relative) path + file name + extension. The path should use “/” (slash) to separate the directories. Extension might be empty.
PASSWORD	PASSWORD variables contain string values. Special requirements are enforced to improve password security. Minimum password length is 8 characters, maximum password length is 32 characters, character set is 7-Bit ASCII. Allowed characters are: • Letters, lower case • Letters, upper case • Digits • Special Characters: 0x2D (-), 0x2E (.), 0x5F (_) The password must contain characters out of at least 3 of the above 4 groups. E.g. the default password for admin is “Pr1vate_”: Capital letters, lower case letters, digits and special character are used.

BUTTON	The BUTTON type is used to execute or start a command. Variables of type BUTTON cannot be edited, just invoked by config do.
PAGE	The PAGE type is used for all menus. Variables of type PAGE cannot be edited, just used in path names.

ALARM	An ALARM is a read only variable with an associated alarm condition. Certain values of the variable will raise the alarm and may trigger an SNMP trap.

4 Menus and Variables in the FSP-RPX CLI

This chapter presents all menus and variables, which can be configured and monitored via Command Line Interface.

The ordering of variables in this chapter follows the hierarchical menu tree of the device. The purpose of individual menus is explained as well.

NOTE: Occasionally, a variable appears at more than one position in the menu tree. This reference guide does not list all occurrences of such variables, only selected ones. Therefore, submenus may be populated with more entries than obvious from studying this document.

An alphabetical list of all variables is given in Fehler: Referenz nicht gefunden on page Fehler: Referenz nicht gefunden.

4.1 Administration

4.1.1 Administration / 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.

When a stored configuration snapshot (Factory Default or a user-prepared configuration) is to be reactivated, one can decide whether all configuration variables are restored or some settings remain unchanged in the current configuration. This is helpful to, for example, keep the IP addresses of the management interfaces or the user database intact.

Besides storing configuration snapshots locally on the arcutronix device, these snapshots can also be stored on external servers or be downloaded from them. This allows creating "master configuration files" and distribute them to a number of arcutronix devices with similar configuration needs.

Three different file transfer protocols are supported to load and store configuration snapshots to and from external servers:

- HTTP up- and downloads via Web-OPI from the browser window, if enabled
- SFTP - SSH File Transfer Protocol to/from a pre-configured server
- TFTP - Trivial File Transfer Protocol to/from a pre-configured server

The pre-configured server used with SFTP and TFTP file transfers is called "Configuration Store" and needs to be set up in the "/Administration/User and Access Administration" menu before those file transfer protocols can be used.

SFTP offers the best security measures of all available options, requiring proper host and user authentication and transferring all data encrypted. As a TCP protocol, it is rather robust w.r.t. network latencies and low bandwidth.

Trivial File Transfer Protocol (TFTP) is a very basic and more traditional method used to transfer files over an IP network, such as the internet. Although easy to set up and use, its drawbacks are missing authentication, missing encryption of data and the use of UDP packets to transfer the data.

HTTP file transfer refers to the transfer of files through a computer's web browser. File transfers via HTTP have been developed as a simple alternative to the various file transfer protocols that need separate server and client programs. For HTTP file transfer the customer only needs access to a web browser. This is sufficient to save and store files to and from the device.

NOTE: The use of HTTP file transfer can be disabled in the "User and Access Administration" menu.

NOTE: If the user is logged onto the device via CONS CLI or SSH CLI, the HTTP upload and download options are not available.

NOTE: A configuration file always has the file name extension "*.cfgx". The file format is designed in such a way as to enable the arcutronix device to recognize invalid files.

Config File Name

config go "/Administration/Configuration Management"
config set "Config File Name" STRING

If a download of a configuration file from the "Configuration Store" server to the device has to be done, this variable is used to specify the file path of the configuration file on the server. The file name may contain directory components. The directory separator is a forward slash ("/").

When the file path is relative (does not start with a directory separator), it is simply appended to the configuration store's server URI to resolve the download URI.

When the file path is absolute (starts with a directory separator), the configured configuration store's directory is ignored.

RW	--	--
STRING		T
EMPTY		

Download from Server

config go "/Administration/Configuration Management"
config do "Download from Server"

Download the named configuration from the configuration server to the device.

RW	--	--
BUTTON		T
EMPTY		

File Transfer State

config go "/Administration/Configuration Management"
config "File Transfer State"

This variable shows information about file transfers to/from the 'Configuration Store'. If the file transfer has been started, progress information about the transfer is given here.

If the file transfer has completed, this variable contains information about success or failure of the file transfer.

RO	--	--
STRING		T
Automatic		

Server Type

config go "/Administration/Configuration Management"
config "Server Type"

The device supports three different servers, which can be configured for usage.

- Firmware Store: This server is used to download firmware files to the device for installation.
- Configuration Store: This server is used to upload and download configuration files from/to the device.
- Logfile Store: This server is used to store log files externally for further handling.

Each server can be configured to use the TFTP or SFTP protocol.

RO -- --
ENUM F
Automatic

Values	Firmware Store	The server is used to download firmware upgrades to the device.
	Configuration Store	The server is used to upload and download configuration data and SSH keys.
	Logfile Store	The server is used to upload log file from the device to the server.

Server URI

config go "/Administration/Configuration Management"
config "Server URI"

This variable shows the URI (Unique Resource Identifier) of the server entry. If the server is set up correctly, the protocol type, IP address and server directory can easily be derived from the value.

If the value of this variable is "Disabled", the server entry has been disabled by the administrator. If it is "Not Valid", the detailed server configuration needs to be completed before the server can be used.

The value of this variable is calculated dynamically from the server settings.

RO -- --
STRING T
Automatic

4.1.1.1 Administration / Configuration Management / <Config Name>

<Config Name>

There are two predefined configurations:

- "Current Configuration" denotes the currently active configuration of the device,
- "Factory Default Configuration" is the configuration with which the device was shipped.

All other *<Config Name>* entries represent configuration snapshots created by the user.

This submenu allows to save/restore or transfer the selected configuration snapshot to the "Configuration Store" server.

The "Current Configuration" allows creating a new configuration snapshot.

The "Factory Default Configuration" can be reactivated here.

The remaining configurations can be reactivated, be deleted from the device or be transferred to the server.

Date

config go "/Administration/Configuration Management/<Config Name>"
config "Date"

This variable indicates at which date and time the selected configuration snapshot was created.

RO	RO	RO
STRING		P
Automatic		

Delete Configuration

config go "/Administration/Configuration Management/<Config Name>"
config do "Delete Configuration"

Delete this saved configuration snapshot.

RW	RO	RO
BUTTON		T
EMPTY		

Constraints	Current or Factory Default Configuration selected	→	--	--	--

Name

config go "/Administration/Configuration Management/<Config Name>"
config set "Name" STRING

This variable holds a textual description of the configuration. The value stored here is also used as file name when storing the configuration on the "Configuration Store" server. The value needs to be unique. Setting this variable to a value that is already in use by a different configuration will cause an error.

RW	RO	RO
STRING		P
Automatic		

Constraints	Current or Factory Default Configuration selected	→	RO	RO	RO

Save Configuration

config go "/Administration/Configuration Management/<Config Name>"
config do "Save Configuration"

Save a snapshot of the current configuration.

RW	RO	RO
BUTTON		T
EMPTY		

Constraints	NOT Current Configuration	→	--	--	--

Upload to Server

config go "/Administration/Configuration Management/<Config Name>"
config do "Upload to Server"

Upload the configuration to the configuration server.

RW -- --
BUTTON T
EMPTY

Constraints	Current or Factory Default Configuration selected	→	--	--	--

4.1.1.1.1 Administration / Configuration Management / <Config Name> / Apply

This submenu allows reactivating the configuration snapshot. For a number of selected parts of the configuration snapshot the user can select whether to reactivate that part from the configuration snapshot or whether to leave that part of the current configuration unchanged.

Apply Configuration Now

config go "/Administration/Configuration Management/<Config Name>/Apply"
config do "Apply Configuration Now"

Apply this configuration now and soft-reboot the device.

RW -- --
BUTTON T
EMPTY

Constraints	Current Configuration selected	→	--	--	--

Dying Gasp for Maintenance Reboots

config go "/Administration/Configuration Management/<Config Name>/Apply"
config "Dying Gasp for Maintenance Reboots"

This variable controls whether the device is emitting Dying Gasp notifications for regular maintenance reboots of the device.

In case of regular maintenance reboots (firmware upgrade, applying configurations, system reset), the device is going out of operation as well. However, since these actions are always initiated by a device operator as part of the device maintenance, it may not be wanted to trigger full error handling procedures here.

RO -- --
ENUM P
Automatic

Values	Disabled	No Dying Gasp on planned maintenance resets
	Enabled	Planned maintenance resets force Dying Gasp

Constraints	Current Configuration selected	→	--	--	--

Preset Configuration Components

config go "/Administration/Configuration Management/<Config Name>/Apply"
config set "Preset Configuration Components" ENUM

This variable allows to preset all selectable configuration components to the selected action.

The default of "No Change" has no effect at all. This variable resets itself to "No Change" value after executing the requested action.

			RW	--	--
			ENUM		T
			No Change		
Values	No Change	Keep all configuration components at their current setting.			
	Overwrite	Set all configuration components to "Overwrite".			
	Keep Current	Set all configuration components to "Keep Current".			
Constraints	Current Configuration selected	→	--	--	--

4.1.1.1.1.1 Administration / Configuration Management / <Config Name> / Apply / <Configuration Component>

<Configuration Component>

One component of a configuration. Each configuration is split into several components to make it easier to apply only parts of a configuration.

Behaviour	config go "/Administration/Configuration Management/<Config Name>/Apply/<Configuration Component>" config set "Behaviour" ENUM			
When a configuration snapshot (Factory Default or one of the user-created snapshots) is to be reactivated, it might be reasonable to keep some settings of the current configuration unchanged, e.g. IP addresses of management interfaces or the user database. There are different parts of the configuration for which this choice exists: • MGMT IP Config: Port and IP configuration of the management interfaces • SNMP Trap Targets: configured SNMP Trap receivers • SNMPv2 Communities: all currently defined SNMPv2c communities • SNMPv3 Users: all currently defined SNMPv3 users • SSH Keys: all stored SSH keys • User Accounts: all stored users, their passwords and access levels • All other configuration: all the rest			RW ENUM Automatic	RO	RO T
Values	Overwrite	Overwrite this part of current configuration with the information from the configuration file.			
	Keep Current	Keep this part of the current configuration and ignore the information from the configuration file.			
	Append	For this part, add the information from the configuration file to the current configuration.			
Constraints	Current Configuration selected	→	--	--	--

4.1.2 Administration / Date and Time Settings

This menu allows configuring NTP servers to use for time synchronization or to disable NTP support and set the device date/time manually.

Setting up NTP requires enabling NTP support altogether and to setup at least one NTP server. The device supports up to 8 different NTP servers. NTP protocol version (NTPv3 or NTPv4) or MD5/SHA1 security keys can be configured separately for each NTP server. NTP Servers can also temporarily be disabled. The device will select the best of the available NTP servers as source for time synchronization.

If NTP support is disabled, the device allows setting date and time manually.

Date

config go "/Administration/Date and Time Settings"
config set "Date" DATE

This variable shows the current date of the device. When the date/time is automatically adjusted via NTP, this variable is not editable.

In order to manually configure the current date on the device, it is necessary to first disable NTP by setting the "NTP Support" variable to "Disabled".

Format: yyyy-MM-dd

			RW	RO	RO
			DATE		T
			Automatic		
Constraints	"NTP Support" IS "Enabled"	→	RO	RO	RO

NTP Support

config go "/Administration/Date and Time Settings"
config set "NTP Support" ENUM

This variable can be used to enable or disable time synchronization via NTP.

If the variable is set to "Enabled", the device will attempt to contact the given NTP servers to synchronize the device date and time to the best of the available NTP servers. The variables to set the device date/time will become read-only.

If the variable is set to "Disabled", NTP time synchronization will be disabled. The variables to set the device date/time can be modified by the device administrator.

			RW	RO	RO
			ENUM		P
			Disabled		

Values	Disabled	NTP not used to manage device Date and Time
	Enabled	NTP is used to manage device Date and Time

Time

config go "/Administration/Date and Time Settings"
config set "Time" TIME

This variable shows the current time of the device. When the date/time is automatically adjusted via NTP, this variable is not editable.

In order to manually configure the current time on the device, it is necessary to first disable NTP by setting the "NTP Support" variable to "Disabled".

Format: hh:mm

			RW	RO	RO
			TIME		T
			Automatic		
Constraints	"NTP Support" IS "Enabled"	→	RO	RO	RO

Time Zone

config go "/Administration/Date and Time Settings"
config set "Time Zone" ENUM

This variable allows to select the correct time zone for the location of the device. When changing the time zone, the current date/time is automatically adjusted. Please note that the device does not automatically switch between summer time and winter time even if NTP is used. GMT (Greenwich Mean Time) is synonymous with UTC (Universal Time Coordinated).

RW	RO	RO
ENUM		P
GMT+1		

Values	GMT-12	
	GMT-11	
	GMT-10	
	GMT-9	
	GMT-8	San Francisco
	GMT-7	
	GMT-6	Dallas
	GMT-5	New York
	GMT-4	
	GMT-3	Brasil
	GMT-2	
	GMT-1	
	GMT	Greenwich Mean Time: London
	GMT+1	Berlin, Paris, Rome
	GMT+2	Istanbul, Cape Town
	GMT+3	
	GMT+4	
	GMT+5	
	GMT+6	
	GMT+7	Bangkok
	GMT+8	Singapore, Beijing
	GMT+9	Tokyo
	GMT+10	Sydney
	GMT+11	
	GMT+12	
	GMT+13	
	GMT+14	

4.1.2.1 Administration / Date and Time Settings / <IP Address>

<IP Address>

Some device indicated by its IP address. Valid IPv4 or IPv6 address required.

This table row shows the statistics of the selected NTP server. Besides detailed timing parameters (network path delay, time offset and jitter) of the selected server, the server's usability status and the NTP reachability register are shown.

Admin Status

config go "/Administration/Date and Time Settings/<IP Address>"
config set "Admin Status" ENUM

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.

When set to "Disabled", the NTP server is not queried and will never be selected as reference clock.

RW	RO	RO
ENUM		P
Disabled		

Values	Disabled	Never used as reference clock.
	Enabled	May be used as reference clock.

Delay [ms]

config go "/Administration/Date and Time Settings/<IP Address>"
config "Delay [ms]"

This variable shows the current network roundtrip time of NTP packets in milliseconds.

RO	RO	RO
STRING		T
Automatic		

Jitter [ms]

config go "/Administration/Date and Time Settings/<IP Address>"
config "Jitter [ms]"

This variable shows the amount of fluctuations between subsequent NTP datetime transactions in milliseconds.

RO	RO	RO
STRING		T
Automatic		

Offset [ms]

config go "/Administration/Date and Time Settings/<IP Address>"
config "Offset [ms]"

This variable shows the current time difference between the selected NTP server and the local system clock in milliseconds.

RO	RO	RO
STRING		T
Automatic		

Protocol Version

config go "/Administration/Date and Time Settings/<IP Address>"
config "Protocol Version"

This variable allows to configure a NTP protocol version to be used in communication with the server. NTPv4 is the current NTP protocol version, but NTPv3 is still widely used.

RO RO RO
ENUM P
Automatic

Values	NTPv3	NTP Protocol Version 3
	NTPv4	NTP Protocol Version 4

Reachability

config go "/Administration/Date and Time Settings/<IP Address>"
config "Reachability"

This variable represents the NTP reachability register. This register is an eight bit shift register that contains the status of the last NTP transactions with the NTP server. A value of zero in this bitfield indicates that a NTP transaction has failed. Possible reasons are:

- network communication has failed
- NTP server is not synchronous to its time source.

A value of 1 indicates a successful transaction. New values are inserted from the right-hand side and move left with every new NTP transaction until they are pushed out at the left-hand side.

RO RO RO
STRING T
Automatic

Server Address

config go "/Administration/Date and Time Settings/<IP Address>"
config "Server Address"

This variable contains the IP address of the NTP server.

RO RO RO
IPADDR P
Automatic

Server Status

config go "/Administration/Date and Time Settings/<IP Address>"
config "Server Status"

This variable shows whether the NTP server is currently usable for selection as reference clock. The NTP selection algorithm includes several data (such as stratum, round-trip time and jitter) to filter unusable NTP servers.

A value of "Not Used" indicates that the NTP server is not usable as reference clock, probably due to communication problems.

A value of "Bad Quality" indicates that the NTP server was determined to have an insufficient quality for selection and cannot be used as reference clock (NTP outlier status).

A value of "Bad DateTime" indicates that the NTP server probably keeps an incorrect DateTime and cannot be used as reference clock (NTP falseticker status).

A value of "Usable" indicates that the NTP server could be used as reference clock, but has not been selected currently.

A value of "Selected" indicates that the NTP server has been selected as reference clock and is currently in use.

RO RO RO
ENUM T
Automatic

Values

Disabled	NTP server has been disabled in the configuration.
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.

Stratum

config go "/Administration/Date and Time Settings/<IP Address>"
config "Stratum"

This variable shows the stratum of the selected NTP server. The stratum is a measure of how far away the NTP server is from an ideal and accurate time source.

A value of 16 is used when the NTP server is not accessible.

RO RO RO
INTEGER(1 - 16)T
Automatic

4.1.2.2 Administration / Date and Time Settings / NTP Server Setup

This submenu allows to manage NTP servers accessible to the device. Up to eight individual NTP servers can be configured here, identified by their IP address.

Add NTP server

config go "/Administration/Date and Time Settings/NTP Server Setup"
config do "Add NTP server"

Add a new NTP server entry with default values.

RW	RO	RO
BUTTON		T
EMPTY		

NTP Status

config go "/Administration/Date and Time Settings/NTP Server Setup"
config "NTP Status"

This field shows the current status of the NTP client on the device.

A value of "NTP Disabled" indicates that NTP support is currently disabled.

A value of "Synchronizing" indicates that the NTP client is evaluating the quality of the known NTP servers and has not yet selected a reference clock.

A value of "Synchronized" indicates that the NTP client has chosen an NTP server that is used as reference clock.

A value of "No Usable NTP Server" indicates that the NTP client is unable to select a reference clock. Possible reasons are:

- no NTP server configured or all NTP servers disabled.
- all NTP servers unreachable (check reachability register).
- all NTP server considered unsuitable.
- no NTP server selected 5 minutes after restarting the NTP client.

RO	RO	RO
ENUM		T
Automatic		

Values	NTP Disabled
	Synchronizing
	Synchronized
	No Usable NTP Server

4.1.2.2.1 Administration / Date and Time Settings / NTP Server Setup / <IP Address>

<IP Address>

Some device indicated by its IP address. Valid IPv4 or IPv6 address required.

This 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.

Delete NTP Server

config go "/Administration/Date and Time Settings/NTP Server Setup/<IP Address>"
config do "Delete NTP Server"

Delete this NTP server entry.

RW	RO	RO
BUTTON		T
EMPTY		

4.1.2.2.1.1 Administration / Date and Time Settings / NTP Server Setup / <IP Address> / Edit NTP Server

This submenu 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.

Admin Status

config go "/Administration/Date and Time Settings/NTP Server Setup/<IP Address>/Edit NTP Server"
config set "Admin Status" ENUM

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.

When set to "Disabled", the NTP server is not queried and will never be selected as reference clock.

RW	RO	RO
ENUM		P
Disabled		

Values		
	Disabled	Never used as reference clock.
	Enabled	May be used as reference clock.

IP Description

config go "/Administration/Date and Time Settings/NTP Server Setup/<IP Address>/Edit NTP Server"
config "IP Description"

This variable shows the type of IP address assigned to this NTP server.

RO	RO	RO
STRING		T
Automatic		

NTP Key Data

config go "/Administration/Date and Time Settings/NTP Server Setup/<IP Address>/Edit NTP Server"
config set "NTP Key Data" STRING

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 a Key ID that is already in use.

The key data can be specified in two different formats:

- ASCII string, 1..20 printable characters excluding "#" and white space
- HEX string, 40 characters This corresponds to a key length of 160 bits.

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".

RW	RO	RO
STRING		P
EMPTY		

NTP Key ID

config go "/Administration/Date and Time Settings/NTP Server Setup/<IP Address>/Edit NTP Server"
config set "NTP Key ID" INTEGER(0 - 65535)

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).

The data associated with the Key ID must be unique. It is not possible to have two different sets of keys for the same Key ID (this also means that if two different NTP servers use the same Key ID but a different key, one of the server entries should be configured to use a different key).

The default value of "0" is not a valid NTP server Key ID and disables NTP server authentication.

In order to change the Key ID for a NTP server it is required to first disable NTP authentication by setting "NTP Key Type" to "None".

RW	RO	RO
INTEGER(0 - 65535)		P
0		

NTP Key Type

config go "/Administration/Date and Time Settings/NTP Server Setup/<IP Address>/Edit NTP Server"
config set "NTP Key Type" ENUM

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.

A setting of "None" must be used to connect to servers without authentication.

A setting of "MD5" must be used if the server does NTP message authentication based on the MD5 message digest algorithm.

A setting of "SHA1" must be used if the server does NTP message authentication based on the SHA1 message digest algorithm.

RW	RO	RO
ENUM		P
None		

Values	None	Don't use NTP server authentication.
	MD5	Use MD5-based NTP server authentication.
	SHA1	Use SHA1-based NTP server authentication.

Protocol Version

config go "/Administration/Date and Time Settings/NTP Server Setup/<IP Address>/Edit NTP Server"
config set "Protocol Version" ENUM

This variable allows to configure a NTP protocol version to be used in communication with the server. NTPv4 is the current NTP protocol version, but NTPv3 is still widely used.

RW	RO	RO
ENUM		P
NTPv3		

Values	NTPv3	NTP Protocol Version 3
	NTPv4	NTP Protocol Version 4

Reachability Register

config go "/Administration/Date and Time Settings/NTP Server Setup/<IP Address>/Edit NTP Server"
config "Reachability Register"

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 zero in this bitfield indicates that a NTP transaction has failed. Possible reasons are:

- network communication has failed
- NTP server is not synchronous to its time source.

A value of 1 indicates a successful transaction. New values are inserted from the right-hand side and move left with every new NTP transaction until they are pushed out at the left-hand side.

RO	RO	RO
STRING		T
Automatic		

Server Address

config go "/Administration/Date and Time Settings/NTP Server Setup/<IP Address>/Edit NTP Server"
config set "Server Address" IPADDR

This variable contains the IP address of the NTP server.

RW	RO	RO
IPADDR		P
0.0.0.0		

Server Status

config go "/Administration/Date and Time Settings/NTP Server Setup/<IP Address>/Edit NTP Server"
config "Server Status"

This variable shows whether the NTP server is currently usable for selection as reference clock. The NTP selection algorithm includes several data (such as stratum, round-trip time and jitter) to filter unusable NTP servers.

A value of "Not Used" indicates that the NTP server is not usable as reference clock, probably due to communication problems.

A value of "Bad Quality" indicates that the NTP server was determined to have an insufficient quality for selection and cannot be used as reference clock (NTP outlier status).

A value of "Bad DateTime" indicates that the NTP server probably keeps an incorrect DateTime and cannot be used as reference clock (NTP falseticker status).

A value of "Usable" indicates that the NTP server could be used as reference clock, but has not been selected currently.

A value of "Selected" indicates that the NTP server has been selected as reference clock and is currently in use.

RO	RO	RO
ENUM		T
Automatic		

Values

Disabled	NTP server has been disabled in the configuration.
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.

4.1.3 Administration / 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.

In this submenu, one of the variables allows to configure the IP address of a test server (that should respond to ICMP and/or UDP packets). For verification, run either the ping or traceroute command and observe the test result(s) in variable "Command Output".

Command Output

config go "/Administration/Diagnostics"
config "Command Output"

This field shows the output of the test run.

RO	RO	--
STRING		T
Automatic		

IP-Address

config go "/Administration/Diagnostics"
config set "IP-Address" STRING

Network diagnostic functions need the IP address of a test server. Assign the IP address of a server that should be reachable with the current network configuration to this variable before starting any of the diagnostic commands. Both, IPv4 and IPv6 addresses are supported here.			RW	RW	--
			STRING		T
			EMPTY		
Constraints	Diagnostic is running	→	RO	RO	--

Ping

config go "/Administration/Diagnostics"
config do "Ping"

Ping the specified network address. The test server must respond to ICMP packets.			RW	RW	--
			BUTTON		T
			EMPTY		
Constraints	Diagnostic is running	→	RO	RO	--

Stop

config go "/Administration/Diagnostics"
config do "Stop"

Stop a running diagnostic.			RW	RW	--
			BUTTON		T
			EMPTY		
Constraints	Diagnostic is not running	→	RO	RO	--

Traceroute_ICMP

config go "/Administration/Diagnostics"
config do "Traceroute_ICMP"

Traceroute with ICMP packets. The test server must respond to ICMP packets.			RW	RW	--
			BUTTON		T
			EMPTY		
Constraints	Diagnostic is running	→	RO	RO	--

Traceroute_UDP	config go "/Administration/Diagnostics" config do "Traceroute_UDP"			
Traceroute with UDP packets. The test server must respond to UDP packets.		RW BUTTON EMPTY	RW	-- T
Constraints	Diagnostic is running →	RO	RO	--

4.1.4 Administration / Firmware Update

This menu allows firmware updates to be performed.

The usual way to perform a firmware update is to first download the firmware file from the 'Firmware Store' server. The next step is to install the downloaded firmware file onto the device. Both steps need to be initiated separately.

A firmware update file always has the file extension *.upx. The file format is designed in a way that allows the device to verify that the file is not corrupted and is suitable for the device.

The installation procedure writes the updated software into the flash memory and reboots the device afterwards with the new firmware to activate the installation. If the software activation fails because the new firmware does not successfully start up, the device tries to reactivate the previous software version that is known to work and raises a "Software Update Fallback Alarm".

Clear update fallback alarm permanently	config go "/Administration/Firmware Update" config do "Clear update fallback alarm permanently"			
When activation of a newly installed software version fails, the device automatically tries to fall back to the previous software version which is known to work. In this case, an alarm is raised to indicate the software update failure. Use this button to acknowledge/remove the software fallback alarm permanently.		RW BUTTON EMPTY	--	-- T
Constraints	"Firmware Update Status" IS NOT "Firmware Fallback after Software Error" →	--	--	--

Download _ Update Progress

config go "/Administration/Firmware Update"
config "Download _ Update Progress"

This variable shows the progress of the current file download and/or update operation.

If the new firmware file is in the progress of being downloaded from the "Firmware Store" server, this variable shows the amount of data transferred (in percent).

NOTE: In case the (S/T)FTP-server does not support the retrieval of the file size before the file transfer is started, only a status string is shown during the download of the file.

If the firmware file is in the progress of being installed, this variable shows the amount of installation work already performed (in percent).

RO	--	--
STRING		T
Automatic		

Dying Gasp for Maintenance Reboots

config go "/Administration/Firmware Update"
config "Dying Gasp for Maintenance Reboots"

This variable controls whether the device is emitting Dying Gasp notifications for regular maintenance reboots of the device.

In case of regular maintenance reboots (firmware upgrade, applying configurations, system reset), the device is going out of operation as well. However, since these actions are always initiated by a device operator as part of the device maintenance, it may not be wanted to trigger full error handling procedures here.

RO	--	--
ENUM		P
Automatic		

Values	Disabled	No Dying Gasp on planned maintenance resets
	Enabled	Planned maintenance resets force Dying Gasp

File Name

config go "/Administration/Firmware Update"
config set "File Name" STRING

This variable holds the file path to a new firmware file on the "Firmware Store" server. The file path may contain directory components, but does not need to.

If the file path is relative (not starting with a directory separator), the file name is appended to the firmware store's URI to form the download link.

If the file path is absolute (starting with a directory separator), the directory setting of the firmware store server is ignored when forming the download link.

RW	--	--			
STRING		T			
EMPTY					

Constraints	"Firmware Update Status" IS "Update Active"	→	RO	--	--
	"Firmware Update Status" IS "Firmware Download Active"	→	RO	--	--

Firmware Update Status

config go "/Administration/Firmware Update"
config "Firmware Update Status"

This variable gives information about the current state of a firmware update. A firmware update consists of two separate steps: the download of a firmware file to the device and, following that, the update of the firmware in flash memory.

If the value of this variable is "Update Active" or "Firmware Download Active", the amount of data already downloaded or written to flash memory can be seen from "Download / Update Progress".

If the value of this variable is not "No Update File", supplementary information about the firmware update can be retrieved from the variable "Update Info" in textual form.

If the value is "Firmware Fallback after Software Error" a new software was installed, but the device did not start up correctly with the new software so the previous software version was reactivated. See the log file for details in this case.

RO -- --
ENUM T
Automatic

Values

No Update File	Indicates that a firmware file needs to be downloaded.
Update File Received	Indicates that a valid firmware file was downloaded and can be installed.
Firmware Download Active	Indicates that a firmware file is in the progress of being downloaded.
Update Error Occurred	Indicates that either a firmware file download or the installation of the firmware file has failed.
Update Active	Indicates that a firmware file is in the progress of being installed.
Firmware Fallback after Software Error	Indicates that the last installed firmware could not be started correctly and a fallback to the previous version has occured.

Server Type

config go "/Administration/Firmware Update"
config "Server Type"

The device supports three different servers, which can be configured for usage.

- Firmware Store: This server is used to download firmware files to the device for installation.
- Configuration Store: This server is used to upload and download configuration files from/to the device.
- Logfile Store: This server is used to store log files externally for further handling.

Each server can be configured to use the TFTP or SFTP protocol.

RO -- --
ENUM F
Automatic

Values

Firmware Store	The server is used to download firmware upgrades to the device.
Configuration Store	The server is used to upload and download configuration data and SSH keys.
Logfile Store	The server is used to upload log file from the device to the server.

Server URI

config go "/Administration/Firmware Update"
config "Server URI"

This variable shows the URI (Unique Resource Identifier) of the server entry. If the server is set up correctly, the protocol type, IP address and server directory can easily be derived from the value.

If the value of this variable is "Disabled", the server entry has been disabled by the administrator. If it is "Not Valid", the detailed server configuration needs to be completed before the server can be used.

The value of this variable is calculated dynamically from the server settings.

RO	--	--
STRING		T
Automatic		

Start Firmware Download

config go "/Administration/Firmware Update"
config do "Start Firmware Download"

Start downloading a firmware file. The file name needs to be configured in advance.

RW	--	--			
BUTTON		T			
EMPTY					

Constraints	"Firmware Update Status" IS "Update Active"	→	RO	--	--
	"Firmware Update Status" IS "Firmware Download Active"	→	RO	--	--

Start Update

config go "/Administration/Firmware Update"
config do "Start Update"

Start installing a firmware file. The firmware file needs to have been downloaded in advance.

RW	--	--			
BUTTON		T			
EMPTY					

Constraints	"Firmware Update Status" IS ("Firmware Download Active" || "Update Error Occurred" || "Update Active")	→	RO	--	--
	"Firmware Update Status" IS "No Update File"	→	RO	--	--

Update Info

config go "/Administration/Firmware Update"
config "Update Info"

This variable gives supplementary information about the current state of the firmware update or firmware file download in textual form. During a firmware file download, it contains current information about the action performed by the device to fetch the file (e.g. connecting to server, opening file, ...). In case of an error, this variable gives information about the kind of error that occurred.

RO	--	--
STRING		T
Automatic		

4.1.5 Administration / Port and IP Configuration

This menu gives access to the configuration of IP parameters and physical port settings of dedicated management interfaces. The RPX device has two of these interfaces:

- local management interface (F-Interface)
- remote management interface (Q-Interface) All management interfaces are available for display/configuration in this menu.

Default IPv4 Gateway

config go "/Administration/Port and IP Configuration"
config "Default IPv4 Gateway"

This variable indicates the selected default IPv4 gateway. It can either be the "Overwrite Default IPv4 Gateway", or one received via DHCP from one of the Q or in-band management ports.

If a valid "Overwrite Default IPv4 Gateway" has been configured and it is found to be reachable with the current IPv4 configuration, that gateway is always preferred over the default IPv4 gateways learned via DHCP.

If no valid "Overwrite Default IPv4 Gateway" has been configured, one of the default IPv4 gateways learned via DHCP is selected, where in-band management is given preference over dedicated Q ports.

RO	RO	RO
STRING		T
Automatic		

IPv4 Default TTL

config go "/Administration/Port and IP Configuration"
config set "IPv4 Default TTL" INTEGER

The default value inserted into the Time-To-Live field of the IPv4 header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol.

RW	RO	RO
INTEGER		P
Automatic		

Overwrite Default IPv4 Gateway

config go "/Administration/Port and IP Configuration"
config set "Overwrite Default IPv4 Gateway" IPADDR

This variable allows to manually specify a default IPv4 gateway to use by the device. It is used to connect to computers outside of any network local to the device. It is normally unnecessary to specify a valid IPv4 gateway IP here if one of the following is true:

- The device is expected to only process network traffic in the local networks.
- The device uses DHCP for automatic network configuration.

Setting the default router address to 0.0.0.0 disables the use of the manually specified IPv4 gateway.

RW	RO	RO
IPADDR		P
EMPTY		

Overwrite IPv4 Gateway Reachable

config go "/Administration/Port and IP Configuration"
config "Overwrite IPv4 Gateway Reachable"

This variable indicates whether the manually configured default IPv4 gateway is reachable according to the current IPv4 network configuration.

A value of "Not in Use" means that no valid IPv4 gateway address has been provided.

A value of "Reachable" means that the device knows a route to the IPv4 gateway. However, no checks are performed to verify that network packet exchange with the gateway server actually works.

A value of "Not Reachable" means that the device knows no route to the IPv4 gateway and cannot contact servers outside of local networks.

Values	Not Reachable
	Reachable
	Not in Use

RO	RO	RO
ENUM		T
Automatic		

4.1.5.1 Administration / Port and IP Configuration / <MGMT Port>

<MGMT Port>

The interfaces that can be selected to be configured:

- Local
- North
- South

This menu gives access to submenus where physical port parameters and IP settings can be viewed and/or modified.

Physical port settings for dedicated management interfaces include port speed, duplex and auto-negotiation.

Physical port settings for in-band management ports shows the list of all Ethernet ports which are allowed to carry in-band management data. Please note that changing the port settings here will also affect the transfer of user data over these ports!

The IPv4 settings allow assigning an IPv4 address manually to the interface or to use a DHCP client for automatic IP address assignment.

The IPv6 settings allow disabling and enabling IPv6 support, to choose various IPv6 Router Advertisement options and to manually assign IPv6 addresses to the interface.

AdminStatus

config go "/Administration/Port and IP Configuration/<MGMT Port>"
config set "AdminStatus" ENUM

This variable allows to specify whether the selected management port is enabled or disabled.

If disabled, the port will bring down the link (except for "Inband Mgmt" ports) and not respond to any network traffic received on the interface.

If enabled, the port will try to establish a link and start responding to management traffic received on this interface.

RW	RO	RO
ENUM		P
Enabled		

Values		
	Disabled	Port disabled
	Enabled	Port enabled

IPv4 Address

config go "/Administration/Port and IP Configuration/<MGMT Port>"
config "IPv4 Address"

This variable shows the current IPv4 address of the interface and how it was learned. The IPv4 address is shown in CIDR notation (e.g. 192.168.0.1/24) to indicate the netmask as well.

RO	RO	RO
STRING		T
Automatic		

Link

config go "/Administration/Port and IP Configuration/<MGMT Port>"
config "Link"

This variable shows the link status of the available management interfaces. Management interfaces may be of type in-band (via LINE ports) or out-band. An out-band management interface is a dedicated extra Ethernet port for TCP/IP access. For in-band management interfaces, the link status will be according the physical status of the (available) LINE ports.

RO	RO	RO
ENUM		T
Automatic		

Values		
	Link Down	The interface's link is down.
	Link Up	The interface's link is up.
	Disabled	The interface has been disabled by the device administrator.

Mech.	config go "/Administration/Port and IP Configuration/<MGMT Port>" config "Mech."		
The physical interface type of the port.	RO	RO	RO
	ENUM		F
	Automatic		

Values		
	undefined	Port's type is unknown.
	RJ45	Copper port with RJ45 connector.
	SFP	Fibre port, a SFP can be plugged.
	RJ45 (SFP)	Combo port: Either Copper or Fibre can be used. No SFP is detected, the copper part is active.
	SFP (RJ45)	Combo port: Either Copper or Fibre can be used. SFP is detected, the copper part may not be used!
	Virtual	Virtual port (in-band mangement)

Name	config go "/Administration/Port and IP Configuration/<MGMT Port>" config "Name"		
Shows port label and port name.	RO	RO	RO
	STRING		T
	Automatic		

4.1.5.1.1 Administration / Port and IP Configuration / <MGMT Port> / Edit

This menu allows configuring physical port parameters for the management interface as well as IPv4 and IPv6 settings.

For dedicated management interfaces, this menu allows to set up port speed, duplex mode and auto-negotiation. The port can be disabled. The generation of SNMP linkUp/linkDown traps is controlled here as well.

For in-band management interfaces, the list of Ethernet ports is shown that are allowed to carry in-band management traffic. Again, it is possible to disable in-band management and to control the generation of SNMP linkUp/linkDown traps.

The IPv4 settings (if available) allow setting up an IPv4 address for the interface and control the use of DHCP for IP address assignment.

The IPv6 settings (if available) allow setting up whether IPv6 is supported on the interface, IPv6 addresses for the interface as well as the response to IPv6 Router Advertisement messages.

Autonegotiation

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config set "Autonegotiation" ENUM

This variable allows to configure whether autonegotiation shall be enabled. If the link partner has autonegotiation enabled, the arcutronix device also needs to have autonegotiation enabled even when using a fixed bit rate. Otherwise the link cannot successfully be established. The same holds true for the opposite case, e.g. if the link partner has autonegotiation disabled, so needs the arcutronix device.

			RW	RO	RO
			ENUM		P
			On		

Values	Off	Autonegotiation disabled.				
	On	Autonegotiation enabled.				
Constraints	"Port Speed" IS "Automatic"	→	RO	RO	RO	

Enable SNMP Link Up_Down Traps

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config set "Enable SNMP Link Up_Down Traps" ENUM

This variable indicates whether Link Up/Link Down events should generate standard SNMP linkUp/linkDown traps or not. For the traps to be sent, it is also required to have SNMP support enabled and to have configured SNMP trap receivers.

			RW	RO	RO
			ENUM		P
			Enabled		

Values	Disabled	Do not send linkUp/linkDown traps for this interface.
	Enabled	Send linkUp/linkDown traps for this interface.

HW MAC Address

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config "HW MAC Address"

The interface's address at its protocol sub-layer, e.g. the MAC address of the Ethernet interface.

RO	RO	RO		
STRING		F		
Automatic				

IPv4 Address

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config "IPv4 Address"

This variable displays the current IP address of the management interface.

The Factory Default Configuration contains an individual IP address for each management interface (usually 192.168.x.100) that becomes re-activated after a factory reset.

			RO	RO	RO
			IPADDR		P
			Automatic		

Constraints	"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--	

IPv4 Address Assignment

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config set "IPv4 Address Assignment" ENUM

RW	RO	RO
ENUM		P
Automatic		

This variable allows to specify the IPv4 DHCP mode to be used for the selected interface.

If the interface type is set to "Local Mgmt (F)", the following values are suitable for this variable:

- "Manual": don't provide IPv4 DHCP Server on this interface
- "Provide DHCP Server": provide a IPv4 DHCP server on this interface.

If the interface type is set to "Remote Mgmt (Q)" or "Inband Mgmt (Q)", the following values are suitable for this variable:

- "Manual": manual IPv4 configuration
- "From DHCP Server": use DHCP for automatic IPv4 address assignment
- "From DHCP Server/Auto IP": use DHCP for automatic IPv4 address assignment or select a random IP in 169.254.x.x, if no DHCP server is responding (a.k.a. Zeroconf dynamic IPv4 Link Local addresses).

When the interface type is changed between F and Q type, this variable may be adjusted automatically if the current setting is inappropriate for the new interface type.

This variable defaults to "Provide DHCP Server" for F interfaces and to "From DHCP Server" for Q and in-band interfaces.

Values	Manual	Manual IP address assignment.
	From DHCP Server	Automatic IP address assignment via DHCP.
	From DHCP Server/Auto IP	Automatic IP address assignment via DHCP or Zeroconf.
	Provide DHCP Server	Provide IP addresses (DHCP Server).

Constraints	"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

IPv4 DHCP Default Gateway

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config "IPv4 DHCP Default Gateway"

RO	RO	RO
STRING		T
Automatic		

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.

Constraints	"IPv4 Address Assignment" IS ("Manual" || "Provide DHCP Server")	→	--	--	--
	"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

IPv4 DHCP Server

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config "IPv4 DHCP Server"

When a network address has been received via DHCP, this variable shows the DHCP server that has answered the DHCP request.

RO	RO	RO
IPADDR		T
Automatic		

Constraints	"IPv4 Address Assignment" IS ("Manual" || "Provide DHCP Server")	→	--	--	--
	"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

IPv4 DHCP Server State

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config "IPv4 DHCP Server State"

When DHCP is enabled, this variable shows the current state of communication with the DHCP server.

RO	RO	RO
STRING		T
Automatic		

Constraints	"IPv4 Address Assignment" IS ("Manual" || "Provide DHCP Server")	→	--	--	--
	"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

IPv4 ICMP Support

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config set "IPv4 ICMP Support" ENUM

This variable controls whether the device will generate and respond to ICMP messages via IPv4. ICMP is a protocol designed to help diagnosing network problems.

If set to "Disabled", the device will neither act upon nor generate ICMP messages via IPv4. This also means that some functionality, e.g. the "ping" diagnostic tool, will stop working.

If set to "Enabled", the device will respond to ICMP requests and may generate ICMP packets.

RW	RO	RO
ENUM		P
Enabled		

Values	Disabled	Disables ICMP support for IPv4
	Enabled	Enables ICMP support for IPv4

Constraints	"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

IPv4 Network Mask

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config "IPv4 Network Mask"

This variable displays the current network mask of the management interface.

RO	RO	RO
IPADDR		P
Automatic		

Constraints	"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

IPv6 Accept Redirects

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config set "IPv6 Accept Redirects" ENUM

This variable allows to configure whether redirect messages sent from IPv6 routers shall be ignored. Redirect messages are sent by routers to inform IPv6 hosts about better routes to a destination, but it may improve network security to ignore those messages.

RW	RO	RO
ENUM		P
Disabled		

Values	Disabled	Do not accept redirects from IPv6 routers.
	Enabled	Accept redirects from IPv6 routers.

Constraints	"IPv6 Support" IS "Disabled"	→	--	--	--
	"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

IPv6 Autoconfiguration

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config set "IPv6 Autoconfiguration" ENUM

This variable allows to control whether the interface should automatically configure IPv6 addresses for prefixes learned from IPv6 router advertisements.

If this variable is set to "Disabled", the interface will never configure IPv6 addresses automatically in response to router advertisement messages.

RW	RO	RO
ENUM		P
Enabled		

Values	Disabled	Do not autoconfigure IPv6 addresses from router advertisements.
	Enabled	Autoconfigure IPv6 addresses from router advertisements.

Constraints	"IPv6 Support" IS "Disabled"	→	--	--	--
	"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

IPv6 Gateway Autoconfiguration

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config set "IPv6 Gateway Autoconfiguration" ENUM

This variable allows to configure whether default gateways learned via router advertisements shall be used.

If this variable is set to "Disabled", default gateways advertised by IPv6 routers will be ignored.

If this variable is set to "Enabled", default gateways advertised by IPv6 routers will be used.

RW	RO	RO
ENUM		P
Enabled		

Values

Disabled	Do not accept IPv6 default gateways from router advertisements.
Enabled	Accept IPv6 default gateways from router advertisements.

Constraints

"IPv6 Support" IS "Disabled"	→	--	--	--
"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

IPv6 Router Advertisements

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config set "IPv6 Router Advertisements" ENUM

This variable allows to control whether the interface listens for IPv6 router advertisement messages for an automatic router detection.

If this variable is set to "Ignoring", the interface will ignore those messages and not detect IPv6 routers automatically.

If this variable is set to "Listening", the interface will listen to router advertisements.

RW	RO	RO
ENUM		P
Listening		

Values

Ignoring	Ignores any IPv6 router advertisements.
Listening	Handles any IPv6 router advertisements.

Constraints

"IPv6 Support" IS "Disabled"	→	--	--	--
"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

IPv6 Support

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config set "IPv6 Support" ENUM

This variable allows to enable or disable IPv6 support for the selected interface. If disabled, the interface will neither transmit nor receive any IPv6 packets.

RW	RO	RO
ENUM		P
Disabled		

Values

Disabled	Disables IPv6 support for this interface.
Enabled	Enables IPv6 support for this interface.

Constraints

"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

Interface Type

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config set "Interface Type" ENUM

RW RO RO
ENUM P
Automatic

This variable allows to specify whether the interface is intended to be used as local management interface (a.k.a. F interface), remote management interface (a.k.a. Q interface) or in-band management interface. The default behaviour of the interface is stated in the device manual.

A local management interface is usually intended for service technicians to connect a laptop to. In this mode the interface will have a fixed IP address and may provide a DHCP server for automatic IP address assignment to the service laptop.

A remote management interface is usually intended to connect devices to the service network where a management station is responsible for the maintenance of the device. The service network is physically separated from the customer's networks.

Switching between local and remote management interface types is supported. The DHCP mode may automatically be adjusted if it is found to be inappropriate for the new interface type.

An in-band management interface is present when the customer's data traffic and the remote management traffic share the same physical network. If an interface is an in-band management interface, the value of this variable cannot be changed.

The Agent Comm port type is only used on a SCX2e-WDM agent device. The agent communication port is used for exclusive communication between a main SCX2e agent and a SCX2e subagent device. Such an agent comm port does not need an IP configuration and communication setup occurs automatically. The subagent can be accessed via the management system of the main SCX2e.

A daisy chain port is used to put two or more devices in a daisy chain, forwarding traffic from the first device in the chain to other devices further up in the chain. This allows to connect an arbitrary number of managed devices to a single management network port without the need to use an intermediate network switch or hub. Since the daisy chain port is only forwarding network packets, it does not need an IP configuration.

Values	Local Mgmt (F)
	Remote Mgmt (Q)
	Inband Mgmt (Q)
	Agent Comm
	Daisy Chain

Constraints	Not configurable for this interface.	→	RO RO RO

Link Status

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config "Link Status"

RO RO RO
STRING T
Automatic

This variable shows the link status of the selected port.

A corresponding alarm can be raised when the Link Status of the port changes. The alarm can be configured to be ignored or to be of error / warning severity.

Management VLAN Setting

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config "Management VLAN Setting"

This variable shows the VLAN configuration that is used to filter management traffic on this port.

If VLAN tagging is not used, this variable holds the value "None".

If single tagging is configured, this variable holds a value in the following format: <C-Tag>:<ID>/<Prio>.

If double tagging is configured, this variable holds a value in the following format: <S-Tag>:<Outer ID>/<Outer Prio>; <C-Tag>:<Inner ID>/<Inner Prio>.

RO	RO	RO
STRING		T
Automatic		

Packet Counter

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config "Packet Counter"

Shows the number of RX/TX packets that went through the interface.

RO	RO	RO
STRING		T
Automatic		

Port Label

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config "Port Label"

The textual name of the interface. The value of this variable is the name of the interface as assigned by the local device and is suitable for use in commands entered at the device's console. This will be a text name, such as 'F/Q MGMT' or 'Inband MGMT', that is also used to label the port on the device casing.

RO	RO	RO
STRING		F
Automatic		

Port Name

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config set "Port Name" STRING

This variable can be used to assign a customized name to the interface.

RW	RO	RO
STRING		P
< ... >		

Port Speed

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit"
config set "Port Speed" ENUM

This variable allows to set the interface speed of the selected interface to a specific value. The setting selects the nominal bit rate in MBits as well as the duplex mode. Please note that not all speed/duplex combinations may be valid with any interface. It should normally be sufficient to leave automatic speed detection enabled. When selecting a fixed nominal bit rate, the autonegotiation setting may also be of importance.

RW	RO	RO
ENUM		P
Automatic		

Values	Automatic	Automatic negotiated speed and duplex mode.
	10 Half Duplex	10Mbps, half duplex mode.
	10 Full Duplex	10Mbps, full duplex mode.
	100 Half Duplex	100Mbps, half duplex mode.
	100 Full Duplex	100Mbps, full duplex mode.
	1000 Half Duplex	1000Mbps, half duplex mode.
	1000 Full Duplex	1000Mbps, full duplex mode.

4.1.5.1.1.1 Administration / Port and IP Configuration / <MGMT Port> / Edit / <IPv6 Address>

<IPv6 Address>

One of the currently assigned IPv6 addresses.

This menu shows the IPv6 addresses currently assigned to the interface. It includes addresses configured automatically as well as those configured manually.

Address

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/<IPv6 Address>"
config "Address"

This variable shows the IPv6 address assigned to the interface.

RO	RO	RO
IPADDR		T
Automatic		

Constraints	"IPv6 Support" IS "Disabled"	→	--	--	--
	"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

Delete Address

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/<IPv6 Address>"
config do "Delete Address"

Deletes the selected IPv6 address.

RW	--	--
BUTTON		T
EMPTY		

Constraints	"Source" IS NOT "Manual"	→	--	--	--
	"IPv6 Support" IS "Disabled"	→	--	--	--
	"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

Flags

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/<IPv6 Address>"
config "Flags"

This variable shows a number of flags associated with the selected IPv6 address. Possible values are:

- temporary - indicates a secondary address with limited life-time
- nodad - indicates that the address is not checked for duplicity
- permanent - indicates that the address does not have a limited life-time
- home - indicates that the address is the home address

RO	RO	RO
STRING		T
Automatic		

Constraints	"IPv6 Support" IS "Disabled"	→	--	--	--
	"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

PfxLen

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/<IPv6 Address>"
config "PfxLen"

This variable shows the length of the prefix of the IPv6 address assigned to the interface. The prefix length is the size of the network address part of the IPv6 address in bits. Remaining bits are considered the host part of the address.

RO	RO	RO
INTEGER		T
Automatic		

Constraints	"IPv6 Support" IS "Disabled"	→	--	--	--
	"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

Source

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/<IPv6 Address>"
config "Source"

This variable shows how the selected IPv6 address was learned.

RO	RO	RO
ENUM		T
Automatic		

Values		
	Link Local	Automatically generated link-local address.
	Automatic	The address is automatically configured.
	Manual	The address is manually configured.

Constraints					
	"IPv6 Support" IS "Disabled"	→	--	--	--
	"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

Status

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/<IPv6 Address>"
config "Status"

This variable shows the current status of the selected IPv6 address, e.g. whether it is waiting for Duplicate Address Detection (DAD) results, is a preferred address or deprecated.

RO	RO	RO
ENUM		T
Automatic		

Values		
	Tentative	The address is waiting for DAD completion.
	Preferred	The address is usable for new connections.
	Deprecated	The address is not used for new connections.
	Optimistic	The address is used although DAD is not completed.
	Duplicate	The address is already used in the network.

Constraints					
	"IPv6 Support" IS "Disabled"	→	--	--	--
	"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

Type

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/<IPv6 Address>"
config "Type"

This variable shows the type of the selected IPv6 address, e.g. whether it is a Link-Local, Unicast or special address.

RO	RO	RO
STRING		T
Automatic		

Constraints					
	"IPv6 Support" IS "Disabled"	→	--	--	--
	"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

4.1.5.1.1.2 Administration / Port and IP Configuration / <MGMT Port> / Edit / Add IPv6 Address

This form page allows creating new static IPv6 addresses. The information needed is the IPv6 address itself as well as the prefix length.

Add IPv6 Address

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/Add IPv6 Address"
config do "Add IPv6 Address"

Adds the newly entered IPv6 address.

RW	--	--			
BUTTON		T			
EMPTY					

Constraints	"IPv6 Support" IS "Disabled"	→	--	--	--
	"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

New IPv6 Address

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/Add IPv6 Address"
config set "New IPv6 Address" IPADDR

This variable allows to enter the new IPv6 address to be created on the selected interface. It must be a valid IPv6 Unicast Address.

RW	--	--			
IPADDR		T			
EMPTY					

Constraints	"IPv6 Support" IS "Disabled"	→	--	--	--
	"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

New Prefix Length

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/Add IPv6 Address"
config set "New Prefix Length" INTEGER(0 - 128)

This variable allows to enter the prefix length of the new IPv6 address to be created on the selected interface.

RW	--	--			
INTEGER(0 - 128)		T			
64					

Constraints	"IPv6 Support" IS "Disabled"	→	--	--	--
	"Interface Type" IS ("Agent Comm" || "Daisy Chain")	→	--	--	--

4.1.5.1.1.3 Administration / Port and IP Configuration / <MGMT Port> / Edit / Change IPv4 Address

This form page allows to manually assign a new IP address to the selected interface.

It is required to enter a valid new IP address as well as the corresponding netmask. If needed, the default gateway can be specified here as well. If the default gateway variable is left empty, the default gateway settings remain unchanged.

Change IPv4 Address	config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/Change IPv4 Address" config do "Change IPv4 Address"			
This command submits the new IP configuration and activates it.		RW BUTTON EMPTY	-- 	-- T
Constraints	"IPv4 Address Assignment" IS ("From DHCP Server" || "From DHCP Server/Auto IP") →	--	--	--
	"Interface Type" IS ("Agent Comm" || "Daisy Chain") →	--	--	--

New IPv4 Address	config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/Change IPv4 Address" config set "New IPv4 Address" IPADDR			
This variable allows to specify the new IPv4 address of the selected management interface. If all form data is successfully validated after submission, the new IPv4 address will be activated.		RW IPADDR EMPTY	-- 	-- T
Constraints	"IPv4 Address Assignment" IS ("From DHCP Server" || "From DHCP Server/Auto IP") →	--	--	--
	"Interface Type" IS ("Agent Comm" || "Daisy Chain") →	--	--	--

New IPv4 Default Gateway	config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/Change IPv4 Address" config set "New IPv4 Default Gateway" IPADDR			
This variable allows to specify the new IPv4 default gateway if it needs to be changed. If the current IPv4 default gateway is still suitable for the new IPv4 network configuration, the variable may be left unchanged.		RW IPADDR EMPTY	-- 	-- T
Constraints	"IPv4 Address Assignment" IS ("From DHCP Server" || "From DHCP Server/Auto IP") →	--	--	--
	"Interface Type" IS ("Agent Comm" || "Daisy Chain") →	--	--	--

New IPv4 Netmask	config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/Change IPv4 Address" config set "New IPv4 Netmask" IPADDR			
This variable allows to specify the new IPv4 netmask of the selected management interface. If all form data is successfully validated after submission, the new IPv4 netmask will be activated.		RW IPADDR EMPTY	-- 	-- T
Constraints	"IPv4 Address Assignment" IS ("From DHCP Server" || "From DHCP Server/Auto IP") →	--	--	--
	"Interface Type" IS ("Agent Comm" || "Daisy Chain") →	--	--	--

4.1.5.1.1.4 Administration / Port and IP Configuration / <MGMT Port> / Edit / Change VLAN Settings

This form page allows to adjust the VLAN settings required to filter the management traffic on ports that support VLAN tagging.

Depending on the port's VLAN capabilities, management VLAN can be disabled or switched to single or double tagging. For some ports (e.g. in-band ports), VLAN tagging is required and cannot be disabled. If VLAN tagging is enabled, the required VLAN IDs and priorities can be configured here.

Change VLAN Settings	config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/Change VLAN Settings" config do "Change VLAN Settings"			
This command submits the new VLAN settings and activates them.		RW BUTTON EMPTY	-- 	-- T

Management VLAN ID	config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/Change VLAN Settings" config set "Management VLAN ID" INTEGER			
This variable allows to set the VLAN ID to be used for management traffic on this interface. In double tagging mode, this variable defines the VLAN ID of the inner VLAN tag.		RW INTEGER 4094	-- 	-- P

Management VLAN ID Usage

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/Change VLAN Settings"
config set "Management VLAN ID Usage" ENUM

This variable allows to set the VLAN tagging mode to be used for the management interface. Depending on the interface type, a different selection of VLAN tagging modes is available.

The default is "Single Tag" except for F interfaces which do not allow VLAN tagging.

RW	--	--
ENUM		P
Automatic		

Values

Disable	Don't use VLAN tagging for the management interface.
Single Tag	Use single tagging for the management interface. The VLAN ID needs to be configured as well.
Double Tag	Use double tagging for the management interface. Both VLAN IDs and the S-TAG for the outer VLAN tag need to be configured as well.

Management VLAN Prio

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/Change VLAN Settings"
config set "Management VLAN Prio" INTEGER

This variable allows to set the priority value to be placed into the VLAN tag to be used for management traffic on this interface. In double tagging mode, this variable defines the priority value for the inner VLAN tag.

RW	--	--
INTEGER		P
3		

Management VLAN S-Tag

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/Change VLAN Settings"
config "Management VLAN S-Tag"

This variable shows the so-called S-TAG used for the management interface in double tagging mode. The S-TAG cannot be configured here, it needs to be globally configured in "/Ethernet Ports/VLAN".

RO	--	--
STRING		P
Automatic		

Outer Management VLAN ID

config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/Change VLAN Settings"
config set "Outer Management VLAN ID" INTEGER

This variable allows to set the VLAN ID of the outer VLAN tag for management traffic on this interface in double tagging mode.

RW	--	--
INTEGER		P
4090		

Outer Management VLAN Prio	config go "/Administration/Port and IP Configuration/<MGMT Port>/Edit/Change VLAN Settings" config set "Outer Management VLAN Prio" INTEGER
This variable allows to set the priority value to be placed into the outer VLAN tag for management traffic on this interface.	RW -- -- INTEGER P 3

4.1.6 Administration / 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. The system reset is a warm-reset, meaning forcing a restart via a reboot but without powering down.

If a system reset was scheduled for a certain time, it is possible to cancel the system reset timer again.

Cancel Reset	config go "/Administration/Reset System" config do "Cancel Reset"	
Cancel the scheduled reset		RW RO RO BUTTON T EMPTY
Constraints	"Reset State" IS NOT "Reset Scheduled" →	-- -- --

Date and Time	config go "/Administration/Reset System" config "Date and Time"	
The current date and time of the device is displayed here.		RO RO RO STRING T Automatic
Constraints	"Reset Mode" IS "Immediate Reset" →	-- -- --

Dying Gasp for Maintenance Reboots

config go "/Administration/Reset System"
config set "Dying Gasp for Maintenance Reboots" ENUM

This variable controls whether the device is emitting Dying Gasp notifications for regular maintenance reboots of the device.

In case of regular maintenance reboots (firmware upgrade, applying configurations, system reset), the device is going out of operation as well. However, since these actions are always initiated by a device operator as part of the device maintenance, it may not be wanted to trigger full error handling procedures here.

RW	RO	RO
ENUM		P
Disabled		

Values		
	Disabled	No Dying Gasp on planned maintenance resets
	Enabled	Planned maintenance resets force Dying Gasp

Reset Date

config go "/Administration/Reset System"
config set "Reset Date" DATE

When the "Reset Mode" is set to "At Specified Time", this variable allows configuring the date at which the reset is to occur. Allowed values for the date are from the current date up to 30 days in future.

The date must be entered in yyyy-mm-dd format, e.g. "1990-12-24".

The "Reset Time" also needs to be configured before a reset can be scheduled.

RW	RO	RO
DATE		T
EMPTY		

Constraints					
	"Reset Mode" IS "Immediate Reset"	→	--	--	--
	"Reset State" IS "Reset Scheduled"	→	RO	RO	RO

Reset Mode

config go "/Administration/Reset System"
config set "Reset Mode" ENUM

This variable specifies whether the system reset shall be executed immediately or at a given date/time.

RW	RO	RO
ENUM		P
Immediate Reset		

Values		
	Immediate Reset	System is reset as soon as the 'Reset System' command is submitted.
	At Specified Time	System is reset at given Date/Time.

Constraints					
	"Reset State" IS NOT "No Reset Scheduled"	→	RO	RO	RO

Reset State

config go "/Administration/Reset System"
config "Reset State"

This variable indicates whether a system reset is being executed or has been planned.

RO	RO	RO
ENUM		T
Automatic		

Values

No Reset Scheduled	No system warm-reset is scheduled by operator.
System is Going Down...	Indicates that the system is in the process of executing a system reset, the reset can no longer be cancelled. A system reset may be deferred by important actions that must not be interrupted (e.g. by a firmware update). In this case, this state remains until the deferring action has been completed.
Reset Scheduled	A reset has been planned at the date/time indicated by "Reset Date" and "Reset Time". It is still possible to cancel this planned reset.

Reset Time

config go "/Administration/Reset System"
config set "Reset Time" TIME

When the 'Reset Mode' is set to 'At Specified Time', this variable allows configuring the time at which the reset is to occur.

The time must be entered in hh:mm format with hh ranging from 0 to 23, e.g. '17:30'.

The 'Reset Date' also needs to be configured before a reset can be scheduled.

RW	RO	RO
TIME		T
EMPTY		

Constraints

"Reset Mode" IS "Immediate Reset"	→	--	--	--
"Reset State" IS "Reset Scheduled"	→	RO	RO	RO

Start Reset

config go "/Administration/Reset System"
config do "Start Reset"

Assign the settings for system reset and start execution.

When "Reset Mode" is set to "Immediate Reset", the reset will be executed immediately.

When "Reset Mode" is set to "At Specified Time", the reset will be executed when the indicated date and time have arrived.

RW	RO	RO
BUTTON		T
EMPTY		

Constraints

"Reset State" IS "Reset Scheduled"	→	--	--	--

4.1.7 Administration / Self-Test

This menu allows running a self-test and inspect the self-test results once the run is complete.

Run Self-test

config go "/Administration/Self-Test"
config do "Run Self-test"

Activate this button to run the device's self-tests.

RW	RW	RO
BUTTON		T
EMPTY		

Self-test Result

config go "/Administration/Self-Test"
config "Self-test Result"

This variable shows the results of a self-test run once it has completed. The information displayed here is some basic information about the system (CPU information, CPU usage information, memory consumption, flash health status).

RO	RO	RO
STRING		T
Automatic		

Self-test Status

config go "/Administration/Self-Test"
config "Self-test Status"

Displays whether the self-test is currently executing.

RO	RO	RO
ENUM		T
Automatic		

Values

Idle	The self-test can be started.
Executing	The self-test is currently running. It can only be restarted after it has completed.

4.1.8 Administration / 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.

NOTE: At least one management access method MUST be enabled. The device will give errors on attempts to disable the last access method.

This menu also allows to setup the auto-logoff time. It defines the time of inactivity after which a user logged on to CLI or Web-OPI will automatically be logged off. Although this is a global setting for all access methods, each session will have its own auto-logoff timer.

The menu also contains a table that shows the current configuration of all three management servers that

the device supports: the "Firmware Store" to download firmware upgrades from, the "Configuration Store" used to exchange configuration snapshots and SSH login keys between RPX device, and the "Logfile Store" that is used by the device to save event logs to.

Auto Logoff Time [min]

config go "/Administration/User and Access Administration"
config set "Auto Logoff Time [min]" INTEGER

This variable allows to adjust the auto-logoff timer for user logons in minutes. Users logged in via CLI or Web will automatically be logged off if their time of inactivity exceeds this value. A value of zero disables auto-logoff.

RW	RO	RO
INTEGER		P
15		

CONS CLI Access

config go "/Administration/User and Access Administration"
config set "CONS CLI Access" ENUM

This variable allows to enable or disable CLI access via CONS port. The CONS port is a standard RS232 port on some arcutronix devices and can be used to access the CLI in situations without networking capability.

Setting this variable to "Enabled" may fail if there is no CONS port equipped.

Setting this variable to "Disabled" may fail if the CONS port is the last enabled access method.

This setting has an immediate effect. When set to "Disabled", the RS232 port will immediately stop to function. Any user logged onto the device using CLI via CONS will be logged off.

RW	RO	RO
ENUM		P
Enabled		

Values	Disabled	Disable CONS CLI access			
	Enabled	Enable CONS CLI access			
Constraints	CONS not equipped	→	--	--	--

HTTP File Transfer

config go "/Administration/User and Access Administration"
config set "HTTP File Transfer" ENUM

This variable allows to enable or disable the file transfer via HTTP[S] (Web-GUI).

HTTP[S] 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.

Depending on the security settings of the device, either HTTP or HTTPS or both protocols are supported for file transfers.

RW	RO	RO
ENUM		P
Enabled		

Values	Disabled	Disables HTTP file transfers			
	Enabled	Enables HTTP file transfers			
Constraints	"Web Access" IS "Disabled"	→	--	--	--

SNMP Access

config go "/Administration/User and Access Administration"
config set "SNMP Access" ENUM

This variable allows to turn SNMP access to the device on and off. This setting has an immediate effect, e.g. when it is set to false, no further SNMP messages will be processed. Setting this variable to false may fail if SNMP is the last active remote access method.

RW	RO	RO
ENUM		P
Enabled		

Values		
	Disabled	Disable SNMP access
	Enabled	Enable SNMP access

SSH CLI Access

config go "/Administration/User and Access Administration"
config set "SSH CLI Access" ENUM

This variable allows to configure whether management access via SSH/CLI is enabled. Setting this variable to "Enabled" enables SSH/CLI access and starts an SSH server on the device.

Setting this variable to "Disabled" may fail because it is not allowed to disable the last management access method.

This setting has an immediate effect. When set to "Disabled", the SSH server will immediately stop to accept new connections. Existing logons will continue to function until the user is being logged off.

RW	RO	RO
ENUM		P
Enabled		

Values		
	Disabled	Disable SSH CLI access
	Enabled	Enable SSH CLI access

Web Access

config go "/Administration/User and Access Administration"
config set "Web Access" ENUM

This variable allows to configure whether management access via HTTP[S] is enabled. Setting this variable to "Enabled" enables HTTP[S] access and starts an HTTP[S] server on the device.

Setting this variable to "Disabled" may fail because it is not allowed to disable the last management access method.

This setting has an immediate effect. When set to "Disabled", the HTTP[S] server will be stopped immediately and users that are logged on via HTTP[S] will suffer from a connection loss.

RW	RO	RO
ENUM		P
Enabled		

Values		
	Disabled	Disable HTTP access
	Enabled	Enable HTTP access

4.1.8.1 Administration / User and Access Administration / <Server>

<Server>

One of three servers, which are used to store and load files to and from the device:

- Firmware Store: The device loads firmware update files via TFTP or SFTP from this server.
- Configuration Store: The device stores and loads configuration files via TFTP or SFTP to/from this server, as well as HTTPS certificates and keys.
- Logfile Store: The device stores log files via TFTP or SFTP to this server.

This menu contains information about the selected management server. It displays the server URI (Unique Resource Identifier) from which the location of remote files is easily visible. It also contains a status variable from which one can see whether the server entry is sufficiently well configured and usable by the device.

The menu also gives access to a submenu that allows the management server to be configured. In this configuration, the servers IP address and default file directory can be set, as well as the file transfer protocol to be used when talking to that server.

URI

config go "/Administration/User and Access Administration/<Server>"
config "URI"

This variable shows the URI (Unique Resource Identifier) of the server entry. If the server is set up correctly, the protocol type, IP address and server directory can easily be derived from the value.

If the value of this variable is "Disabled", the server entry has been disabled by the administrator. If it is "Not Valid", the detailed server configuration needs to be completed before the server can be used.

The value of this variable is calculated dynamically from the server settings.

RO	RO	RO
STRING		T
Automatic		

Valid

config go "/Administration/User and Access Administration/<Server>"
config "Valid"

This variable indicates whether the settings for the server are consistent and complete. As long as this variable shows "Not Valid", at least one setting needs adoption.

RO	RO	RO
ENUM		T
Automatic		

Values	Not Valid	Settings for server access not valid, yet.
	Valid	Settings for server access are valid and complete.

4.1.8.1.1 Administration / User and Access Administration / <Server> / Edit

This submenu allows to modify the properties of the selected file server in detail. It allows to specify IP address and port number, protocol type, default directory and authentication data for protocols requiring user authentication.

The server can be disabled completely (so that no file transfers to/from this server are possible) by setting the "Transfer Protocol" to "Disabled".

Clear Server Info

config go "/Administration/User and Access Administration/<Server>/Edit"
config do "Clear Server Info"

This action will delete all stored information about the server (including IP address, user name and password). Afterwards, the server will not be usable for data transfer.

RW	--	--
BUTTON		T
EMPTY		

IP Description

config go "/Administration/User and Access Administration/<Server>/Edit"
config "IP Description"

This variable indicates the type of IP address assigned to this server.

RO	--	--
STRING		T
Automatic		

Constraints	"Transfer Protocol" IS "Disabled"	→	--	--	--

Password

config go "/Administration/User and Access Administration/<Server>/Edit"
config set "Password" PASSWORD

This variable specifies the password that is passed to the server if authentication is required for a file transfer.

RW	--	--
PASSWORD		P
EMPTY		

Constraints	"Transfer Protocol" IS NOT "SFTP"	→	--	--	--

Server Directory

config go "/Administration/User and Access Administration/<Server>/Edit"
config set "Server Directory" STRING

This variable allows to specify a common directory on the server which is appropriate for all files transferred to/from the server.

The directory needs to be specified starting from the root directory of the file server. The directory separator is a forward slash ("/").

RW	--	--
STRING		P
EMPTY		

Constraints	"Transfer Protocol" IS "Disabled"	→	--	--	--

Server IP

config go "/Administration/User and Access Administration/<Server>/Edit"
config set "Server IP" IPADDR

This variable holds the IP address of the selected server. IPv4 as well as IPv6 addresses may be entered here.

RW	--	--
IPADDR		P
0.0.0.0		

Constraints	"Transfer Protocol" IS "Disabled"	→	--	--	--

Server Port

config go "/Administration/User and Access Administration/<Server>/Edit"
config set "Server Port" INTEGER

This variable specifies the port number used by the server for file transfer requests. If set to zero (0), the default port number for the selected file transfer protocol will be used.

The default value of this variable is detected from the default transfer protocol.

RW	--	--
INTEGER		P
Automatic		

Constraints	"Transfer Protocol" IS "Disabled"	→	--	--	--

Server Type

config go "/Administration/User and Access Administration/<Server>/Edit"
config "Server Type"

The device supports three different servers, which can be configured for usage.

- Firmware Store: This server is used to download firmware files to the device for installation.
- Configuration Store: This server is used to upload and download configuration files from/to the device.
- Logfile Store: This server is used to store log files externally for further handling.

Each server can be configured to use the TFTP or SFTP protocol.

RO	--	--
ENUM		F
Automatic		

Values		
	Firmware Store	The server is used to download firmware upgrades to the device.
	Configuration Store	The server is used to upload and download configuration data and SSH keys.
	Logfile Store	The server is used to upload log file from the device to the server.

Transfer Protocol

config go "/Administration/User and Access Administration/<Server>/Edit"
config set "Transfer Protocol" ENUM

This variable specifies the file transfer protocol to use in communication with the selected server. Setting this variable to "Disabled" makes this server entry invalid (but keeps it present). In that case, files cannot be transferred to or from this server.

SFTP offers the best security measures of all available options, requiring proper host and user authentication and transferring all data encrypted. As a TCP protocol, it is rather robust w.r.t. network latencies and low bandwidth.

Trivial File Transfer Protocol (TFTP) is a very basic and more traditional method used to transfer files over an IP network, such as the internet. Although easily to set up and use, its drawbacks are missing authentication, missing encryption of data and the use of UDP packets to transfer the data.

Values	Disabled	Server access disabled
	TFTP	Server access via TFTP
	SFTP	Server access via SFTP

RW	--	--	
ENUM			P
SFTP			

User Name

config go "/Administration/User and Access Administration/<Server>/Edit"
config set "User Name" STRING

This variable specifies the user name that is passed to the server if authentication is required for a file transfer.

RW	--	--	
STRING			P
EMPTY			

Constraints	"Transfer Protocol" IS NOT "SFTP"	→	--	--	--

4.1.8.2 Administration / User and Access Administration / 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.

If required, SNMP access can be completely disabled to avoid illegal access to the device.

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.

SNMP Access Configuration

config go "/Administration/User and Access Administration/SNMP Configuration"
config set "SNMP Access Configuration" ENUM

RW RO RO
ENUM P
User/Target Configuration via Web/CLI

This variable allows to specify how the detailed configuration of SNMP access parameters must be performed.

When this variable is set to "User/Target Configuration via Web/CLI", detailed SNMP access configuration can only be performed using the Web/CLI based configuration methods. The following MIBs will then be read-only:

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

When this variable is set to "User/Target Configuration via SNMP", detailed SNMP access configuration can only be performed via SNMP. The tables in named MIBs can then be written to and the configuration options are no longer visible in Web/CLI GUI.

When the value changes from Web/CLI based to SNMP based configuration, the current configuration is retained and can be modified via SNMP.

When the value changes from SNMP based to Web/CLI based configuration, all data tables in named MIBs are completely cleared.

The usual mode of operation will be configuring initial access restrictions via Web/CLI so that SNMP access to the device is possible for trusted management stations. Once those management stations can connect to the device via SNMP, they take over detailed configuration.

Values	User/Target Configuration via Web/CLI	Enable configuration via Web/CLI
	User/Target Configuration via SNMP	Enable configuration via SNMP

SNMP Engine ID

config go "/Administration/User and Access Administration/SNMP Configuration"
config set "SNMP Engine ID" STRING

RW RO RO
STRING P
EMPTY

This variable allows to specify the SNMP Engine ID that the SNMP agent on the device considers its own authoritative engine ID. This setting has an immediate effect, e.g. changes to this value will force the SNMP agent on the device to immediately listen to the new SNMP Engine ID.

Changing this variable will only succeed if the "SNMP Engine ID Mode" was set to "Manually" in advance.

Constraints	"SNMP Engine ID Mode" IS NOT "Manually"	→	RO RO RO

SNMP Engine ID Mode

config go "/Administration/User and Access Administration/SNMP Configuration"
config set "SNMP Engine ID Mode" ENUM

This variable allows to specify how the SNMP Engine ID of the SNMP agent on the device is calculated. This setting has an immediate effect, e.g. when this value is changed, the SNMP agent may change its own SNMP Engine ID immediately and no longer be listening to the previous SNMP Engine ID.

A value of "Based on MAC address" means that the agents SNMP Engine ID is automatically calculated from the MAC address of one of the management interfaces as described in the textual convention for SnmpEngineID in SNMP-FRAMEWORK-MIB (item 3 subitem 3).

A value of "Based on sysName" means that the agents SNMP Engine ID is automatically calculated from the variable "/General System Information/Device Name" (SNMP object sysName.0) and encoded as described in the textual convention for SnmpEngineID in the SNMP-FRAMEWORK-MIB (item 3 subitem 4).

A value of "Manually" means that the SNMP engine ID must be manually configured by the administrator. For convenience, the current value of the SNMP Engine ID is retained until the ID is manually changed.

RW	RO	RO
ENUM		P
Based on MAC address		

Values

Based on MAC address	SNMP Engine ID is based on the MAC address of the first management interface.
Based on sysName	SNMP Engine ID is based on device name.
Manually	SNMP Engine ID can be manually configured.

SNMP Max Message Size

config go "/Administration/User and Access Administration/SNMP Configuration"
config set "SNMP Max Message Size" INTEGER

This variable holds the maximum size of a single SNMP message that the device shall support. A SNMP management station may send SNMP messages (UDP packets) that are as large as this number.

Larger UDP packets sent by a management station are considered as being errorneous.

RW	RO	RO
INTEGER		P
2048		

SNMP UDP Port

config go "/Administration/User and Access Administration/SNMP Configuration"
config set "SNMP UDP Port" INTEGER

This variable allows to change the default SNMP port number (UDP port 161) to any valid port number. Please note that any SNMP manager must also be aware of this change.

RW	RO	RO
INTEGER		P
161		

SNMP Version

config go "/Administration/User and Access Administration/SNMP Configuration"
config set "SNMP Version" ENUM

This variable describes which SNMP protocol versions the SNMP agent on the device responds to. The device has built-in support for SNMPv2c (authentication via a SNMP community name, no encryption), as well as SNMPv3 (full USM with DES/AES encryption and VACM).

If a certain SNMP protocol version is disabled here, the SNMP agent discards all incoming requests that use this protocol version.

RW	RO	RO
ENUM		P
SNMP V2c, V3		

Values		
	SNMP V2c	Only SNMP v2c is supported.
	SNMP V2c, V3	The agent supports both, SNMPv2c and SNMPv3 communications simultaneously.
	SNMP V3	Only SNMP v3 is supported.

4.1.8.2.1 Administration / User and Access Administration / SNMP Configuration / SNMP Traps

This menu allows configuring the list of management stations to which SNMP traps generated by the device will be delivered.

The generation of various traps by the device can also be controlled here. However, this menu does not allow to set up whether SNMP traps are generated for alarms. That information must be specified individually for each alarm in the "/Alarm Management" menu.

ALARM Message Traps

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps"
config set "ALARM Message Traps" ENUM

This variable allows to configure whether new alarm status messages in the event log of the device should generate notifications of type axCommonEventTrap or not. For this to work, the "Event Log Traps" variable also needs to be set to "Enabled".

RW	RO	RO
ENUM		P
Enabled		

Values		
	Disabled	Disable SNMP Event traps for ALARM messages.
	Enabled	Enable SNMP Event traps for ALARM messages.

Constraints					
	"Event Log Traps" IS "Disabled"	→	--	--	--

AUDIT Message Traps

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps"
config set "AUDIT Message Traps" ENUM

This variable allows to configure whether new audit messages in the event log of the device should generate notifications of type axCommonEventTrap or not. For this to work, the "Event Log Traps" variable also needs to be set to "Enabled".

RW	RO	RO
ENUM		P
Enabled		

Values		
	Disabled	Disable SNMP Event traps for AUDIT messages.
	Enabled	Enable SNMP Event traps for AUDIT messages.

Constraints					
	"Event Log Traps" IS "Disabled"	→	--	--	--

Add Trap Receiver

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps"
config do "Add Trap Receiver"

This command adds a new SNMP trap receiver with an IP address of "0.0.0.0" and default values.

RW	--	--
BUTTON		T
EMPTY		

Constraints					
	"SNMP Access Configuration" IS "User/Target Configuration via SNMP"	→	--	--	--

ERROR Message Traps

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps"
config set "ERROR Message Traps" ENUM

This variable allows to configure whether new error messages in the event log of the device should generate notifications of type axCommonEventTrap or not. For this to work, the "Event Log Traps" variable also needs to be set to "Enabled".

RW	RO	RO
ENUM		P
Enabled		

Values		
	Disabled	Disable SNMP Event traps for ERROR messages.
	Enabled	Enable SNMP Event traps for ERROR messages.

Constraints					
	"Event Log Traps" IS "Disabled"	→	--	--	--

Event Log History Size

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps"
config set "Event Log History Size" INTEGER

The device exports the event log (available with the "log" command in CLI) in a SNMP table with one log entry per table row. Fetching the complete table may take a significant time, so the size of the table can be limited to a reasonable and yet practical value using this variable.

RW	RO	RO
INTEGER		P
100		

Event Log Traps

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps"
config set "Event Log Traps" ENUM

RW	RO	RO
ENUM		P
Disabled		

The device may generate a SNMP trap for each new message that appears in the event log. The trap that is generated is axCommonEventTrap defined in AX-COMMON-MIB.mib.

This variable controls whether event traps are generated or not. The types of log events for which traps are generated can be configured individually.

Values	Disabled	Disable SNMP Event traps.
	Enabled	Enable SNMP Event traps.

INFO Message Traps

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps"
config set "INFO Message Traps" ENUM

RW	RO	RO
ENUM		P
Enabled		

This variable allows to configure whether new informational messages in the event log of the device should generate notifications of type axCommonEventTrap or not. For this to work, the "Event Log Traps" variable also needs to be set to "Enabled".

Values	Disabled	Disable SNMP Event traps for INFO messages.
	Enabled	Enable SNMP Event traps for INFO messages.

Constraints	"Event Log Traps" IS "Disabled"	→	--	--	--

SNMP Alarm Trap Type

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps"
config set "SNMP Alarm Trap Type" ENUM

RW	RO	RO
ENUM		P
Common Alarm Trap		

This variable specifies the type of trap that is sent by the device to configured SNMP trap receivers when the status of an alarm changes.

If set to "Common Alarm Trap", each alarm will cause the same trap type axCommonAlarmTrap to be sent with the data inside the trap set to appropriate values identifying the corresponding alarm.

If set to "Individual Alarm Traps", each alarm will cause a different trap type to be sent. These alarm traps are defined in AX-ALARM-MIB.mib.

Values	Individual Alarm Traps	Individual trap for each alarm
	Common Alarm Trap	Common trap for all alarms

SNMP Authen Traps

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps"
config set "SNMP Authen Traps" ENUM

This variable allows the sending of SNMP authenticationFailure traps to be enabled or disabled. If enabled, this trap is generated each time the SNMP agent receives SNMP messages that are not properly authenticated.

RW	RO	RO
ENUM		P
Enabled		

Values

Disabled	Disable SNMP Authentication failure traps.
Enabled	Enable SNMP Authentication failure traps.

SNMP Trap Counter

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps"
config "SNMP Trap Counter"

This variable shows the number of SNMP traps that the device has emitted since the last start of the SNMP agent. The same number is also included in each SNMP trap generated by the device to allow an automatic detection of lost traps.

RO	RO	RO
INTEGER		T
Automatic		

Send Test Trap

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps"
config do "Send Test Trap"

Sends a test trap to all configured trap receivers to test SNMP trap settings.

RW	RW	RO
BUTTON		T
EMPTY		

Web_CLI Authen Traps

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps"
config set "Web_CLI Authen Traps" ENUM

This variable allows the sending of SNMP traps in response to authentication events (login, logoff or authentication failures) for Web and CLI access to be enabled or disabled. If enabled, those traps are generated each time a user login to Web/CLI is detected to have failed or is successfully completed.

The traps include the user name for which the authentication event was recorded, as well as the access type (Web/CLI) and the origin of the login attempt (CONS port or IP address).

RW	RO	RO
ENUM		P
Enabled		

Values

Disabled	Disable SNMP traps for Web/CLI authentication events.
Enabled	Enable SNMP traps for Web/CLI authenticiation events.

4.1.8.2.1.1 Administration / User and Access Administration / SNMP Configuration / SNMP Traps / <IP Address>

<IP Address>

Some device indicated by its IP address. Valid IPv4 or IPv6 address required.

This menu allows to delete a trap receiver from the device and gives access to a submenu that allows modifying the properties of the trap receiver.

Delete Entry	config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps/<IP Address>" config do "Delete Entry"			
This deletes the SNMP trap receiver permanently from the device.		RW BUTTON EMPTY	-- 	-- T
Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	--	--	--

4.1.8.2.1.1.1 Administration / User and Access Administration / SNMP Configuration / SNMP Traps / <IP Address> / Edit Settings

This menu allows to modify the configuration of the trap receiver (e.g. management station). Things like SNMP protocol version, SNMP community/user name and IP address of the management station can be set up.

IP Address	config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps/<IP Address>/Edit Settings" config set "IP Address" STRING			
The IPv4 or IPv6 address of the SNMP management station to which the traps should be sent.		RW STRING 0.0.0.0	-- 	-- P
Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	--	--	--

IP Description

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps/<IP Address>/Edit Settings"
config "IP Description"

This variable shows the type of IP address assigned to this SNMP trap receiver.

RO	--	--	
STRING			T
Automatic			

Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	--	--	--

SNMP Version

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps/<IP Address>/Edit Settings"
config set "SNMP Version" ENUM

This variable determines the SNMP protocol version that is used to deliver SNMP traps to the trap receiver.

RW	--	--	
ENUM			P
SNMP V2c			

Values	SNMP V2c	SNMP v2c is used for traps.
	SNMP V3	SNMP v3 is used for traps.

Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	--	--	--

Security Name

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps/<IP Address>/Edit Settings"
config set "Security Name" STRING

This variable holds the SNMP security name that shall be used by the SNMP agent when generating traps dedicated to the trap receiver.

If the trap receiver is configured to receive SNMPv2 traps, the security name must be an SNMPv2 community that is set up and enabled in the "SNMPv2 Communities" menu.

If the trap receiver is configured to receive SNMPv3 traps, the security name must be an SNMPv3 user that is set up and enabled in the "SNMPv3 Users" menu.

If the SNMPv2 community or SNMPv3 user becomes disabled or deleted and is no longer usable, traps will stop to be delivered to any trap receiver using it.

RW	--	--	
STRING			P
public			

Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	--	--	--

Status	config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps/<IP Address>/Edit Settings" config set "Status" ENUM			
This variable allows to temporarily enabling or disabling SNMP traps to the trap receiver without having to delete the entry.		RW ENUM Disabled	-- 	-- P
Values	Disabled Enabled			
Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	--	--	--

UDP Port	config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps/<IP Address>/Edit Settings" config set "UDP Port" INTEGER(max: 65535)			
The port number where the SNMP management station expects SNMP traps. The default port 162 is usually correct.		RW INTEGER(max: 65535) 162	-- 	-- P
Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	--	--	--

4.1.8.2.2 Administration / User and Access Administration / SNMP Configuration / SNMP Users

4.1.8.2.2.1 Administration / User and Access Administration / SNMP Configuration / SNMP Users / SNMPv2 Communities

This menu allows to set up or delete SNMPv2 community strings that are recognized by the SNMP agent on the device. SNMPv2 communities can also be disabled temporarily without needing to be deleted.

Add Community

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Users/SNMPv2 Communities"
config do "Add Community"

This command adds a new SNMP community with a name of "public".

RW -- --
BUTTON T
EMPTY

Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	--	--	--

4.1.8.2.2.1.1 Administration / User and Access Administration / SNMP Configuration / SNMP Users / SNMPv2 Communities / <Community>

<Community>

One of user-defined SNMPv2 communities, which shall be modified.

This submenu allows to modify/disable/delete an SNMPv2 community.

Access Level

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Users/SNMPv2 Communities/<Community>"
config set "Access Level" ENUM

This variable allows to specify the access level that SNMP requests are granted that reference the selected community string. Depending on the access level, read and write access to SNMP objects and tables may be restricted.

RW RO RO
ENUM P
Service

Values	Monitor	Lowest access level: can view most settings but not change anything.
	Service	Medium access level: cannot perform administrative tasks, but can view settings and operate the device.
	Administrator	Highest access level: administrative permissions.

Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	--	--	--

Community	config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Users/SNMPv2 Communities/<Community>" config set "Community" STRING			
This variable holds the community string. The community string can be thought of as a "shared secret".		RW STRING public	RO	RO P
Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	--	--	--

Delete Community	config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Users/SNMPv2 Communities/<Community>" config do "Delete Community"			
Deletes the community.		RW BUTTON EMPTY	--	-- T
Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	--	--	--

State	config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Users/SNMPv2 Communities/<Community>" config set "State" ENUM			
This variable determines whether the SNMP community string is available for the SNMP agent on the device. If set to "Disabled", SNMP requests referencing the community are considered invalid. If set to "Enabled", the SNMP agent will respond to those requests.		RW ENUM Disabled	RO	RO P
Values	Disabled Enabled			
Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	--	--	--

4.1.8.2.2.2 Administration / User and Access Administration / SNMP Configuration / SNMP Users / SNMPv3 Users

This menu contains a table of all currently supported SNMPv3 users and allows to modify/delete them. New SNMPv3 users can be added.

Add User	config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Users/SNMPv3 Users" config do "Add User"			
This command adds a new SNMPv3 user with a name of "public" and default values.		RW BUTTON EMPTY	-- 	-- T
Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	--	--	--

4.1.8.2.2.1 Administration / User and Access Administration / SNMP Configuration / SNMP Users / SNMPv3 Users / <SNMPv3 User Name>

<SNMPv3 User Name>

One of user-defined SNMPv3 users, which shall be modified.

This menu allows to delete the SNMPv3 user and gives access to submenus allowing configuring the properties of the SNMPv3 user.

Delete Entry	config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Users/SNMPv3 Users/<SNMPv3 User Name>" config do "Delete Entry"			
This deletes the SNMPv3 user permanently from the device.		RW BUTTON EMPTY	-- 	-- T
Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	--	--	--

State

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Users/SNMPv3 Users/<SNMPv3 User Name>"
config set "State" ENUM

This variable allows to temporarily disable the SNMPv3 user without having to delete the user's table entry.

When set to "Disabled", no messages in behalf of this used will be accepted.

RW	RO	RO
ENUM		P
Disabled		

Values	Disabled Enabled			
Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	--	--	--

4.1.8.2.2.1.1 Administration / User and Access Administration / SNMP Configuration / SNMP Users / SNMPv3 Users / <SNMPv3 User Name> / Edit Settings

4.1.8.2.2.1.1.1 Administration / User and Access Administration / SNMP Configuration / SNMP Users / SNMPv3 Users / <SNMPv3 User Name> / Edit Settings / Change SNMPv3 User

This form page allows to modify all properties of the SNMPv3 user being edited. The changes will not have an immediate effect, they will only become active after submitting the data explicitly at the end of all modifications.

Access Level

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Users/SNMPv3 Users/<SNMPv3 User Name>/Edit Settings/Change SNMPv3 User"
config set "Access Level" ENUM

This variable allows to specify the access level that SNMP requests are granted that reference the selected user name. Depending on the access level, read and write access to SNMP objects and tables may be restricted.

RW	--	--
ENUM		P
Service		

Values	Monitor	Lowest access level: can view most settings but not change anything.
	Service	Medium access level: cannot perform administrative tasks, but can view settings and operate the device.
	Administrator	Highest access level: administrative permissions.

Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	--	--	--

Authentication Passphrase

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Users/SNMPv3 Users/<SNMPv3 User Name>/Edit Settings/Change SNMPv3 User"
config set "Authentication Passphrase" PASSWORD

When the authentication method is set to "HMAC-MD5" or "HMAC-SHA1", this variable holds the user's password. The password will be used to generate an authentication key according to RFC3414 that is used to verify message authentication.

If a valid password is stored on the device, it will be shown as '<hidden>'.

RW -- --
PASSWORD P
EMPTY

Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	-- -- --

Authentication Type

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Users/SNMPv3 Users/<SNMPv3 User Name>/Edit Settings/Change SNMPv3 User"
config set "Authentication Type" ENUM

This variable determines the authentication method in use for authenticating messages for this user.

RW -- --
ENUM P
HMAC-MD5

Values		
	No Authentication	Accept unauthenticated SNMP messages only.
	HMAC-MD5	SNMP messages may be authenticated using the MD5 message digest algorithm.
	HMAC-SHA	SNMP messages may be authenticated using the SHA1 message digest algorithm.

Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	-- -- --

Change SNMPv3 User

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Users/SNMPv3 Users/<SNMPv3 User Name>/Edit Settings/Change SNMPv3 User"
config do "Change SNMPv3 User"

Update the SNMPv3 settings of this user to new values.

RW -- --
BUTTON T
EMPTY

Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	-- -- --

Encryption Passphrase

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Users/SNMPv3 Users/<SNMPv3 User Name>/Edit Settings/Change SNMPv3 User"
config set "Encryption Passphrase" PASSWORD

When the encryption algorithm is set to DES or AES encryption, this variable holds the user's password for message decryption. The password will be used to generate a decryption key according to RFC3414.

If a valid password is stored on the device, it will be shown as '<hidden>'.

RW -- --
PASSWORD P
EMPTY

Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	--	--	--

Encryption Type

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Users/SNMPv3 Users/<SNMPv3 User Name>/Edit Settings/Change SNMPv3 User"
config set "Encryption Type" ENUM

This variable determines whether to accept encrypted SNMP messages of this user and which encryption algorithm is in use (DES/AES).

RW -- --
ENUM P
No Encryption

Values	No Encryption	Accept unencrypted SNMP messages only.
	DES Encryption	SNMP messages may be encrypted using the DES encryption algorithm.
	AES Encryption	SNMP messages may be encrypted using the AES encryption algorithm.

Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	--	--	--

User Name

config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Users/SNMPv3 Users/<SNMPv3 User Name>/Edit Settings/Change SNMPv3 User"
config set "User Name" STRING

The 'User-based Security Model' (USM) SNMPv3 user name. In SNMPv3, the user name is also used as security name.

RW -- --
STRING P
public

Constraints	"SNMP Access Configuration" IS "User/Target Configuration via SNMP" →	--	--	--

4.1.8.3 Administration / User and Access Administration / 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.

SSH CLI Port	config go "/Administration/User and Access Administration/SSH Access" config set "SSH CLI Port" INTEGER			
This variable holds the TCP Port number the SSH CLI server listens to. This variable can only be modified if SSH access is disabled.		RW INTEGER 22	RO	RO P
Constraints	"SSH CLI Access" IS "Enabled" →	RO	RO	RO

SSH Host Key Fingerprint	config go "/Administration/User and Access Administration/SSH Access" config "SSH Host Key Fingerprint"			
At the first startup, a pair of unique private and public SSH host keys is created and stored permanently on the device. These keys serve to uniquely identify the arcutronix device to any SSH client. The fingerprint is a hashed and therefore shorter representation of the key. The main purpose of the fingerprint is to give a (somewhat) human-readable representation of the key that can be compared to an expected value by humans to verify that the key has not been altered.		RO STRING Automatic	RO	RO F

4.1.8.3.1 Administration / User and Access Administration / SSH Access / SSH Keys

This submenu shows the SSH keys currently available for key-based logins to the device and allows to install further keys by downloading them from the "Configuration Store" server.

Transfers of new SSH keys to the device via TFTP/SFTP require that the "Configuration Store" is properly set up. Then, only the file name of the SSH key file must be given before the transfer can be started using the "Download Key" command.

When an SSH key has successfully been downloaded from the Configuration Store server, a new entry appears in the SSH key table that shows information about the key itself. Newly downloaded keys are initially inactive. After adjusting the key properties as needed, the key can be activated.

NOTE: the SSH key file to be transferred to the device must be the public key file and have the file extension "*.pub".

Download Key

config go "/Administration/User and Access Administration/SSH Access/SSH Keys"
config do "Download Key"

Download the SSH key from the server. A file name needs to be configured in "SSH Key Filename" first.

RW	RO	RO
BUTTON		T
EMPTY		

File Transfer State

config go "/Administration/User and Access Administration/SSH Access/SSH Keys"
config "File Transfer State"

The File Transfer State shows the current status of any SSH key file download from the "Configuration Store", i.e. "Transfer complete".

After successful completion of such a transfer, a new entry is created in the SSH key table showing information about the transferred SSH key.

RO	RO	RO
STRING		T
Automatic		

SSH Key Filename

config go "/Administration/User and Access Administration/SSH Access/SSH Keys"
config set "SSH Key Filename" STRING

If a download of an SSH key file from the "Configuration Store" server to the device has to be done, this variable is used to specify the file path of the key file on the server. The file path may contain directory components. The directory separator is a forward slash ("/").

When the file path is relative (does not start with a directory separator), it is simply appended to the configuration store's server URI to build the download link.

When the file path is absolute (starts with a directory separator), the configured configuration store's server directory is ignored.

The key file that needs to be installed on the device is the **public** key part of the SSH key. The device expects that the key file has the extension "*.pub".

RW	RO	RO
STRING		T
EMPTY		

Server Type

config go "/Administration/User and Access Administration/SSH Access/SSH Keys"
config "Server Type"

The device supports three different servers, which can be configured for usage.

- Firmware Store: This server is used to download firmware files to the device for installation.
- Configuration Store: This server is used to upload and download configuration files from/to the device.
- Logfile Store: This server is used to store log files externally for further handling.

Each server can be configured to use the TFTP or SFTP protocol.

RO RO RO
ENUM F
Automatic

Values	Firmware Store	The server is used to download firmware upgrades to the device.
	Configuration Store	The server is used to upload and download configuration data and SSH keys.
	Logfile Store	The server is used to upload log file from the device to the server.

Server URI

config go "/Administration/User and Access Administration/SSH Access/SSH Keys"
config "Server URI"

This variable shows the URI (Unique Resource Identifier) of the server entry. If the server is set up correctly, the protocol type, IP address and server directory can easily be derived from the value.

If the value of this variable is "Disabled", the server entry has been disabled by the administrator. If it is "Not Valid", the detailed server configuration needs to be completed before the server can be used.

The value of this variable is calculated dynamically from the server settings.

RO RO RO
STRING T
Automatic

4.1.8.3.1.1 Administration / User and Access Administration / SSH Access / SSH Keys / <SSH Key ID>

<SSH Key ID>

One of the installed SSH-keys.

This submenu allows to (de-)activate the SSH key. If the SSH key is deactivated, some of the key properties can be modified or it can be deleted from the device.

Bits

config go "/Administration/User and Access Administration/SSH Access/SSH Keys/<SSH Key ID>"
config "Bits"

The integer value of this variable shows the length of the SSH key in bits and is detected from the SSH key itself, i.e. "1024".

RO	RO	RO
INTEGER		P
Automatic		

Cipher

config go "/Administration/User and Access Administration/SSH Access/SSH Keys/<SSH Key ID>"
config "Cipher"

"Cipher" specifies the name of the algorithm that is used to encrypt / decrypt data. The value shown in this variable is detected from the SSH key itself, i.e. "RSA".

RO	RO	RO
STRING		P
Automatic		

Comment

config go "/Administration/User and Access Administration/SSH Access/SSH Keys/<SSH Key ID>"
config set "Comment" STRING

This variable initially is read from the key file itself but can be changed later on as long as this key is not active. The comment can be used to add a kind of explanation to the key.

RW	RO	RO
STRING		P
Automatic		

Constraints	"Status" IS "Active"	→	RO	RO	RO

Delete Key

config go "/Administration/User and Access Administration/SSH Access/SSH Keys/<SSH Key ID>"
config do "Delete Key"

This command deletes the SSH key from the device. It is only available when the SSH key is not active.

RW	RO	RO
BUTTON		T
EMPTY		

Constraints	"Status" IS "Active"	→	RO	RO	RO

Key ID

config go "/Administration/User and Access Administration/SSH Access/SSH Keys/<SSH Key ID>"
config "Key ID"

This variable shows the SSH key fingerprint. The so called fingerprint is a hashed and therefore shorter representation of the original key.

Its main purpose is to give a (somewhat) human-readable representation of the key that can be compared to an expected value by humans to verify that the key has not been altered.

RO	RO	RO
STRING		P
Automatic		

Status

config go "/Administration/User and Access Administration/SSH Access/SSH Keys/<SSH Key ID>"
config set "Status" ENUM

The variable shows information about whether the key is activated and therefore usable for authentication or not.

RW	RO	RO
ENUM		P
Inactive		

Values	Inactive	Key inactive; it may not be used for authentication.
	Active	Key active; it may be used for authentication.

Used as

config go "/Administration/User and Access Administration/SSH Access/SSH Keys/<SSH Key ID>"
config set "Used as" ENUM

This variable describes the type of login that is performed for users using the SSH key to establish the SSH session.

When this variable is set to "Connection Key", the SSH key is used to establish an SSH session to the device only. Users are then confronted with a login prompt before they can access the CLI. The user name associated with the key may or may not be one of the users described in the local user database because the logon to the CLI is a separate step and is able to employ TACACS+ authentication as well as the local user database.

When this variable is set to "Direct login key", the key is not only used to establish a secure SSH session to the device, but also to login the user to the CLI in the same step. For this method to work, the user name associated with the key must be one of the user names of the local user database. Most notably, TACACS+ users are not supported.

This variable can only be changed if the SSH key is not active.

RW	RO	RO
ENUM		P
Connection key		

Values	Connection key	Establish SSH session only.
	Direct login key	Establish SSH session with user login included.

Constraints	"Status" IS "Active"	→	RO	RO	RO

User	config go "/Administration/User and Access Administration/SSH Access/SSH Keys/<SSH Key ID>" config set "User" STRING			
This variable allows to associate a user name with the SSH key. Whenever the SSH key is used, this user name must be supplied to SSH when connecting. If the key is to be used as "Connection Key" only, the user name does not have to be known to the local user database of the device (because no login to the device CLI is performed with the SSH key). If the key is to be used as "Direct login key", the user name needs to be known to the local user database of the device for the automatic login to the CLI to be successful. This variable can only be changed if the SSH key is not active.		RW STRING EMPTY	RO	RO P
Constraints	"Status" IS "Active" →	RO	RO	RO

4.1.8.3.2 Administration / User and Access Administration / SSH Access / SSH Passwords

This submenu offers the possibility to configure or disable SSH password authentication and to set a global SSH connection password.

Global Access Password	config go "/Administration/User and Access Administration/SSH Access/SSH Passwords" config set "Global Access Password" PASSWORD			
This variable allows to set a global connection password that must be known to all users wishing to use the SSH CLI with password authentication when the variable "Password Authentication" is set to "Use global SSH connection password". This variable can only be modified if SSH access is disabled and the "Password Authentication" variable has the appropriate value.		RW PASSWORD EMPTY	RO	RO P
Constraints	"Password Authentication" IS NOT "Use global SSH connection password" →	--	--	--

Password Authentication

config go "/Administration/User and Access Administration/SSH Access/SSH Passwords"
config set "Password Authentication" ENUM

RW RO RO
ENUM P
Web users and passwords

This variable allows configuring whether SSH connections with password authentication are allowed. Independent of this setting, SSH key-based logins are always possible.

If the variable is set to "Password authentication disabled", SSH connections that attempt password authentication are rejected by the device. The only possibility to establish an SSH session is to use an SSH key that is known to the device.

If the variable is set to "Web users and passwords", SSH connections using password authentication are allowed. In this mode, the user name and password required to establish an SSH session are the same that are also needed to login to the Web-OPI or via CONS CLI. When the SSH session is fully established, the user is already logged in at the device and the command prompt is shown.

If the variable is set to "Use global SSH connection password", SSH connections using password authentication are allowed. In this mode, all users need to establish a SSH session using the user name "cli" and a global password that can be configured in the variable "Global Access Password". If the SSH session is fully established, the user gets a login prompt to logon to the CLI.

This variable can only be modified if SSH access is disabled.

Values	Password authentication disabled	SSH access is only possible using SSH keys for authentication.
	Web users and passwords	Establish SSH session and logon to CLI as device user.
	Use global SSH connection password	Establish SSH session as user 'cli'. Logon to CLI follows afterwards.

Constraints	"SSH CLI Access" IS "Enabled"	→	RO	RO	RO

4.1.8.4 Administration / User and Access Administration / Users and Passwords

This menu provides possibilities to set up the local user database of the device and additional authentication methods (e.g. TACACS+).

The authentication methods and users configured here are used to authenticate logins to the device via Web-OPI, CONS CLI as well as SSH CLI. It is therefore important to keep these settings up-to-date.

The database describing SNMP access to the device is NOT configured here.

Authentication Priority

config go "/Administration/User and Access Administration/Users and Passwords"
config set "Authentication Priority" ENUM

The priority of the locally stored user database in relation to TACACS+ authentication.

RW	RO	RO
ENUM		P
Local User DB / TACACS+		

Values

TACACS+ Authentication Only	The local user database will not be considered for logins.
TACACS+ / Local User DB	Any login will first be authenticated using TACACS+. On failures, the local user database will be consulted
Local User DB / TACACS+	Any login will first be authenticated using the local user database. On failures, TACACS+ authentication is attempted.

IP Description

config go "/Administration/User and Access Administration/Users and Passwords"
config "IP Description"

This variable shows the type of IP address assigned to this TACACS+ server.

RO	RO	RO
STRING		T
Automatic		

TACACS+

config go "/Administration/User and Access Administration/Users and Passwords"
config set "TACACS+" ENUM

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.

RW	RO	RO
ENUM		P
Disabled		

Values

Disabled	TACACS+ authentication is disabled.
Enabled	TACACS+ authentication is enabled.

TACACS+ Connect Timeout

config go "/Administration/User and Access Administration/Users and Passwords"
config set "TACACS+ Connect Timeout" INTEGER

Networking problems can cause severe delays in attempts to login to the device via TACACS+.

This variable specifies the maximum time in seconds that the device waits for the connection to the TACACS+ server to be established before considering TACACS+ authentication to have failed.

RW	RO	RO
INTEGER		P
5		

TACACS+ Receive Timeout	config go "/Administration/User and Access Administration/Users and Passwords" config set "TACACS+ Receive Timeout" INTEGER			
Networking problems can cause severe delays in attempts to login to the device via TACACS+. This variable specifies the maximum time in seconds that the device waits for a reply from the TACACS+ server after having established a connection and sent the authentication request before considering TACACS+ authentication to have failed.	RW INTEGER 5	RO	RO P	

TACACS+ Server	config go "/Administration/User and Access Administration/Users and Passwords" config set "TACACS+ Server" STRING		
This variable holds the IP address of the TACACS+ authentication server to use for TACACS authentication. TACACS+ (Terminal Access Controller Access Control System Plus) can be used instead of the local user database to logon to the Web GUI and CLI.	RW STRING 0.0.0.0	RO	RO P

TACACS+ Shared Secret	config go "/Administration/User and Access Administration/Users and Passwords" config set "TACACS+ Shared Secret" STRING		
Communication with TACACS+ servers is encrypted. The encryption key is calculated from a passphrase (the shared secret), that needs to be configured here before TACACS+ authentication can be enabled.	RW STRING public	--	-- P

4.1.8.4.1 Administration / User and Access Administration / Users and Passwords / <Local User Name>

<Local User Name>

One of the defined users.

This submenu allows administrators to delete or modify the user account. Any user can change his/her own password in further submenus.

NOTE: Passwords for a user can only be changed by the user itself. Therefore, if the user has forgotten his password, the user entry must be deleted and re-created in order to reset the password.

Delete Account

config go "/Administration/User and Access Administration/Users and Passwords/<Local User Name>"
config do "Delete Account"

This command deletes the selected user.

RW	--	--
BUTTON		T
EMPTY		

Status

config go "/Administration/User and Access Administration/Users and Passwords/<Local User Name>"
config set "Status" ENUM

This variable allows configuring whether the user is allowed to logon to the device or not. If "Disabled", the user is denied access to the device. If "Enabled", the user may logon to the device via Web-OPI, SSH CLI or CONS CLI.

RW	RO	RO
ENUM		T
Enabled		

Values:
- Enabled
- Disabled

User Group

config go "/Administration/User and Access Administration/Users and Passwords/<Local User Name>"
config set "User Group" ENUM

This variable contains the access level for the user. When the user logs in, his permissions will be restricted to this access level.

RW	RO	RO
ENUM		T
admin		

Values:

admin	Highest access level: administrative permissions
user	Medium access level: cannot perform administrative tasks, but can view settings and operate the device.
guest	Low access level: can view most settings but not change anything.

4.1.8.4.1.1 Administration / User and Access Administration / Users and Passwords / <Local User Name> / Change Password

4.1.8.4.1.1.1 Administration / User and Access Administration / Users and Passwords / <Local User Name> / Change Password / Change Password

This form page is only available for the user entry in the local user database that refers to the user that is logged in. It allows to set a new password that will become active when the user logs in next.

Change Password

config go "/Administration/User and Access Administration/Users and Passwords/<Local User Name>/Change Password/Change Password"
config do "Change Password"

This command submits the user data and changes the password.

RW	RW	RW	
BUTTON		T	
EMPTY			

Constraints	Selected user does not match the user logged in	→	--	--	--

New Password

config go "/Administration/User and Access Administration/Users and Passwords/<Local User Name>/Change Password/Change Password"
config set "New Password" PASSWORD

The password for the user. When logging onto the device via Web/CLI, the password is used to authenticate the user.

The password given to a user must fulfil several security rules. If a new password does not fulfil these rules, it will be not accepted by the device. The rules are as follows:

- Minimum password length is 8 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 must contain characters out of at least 3 of the above 4 groups.

RW	RW	RW	
PASSWORD		T	
EMPTY			

Constraints	Selected user does not match the user logged in	→	--	--	--

Username

config go "/Administration/User and Access Administration/Users and Passwords/<Local User Name>/Change Password/Change Password"
config "Username"

This variable holds the login name of the user.

Please note that the only way to change the login name of the user after creation is to delete and re-create the corresponding user entry.

RO	RO	RO	
STRING		T	
Automatic			

Constraints	Selected user does not match the user logged in	→	--	--	--

4.1.8.4.2 Administration / User and Access Administration / Users and Passwords / Add New Account

4.1.8.4.2.1 Administration / User and Access Administration / Users and Passwords / Add New Account / Create Account

This form page allows to create a new user entry. All information related to the used (e.g. password, access level, login name) must be given before the new user can be created. The password entered must follow the documented security rules for the device.

Create Account	config go "/Administration/User and Access Administration/Users and Passwords/Add New Account/Create Account" config do "Create Account"	
This command submits the user data and creates the new user.		RW -- -- BUTTON T EMPTY

Password	config go "/Administration/User and Access Administration/Users and Passwords/Add New Account/Create Account" config set "Password" PASSWORD	
The password for the user. When logging onto the device via Web/CLI, the password is used to authenticate the user. The password given to a user or other usage must fulfil several security rules. If a new password does not fulfil this rules, it will be not accepted by the device. The rules are as follows: • Minimum password length is 8 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 must contain characters out of at least 3 of the above 4 groups.		RW -- -- PASSWORD T EMPTY

Status

config go "/Administration/User and Access Administration/Users and Passwords/Add New Account/Create Account"
config set "Status" ENUM

This variable allows configuring whether the user is allowed to logon to the device or not. If "Disabled", the user is denied access to the device. If "Enabled", the user may logon to the device via Web-OPI, SSH CLI or CONS CLI.

RW	--	--
ENUM		T
Enabled		

Values:
- Enabled
- Disabled

User Group

config go "/Administration/User and Access Administration/Users and Passwords/Add New Account/Create Account"
config set "User Group" ENUM

This variable allows to specify an access level for the user. When the user logs in next time, his permissions will be restricted to the new access level.

RW	--	--
ENUM		T
admin		

Values:

admin	Highest access level: administrative permissions.
user	Medium access level: cannot perform administrative tasks, but can view settings and operate the device.
guest	Lowest access level: can view most settings but not change anything.

Username

config go "/Administration/User and Access Administration/Users and Passwords/Add New Account/Create Account"
config set "Username" STRING

Enter the login name of the newly created user here. The name must be unique on the device (e.g. a different user entry with the same login name must not yet exist).

Please note that the only way to change the login name of the user after creation is to delete and re-create the corresponding user entry.

RW	--	--
STRING		T
EMPTY		

4.1.8.5 Administration / User and Access Administration / Web Configuration

This menu contains settings affecting HTTP and/or HTTPS support. Besides selecting between HTTP and HTTPS operation, it also allows to set up the necessary parameters for HTTPS operation.

Download File Name

config go "/Administration/User and Access Administration/Web Configuration"
config set "Download File Name" STRING

When a download of a certificate or private key file from the configuration server has to be done, this variable holds the path to the file to be downloaded from the server. The file path may contain directory components. The directory separator is the forward slash ("/").

When the file path is relative (e.g. does not start with a directory separator), it is simply appended to the configuration store's server URI to resolve the download URI.

When the file path is absolute (starts with a directory separator), the configured configuration store's directory is ignored.

RW -- --
STRING T
EMPTY

Constraints	"Web Access Mode" IS NOT "HTTP"	→	RO -- --

File Transfer State

config go "/Administration/User and Access Administration/Web Configuration"
config "File Transfer State"

This variable shows information about file transfers to/from the 'Configuration Store'. If the file transfer has been started, progress information about the transfer is given here.

If the file transfer has completed, this variable contains information about success or failure of the file transfer.

RO -- --
STRING T
Automatic

Load Private Key

config go "/Administration/User and Access Administration/Web Configuration"
config do "Load Private Key"

Starts a download of the private key file from the 'Configuration Store' server.

RW -- --
BUTTON T
EMPTY

Constraints	"Web Access Mode" IS NOT "HTTP"	→	RO -- --

Load Server Certificate

config go "/Administration/User and Access Administration/Web Configuration"
config do "Load Server Certificate"

Starts a download of the server certificate from the 'Configuration Store' server.

RW -- --
BUTTON T
EMPTY

Constraints	"Web Access Mode" IS NOT "HTTP"	→	RO -- --

Server Cert Issuer

config go "/Administration/User and Access Administration/Web Configuration"
config "Server Cert Issuer"

When a valid server certificate has been uploaded to the device, this field shows information about the issuer of the server certificate (e.g. the Certificate Authority, CA). Usually, the information displayed here should reflect the identity of the company that created this certificate.

RO	RO	RO
STRING		T
Automatic		

Server Cert Key Status

config go "/Administration/User and Access Administration/Web Configuration"
config "Server Cert Key Status"

The server certificate contains a public key that allows the client to verify that the server really owns the certificate. For this to work, the server must also have access to the corresponding private key to be able to encrypt data requested by the client.

This field reveals whether a suitable private key has been uploaded already. A suitable private key file is encoded in PEM format and contains the private key **without** passphrase (because the system must be able to start the HTTPS server without entering the passphrase). Furthermore, the private key must match the public key contained in the server certificate.

RO	RO	RO
ENUM		T
Automatic		

Values

Key Missing	No keyfile has been uploaded
No Certificate	No valid certificate is present.
Key Invalid	An invalid keyfile has been uploaded
Key Mismatch	The keyfile does not match the server certificate
Key Valid	The keyfile is valid.

Server Cert Parse Status

config go "/Administration/User and Access Administration/Web Configuration"
config "Server Cert Parse Status"

The server certificate must be uploaded as PEM file containing the certificate first. Further entries are ignored.

This field shows whether the server certificate can successfully be interpreted. If not, it shows an error message from the OpenSSL library that gives details about the problem.

RO	RO	RO
STRING		T
Automatic		

Server Cert Serial

config go "/Administration/User and Access Administration/Web Configuration"
config "Server Cert Serial"

When a valid server certificate has been uploaded to the device, this field shows the serial number of the certificate.

RO	RO	RO
STRING		T
Automatic		

Server Cert Subject

config go "/Administration/User and Access Administration/Web Configuration"
config "Server Cert Subject"

When a valid server certificate has been uploaded to the device, this field shows information about the owner of the server certificate. Usually, the information displayed in the CN section should match the server name / IP address. A HTTPS client should not accept any server certificate that does not match the server identity (IP address, DNS name).

RO	RO	RO
STRING		T
Automatic		

Server Cert Valid From

config go "/Administration/User and Access Administration/Web Configuration"
config "Server Cert Valid From"

When a valid server certificate has been uploaded to the device, this field shows information about the date/time when the HTTPS server certificate became/becomes valid. A HTTPS client should not accept any server certificate that is not yet valid.

RO	RO	RO
STRING		T
Automatic		

Server Cert Valid Till

config go "/Administration/User and Access Administration/Web Configuration"
config "Server Cert Valid Till"

When a valid server certificate has been uploaded to the device, this field shows information about the date/time when the HTTPS server certificate became/becomes invalid. A HTTPS client should not accept any server certificate that has already expired.

RO	RO	RO
STRING		T
Automatic		

Server Key Parse Status

config go "/Administration/User and Access Administration/Web Configuration"
config "Server Key Parse Status"

The HTTPS server must know the private key belonging to the server certificate in PEM file format without passphrase.

This field shows whether the private key can successfully be interpreted. If not, it shows an error message from the OpenSSL library that gives details about the problem.

RO	RO	RO
STRING		T
Automatic		

Server Type

config go "/Administration/User and Access Administration/Web Configuration"
config "Server Type"

The device supports three different servers, which can be configured for usage.

- Firmware Store: This server is used to download firmware files to the device for installation.
- Configuration Store: This server is used to upload and download configuration files from/to the device.
- Logfile Store: This server is used to store log files externally for further handling.

Each server can be configured to use the TFTP or SFTP protocol.

RO -- --
ENUM F
Automatic

Values	Firmware Store	The server is used to download firmware upgrades to the device.
	Configuration Store	The server is used to upload and download configuration data and SSH keys.
	Logfile Store	The server is used to upload log file from the device to the server.

Server URI

config go "/Administration/User and Access Administration/Web Configuration"
config "Server URI"

This variable shows the URI (Unique Resource Identifier) of the server entry. If the server is set up correctly, the protocol type, IP address and server directory can easily be derived from the value.

If the value of this variable is "Disabled", the server entry has been disabled by the administrator. If it is "Not Valid", the detailed server configuration needs to be completed before the server can be used.

The value of this variable is calculated dynamically from the server settings.

RO -- --
STRING T
Automatic

Web Access Mode

config go "/Administration/User and Access Administration/Web Configuration"
config set "Web Access Mode" ENUM

This variable allows to select whether HTTP and/or HTTPS are supported by the device. In case of HTTP only operation, the HTTPS port is disabled. In case of HTTPS only operation, the default HTTP port (80) will be redirected to the HTTPS port. If both, HTTP and HTTPS are enabled, both ports are independently operated to allow secure as well as insecure Web access.

RW RO RO
ENUM P
HTTP + HTTPS

Values	HTTP	HTTP only
	HTTPS	HTTPS only
	HTTP + HTTPS	HTTP and HTTPS

4.2 Alarm Management

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

This menu contains an overview of the current overall alarm state of the device and lists available alarm groups with their most important properties.

See the <Alarm Group> description for more information on available alarm groups.

Acknowledge All

config go "/Alarm Management"
config do "Acknowledge All"

This command allows to acknowledge all unacknowledged, active alarms.

RW	RW	RO
BUTTON		T
EMPTY		

Alarm Acknowledgement Policy

config go "/Alarm Management"
config set "Alarm Acknowledgement Policy" ENUM

The value of this variable determines what happens to an acknowledged alarm when the alarm severity changes. There are three different behaviours available.

Please note that acknowledged alarms will always become unacknowledged when the alarm condition gets cleared and the alarm becomes inactive.

RW	RO	RO
ENUM		P
Unacknowledge When Raising Severity		

Values

Keep Acknowledged Until Inactive	An acknowledged alarm will remain acknowledged until the alarm condition ceases.
Unacknowledge When Raising Severity	An acknowledged alarm will become active again when the alarm severity increases (e.g. from "Warning" to "Error").
Unacknowledge on State Change	An acknowledged alarm will become active again as soon as the alarm severity changes.

4.2.1 Alarm Management / <Alarm Group>

<Alarm Group>

Name of one of the (pre-defined) alarm groups:

- System Alarms

- RF Port Alarm

This submenu refers to a line of the alarm group table. It allows to modify editable values in the table and to descend into further submenus that describe the configuration of alarms in this alarm group.

Acknowledge Group Alarms

config go "/Alarm Management/<Alarm Group>"
config do "Acknowledge Group Alarms"

This command acknowledges all unacknowledged active alarms in the alarm group.

RW	RW	RO
BUTTON		T
EMPTY		

Acknowledged

config go "/Alarm Management/<Alarm Group>"
config "Acknowledged"

This variable contains the number of alarms in this alarm group that have an active alarm condition and have already been acknowledged by the operator.

RO	RO	RO
INTEGER		T
Automatic		

Ignored

config go "/Alarm Management/<Alarm Group>"
config "Ignored"

Shows the number of ignored alarms with active alarm condition.

RO	RO	RO
INTEGER		T
Automatic		

Max. Severity

config go "/Alarm Management/<Alarm Group>"
config set "Max. Severity" ENUM

This variables indicates the maximum severity that is allowed for any alarm in the alarm group. It can be used to degrade all "Error" states to "Warning" or to ignore all alarms in the alarm group.

RW	RO	RO
ENUM		P
Error		

Values	Ignore	All alarm conditions in the alarm group are to be ignored.
	Warning	All alarm conditions in the alarm group with severity "Error" are degraded to a "Warning".
	Error	The severity of alarms in the alarm group is not changed.

4.2.1.1 Alarm Management / <Alarm Group> / Group Details

This submenu shows an overview of the alarm state of the alarm group and a list of alarms currently available in the alarm group. It also allows to change individual alarm properties in further submenus.

Alarm Group Name

config go "/Alarm Management/<Alarm Group>/Group Details"
config "Alarm Group Name"

This variable holds a descriptive name of the alarm group.

RO	RO	RO
STRING		F
Automatic		

Alarm Group State

config go "/Alarm Management/<Alarm Group>/Group Details"
config "Alarm Group State"

This variable shows the maximum alarm severity of any alarm in the alarm group.

RO	RO	RO
ENUM		T
Automatic		

Values

No Alarm	Indicates that all alarm conditions in the alarm group are cleared.
Error	Indicates unacknowledged active alarms with "Error" severity in the alarm group.
Acknowledged	Indicates acknowledged active alarms in the alarm group.
Warning	Indicates unacknowledged active alarms with "Warning" severity in the alarm group

Current Errors

config go "/Alarm Management/<Alarm Group>/Group Details"
config "Current Errors"

Shows the number of unacknowledged active alarms with severity "Error" in this alarm group.

RO	RO	RO
INTEGER		T
Automatic		

Current Warnings

config go "/Alarm Management/<Alarm Group>/Group Details"
config "Current Warnings"

Shows the number of unacknowledged active alarms with severity "Warning" in this alarm group.

RO	RO	RO
INTEGER		T
Automatic		

4.2.1.1.1 Alarm Management / <Alarm Group> / Group Details / <Alarm Item>

<Alarm Item>

Name of an alarm which is a member of the selected alarm group.

This submenu allows modifying the properties of the alarm and to acknowledge the alarm if it is currently active.

Acknowledge

config go "/Alarm Management/<Alarm Group>/Group Details/<Alarm Item>"
config do "Acknowledge"

Command to acknowledge an active alarm. An acknowledged alarm will no longer affect the overall alarm state of the device.

RW	RW	RO
BUTTON		T
EMPTY		

Constraints					
	"State" IS ("Ignored" || "Acknowledged")	→	RO	RO	RO
	"State" IS ("n.a." || "Ok")	→	RO	RO	RO

SNMP Notification

config go "/Alarm Management/<Alarm Group>/Group Details/<Alarm Item>"
config set "SNMP Notification" ENUM

This variable indicates whether alarm state changes will cause an SNMP trap to be sent. The SNMP trap type that is sent depends on further configuration in the SNMP section.

For this feature to work, SNMP support must be enabled and valid SNMP Trap Receivers must have been configured.

RW	RO	RO
ENUM		P
SNMP Trap		

Values		
	No Notification	Do not send SNMP traps when the alarm state changes.
	SNMP Trap	Any alarm state change will cause an SNMP trap to be sent.

State	config go "/Alarm Management/<Alarm Group>/Group Details/<Alarm Item>" config "State"

This variable holds the current status of the alarm.

A value of "Warning" or "Error" does not only indicate that the alarm condition is active, but also that the alarm is still active.

A value of "Acknowledged" or "Ignored" is used to indicate that the alarm condition is active, although the alarm itself is either acknowledged or was configured to not raise an alarm as well.

All other values indicate that the alarm condition is inactive or that the monitored quantity is not available.

RO	RO	RO
ENUM		T
Automatic		

Values	n.a.	The alarm is not available in the current device configuration.
	Ok	The alarm is available and the alarm condition is cleared.
	Warning	The alarm is active with a severity of "Warning".
	Error	The alarm is active with a severity of "Error".
	Ignored	The alarm condition is active but ignored.
	Acknowledged	The alarm condition is active but the alarm is acknowledged.

4.2.1.1.1.1 Alarm Management / <Alarm Group> / Group Details / <Alarm Item> / Settings

This submenu allows configuring alarm details.

For analogue alarms, the submenu allows configuring both, warning and error level thresholds for the quantity. Depending on the quantity being monitored, overrun or underrun thresholds can be set that provide an upper or a lower bound on the value of the quantity. To prevent the alarm state from oscillating between states quickly, a suitable hysteresis must be configured.

For digital alarms, the alarm severity can be configured.

Both alarm types allow to set the alarm hold time. This is a time interval that determines how long the alarm is still kept in active state when the alarm condition has gone. This is intended to prevent the alarm state from oscillating quickly.

Alarm Hold Time

config go "/Alarm Management/<Alarm Group>/Group Details/<Alarm Item>/Settings"
config set "Alarm Hold Time" STRING

This variable contains the alarm hold time, that is the time for which the alarm is held active after the alarm condition has gone.

Whenever an alarm state toggles quickly, this setting can be used to limit the rate with which SNMP traps or log entries are generated. If the alarm condition reappears before the alarm hold time has passed, the alarm will still be active and the reoccurrence of the alarm condition will not cause a change in the alarm state (and, hence, no notifications will be generated). If the alarm condition stays clear for longer than the alarm hold time, the alarm becomes inactive.

Setting this variable to zero disables the alarm hold time and the disappearance of the alarm condition will immediately be reflected in the alarm state. The maximum time that can be entered is 300 seconds.

RW	RO	RO
STRING		P
Automatic		

Alarm Name

config go "/Alarm Management/<Alarm Group>/Group Details/<Alarm Item>/Settings"
config "Alarm Name"

This variable holds a descriptive name of the alarm.

RO	RO	RO
STRING		F
Automatic		

Alarm Severity

config go "/Alarm Management/<Alarm Group>/Group Details/<Alarm Item>/Settings"
config set "Alarm Severity" ENUM

This variable indicates the severity of the digital alarm when the alarm becomes active.

The default value after a factory reset can be different from alarm to alarm and is defined by the device software.

RW	RO	RO
ENUM		P
Automatic		

Values	Ignore	Indicates that the digital alarm is to be ignored.
	Warning	Indicates that the alarm severity of the digital alarm is "Warning" when being active.
	Error	Indicates that the alarm severity of the digital alarm is "Error" when being active.

Constraints	Alarm is an analog alarm	→	--	--	--

Hysteresis

config go "/Alarm Management/<Alarm Group>/Group Details/<Alarm Item>/Settings"
config set "Hysteresis" STRING

This variable holds the hysteresis that is used to detect clearing conditions for alarms monitoring physical quantities. If the quantity crosses a threshold and causes the alarm to become active, the alarm will not be cleared before the quantity has gone back behind the threshold by more than the hysteresis value.

The hysteresis must either be given in percent (of the threshold value being crossed), or in physical units. The percentage mode is enforced by the device where the monitored quantity (and its thresholds, naturally) varies by several orders of magnitude so that a single hysteresis value in physical units seems inappropriate (e.g. SFP receive power in mW).

The physical unit mode is enforced by the device in cases where the monitored quantity is always in the same order of magnitude (e.g. device temperature in degrees Celsius).

To change the hysteresis value, assign a floating point number to this variable. Specifying the unit (percent or physical unit) is optional. Unit conversions are not performed, an error is returned when a wrong physical unit is specified. Changes between percentage mode and physical unit mode are not allowed.

The software defines a suitable default value for each alarm individually that becomes active after restoring factory default settings.

			RW	RO	RO
			STRING		P
			Automatic		
Constraints	Alarm is a digital alarm	→	--	--	--

Overrun Error Level

config go "/Alarm Management/<Alarm Group>/Group Details/<Alarm Item>/Settings"
config set "Overrun Error Level" STRING

This variable holds a threshold value that will cause the alarm to become active with "Error" severity when the monitored quantity raises above the threshold.

To change the threshold value, assign a floating point number to this variable. Specifying the physical unit is optional. Unit conversions are not performed, an error is returned when a wrong physical unit is specified.

To disable this threshold, assign the special value "Off" to this variable.

The software defines a suitable default value for each alarm individually that becomes active after restoring factory default settings.

NOTE: When the error threshold is configured to be within the corresponding warning range, no warning will ever be emitted.

			RW	RO	RO
			STRING		P
			Automatic		
Constraints	Alarm supports no overrun checks	→	--	--	--
	Alarm is a digital alarm	→	--	--	--

Overrun Warning Level

config go "/Alarm Management/<Alarm Group>/Group Details/<Alarm Item>/Settings"
config set "Overrun Warning Level" STRING

This variable holds a threshold value that will cause the alarm to become active with "Warning" severity when the monitored quantity raises above the threshold.

To change the threshold value, assign a floating point number to this variable. Specifying the physical unit is optional. Unit conversions are not performed, an error is returned when a wrong physical unit is specified.

To disable this threshold, assign the special value "Off" to this variable.

The software defines a suitable default value for each alarm individually that becomes active after restoring factory default settings.

NOTE: When the corresponding error threshold is configured to be within the warning range, no warning will ever be emitted.

			RW	RO	RO
			STRING		P
			Automatic		
Constraints	Alarm supports no overrun checks	→	--	--	--
	Alarm is a digital alarm	→	--	--	--

System Component

config go "/Alarm Management/<Alarm Group>/Group Details/<Alarm Item>/Settings"
config "System Component"

Some alarms refer to a certain hardware component in the system, of which multiple similar instances are equipped (e.g. Ethernet ports). In such a case, this variable identifies the system component that an alarm actually refers to.

RO	RO	RO		
STRING		F		
Automatic				

Underrun Error Level

config go "/Alarm Management/<Alarm Group>/Group Details/<Alarm Item>/Settings"
config set "Underrun Error Level" STRING

This variable holds a threshold value that will cause the alarm to become active with "Error" severity when the monitored quantity falls below the threshold.

To change the threshold value, assign a floating point number to this variable. Specifying the physical unit is optional. Unit conversions are not performed, an error is returned when a wrong physical unit is specified.

To disable this threshold, assign the special value "Off" to this variable.

The software defines a suitable default value for each alarm individually that becomes active after restoring factory default settings.

NOTE: When the error threshold is configured to be within the corresponding warning range, no warning will ever be emitted.

			RW	RO	RO
			STRING		P
			Automatic		
Constraints	Alarm supports no underrun checks	→	--	--	--
	Alarm is a digital alarm	→	--	--	--

Underrun Warning Level

config go "/Alarm Management/<Alarm Group>/Group Details/<Alarm Item>/Settings"
config set "Underrun Warning Level" STRING

This variable holds a threshold value that will cause the alarm to become active with "Warning" severity when the monitored quantity falls below the threshold.

To change the threshold value, assign a floating point number to this variable. Specifying the physical unit is optional. Unit conversions are not performed, an error is returned when a wrong physical unit is specified.

To disable this threshold, assign the special value "Off" to this variable.

The software defines a suitable default value for each alarm individually that becomes active after restoring factory default settings.

NOTE: When the corresponding error threshold is configured to be within the warning range, no warning will ever be emitted.

			RW	RO	RO
			STRING		P
			Automatic		
Constraints	Alarm supports no underrun checks	→	--	--	--
	Alarm is a digital alarm	→	--	--	--

Value

config go "/Alarm Management/<Alarm Group>/Group Details/<Alarm Item>/Settings"
config "Value"

This variable holds the current value of the quantity monitored by the alarm. For threshold-crossing (analogue) alarms, it shows the current numerical value and the physical unit (if applicable).

For discrete state (digital) alarms, it shows a textual description of the current state. Only a subset of the available states represent active error conditions.

RO	RO	RO
STRING		T
Automatic		

4.2.2 Alarm Management / Active Alarm List

This menu gives a quick overview of all alarms with an active alarm condition. The menu contains a table that is ordered by alarm severity and allows to easily acknowledge active alarms.

The information shown in this menu includes the current alarm name and alarm group as well as the current alarm state. The alarm configuration itself cannot be changed here.

Current Errors

config go "/Alarm Management/Active Alarm List"
config "Current Errors"

This variable shows the total number of unacknowledged device alarms that have a severity of "Error".

RO	RO	RO
INTEGER		T
Automatic		

Current Warnings

config go "/Alarm Management/Active Alarm List"
config "Current Warnings"

This variable shows the total number of unacknowledged device alarms that have a severity of "Warning".

RO	RO	RO
INTEGER		T
Automatic		

Global Alarm Status

config go "/Alarm Management/Active Alarm List"
config "Global Alarm Status"

This variable contains information about the current system alarm state. It reflects the highest alarm state that any of the device alarms is in. This status is shown on the ALM-LED and in case of Alarm, the relay is closed.

RO	RO	RO
ENUM		T
Automatic		

Values

No Alarm	Indicates that all alarm conditions in the alarm group are cleared. Alarm LED is off.
Error	Indicates unacknowledged active alarms with "Error" severity. Alarm LED is on.
Acknowledged	Indicates acknowledged active alarms. Alarm LED is off.
Warning	Indicates unacknowledged active alarms with "Warning" severity. Alarm LED is blinking.

4.2.2.1 Alarm Management / Active Alarm List / <Alarm Num>

<Alarm Num>

Alarm (line) number in alarm list.

This submenu refers to a line of the alarm list table. It allows to acknowledge the selected alarm if it is still in "Error" or "Warning" state. Configuration of the alarm details is not possible here.

Acknowledge

config go "/Alarm Management/Active Alarm List/<Alarm Num>"
config do "Acknowledge"

Command to acknowledge an active alarm. An acknowledged alarm will no longer affect the overall alarm state of the device.

RW	RW	RO
BUTTON		T
EMPTY		

Constraints	"State" IS "Acknowledged" →	RO	RO	RO

Alarm Name

config go "/Alarm Management/Active Alarm List/<Alarm Num>"
config "Alarm Name"

Shows the name of the alarm.

RO	RO	RO
STRING		T
Automatic		

Group Name

config go "/Alarm Management/Active Alarm List/<Alarm Num>"
config "Group Name"

Identifies the alarm group that the alarm belongs to.

RO	RO	RO
STRING		T
Automatic		

No

config go "/Alarm Management/Active Alarm List/<Alarm Num>"
config "No"

This variable enumerates entries in the list of active alarms. It is identical to the row number in which an alarm appears and, therefore, does not always refer to the same alarm.

RO	RO	RO
INTEGER		T
Automatic		

State

config go "/Alarm Management/Active Alarm List/<Alarm Num>"
config "State"

Shows the current value of the alarm.

RO	RO	RO
STRING		T
Automatic		

State

config go "/Alarm Management/Active Alarm List/<Alarm Num>"
config "State"

This variable holds the current status of the alarm. Since the list only shows alarms with an active alarm condition, the only values valid in this field are "Error", "Warning" and "Acknowledged".

RO	RO	RO
ENUM		T
Automatic		

Values	Error	The alarm is active with a severity of "Error".
	Warning	The alarm is active with a severity of "Warning".
	Acknowledged	The alarm condition is active but the alarm is acknowledged.

System Component

config go "/Alarm Management/Active Alarm List/<Alarm Num>"
config "System Component"

Shows the system component to which the alarm relates.

RO	RO	RO
STRING		T
Automatic		

4.3 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.

Contact Person

config go "/General System Information"
config set "Contact Person" STRING

This variable allows to specify the name of a reference person that is responsible for the device. The name is also reported as sysContact via SNMP.

RW	RO	RO
STRING		P
< ... >		

Current System Uptime

config go "/General System Information"
config "Current System Uptime"

This variable contains the time since last reboot, formatted according to "Dd hh:mm" where 'D' is the number of days, 'hh' is a two-digit hours indication in 24h format, 'mm' is a two-digit minutes indication.

RO	RO	RO
STRING		T
Automatic		

Date and Time

config go "/General System Information"
config "Date and Time"

The current date and time of the device is displayed here.

RO	RO	RO
STRING		T
Automatic		

Device Location

config go "/General System Information"
config set "Device Location" STRING

This variable allows to specify the location of the device. It is also reported as sysLocation via SNMP.

RW	RO	RO
STRING		P
< ... >		

Device Name

config go "/General System Information"
config set "Device Name" STRING

This variable allows to provide an administratively assigned name to the device. This name is also reported as sysName via SNMP.

After restoring factory default settings, this variable defaults to the serial number of the device.

RW	RO	RO
STRING		P
Automatic		

Device Temperature

config go "/General System Information"
config "Device Temperature"

This variable contains the current device temperature in degrees Celsius.

RO	RO	RO
STRING		T
Automatic		

Total System Uptime

config go "/General System Information"
config "Total System Uptime"

This variable contains the total runtime of the device since production, formatted according to "Dd hh:mm" where 'D' is the number of days, 'hh' is a two-digit hours indication in 24h format and 'mm' is a two-digit minutes indication. This value continues to count up even after system resets.

RO	RO	RO
STRING		P
Automatic		

4.3.1 General System Information / 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.

Article Revision

config go "/General System Information/Inventory"
config "Article Revision"

This variable contains the article revision of the device.

RO RO RO
STRING F
Automatic

Bootloader Version

config go "/General System Information/Inventory"
config "Bootloader Version"

This variable contains the version number of the boot loader that is currently used on the device.

RO RO RO
STRING P
Automatic

Customization

config go "/General System Information/Inventory"
config "Customization"

This variable identifies the customer to which the device has been adopted.

RO RO RO
ENUM F
Automatic

Values	Dynamic	Available entries depend on device configuration.

Date of Production

config go "/General System Information/Inventory"
config "Date of Production"

This variable contains the manufacturing date of the device.

RO RO RO
STRING F
Automatic

Device Type

config go "/General System Information/Inventory"
config "Device Type"

This variable contains the device type of the device.

RO RO RO
STRING F
Automatic

FPGA Version

config go "/General System Information/Inventory"
config "FPGA Version"

This variable contains the version number of the FPGA that is currently used on the device.

RO	RO	RO
STRING		P
Automatic		

Constraints	no FPGA equipped	→	--	--	--

Hardware Revision

config go "/General System Information/Inventory"
config "Hardware Revision"

This variable contains the hardware revision of the device.

RO	RO	RO
STRING		F
Automatic		

Manufacturer

config go "/General System Information/Inventory"
config "Manufacturer"

This variable contains the manufacturer of the device (usually: arcutronix GmbH).

RO	RO	RO
STRING		F
Automatic		

Order No.

config go "/General System Information/Inventory"
config "Order No."

This variable contains the order number of the device. The order number is used to order devices at arcutronix GmbH.

RO	RO	RO
STRING		F
Automatic		

Serial Number

config go "/General System Information/Inventory"
config "Serial Number"

This variable contains the serial number of the device.

RO	RO	RO
STRING		F
Automatic		

Software Version

config go "/General System Information/Inventory"
config "Software Version"

This variable contains the version number of the system software that is currently used by the device. A different software version can be installed in the menu "/Administration/Firmware Update".

RO	RO	RO
STRING		P
Automatic		

Vendor ID

config go "/General System Information/Inventory"
config "Vendor ID"

This field shows the international unique vendor ID (usually: UN341185881 = arcutronix GmbH).

RO	RO	RO
STRING		T
Automatic		

4.4 Log View

This submenu allows transferring the event log to the remote 'Logfile Store' server defined under '/Administration/User and Access Administration'.

Saving the log file is always a two-step process. The first step is to specify the file name under which the log file shall be stored on the server. Please note that the device will abort the file transfer with an error if it finds that a file with the same name already exists on the server.

The second step is to initiate the transfer.

File Transfer State

config go "/Log View"
config "File Transfer State"

This variable holds information about the last file transfer of an event log file to the log file storage server. This includes status messages about an ongoing transfer as well as the file transfer result. The value is intended to be displayed to an operator for interpretation.

RO	RO	--
STRING		T
Automatic		

Logfile Name

config go "/Log View"
config set "Logfile Name" STRING

This variable allows to specify a file name for an event log file that is to be uploaded to the "Logfile Store". For the upload to succeed it is required that no file with the same name is already present on the "Logfile Store".

RW	RW	--
STRING		T
EMPTY		

Server Type

config go "/Log View"
config "Server Type"

The device supports three different servers, which can be configured for usage.

- Firmware Store: This server is used to download firmware files to the device for installation.
- Configuration Store: This server is used to upload and download configuration files from/to the device.
- Logfile Store: This server is used to store log files externally for further handling.

Each server can be configured to use the TFTP or SFTP protocol.

RO	RO	RO
ENUM		F
Automatic		

Values	Firmware Store	The server is used to download firmware upgrades to the device.
	Configuration Store	The server is used to upload and download configuration data and SSH keys.
	Logfile Store	The server is used to upload log file from the device to the server.

Server URI

config go "/Log View"
config "Server URI"

This variable shows the URI (Unique Resource Identifier) of the server entry. If the server is set up correctly, the protocol type, IP address and server directory can easily be derived from the value.

If the value of this variable is "Disabled", the server entry has been disabled by the administrator. If it is "Not Valid", the detailed server configuration needs to be completed before the server can be used.

The value of this variable is calculated dynamically from the server settings.

RO	RO	RO
STRING		T
Automatic		

Upload to 'Logfile Store'

config go "/Log View"
config do "Upload to 'Logfile Store'"

Upload the log file to the server.

RW	RW	--
BUTTON		T
EMPTY		

4.5 Remote Feeding Control

4.5.1 Remote Feeding Control / <RF Port No.>

<RF Port No.>

One of the Remote Feeding ports named Port 1 ... Port 16.

Admin Status

config go "/Remote Feeding Control/<RF Port No.>"
config set "Admin Status" ENUM

This object allows to turn remote feeding on or off on the remote feeding port.

A value of 'disabled' disables remote feeding on the port.

A value of 'enabled' enables remote feeding on the port.

RW	RW	RO
ENUM		P
Automatic		

Values	Disabled	Port disabled
	Enabled	Port enabled

SNMP Traps

config go "/Remote Feeding Control/<RF Port No.>"
config set "SNMP Traps" ENUM

This variable allows to configure whether the SNMP trap axRPXOperStatusTrap shall be sent whenever the operation status of the selected Remote Feeding port changes.

The sending of alarm traps from alarm management (axRPXOperationStatusAlarm) is independent of this setting, though, and needs to be enabled or disabled separately.

RW	RO	RO
ENUM		P
Enabled		

Values	Disabled	Disables sending of axRPXOperStatusTrap traps
	Enabled	Enables sending of axRPXOperStatusTrap traps

4.5.1.1 Remote Feeding Control / <RF Port No.> / RF Port Configuration

Ground Leakage Alarm Status

config go "/Remote Feeding Control/<RF Port No.>/RF Port Configuration"
config "Ground Leakage Alarm Status"

This object shows the current ground leakage condition. Ground leakage is detected if the resistance between wire A (or wire B) of the DSL port and GND drops below 16 kOhm.

A value of 'no ground leakage' indicates that ground leakage has not been detected.

A value of 'ground leakage' indicates that ground leakage has been detected. The condition will be cleared if the resistance raises above 250 kOhm again.

RO	RO	RO
ENUM		T
Automatic		

Values

no ground leakage alarm	No active leakage alarm detected.
ground leakage detected	Ground leakage alarm active.

HCLT [mA]

config go "/Remote Feeding Control/<RF Port No.>/RF Port Configuration"
config set "HCLT [mA]" INTEGER

This object holds the lower feeding current threshold for the 'high current' alarm detection. An existing high current alarm is cleared if the feeding current falls below the value indicated here.

Both, high current lower threshold (HCLT) and high current upper threshold (HCUT) are used in high current alarm detection to form a hysteresis.

This object can be modified to change the high current clearance threshold. Allowed values are between low current upper threshold (LCUT) and high current upper threshold (HCUT) - 1 (less than HCUT): LCUT <= HCLT <= (HCUT-1).

The device will respond with an error if the new value is out of bounds.

RW	RO	RO
INTEGER		P
49		

HCUT [mA]

config go "/Remote Feeding Control/<RF Port No.>/RF Port Configuration"
config set "HCUT [mA]" INTEGER

This object holds the upper feeding current threshold for the 'high current' alarm detection. A high current alarm will be raised if the feeding current raises above the value indicated here.

Both, high current lower threshold (HCLT) and high current upper threshold (HCUT) are used in high current alarm detection to form a hysteresis.

This object can be modified to change the high current alarm threshold. Allowed values are between high current lower threshold (HCLT) + 1 (larger than HCLT) and overload lower threshold (OVLT): (HCLT+1) <= HCUT <= OVLT.

The device will respond with an error if the new value is out of bounds.

RW	RO	RO
INTEGER		P
50		

LCLT [mA]

config go "/Remote Feeding Control/<RF Port No.>/RF Port Configuration"
config set "LCLT [mA]" INTEGER

This object holds the lower feeding current threshold for the 'low current' alarm detection. A low current alarm is raised if the feeding current falls below the value indicated here.

Both, low current lower threshold (LCLT) and low current upper threshold (LCUT) are used in low current alarm detection to form a hysteresis.

This object can be modified to change the low current alarm threshold. Allowed values are between open circuit upper threshold (OCUT) and low current upper threshold (LCUT) - 1 (less than LCUT): OCUT <= LCLT <= (LCUT-1).

The device will respond with an error if the new value is out of bounds.

RW	RO	RO
INTEGER		P
9		

LCUT [mA]

config go "/Remote Feeding Control/<RF Port No.>/RF Port Configuration"
config set "LCUT [mA]" INTEGER

This object holds the upper feeding current threshold for the 'low current' alarm detection. An existing low current alarm is cleared if the feeding current rises above the value indicated here.

Both, low current lower threshold (LCLT) and low current upper threshold (LCUT) are used in low current alarm detection to form a hysteresis.

This object can be modified to change the low current clearance threshold. Allowed values are between low current lower threshold (LCLT) + 1 (more than LCLT) and high current lower threshold: (LCLT+1) <= LCUT <= HCLT.

The device will respond with an error if the new value is out of bounds.

RW	RO	RO
INTEGER		P
10		

OCLT [mA]

config go "/Remote Feeding Control/<RF Port No.>/RF Port Configuration"
config set "OCLT [mA]" INTEGER(2 - 5)

This object holds the lower feeding current threshold for the 'open circuit' alarm detection. An open circuit is detected if the feeding current falls below the value indicated here.

Both, open circuit lower threshold (OCLT) and open circuit upper threshold (OCUT) are used in open circuit alarm detection to form a hysteresis.

This object can be modified to change the open circuit detection threshold. Allowed values are between 2 and 5 mA: 2mA <= OCLT <= 5mA.

The device will respond with an error if the new value is out of bounds.

RW	RO	RO
INTEGER(2 - 5)		P
5		

OCUT [mA]

config go "/Remote Feeding Control/<RF Port No.>/RF Port Configuration"
config set "OCUT [mA]" INTEGER(3 - 6)

This object holds the upper feeding current threshold for the 'open circuit' alarm detection. An existing open circuit alarm is cleared if the feeding current rises above the value indicated here.

Both, open circuit lower threshold (OCLT) and open circuit upper threshold (OCUT) are used in open circuit alarm detection to form a hysteresis.

This object can be modified to change the open circuit clearance threshold. Allowed values are between OCLT+1 and 6mA: (OCLT+1) <= OCUT <= 6mA.

The device will respond with an error if the new value is out of bounds.

RW	RO	RO
INTEGER(3 - 6)		P
6		

OVLT [mA]

config go "/Remote Feeding Control/<RF Port No.>/RF Port Configuration"
config set "OVLT [mA]" INTEGER

This variable holds the lower feeding current threshold for the 'overload' alarm detection. An existing overload alarm will be cleared if the feeding current falls below this threshold.

Both, overload lower threshold (OVLT) and overload upper threshold (OVUT) are used in overload alarm detection to form a hysteresis.

This variable can be modified to change the overload alarm threshold. Allowed values are between high current upper threshold (HCUT) and overload upper threshold (OVUT) - 1: HCUT <= OVLT <= (OVUT - 1).

The device will respond with an error if the new value is out of bounds.

RW	RO	RO
INTEGER		P
60		

OVUT [mA]

config go "/Remote Feeding Control/<RF Port No.>/RF Port Configuration"
config set "OVUT [mA]" INTEGER(max: 64)

This variable holds the upper feeding current threshold for the 'overload' alarm detection. An 'overload' alarm will be raised if the feeding current raises above the value indicated here.

Both, overload lower threshold (OVLT) and overload upper threshold (OVUT) are used in overload alarm detection to form a hysteresis.

This variable can be modified to change the overload clearance threshold. Allowed values are between overload lower threshold (OVLT) + 1 (larger than OVLT) and 64 mA: (OVLT + 1) <= OVUT <= 64 mA.

The device will respond with an error if the new value is out of bounds.

RW	RO	RO
INTEGER(max: 64)		P
61		

RF Control FW Version

config go "/Remote Feeding Control/<RF Port No.>/RF Port Configuration"
config "RF Control FW Version"

This variable shows the current controller fimware version of the remote feeding port.

RO	RO	RO
STRING		T
Automatic		

RF Current [mA]

config go "/Remote Feeding Control/<RF Port No.>/RF Port Configuration"
config "RF Current [mA]"

This object shows the current remote feeding current in milliampere.

RO	RO	RO
INTEGER		T
Automatic		

RF Operation Status

config go "/Remote Feeding Control/<RF Port No.>/RF Port Configuration"
config "RF Operation Status"

This variable shows the current operation status of the remote feeding port.

A value of "disabled" indicates that the remote feeding port is disabled by admin.

A value of "normal operation" means that remote feeding port is operating normally.

A value of "open circuit" indicates that the remote feeding current has dropped below the low open circuit lower threshold.

A value of "low current" indicates that the remote feeding current has dropped below the low current lower threshold.

A value of "high current" indicates that the remote feeding power has raised above the high current upper threshold.

A value of "overload" indicates that the remote feeding voltage has dropped below the overload lower threshold and current is limited to 70mA.

A value of "overload shutdown" indicates that the "overload" status lasts for a time > 3 seconds and the remote feeding port has been switched off for thermal protection reasons.

A value of "overvoltage shutdown" indicates that the remote feeding port has been switched off immediately for safety reasons.

RO	RO	RO
ENUM		T
Automatic		

Values

disabled	RF Port is disabled
open circuit	RF Port has open circuit detected
low current	RF Port has low current detected
normal operation	RF Port is in normal operation condition
high current	RF Port has high current detected
overload	RF Port has overload detected
overvoltage shutdown	Remote power has been switched off immediately due to overvoltage detection.
overload shutdown	Remote power has been switched off due to a lasting overload.

RF Port No.

config go "/Remote Feeding Control/<RF Port No.>/RF Port Configuration"
config "RF Port No."

This object uniquely identifies the remote feeding port.

RO	RO	RO
INTEGER		T
Automatic		

RF Voltage (a_b) [V]

config go "/Remote Feeding Control/<RF Port No.>/RF Port Configuration"
config "RF Voltage (a_b) [V]"

This object shows the current remote feeding voltage between A and B wires of the DSL port.

RO	RO	RO
INTEGER		T
Automatic		

RF Voltage (a_gnd) [V]

config go "/Remote Feeding Control/<RF Port No.>/RF Port Configuration"
config "RF Voltage (a_gnd) [V]"

This object shows the current remote feeding voltage between wire A of the DSL port and GND.

RO	RO	RO
INTEGER		T
Automatic		

RF Voltage (b_gnd) [V]

config go "/Remote Feeding Control/<RF Port No.>/RF Port Configuration"
config "RF Voltage (b_gnd) [V]"

This object shows the current remote feeding voltage between wire B of the DSL port and GND.

RO	RO	RO
INTEGER		T
Automatic		

5 Examples and Use Cases

This chapter provides examples and use cases for common operation tasks. They are typical for setting up services, enabling interfaces etc.

Each use case offers a short description that helps to understand the example. The values that are required to be configured for the intended operation are summarized, followed by a list of CLI commands to achieve the wanted configuration.

The intention is to use the examples as a reference that can be copied from this document directly to the CLI or into a new document, where the examples can be edited and extended.

A typical example looks like this:

```
$>  config go /somewhere_in_the_CLI
$>  config set any_variable1 any_valueA
$>  config set any_variable2 any_valueB
```

The first “column” always shows the CLI prompt in short form ($>) to indicate a new CLI command. The command follows the prompt in the second column. It is easy to copy the ccommands from this document with the Acrobat Reader: Press the <ALT> key when you use the Select tool () to enable rectangle selection:

```
$> config go /somewhere_in_the_CLI
$> config set any_variable1 any_valueA
$> config set any_variable2 any_valueB
```

5.1 Configuring the Local Management Port

The device comes with three dedicated management ports, one of which is for local management access (F interface), a second one for remote management access (Q interface) and the third one just forwards remote management access to other IP addresses.

This chapter describes the IP configuration of the local management port (named "Local").

The "Local" port is an F interface and, as such, always has a fixed IPv4 address. It is possible to configure the interface to automatically provide IPv4 addresses to connected devices (via DHCP server). IPv6 for F ports is disabled in the factory default configuration because it is usually not required, but can be enabled.

The operator has to be logged on to the device as a user within the group "admin".

NOTE: The CLI of the device allows abbreviations of individual elements of the paths to variables as long as those abbreviations are unique. In the examples below, the path always contains the full port name ("Local <...>") which is composed of the port label and the port name. The examples below use the port label only, which is a valid and unique abbreviation of the full port name.

5.1.1 Enabling the Local Port

This step describes how the "Local" port is enabled and set up for auto-negotiation.

At the end of this use case the following settings are active:

Item	Value	Alternative Value(s)
Port Speed	Automatic	"10 Full Duplex", "10 Half Duplex", "100 Full Duplex", "100 Half Duplex"
Admin Status	Enabled	Disabled

```
$> config go "/Administration/Port and IP Configuration/Local/Edit"
$> config set "Port Speed" "Automatic"
$> config set "Admin Status" Enabled
```

5.1.2 Configuring a Fixed IPv4 Address

This step describes how the default IPv4 address of the Local port is changed. The IPv4 address and netmask are changed simultaneously in a form group.

Additionally, DHCP server support will be enabled for this port.

At the end of this use case the following settings are active:

Item	Value	Alternative Value(s)
IPv4 Address	192.168.0.101	any valid IPv4 unicast address
IPv4 Network Mask	255.255.255.0	any valid IPv4 netmask
IPv4 Address Assignment	"Provide DHCP Server"	Manual

```
$> config go "/Administration/Port and IP Configuration/Local/Edit"
$> config set "IPv4 Address Assignment" "Provide DHCP Server"
$> config go "Change IPv4 Address"
$> config set "New IPv4 Address" 192.168.0.101
$> config set "New IPv4 Netmask" 255.255.255.0
$> config do "Change IPv4 Address"
$> yes
```

5.1.3 Disabling IPv6 Support

F interfaces are used as local management interfaces. As long as all operating systems used on service laptops ship with IPv4 support, there is usually no need to have IPv6 enabled on the local management interface (if need be, the procedure to configure IPv6 is the same as for the remote management port).

For this reason, this step describes how to disable IPv6 support explicitly on the "Local" port.

At the end of this use case the following settings are active:

Item	Value	Alternative Value(s)
IPv6 Support	Disabled	Enabled

```
$>  config go "/Administration/Port and IP Configuration/Local/Edit"
$>  config set "IPv6 Support" Disabled
```

5.1.4 Verifying the Network Configuration

This step describes how the Port and IP settings of the "Local" port can be verified.

```
$>  config go "/Administration/Port and IP Configuration/Local/Edit"
$>  config
```

```
-- Edit
  Port Label:                 Local
* Port Name:                    < ... >
  HW MAC Address:                00:1E:16:00:26:CE

  Link Settings
* Admin Status:                 Enabled
* Port Speed:                   Automatic
  Autonegotiation:              On
  Link Status:                  up 100MBit full duplex
  Packet Counter:               RX:113806317   TX:60737475
* Enable SNMP Link Up_Down Traps: Enabled

  Type and VLAN Settings
  Interface Type:               Local Mgmt (F)
  Management VLAN Setting:      None

  IPv4 Settings
* IPv4 ICMP Support:            Enabled
* IPv4 Address Assignment:      Provide DHCP Server
  IPv4 Address:                 192.168.0.101
  IPv4 Network Mask:            255.255.255.0
F Change IPv4 Address

  IPv6 Settings
* IPv6 Support:                 Disabled
```

5.2 Configuring the Remote Management Port

The device comes with three dedicated management ports, one of which is for local management access (F interface), a second one for remote management access (Q interface) and the third one just forwards remote management access to other IP addresses.

This chapter describes the IP configuration of the remote management port (named "North").

The "North" port is a Q interface and, as such, will be connected to a larger management network.

Automatic as well as manual IP address configuration for IPv4 and IPv6 is supported.

The operator has to be logged on to the device as a user within the group "admin".

NOTE: The CLI of the device allows abbreviations of individual elements of the paths to variables as long as those abbreviations are unique. In the examples below, the path always contains the full port name ("North <...>") which is composed of the port label and the port name. The examples below use the port label only, which is a valid and unique abbreviation of the full port name.

5.2.1 Enabling the North Port

This step describes how the "North" port is enabled and set up for autonegotiation.

At the end of this use case the following settings are active:

Item	Value	Alternative Value(s)
Port Speed	Automatic	"10 Full Duplex", "10 Half Duplex", "100 Full Duplex", "100 Half Duplex"
Admin Status	Enabled	Disabled

```
$>  config go "/Administration/Port and IP Configuration/North/Edit"
$>  config set "Port Speed" Automatic
$>  config set "Admin Status" Enabled
```

5.2.2 Configuring a Fixed IPv4 Address and Default Gateway

This step describes how the default IPv4 address of the "North" port is changed. The IPv4 address, netmask and default gateway are changed simultaneously in a form group.

NOTE: The IPv4 address can only be changed if DHCP support has been disabled in advance.

At the end of this use case the following settings are active:

Item	Value	Alternative Value(s)
IPv4 Address Assignment	Manual	"From DHCP Server", "From DHCP Server/Auto IP"
IPv4 Address	10.10.0.101	any valid IPv4 unicast address
IPv4 Network Mask	255.255.255.0	any valid IPv4 netmask
IPv4 Default Gateway	10.10.0.1	any valid IPv4 unicast address

```
$>  config go "/Administration/Port and IP Configuration/North/Edit"
$>  config set "IPv4 Address Assignment" "Manual"
$>  config
$>  config go "Change IPv4 Address"
$>  config set "New IPv4 Address" 10.10.0.101
$>  config set "New IPv4 Netmask" 255.255.255.0
$>  config set "New IPv4 Default Gateway" 10.10.0.1
```

```
$> config do "Change IPv4 Address"
$> yes
```

5.2.3 Enabling IPv6 Support

Q interfaces are intended to be connected to larger management networks for which IPv6 support might be required. This step describes how to activate IPv6 support for the "North" port.

At the end of this use case the following settings are active:

Item	Value	Alternative Value(s)
IPv6 Support	Enabled	Disabled

```
$> config go "/Administration/Port and IP Configuration/North/Edit"
$> config set "IPv6 Support" Enabled
```

5.2.4 Setting up IPv6 Automatic Address Configuration

IPv6 comes with built-in support for automatic address configuration without the need to run DHCP. The device is able to listen to IPv6 Router Advertisement messages to automatically assign IPv6 addresses to its interfaces, if configured to do so.

This step describes how the IPv6 automatic address configuration is activated on the "North" port.

At the end of this use case the following settings are active:

Item	Value	Alternative Value(s)
IPv6 Router Advertisements	Listening	Ignoring
IPv6 Autoconfiguration	Enabled	Disabled
IPv6 Gateway Autoconfiguration	Enabled	Disabled

```
$> config go "/Administration/Port and IP Configuration/North/Edit"
$> config set "IPv6 Router Advertisements" Listening
$> config set "IPv6 Autoconfiguration" Enabled
$> config set "IPv6 Gateway Autoconfiguration" Enabled
```

5.2.5 Manually Adding IPv6 Addresses

IPv6 allows multiple IPv6 addresses per interface. Additionally, automatic IPv6 address configuration and manual IPv6 address assignment can be mixed.

This step describes how to manually assign a persistent IPv6 address to the "North" port. The IPv6

address and prefix length are simultaneously specified in a form group.

At the end of this use case the following settings are active:

Item	Value	Alternative Value(s)
IPv6 Address	2001::0a0a	any valid IPv6 unicast address
Prefix Length	64	any valid IPv6 address prefix length

```
$>  config go "/Administration/Port and IP Configuration/North/Edit"
$>  config go "Add IPv6 Address"
$>  config set "New IPv6 Address" 2001::0a0a
$>  config set "New Prefix Length" 64
$>  config do "Add IPv6 Address"
```

5.2.6 Verifying the Network Configuration

This step describes how the Port and IP settings of the "North" port can be verified.

```
$>  config go "/Administration/Port and IP Configuration/North/Edit"
$>  config
```

```
-- Edit
  Port Label:                 North
* Port Name:                   < ... >
  HW MAC Address:               00:1E:16:00:26:CF

  Link Settings
* Admin Status:                 Enabled
* Port Speed:                   Automatic
  Autonegotiation:              On
  Link Status:                  Down
  Packet Counter:               RX:0   TX:0
* Enable SNMP Link Up_Down Traps: Enabled

  Type and VLAN Settings
  Interface Type:               Remote Mgmt (Q)
  Management VLAN Setting:      None
F Change VLAN Settings

  IPv4 Settings
* IPv4 ICMP Support:            Enabled
* IPv4 Address Assignment:      Manual
  IPv4 Address:                 10.10.0.101
  IPv4 Network Mask:            255.255.255.0
F Change IPv4 Address
```

```
 IPv6 Settings
* IPv6 Support:                  Enabled
* IPv6 Router Advertisements:    Listening
* IPv6 Autoconfiguration:        Enabled
* IPv6 Gateway Autoconfiguration: Enabled
* IPv6 Accept Redirects:         Disabled
          "Address"   "PfxLen" "Type"                    "Status"    "Flags" "Source"
> 2001::A0A: "2001::A0A" "64"     "IPv6 Global Unicast Address" "Preferred" ""      "Manual"
F Add IPv6 Address
```

5.3 Configuring the Forwarding Management Port

The device comes with three dedicated management ports, one of which is for local management access (F interface), a second one for remote management access (Q interface) and the third one just forwards remote management access to other IP addresses.

This chapter describes the IP configuration of the forwarding management port (named "South").

The "South" port is only a forwarding port that forwards network traffic from the "North" port that is not destined to the "North" port. The forwarding happens on the lower layers of the networking stack, therefore the interface needs no IP configuration at all. Only "physical" port parameters can be configured.

The operator has to be logged on to the device as a user within the group "admin".

NOTE: The CLI of the device allows abbreviations of individual elements of the paths to variables as long as those abbreviations are unique. In the examples below, the path always contains the full port name ("South <...>") which is composed of the port label and the port name. The examples below use the port label only, which is a valid and unique abbreviation of the full port name.

5.3.1 Enabling the South Port

This step describes how the "South" port is enabled and set up for autonegotiation.

At the end of this use case the following settings are active:

Item	Value	Alternative Value(s)
Port Speed	Automatic	"10 Full Duplex", "10 Half Duplex", "100 Full Duplex", "100 Half Duplex"
Admin Status	Enabled	Disabled

```
$> config go "/Administration/Port and IP Configuration/South/Edit"
$> config set "Port Speed" Automatic
$> config set "Admin Status" Enabled
```

5.3.2 Verifying the Network Configuration

This step describes how the Port and IP settings of the "South" port can be verified.

```
$>  config go "/Administration/Port and IP Configuration/South/Edit"
$>  config
```

```
-- Edit
  Port Label:                 South
* Port Name:                   < ... >
  HW MAC Address:               00:00:00:00:00:00

  Link Settings
* Admin Status:                 Enabled
* Port Speed:                   Automatic
  Autonegotiation:              On
  Link Status:                  Down
  Packet Counter:               RX:0   TX:0
* Enable SNMP Link Up_Down Traps: Enabled

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

5.4 Improving Networking Security

This use case explains how the networking security can be improved. Here, the operator will see how to allow SNMPv3 only, disable ICMP for IPv4 and disable HTTP access.

Other measures that further enhance the networking security cannot generally be advised because they depend on the interaction of the device with users and other computers in the network. Among those measures are disabling unused network ports, disabling unused access methods, choosing cryptographically strong passwords and disabling unsafe file transfer methods like FTP.

The operator has to be logged on to the device as a user within the group "admin".

5.4.1 Restricting SNMP access to SNMPv3

The device comes with support for SNMP versions v2c (community-name based security) and v3 (USM/VACM with authentication and encryption). SNMPv2c is generally considered unsafe because the community names used in successful communications can easily be spied out by simple wire tapping.

This step therefore describes how to explicitly disable SNMPv2c support.

At the end of this use case, the following settings will be active:

Item	Value	Alternative Value(s)
SNMP Version	"SNMP V3"	"SNMP V2c", "SNMP V2c, V3"

```
$>  config go "/Administration/User and Access Administration/SNMP Configuration/"
```

```
$> config set "SNMP Version" "SNMP V3"
```

NOTE: This command has an immediate effect. SNMPv2 access to the device will be blocked directly after executing this command.

5.4.2 Disabling ICMP for IPv4

The device comes with a full network stack, including support for the ICMP protocol. This protocol is very useful for diagnosing networking problems because it provides a simple "echo" mechanism to ping other computers in the network and also includes error messages as a reaction to failed connection attempts. However, attackers find ICMP useful as well because it allows them to discover network topologies, available hosts, open ports and operating system versions easily.

The ICMP protocol is an integral part of IPv6. Router Advertisements as well as the Neighbour Discovery Protocol use ICMPv6 messages and, therefore, IPv6 will not function if ICMPv6 is disabled. For this reason, the device offers no possibilities to disable ICMPv6 support other than by disabling IPv6 completely.

Each management port with IPv4 capabilities can be configured to drop all incoming and outgoing IPv4 ICMP messages. The example below will disable ICMP support for the "North" port (remote management interface) because that port will usually be connected to a larger management network. ICMP is usually not considered a large risk for local management ports because physical access to the device is needed to connect to that port (although ICMP can be disabled for local management ports as well).

NOTE: Disabling ICMP support for IPv4 will restrict the functionality of the network diagnostics in the menu "/Administration/Diagnostics".

At the end of this use case, the following settings will be active:

Item	Value	Alternative Value(s)
North: IPv4 ICMP Support	Disabled	Enabled

```
$> config go "/Administration/Port and IP Configuration/North/Edit/"
$> config set "IPv4 ICMP Support" Disabled
```

5.4.3 Disabling HTTP Access

The device has built-in support for the HTTPS protocol. This protocol has advantages over the simpler HTTP protocol in that it provides server authentication as well as full encryption of the content. A drawback is the certificate management required for HTTPS to actually be secure.

The device comes with pre-installed HTTPS Server Certificates that will definitely cause certificate validation errors in the browser because of two reasons: firstly because the certificate issuer is unknown to the browser, and secondly because the certificate is issued for the wrong server address.

It is therefore suggested that the operator obtains a HTTPS Server Certificate that matches the device configuration and installs that before disabling HTTP support completely.

The device needs to know both, the server certificate as well as the private key belonging to that certificate. The private key must not be protected by a passphrase, because the device has to be able to use the private key without manual intervention by an operator.

Both data items (certificate and key) must be stored in different, PEM-encoded files (suitable for the

OpenSSL library) on the "Configuration Store" server. It is assumed that the "Configuration Store" server is already correctly configured, the key file is stored on the server as "keys/https_cert.key", and the certificate is stored on the server as "keys/https_cert.crt".

NOTE: HTTPS access must have been disabled before the certificate or the key can be uploaded. In the example below, the web access is disabled completely to avoid the temporary vulnerability.

```
$> config go "/Administration/User and Access Administration/Web Configuration/"
$> config set "Web Access" Disabled
$> config set "Web Access Mode" HTTP
```

Next, the certificate will be downloaded from the "Configuration Store" server.

```
$> config set "Download File Name" "keys/https_cert.crt"
$> config do "Load Server Certificate"
```

It is now required to wait until the file transfer has completed. The current file transfer status can be retrieved by monitoring the variable "File Transfer State".

```
$> config "File Transfer State"
```

The file transfer has successfully completed when this variable holds the text "Transfer Complete", other values indicate ongoing progress or failure conditions. This step may need to be repeated until the file download has finished.

Next, the corresponding private key file will be downloaded from the "Configuration Store" server.

```
$> config set "Download File Name" "keys/https_cert.key"
$> config do "Load Private Key"
```

It is now required to wait until the file transfer has completed. The current file transfer status can be retrieved by monitoring the variable "File Transfer State".

```
$> config "File Transfer State"
```

The file transfer has successfully completed when this variable holds the text "Transfer Complete", other values indicate ongoing progress or failure conditions. This step may need to be repeated until the file download has finished.

Next, the new certificate and private key will be reviewed. This step is required to be certain that the correct certificate and key files have been downloaded from the "Configuration Store" server.

```
$> config
```

```
-- Web Configuration
* Web Access:              Disabled
```

```
* Web Access Mode:          HTTP
  Server Cert Parse Status: Ok
  Server Key Parse Status:  Ok

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

  Server Certificate Upload

  Server Type:              Configuration Store
  Server URI:               sftp://arc@192.168.1.1/config_files
  File Transfer State:      Transfer Complete
* Download File Name:       keys/https_cert.key
+ [Load Server Certificate]
+ [Load Private Key]
```

NOTE: The certificate information shown in the sample output above reflects the built-in server certificate and **not** the information that would be expected from a newly downloaded certificate.

It is important to inspect the following variables carefully:

"Server Cert Parse Status" indicates errors while parsing the certificate file.

"Server Key Parse Status" indicates errors while parsing the private key file.

"Server Cert Key Status" indicates whether certificate and private key match.

"Server Cert Subject" should match the IP configuration of the device.

"Server Cert Issuer" should match the certificate issuer information.

"Server Cert Valid From" should be a date/time in the past.

"Server Cert Valid Till" should be a date/time in the future.

If the information in all those variables has been verified, the final step is to switch to HTTPS-only operation and re-enable web access.

```
$>  config set "Web Access Mode" HTTPS
$>  config set "Web Access" Enabled
```

After all those steps have successfully been executed, the device should be reachable on the default HTTPS port. Access to the HTTP port will be redirected to the HTTPS port so that only secure connections can be established.

5.5 Adding a User and Defining a Password

This use case describes how to add a new user, set a user group and set a new password for it.

Item	Value	Alternative Value(s)
User Name	arctest	any name allowed
User Group	user	admin, guest
Status	Enabled	Disabled
Password	*normally not visible, here: 1Qayxsw2*	

The operator has to be logged on to the device as a user within the group "admin".

5.5.1 Creating a new User Account

```
$> config go "/Administration/User and Access Administration/Users and Passwords/Add New Account/Create Account"
$> config set Username arctest
$> config set Password 1Qayxsw2
$> config set "User Group" user
$> config do "Create Account"
```

After this step the new user is created and the account is enabled.

Instead of using **config set** for setting the passwords one can also use **config hidden** to allow hidden entry of the passphrase. The characters entered at the prompt "Enter password:" will **not** be displayed then.

```
$> config go "/Administration/User and Access Administration/Users and Passwords/Add New Account/Create Account"
$> config hidden "Password"
```

```
Enter password:
Retype password:
```

5.5.2 Verifying the Settings

After creating the new user there is a new entry in the user table which should be reviewed in the next step.

```
$> config go "/Administration/User and Access Administration/Users and Passwords"
$> config
```

```
-- Users and Passwords
* TACACS+:              Disabled
```

```
* Shared Secret:          public
* IP Address:            0.0.0.0
* TACACS+ Connect Timeout: 5
* TACACS+ Receive Timeout:  5
      "User Name" "User Group"  "Status"
> admin:       "admin"        "admin"      "Enabled"
> arctest:     "arctest"      "user"       "Enabled"
> Add New Account
```

Please note that the given password is not visible and that only the User Group is changeable by the currently logged in "admin". A log off and re-login as the new user shows that the new user can change his own password only. That is because of the access restrictions for users in the group "user".

5.6 Replacing the Default Admin User

The device comes with a default user named "admin" in the factory default configuration that has full access permissions.

If security guidelines require that the default admin user be renamed, this can be achieved by creating a new user with full access permissions and deleting the default admin user.

NOTE: The device **always** requires to have at least one active user with "admin" permissions. This last user cannot be disabled or deleted, before another user with "admin" permissions has been created and enabled.

The operator has to be logged on to the device as a user within the group "admin".

5.6.1 Creating a new Admin User

This step describes how a new admin user is created.

At the end of this use case, the following user will have been created:

Item	Value	Alternative Value(s)
Username	Admin_T	any other valid user name
Password	5678_ADM	any other valid device password
User Group	admin	guest or user
Status	Enabled	Disabled

```
$> config go "/Administration/User and Access Administration/Users and Passwords/Add New Account/Create Account"
$> config set "Username" "Admin_T"
$> config set "Password" "5678_ADM"
$> config set "User Group" admin
$> config set "Status" Enabled
$> config do "Create Account"
```

5.6.2 Verifying the User Creation

This step uses the "config" command to view the menu page containing the user table to verify that the new user has been created and is enabled.

```
$>  config go ../..
$>  config
```

```
-- Users and Passwords
* Authentication Priority: Local User DB / TACACS+
* TACACS+:                 Disabled
* TACACS+ Server:          0.0.0.0
  IP Description:          IPv4 Invalid Address
* TACACS+ Shared Secret:   public
* TACACS+ Connect Timeout: 5
* TACACS+ Receive Timeout: 5
          "User Name" "User Group" "Status"
> admin:   "admin"     "admin"      "Enabled"
> arctest: "arctest"   "user"       "Enabled"
> Admin_T: "Admin_T"   "admin"      "Enabled"
> Add New Account
```

5.6.3 Deleting the Default Admin User

In this step, the default admin user named "admin" will be deleted.

```
$>  config do "admin/Delete Account"
$>  yes
```

5.7 Automatic Date/Time Setting Using NTP

This use case describes how to configure the time zone for the device and how to enable NTP for automatic date/time management.

At the end of this use case the following settings are active:

Item	Value	Alternative Value(s)
Timezone	GMT+1	GMT-12 to GMT+14
NTP Support	Enabled	Disabled
NTP Time Server	78.46.85.230	any valid IPv4 or IPv6 unicast address
NTP Protocol Version	NTPv4	NTPv3

The operator has to be logged on to the device as a user within the group "admin".

```
$>  config go "/Administration/Date and Time Settings"
$>  config set "Time Zone" GMT+1
$>  config set "NTP Support" Enabled
$>  config go "NTP Server Setup"
$>  config do "Add NTP Server"
$>  config go "0.0.0.0/Edit NTP Server"
$>  config set "Server Address" 78.46.85.230
$>  config set "Protocol Version" NTPv4
$>  config set "Admin Status" Enabled
```

After this step the new NTP server is configured and enabled. The device will start to contact the server and displays that in the so-called "Reachability Register".

To verify the reachability and usage of the (new) NTP server, follow the steps in next chapter.

5.7.1 Verifying the Settings

After defining a new NTP server, it is required to verify connectivity to that server. The value in the "Reachability" table column is a shift register indicating success (1) or failure (0) of the last 8 successive communication attempts with the NTP server. Only servers for which the "Admin Status" is "Enabled" are queried. A working NTP server has a "Reachability" composed of at least some 1's.

NOTE: NTP servers are queried in intervals of 60 seconds, so it may take several minutes until a sufficiently high number of queries succeeded for the NTP server to be assumed usable.

If one of the NTP servers is considered usable by the NTP server selection algorithm, its "Server Status" value changes to "Selected" and the variable "NTP Status" changes to "Synchronized".

```
$>  config go "/Administration/Date and Time Settings"
$>  config
```

```
-- Date and Time Settings
  Date:             2013-02-14
  Time:             09:48
* Time Zone:      GMT+1
* NTP Support: Enabled
  NTP Status:   Synchronized
                    "Server Address" "Protocol Version" "Admin Status" "Server Status" "Stratum" "Reachability"
"Delay [ms]" "Offset [ms]" "Jitter [ms]"
> 78.46.85.230:  "78.46.85.230"    "NTPv4"              "Enabled"        "Selected"       "2"          "01111110"
"21.238"       "0.891"         "15.263"
> NTP Server Setup
```

5.8 Manually Setting Date and Time

This use case describes how to manually configure time, time zone and date, in contrast to using NTP for date/time management.

At the end of this use case the following settings are active:

Item	Value	Alternative Value(s)
NTP Support	Disabled	NTP must be disabled to allow manual settings
Date	2003-10-06	any other date in YYYY-MM-DD format
Time	13:36	any other time in HH:MM 24h-format
Timezone	GMT+1	GMT-12 to GMT+14

The operator has to be logged on to the device as a user within the group "admin".

```
$> config go "/Administration/Date and Time Settings"
$> config set "Time Zone" GMT+1
$> config set "NTP Support" Disabled
$> config set "Date" 2003-10-06
$> config set "Time" 13:36
```

After this step my daughter's birthday is configured as current date and time on the device.

5.9 Ping Connectivity Test

This use case describes how to test management network connectivity using the "ping" utility. Other connectivity diagnostics (traceroute) are also available.

At the end of this use case the following settings are active:

Item	Value	Alternative Value(s)
Test Server IP Address	192.168.1.1	any valid IPv4 or IPv6 unicast address

The operator has to be logged on to the device as a user within the group "user" or "admin".

```
$> config go /Administration/Diagnostics
$> config set IP-Address 192.168.1.1
$> config do Ping
```

The output of the ping command can be seen in the variable "Command Output". The diagnostic tools may take some time (~30 seconds) before they produce some output, so the following procedure may need to be repeated.

```
$> config "Command Output"
```

This command may result in the following output.

```
"Executing ping:
PING 192.168.1.100 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=127 time=1.372 ms
64 bytes from 192.168.1.1: seq=1 ttl=127 time=0.374 ms
64 bytes from 192.168.1.1: seq=2 ttl=127 time=0.385 ms
64 bytes from 192.168.1.1: seq=3 ttl=127 time=0.368 ms
--- 192.168.1.100 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.368/0.674/1.372 ms
"
```

5.10 Transferring Device Logfiles to a Storage Server

This use case describes how to transfer the device logfile from the device to an external storage server.

5.10.1 Configuring the Storage Server

This step describes the configuration of access data and transfer protocol for the "Logfile Store" server.

NOTE: This needs to be done once only. When the configuration of the "Configuration Store" server is already done, this step can be skipped.

At the end of this step the following settings are active:

Item	Value	Alternative Value(s)
Transfer Protocol	SFTP	TFTP
SFTP Server IP	192.168.0.6	any valid IPv4 or IPv6 unicast address
SFTP Server Directory	/log_files	destination path at the SFTP server
SFTP Username	arc	login name for the server
SFTP Password	!qayxsw2	login password for the server

The operator has to be logged on to the device as a user within the group "admin".

The following commands configure the "Logfile Store" external server.

```
$> config go "/Administration/User and Access Administration/Logfile Store/Edit"
$> config set "Transfer Protocol" SFTP
$> config set "Server IP" 192.168.0.6
$> config set "Server Directory" log_files
$> config set "User Name" arc
$> config set Password !qayxsw2
```

Instead of using **config set** for setting passwords one can also use **config hidden** to allow hidden entry of the passphrases. The characters entered at the prompt "Enter password:" will **not** be displayed.

```
$>  config go "/Administration/User and Access Administration/Logfile Store/Edit"
$>  config hidden "Password"
```

```
Enter password:
Retype password:
```

5.10.2 Uploading the Logs to the Storage Server

This step sets the name of the file to be uploaded and initiates the upload to the external storage server.
NOTE: The file extension ".log" is automatically appended to the file name if omitted.

```
$>  config go "/Log View/"
$>  config set "Logfile Name" AX_logs
$>  config do "Upload to 'Logfile Store'"
```

5.10.3 Verification

Use the "config" command after a few seconds to monitor the file upload progress. For a successfully completed transfer, the variable "File Transfer State" must have the value "Transfer Complete", other values indicate ongoing progress or failure conditions. This step may need to be repeated until the file upload has finished.

```
$>  config go "/Log View/"
$>  config
```

```
-- Save Logfile
  Server Type:         Logfile Store
  Server URI:          sftp://arc@192.168.0.6/log_files
  File Transfer State: Transfer Complete
* Logfile Name:        AX_logs
+ [Upload to 'Logfile Store']
```

In case the variable "File Transfer State" holds the text "Remote file already exists.", the transfer failed and the variable "Logfile Name" needs to be changed to a unique file name.

5.11 Transferring Configuration Snapshots to a Storage Server

This use case describes how to transfer configuration snapshots from the device to an external storage server and vice versa.

5.11.1 Configuring the Storage Server

This step describes the configuration of access data and transfer protocol for the "Configuration Store" server.

NOTE: This needs to be done once only. When the configuration of the "Configuration Store" server is already done, this step can be skipped.

At the end of this use case, the following settings will be active:

Item	Value	Alternative Value(s)
Transfer Protocol	SFTP	TFTP
SFTP Server IP	192.168.1.1	any valid IPv4 or IPv6 unicast address
SFTP Server Directory	/config_files	destination path at the SFTP server
SFTP Username	arc	login name for the server
SFTP Password	!qayxsw2	login password for the server

The operator has to be logged on to the device as a user within the group "admin".

```
$> config go "/Administration/User and Access Administration/Configuration Store/Edit"
$> config set "Transfer Protocol" SFTP
$> config set "Server IP" 192.168.1.1
$> config set "Server Directory" config_files
$> config set "User Name" arc
$> config set Password !qayxsw2
```

Instead of using **config set** for setting passwords one can also use **config hidden** to allow hidden entry of the passphrases. The characters entered at the prompt "Enter password:" will **not** be displayed.

```
$> config go "/Administration/User and Access Administration/Logfile Store/Edit"
$> config hidden "Password"
```

```
Enter password:
Retype password:
```

5.11.2 Uploading the Snapshot to the Storage Server

In this step, a snapshot of the current configuration is created and renamed to "Config upload". The upload to the external storage server is initiated.

```
$>  config go "/Administration/Configuration Management"
$>  config do "Current Configuration/Save Configuration"
$>  config go "Config backup"
$>  config set Name "Config upload"
$>  config do "Upload to Server"
$>  config go ".."
```

Use the "config" command after a few seconds to monitor the file upload progress. For a successfully completed transfer, the variable "File Transfer State" must have the value "Transfer Complete", other values indicate ongoing progress or failure conditions. This step may need to be repeated until the file upload has finished.

```
$>  config
```

```
-- Configuration Management
                          Name                        Date
> Current Configuration:        Current Configuration        2013/02/07 12:20:56
> Factory Default Configuration: Factory Default Configuration --
> Config upload:                Config upload                2013/02/07 12:10:21

  Server Type:         Configuration Store
  Server URI:          sftp://arc@192.168.1.1/config_files
  File Transfer State: Transfer Complete
* Config File Name:
+ [Download from Server]
```

5.11.3 Deleting old Configuration Snapshots

After the configuration snapshot has successfully been transferred to the storage server, it can be deleted on the device itself (to save some space).

```
$>  config go "/Administration/Configuration Management"
$>  config do  "Config upload/Delete Configuration"
$>  config
```

5.12 Immediate System Reset

This use case describes how an instantaneous system reset is performed. It is also possible to plan a system reset that is automatically performed by the device at a future time (up to 30 days ahead).

At the end of this use case the following settings are active:

Item	Value	Alternative Value(s)
Reset Mode	Immediate Reset	At Specified Time

The operator has to be logged on to the device as a user within the group "admin".

```
$> config go "/Administration/Reset System/"
$> config set "Reset Mode" "Immediate Reset"
$> config do "Start Reset"
$> yes
```

The Device will be reboot immediately.

5.13 Scheduled Reset

This use case describes how an automatic system reset at a future time is configured.

At the end of this use case the following settings are active:

Item	Value	Alternative Value(s)
Reset Mode	At Specified Time	Immediate Reset
Reset Date	2013-02-21	any date in the format YYYY-MM-DD
Reset Time	15:30	00:00 to 23:59 in the format HH:MM

The operator has to be logged on to the device as a user within the group "admin".

```
$> config go "/Administration/Reset System"
$> config set "Reset Mode" "At Specified Time"
$> config set "Reset Date" 2013-02-21
$> config set "Reset Time" 15:30
$> config do "Start Reset"
$> yes
```

The Device will be reboot at the scheduled time.

5.14 Reset to Factory Defaults

This use case describes how to reset all settings of the device to their factory defaults. **Please note that the IP configuration of the management interfaces will also be reset!**

At the end of this use case the following settings are active:

Item	Value	Alternative Value(s)
MGMT IP Config	Overwrite	Keep Current
SNMP Trap Targets	Overwrite	Keep Current
SNMPv2 Communities	Overwrite	Keep Current
SNMPv3 User	Overwrite	Keep Current
SSH keys	Overwrite	Keep Current
User Accounts	Overwrite	Keep Current
All Other Configuration	Overwrite	Keep Current

The operator has to be logged on to the device as a user within the group "admin".

```
$> config go "/Administration/Configuration Management/Factory Default Configuration/Apply"
$> config set "MGMT IP Config" Overwrite
$> config set "SNMP Trap Targets" Overwrite
$> config set "SNMPv2 Communities" Overwrite
$> config set "SNMPv3 User" Overwrite
$> config set "SSH keys" Overwrite
$> config set "User Accounts" Overwrite
$> config set "All Other Configuration" Overwrite
$> config do "Apply Configuration Now"
$> yes
```

Alternatively it is also possible to specify a default behaviour for all configuration components using the menu item "Preset Configuration Components".

```
$> config go "/Administration/Configuration Management/Factory Default Configuration/Apply"
$> config set "Preset Configuration Components" Overwrite
$> config do "Apply Configuration Now"
$> yes
```

The device will be reboot immediately and start up with the factory default configuration.

5.15 Configure Alarm Settings

This use case describes briefly how to operate the alarm management of the device.

5.15.1 Setting the Severity of a Digital Alarm

This use case will set the "Dying Gasp Indication" alarm (a digital alarm) to be ignored.

At the end of this use case the following settings are active:

Item	Value	Alternative Value(s)
Dying Gasp Indication: Severity	Ignore	Error, Warning

The operator has to be logged on to the device as a user within the group "admin".

```
$> config go "/Alarm Management/System Alarms/Group Details"
$> config set "Dying Gasp Indication/Settings/Alarm Severity" Ignore
```

5.15.2 Display and Change Thresholds of an Analog Alarm

This use case describes how to view and configure thresholds for an analog alarm. The example uses the "Device Temperature" alarm which supports overrun and underrun thresholds.

NOTE: Some analog alarms support either overrun or underrun thresholds, but not both.

At the end of this use case, the following settings are active:

Item	Value	Alternative Value(s)
Overrun Warning Level	55°C	min: 40°C, max:70°C
Overrun Error Level	65°C	min: 40°C, max:85°C
Underrun Warning Level	10°C	min: -50°C, max:10°C
Underrun Error Level	5°C	min: -50°C, max:10°C

The operator has to be logged on to the device as a user within the group "admin".

```
$> config go "/Alarm Management/System Alarms/Group Details/Device Temperature/Settings"
$> config set "Overrun Warning Level" 55
$> config set "Overrun Error Level" 65
$> config set "Underrun Warning Level" 10
$> config set "Underrun Error Level" 5
```

Please verify the changed threshold settings with the "config" command. The menu item "Value" displays the current device temperature.

5.15.3 Configuring SNMP Notification for an Alarm

This use case will disable sending SNMP Traps for the "NTP Status" alarm.

At the end of this use case the following settings are active:

Item	Value	Alternative Value(s)
NTP Status: SNMP Notification	No Notification	SNMP Trap

The operator has to be logged on to the device as a user within the group "admin".

```
$> config go "/Alarm Management/System Alarms/Group Details"
$> config set "NTP Status/SNMP Notification" "No Notification"
```

5.15.4 Acknowledging a Single Alarm

This use case will acknowledge the "Device Temperature" alarm.

NOTE: This use case will fail if the "Device Temperature" alarm is not active at the time of execution.

The operator has to be logged on to the device as a user with at least "user" access permissions.

```
$> config go "/Alarm Management/System Alarms/Group Details"
$> config do "Device Temperature/Acknowledge"
```

5.15.5 Acknowledging all Group Alarms

This use case will acknowledge all alarms in the alarm group "System Alarms" at once.

NOTE: This use case will fail if all alarms in the alarm group "System Alarms" are inactive at the time of execution.

The operator has to be logged on to the device as a user with at least "user" access permissions.

```
$> config go "/Alarm Management/System Alarms/"
$> config do "Acknowledge Group Alarms"
$> yes
```

5.15.6 Acknowledging all Alarms

This use case will acknowledge all alarms known to the device at once.

The operator has to be logged on to the device as a user with at least "user" access permissions.

```
$> config go "/Alarm Management"
$> config do "Acknowledge All"
$> yes
```

5.15.7 View Active Alarm List

A list of all alarms with an active alarm condition is available in a separate menu. That menu gives a quick overview of the device's operational state and also allows to acknowledge individual alarms or all alarms at once.

The content of the active alarm list is dynamically calculated and indexed by an integer number.

The following commands show the active alarm list:

```
$> config go "/Alarm Management/Active Alarm List/"
$> config
```

The following command acknowledges the first alarm in the active alarm list. The active alarm list is dumped before and after the alarm acknowledgement to be able to observe the difference.

NOTE: This procedure may fail if there is no active alarm.

The operator has to be logged on to the device as a user with at least "user" access permissions.

```
$> config go "/Alarm Management/Active Alarm List/"
$> config
$> config do "1/Acknowledge"
$> config
```

Please observe that the first item in the active alarm list has changed its position in the list (the list is ordered by the alarm severity in the "State" column.

5.16 Adding an SNMPv3 User and Setting Authentication Parameters

This use case describes how to add an SNMPv3 user, how to set the corresponding access permissions and the authentication parameters.

At the end of this use case, an SNMP user with the following settings will have been created:

Item	Value	Alternative Value(s)
User Name	Operator	any unique name (ASCII characters) allowed
Access Level	Service	Administrator, Monitor
Authentication Type	HMAC-MD5	HMAC-SHA, No Authentication
Authentication Passphrase	1Qayxsw2	see manual "Rules for Passwords"
Encryption Type	AES Encryption	DES Encryption, No Encryption
Encryption Passphrase	Mju76tfC	see manual "Rules for Passwords"
Status	Enabled	Disabled

The operator has to be logged on to the device as a user within the group "admin".

5.16.1 Adding a New SNMPv3 User

The first step is to create a new entry in the SNMPv3 user table. The following command creates a new SNMPv3 user that is always named "public", has default settings and is initially disabled.

```
$> config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Users/SNMPv3
```

```
    Users"
$>  config do "Add User"
```

5.16.2 Setting the User Name and Authentication Parameters

The default user name ("public") and the authentications settings must be edited to adapt them to the given situation. Finally, the newly added SNMPv3 user has to be enabled. The settings to achieve this goal are embedded into a form page and need to be submitted explicitly before they become active. Attempts to leave a form page with modified settings will cause the device to ask for confirmation.

```
$>  config go "public/Edit Settings/Change SNMPv3 User"
$>  config set "User Name" Operator
$>  config set "Access Level" Service
$>  config set "Authentication Type" HMAC-MD5
$>  config set "Authentication Passphrase" 1Qayxsw2
$>  config set "Encryption Type" "AES Encryption"
$>  config set "Encryption Passphrase" Mju76tfC
$>  config set Status Enabled
$>  config do "Change SNMPv3 User"
```

Instead of using **config set** for setting passwords you can also use **config hidden** to allow hidden entry of the passphrases. The characters entered at the prompt "Enter password:" will **not** not displayed.

```
$>  config hidden "Authentication Passphrase"
$>  config hidden "Encryption Passphrase"
```

```
Enter password:
Retype password:
```

Enable the SNMP Access to the device.

```
$>  config go "/Administration/User and Access Administration"
$>  config set "SNMP Access" Enabled
```

5.17 Adding an SNMPv3 Trap Receiver

This use case describes how to add an SNMPv3 Trap Receiver. **NOTE:** As a prerequisite, an already configured SNMPv3 user is needed.

At the end of this use case the following settings are active:

Item	Value	Alternative Value(s)
SNMP Trap Receiver IP Address	192.168.1.1	any valid IPv4 or IPv6 unicast address
SNMP Version	SNMP V3	SNMP V2c

The operator has to be logged on to the device as a user within the group "admin".

5.17.1 Adding a new SNMP Trap Receiver

The first step is to create a new entry in the SNMP trap receiver table. SNMP trap receivers are always created with a default IP address of 0.0.0.0 and are initially disabled.

```
$> config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps"
$> config do "Add Trap Receiver"
```

5.17.2 Setting Up the Trap Receiver's Configuration

It is now required to edit the settings of the newly created trap receiver and to enable it.

```
$> config go "0.0.0.0/Edit Settings"
$> config set "IP Address" 192.168.1.1
$> config set "Security Name" Operator
$> config set "SNMP Version" "SNMP V3"
$> config set Status Enabled
```

If there is no valid SNMPv3 user account named "Operator", its not possible to set the Status to "Enabled" and you will get this error message:

```
Err: Submit failed: Security Name does not refer to an active SNMP User
```

Please create a valid SNMPv3 user with a name that matches the value of the "Security Name" field before you enable the trap receiver.

5.17.3 Checking the Trap Receiver Setup

The device allows sending a test trap to all configured SNMP trap receivers for the purpose of testing the configuration.

The operator has to be logged on to the device as a user with at least "user" access permissions.

```
$> config go "/Administration/User and Access Administration/SNMP Configuration/SNMP Traps"
$> config do "Send Test Trap"
```

Executing the above commands will cause the test trap to be sent (provided that networking is operational). The operator should check whether the newly added SNMP trap receiver has received a trap of type "axCommonTestTrap" in response to the performed action.

5.18 Updating the Device Firmware

This use case describes how the firmware of the device is updated. The firmware update is a multi-step procedure.

The first step is to configure all required details to access the "Firmware Store" download server from which the firmware update file will be downloaded. The second step is to perform the firmware download, and the last step is to initiate the actual firmware update which will copy the downloaded firmware into flash and reboot the device.

5.18.1 Configuring the Storage Server

This step describes the configuration of access data and transfer protocol for the "Firmware Store" server.

NOTE: This needs to be done once only. When the configuration of the "Firmware Store" server is already done, this step can be skipped.

At the end of this use case, the following settings will be active:

Item	Value	Alternative Value(s)
Transfer Protocol	SFTP	TFTP
SFTP Server IP	192.168.1.1	any valid IPv4 or IPv6 unicast address
SFTP Server Port	22	SSH port number used by the server
SFTP Server Directory	/	path to the directory with update files on the server
SFTP User Name	fwupdate	login name for the server
SFTP User Password	1Qayxsw2	login password for the server

The operator has to be logged on to the device as a user within the group "admin".

```
$> config go "/Administration/User and Access Administration/Firmware Store/Edit"
$> config set "Transfer Protocol" SFTP
$> config set "Server IP" 192.168.1.1
$> config set "Server Port" 22
$> config set "Server Directory" /
$> config set "User Name" fwupdate
$> config set Password 1Qayxsw2
```

Instead of using **config set** for setting passwords one can also use **config hidden** to allow hidden entry of the passphrases. The characters entered at the prompt "Enter password:" will **not** be displayed.

```
$> config go "/Administration/User and Access Administration/Firmware Store/Edit"
$> config hidden "Password"
```

```
Enter password:
Retype password:
```

5.18.2 Downloading the Firmware Update File to the Device.

This section describes how to configure the firmware file name and to activate the download of the firmware file to the device.

```
$> config go "/Administration/Firmware Update"
$> config set "File Name" <devtype>-<version>.upx
$> config do "Start Firmware Download"
```

Two variables in this menu page can be used to get detailed knowledge of the current status of the firmware file download. As long as the variable "Firmware Update Status" contains the text "Firmware Download Active", the file transfer is still ongoing. A value of "Update File Received" indicates that the file has successfully been downloaded. A value of "No Update File" indicates that the transfer has failed.

The variable "Update Info" contains further information in textual form. It indicates the current download progress as long as the download is not complete. It contains an error message if the download has failed for some reason, or the version number of the new firmware if the download has succeeded.

You can use the "config" command to monitor the download progress, every few seconds, until the download is complete.

```
$> config
```

5.18.3 Starting the Firmware Update

After successful download of the new firmware file, start the firmware update.

```
$> config do "Start Update"
```

After a successful update, which takes about 4 minutes, the device will automatically reboot to activate the new software. When the device has rebooted, please check that the new software is indeed active by looking at the Inventory page.

5.18.4 Verifying the Software Version

Verification of the installed firmware version.

```
$> config "/General System Information/Inventory/Software Version"
```

Please verify that the value shown corresponds to the new software version.

5.19 Enabling Remote Feeding for a Port

This use case describes how remote feeding for a port can be enabled or disabled. In the factory default configuration, remote feeding is disabled for all ports.

At the end of this use case, the following settings will be active:

Item	Value	Alternative Value(s)
Port 1: Admin Status	Enabled	Disabled
Port 10: Admin Status	Disabled	Enabled

The operator has to be logged on to the device as a user with at least "user" permissions.

```
$> config go "/Remote Feeding Control"
$> config set "Port 1/Admin Status" Enabled
$> config set "Port 10/Admin Status" Disabled
```

The effectiveness of the changes can be observed by using the "config" command. The table columns "Admin Status" should reflect the changes done to the configuration, and the column "Operation Status" should contain the value "disabled" for all disabled RF ports.

5.20 Setting Remote Feeding Current Thresholds

This use case describes how the current thresholds of individual remote feeding ports can be changed. The factory default configuration contains reasonable default values for the thresholds already, but a change may be required under special circumstances.

NOTE: Each RF port has its own threshold configuration menu under "/Remote Feeding Control/<Port>/RF Port Configuration" where "<Port>" indicates one of the remote feeding ports named "Port 1" through "Port 16".

NOTE: Some of the threshold values are constrained by neighboring thresholds. For example, the value of OVLT must satisfy the inequation HCUT <= OVLT <= (OVUT - 1). It may therefore be required to change the order in which thresholds are configured, so that none of the constraints is ever violated by intermediate configuration steps.

At the end of this use case, the following settings will be active for Port 2:

Item	Value	Alternative Value(s)
OCLT [mA]	5	any integer X, 2 <= X <= 5, X < OCUT
OCUT [mA]	6	any integer X, OCLT < X <= 6
LCLT [mA]	9	any integer X, OCUT <= X < LCUT
LCUT [mA]	10	any integer X, LCLT < X <= HCLT
HCLT [mA]	49	any integer X, LCUT <= X < HCUT
HCUT [mA]	50	any integer X, HCLT < X <= OVLT
OVLT [mA]	60	any integer X, HCUT <= X < OVUT
OVUT [mA]	61	any integer X, OVLT < X <= 64

```
$> config go "/Remote Feeding Control/Port 2/RF Port Configuration"
$> config set "OCLT [mA]" 5
$> config set "OCUT [mA]" 6
$> config set "LCLT [mA]" 9
$> config set "LCUT [mA]" 10
$> config set "HCLT [mA]" 49
$> config set "HCUT [mA]" 50
$> config set "OVLT [mA]" 60
$> config set "OVUT [mA]" 61
```

After each of the above "config set" commands, the device should reply with the message "Data submitted." The new settings can be verified with the "config" command.

```
$> config
```

The new contents of the menu page should reflect all changes performed in the above steps.

5.21 Enabling Remote Feeding Traps

The device supports two different SNMP traps for the remote feeding function. One trap is named "axRPXOperStatusTrap" and signals normal or exceptional remote feeding situations (open circuit, high/low current, normal operation, overload, overload shutdown, overvoltage shutdown). The second trap is named "axRPXGroundLeakageAlarm" and signals ground leakage conditions.

In order to enable or disable these traps, the operator has to be logged on to the device as a user within the group "admin".

5.21.1 Enabling the OperStatus trap

The trap named "axRPXOperStatusTrap" can be enabled in the menu "/Remote Feeding Control" for each port individually.

The following example will enable the trap for ports 1, 8, and 16.

NOTE: The name of the remote feeding port is part of the variable path. The ports are named "Port 1" through "Port 16".

```
$> config go "/Remote Feeding Control/"
$> config set "Port 1/SNMP Traps" Enabled
$> config set "Port 8/SNMP Traps" Enabled
$> config set "Port 16/SNMP Traps" Enabled
```

5.21.2 Enabling the GroundLeakage trap

The trap named "axRPXGroundLeakageAlarm" can be enabled in the alarm management menu for each port individually.

The following example will enable the trap for ports 1, 8, and 16.

NOTE: The name of the remote feeding port is part of the variable path. The ports are named "Port 1" through "Port 16".

```
$> config go "/Alarm Management/RF Port Alarm/Group Details/"
$> config set "Ground Leakage Alarm Status Port 1/SNMP Notification" "SNMP Trap"
$> config set "Ground Leakage Alarm Status Port 8/SNMP Notification" "SNMP Trap"
$> config set "Ground Leakage Alarm Status Port 16/SNMP Notification" "SNMP Trap"
```

Alphabetical Index

Access Level 87, 90
Acknowledge 113, 120
Acknowledge All 110
Acknowledge Group Alarms 111
Acknowledged 111
Active Alarm List.....
  Acknowledge 120
  Alarm Name 120
  Current Errors 119
  Current Warnings 119
  Global Alarm Status 119
  Group Name 120
  No 120
  State ..... 120p.
  System Component 121
Add Community 87
Add IPv6 Address 64
Add NTP server 40
Add Trap Receiver 81
Add User 89
Address 61
Admin Status 37, 41, 127
AdminStatus 52
Alarm Acknowledgement Policy 110
Alarm Group Name 112
Alarm Group State 112
Alarm Hold Time 115
Alarm Management.....
  Acknowledge 113
  Acknowledge All 110
  Acknowledge Group Alarms 111
  Acknowledged 111
  Alarm Acknowledgement Policy 110
  Alarm Group Name 112
  Alarm Group State 112
  Alarm Hold Time 115
  Alarm Name 115
  Alarm Severity 115
  Current Errors 112
  Current Warnings 112
  Hysteresis 116
  Ignored 111
  Max. Severity 111
  Overrun Error Level 116
  Overrun Warning Level 117
  SNMP Notification 113
  State 114
  System Component 117
  Underrun Error Level 117
  Underrun Warning Level 118
  Value 118
ALARM Message Traps 80
Alarm Name 115, 120
Alarm Severity 115

Apply Configuration Now 32
Article Revision 123
AUDIT Message Traps 81
Authentication Passphrase 91
Authentication Priority 100
Authentication Type 91
Auto Logoff Time [min] 72
Autonegotiation 54
Behaviour 34
Bits 96
Bootloader Version 123
Cancel Reset 68
Change IPv4 Address 65
Change Password 103
Change SNMPv3 User 91
Change VLAN Settings 66
Cipher 96
Clear Server Info 75
Clear update fallback alarm permanently 46
Command Output 44
Comment 96
Community 88
Config File Name 29
Configuration Management.....
- Apply Configuration Now 32
- Behaviour 34
- Config File Name 29
- Date 31
- Delete Configuration 31
- Download from Server 29
- Dying Gasp for Maintenance Reboots 32
- File Transfer State 29
- Name 31
- Preset Configuration Components 33
- Save Configuration 31
- Server Type 30
- Server URI 30
- Upload to Server 32

CONS CLI Access 72
Contact Person 121
Create Account.....
- Create Account 104
- Password 104
- Status 105
- User Group 105
- Username 105

Create Account 104
Current Errors 112, 119
Current System Uptime 121
Current Warnings 112, 119
Customization 123
Date 31, 35
Date and Time 68, 122
Date and Time Settings.....
- Admin Status 37
- Date 35
- Delay [ms] 37
- Jitter [ms] 37
- NTP Support 35

Offset [ms] 37
Protocol Version 38
Reachability 38
Server Address 38
Server Status 39
Stratum 39
Time 35
Time Zone 36
Date of Production 123
Default IPv4 Gateway 50
Delay [ms] 37
Delete Account 102
Delete Address 62
Delete Community 88
Delete Configuration 31
Delete Entry 84, 89
Delete Key 96
Delete NTP Server 41
Device Location 122
Device Name 122
Device Temperature 122
Device Type 123
Diagnostics.....
Command Output 44
IP-Address 45
Ping 45
Stop 45
Traceroute_ICMP 45
Traceroute_UDP 46
Download _ Update Progress 47
Download File Name 106
Download from Server 29
Download Key 94
Dying Gasp for Maintenance Reboots 32, 47, 69
EFM-Mode 24
Enable SNMP Link Up_Down Traps 54
Encryption Passphrase 92
Encryption Type 92
ERROR Message Traps 81
Ethernet First Mile.....
EFM-Mode..... 24
..... 24
Event Log History Size 81
Event Log Traps 82
File Name 47
File Transfer State 29, 94, 106, 125
Firmware Update.....
Clear update fallback alarm permanently 46
Download _ Update Progress 47
Dying Gasp for Maintenance Reboots 47
File Name 47
Firmware Update Status 48
Server Type 48
Server URI 49
Start Firmware Download 49
Start Update 49
Update Info 49
Firmware Update Status 48
Flags 62

FPGA Version 124
General System Information.....
Contact Person 121
Current System Uptime 121
Date and Time 122
Device Location 122
Device Name 122
Device Temperature 122
Total System Uptime 122
Global Access Password 98
Global Alarm Status 119
Ground Leakage Alarm Status 128
Group Name 120
Hardware Revision 124
HCLT [mA] 128
HCUT [mA] 128
HTTP File Transfer 72
HW MAC Address 54
Hysteresis 116
Ignored 111
INFO Message Traps 82
Interface Type 59
Inventory.....
Article Revision 123
Bootloader Version 123
Customization 123
Date of Production 123
Device Type 123
FPGA Version 124
Hardware Revision 124
Manufacturer 124
Order No. 124
Serial Number 124
Software Version 125
Vendor ID 125
IP Address 84
IP Description 41, 75, 85, 100
IP-Address 45
IPv4 Address 52, 54
IPv4 Address Assignment 55
IPv4 Default TTL 50
IPv4 DHCP Default Gateway 55
IPv4 DHCP Server 56
IPv4 DHCP Server State 56
IPv4 ICMP Support 56
IPv4 Network Mask 57
IPv6 Accept Redirects 57
IPv6 Autoconfiguration 57
IPv6 Gateway Autoconfiguration 58
IPv6 Router Advertisements 58
IPv6 Support 58
Jitter [ms] 37
Key ID 97
LCLT [mA] 129
LCUT [mA] 129
Link 52
Link Status 59
Load Private Key 106
Load Server Certificate 106

Log View.....
File Transfer State 125
Logfile Name 125
Server Type 126
Server URI 126
Upload to 'Logfile Store' 126
Logfile Name 125
Management VLAN ID 66
Management VLAN ID Usage 67
Management VLAN Prio 67
Management VLAN S-Tag 67
Management VLAN Setting 60
Manufacturer 124
Max. Severity 111
Mech. 53
Name 31, 53
New IPv4 Address 65
New IPv4 Default Gateway 65
New IPv4 Netmask 66
New IPv6 Address 64
New Password 103
New Prefix Length 64
No 120
NTP Key Data 42
NTP Key ID 42
NTP Key Type 42
NTP Server Setup.....
Add NTP server 40
Admin Status 41
Delete NTP Server 41
IP Description 41
NTP Key Data 42
NTP Key ID 42
NTP Key Type 42
NTP Status 40
Protocol Version 43
Reachability Register 43
Server Address 43
Server Status 44
NTP Status 40
NTP Support 35
OCLT [mA] 129
OCUT [mA] 130
Offset [ms] 37
Order No. 124
Outer Management VLAN ID 67
Outer Management VLAN Prio 68
Overrun Error Level 116
Overrun Warning Level 117
Overwrite Default IPv4 Gateway 50
Overwrite IPv4 Gateway Reachable 51
OVLT [mA] 130
OVUT [mA] 130
Packet Counter 60
Password 75, 104
Password Authentication 99
PfxLen 62
Ping 45
Port and IP Configuration.....

Add IPv6 Address 64
Address 61
AdminStatus 52
Autonegotiation 54
Change IPv4 Address 65
Change VLAN Settings 66
Default IPv4 Gateway 50
Delete Address 62
Enable SNMP Link Up_Down Traps 54
Flags 62
HW MAC Address 54
Interface Type 59
IPv4 Address 52, 54
IPv4 Address Assignment 55
IPv4 Default TTL 50
IPv4 DHCP Default Gateway 55
IPv4 DHCP Server 56
IPv4 DHCP Server State 56
IPv4 ICMP Support 56
IPv4 Network Mask 57
IPv6 Accept Redirects 57
IPv6 Autoconfiguration 57
IPv6 Gateway Autoconfiguration 58
IPv6 Router Advertisements 58
IPv6 Support 58
Link 52
Link Status 59
Management VLAN ID 66
Management VLAN ID Usage 67
Management VLAN Prio 67
Management VLAN S-Tag 67
Management VLAN Setting 60
Mech. 53
Name 53
New IPv4 Address 65
New IPv4 Default Gateway 65
New IPv4 Netmask 66
New IPv6 Address 64
New Prefix Length 64
Outer Management VLAN ID 67
Outer Management VLAN Prio 68
Overwrite Default IPv4 Gateway 50
Overwrite IPv4 Gateway Reachable 51
Packet Counter 60
PfxLen 62
Port Label 60
Port Name 60
Port Speed 61
Source 63
Status 63
Type 63
Port Label 60
Port Name 60
Port Speed 61
Preset Configuration Components 33
Protocol Version 38, 43
Reachability 38
Reachability Register 43
Remote Feeding Control.....

Admin Status 127
Ground Leakage Alarm Status 128
HCLT [mA] 128
HCUT [mA] 128
LCLT [mA] 129
LCUT [mA] 129
OCLT [mA] 129
OCUT [mA] 130
OVLT [mA] 130
OVUT [mA] 130
RF Control FW Version 130
RF Current [mA] 131
RF Operation Status 131
RF Port No. 131
RF Voltage (a_b) [V] 132
RF Voltage (a_gnd) [V] 132
RF Voltage (b_gnd) [V] 132
SNMP Traps 127
Reset Date 69
Reset Mode 69
Reset State 70
Reset System.....
Cancel Reset 68
Date and Time 68
Dying Gasp for Maintenance Reboots 69
Reset Date 69
Reset Mode 69
Reset State 70
Reset Time 70
Start Reset 70
Reset Time 70
RF Control FW Version 130
RF Current [mA] 131
RF Operation Status 131
RF Port No. 131
RF Voltage (a_b) [V] 132
RF Voltage (a_gnd) [V] 132
RF Voltage (b_gnd) [V] 132
Run Self-test 71
Save Configuration 31
Security Name 85
Self-Test.....
Run Self-test 71
Self-test Result 71
Self-test Status 71
Self-test Result 71
Self-test Status 71
Send Test Trap 83
Serial Number 124
Server Address 38, 43
Server Cert Issuer 107
Server Cert Key Status 107
Server Cert Parse Status 107
Server Cert Serial 107
Server Cert Subject 108
Server Cert Valid From 108
Server Cert Valid Till 108
Server Directory 75
Server IP 76

Server Key Parse Status 108
Server Port 76
Server Status 39, 44
Server Type 30, 48, 76, 95, 109, 126
Server URI 30, 49, 95, 109, 126
SNMP Access 73
SNMP Access Configuration 78
SNMP Alarm Trap Type 82
SNMP Authen Traps 83
SNMP Configuration.....
  SNMP Access Configuration 78
  SNMP Engine ID 78
  SNMP Engine ID Mode 79
  SNMP Max Message Size 79
  SNMP UDP Port 79
  SNMP Version 80
SNMP Engine ID 78
SNMP Engine ID Mode 79
SNMP Max Message Size 79
SNMP Notification 113
SNMP Trap Counter 83
SNMP Traps.....
  Add Trap Receiver 81
  ALARM Message Traps 80
  AUDIT Message Traps 81
  Delete Entry 84
  ERROR Message Traps 81
  Event Log History Size 81
  Event Log Traps 82
  INFO Message Traps 82
  IP Address 84
  IP Description 85
  Security Name 85
  Send Test Trap 83
  SNMP Alarm Trap Type 82
  SNMP Authen Traps 83
  SNMP Trap Counter 83
  SNMP Version 85
  Status 86
  UDP Port 86
  Web_CLI Authen Traps 83
SNMP Traps 127
SNMP UDP Port 79
SNMP Version 80, 85
SNMPv2 Communities.....
  Access Level 87
  Add Community 87
  Community 88
  Delete Community 88
  State 88
SNMPv3 Users.....
  Access Level 90
  Add User 89
  Authentication Passphrase 91
  Authentication Type 91
  Change SNMPv3 User 91
  Delete Entry 89
  Encryption Passphrase 92
  Encryption Type 92

State 90
User Name 92
Software Version 125
Source 63
SSH Access.....
SSH CLI Port 93
SSH Host Key Fingerprint 93
SSH CLI Access 73
SSH CLI Port 93
SSH Host Key Fingerprint 93
SSH Key Filename 94
SSH Keys.....
Bits 96
Cipher 96
Comment 96
Delete Key 96
Download Key 94
File Transfer State 94
Key ID 97
Server Type 95
Server URI 95
SSH Key Filename 94
Status 97
Used as 97
User 98
SSH Passwords.....
Global Access Password 98
Password Authentication 99
Start Firmware Download 49
Start Reset 70
Start Update 49
State ..... 88, 90, 114, 120p.
Status 63, 86, 97, 102, 105
Stop 45
Stratum 39
System Component 117, 121
Table Keys.....
<Alarm Group>..... 110
<Alarm Item>..... 113
<Alarm Num>..... 119
<Community>..... 87
<Config Name>..... 30
<Configuration Component>..... 33
<IP Address>..... 36, 40, 83
<IPv6 Address>..... 61
<Local User Name>..... 101
<MGMT Port>..... 51
<RF Port No.>..... 127
<Server>..... 73
<SNMPv3 User Name>..... 89
<SSH Key ID>..... 95
TACACS+ 100
TACACS+ Connect Timeout 100
TACACS+ Receive Timeout 101
TACACS+ Server 101
TACACS+ Shared Secret 101
Time 35
Time Zone 36
Total System Uptime 122

Traceroute_ICMP 45
Traceroute_UDP 46
Transfer Protocol 77
Type 63
UDP Port 86
Underrun Error Level 117
Underrun Warning Level 118
Update Info 49
Upload to 'Logfile Store' 126
Upload to Server 32
URI 74
Used as 97
User 98
User and Access Administration.....
  Auto Logoff Time [min] 72
  Clear Server Info 75
  CONS CLI Access 72
  HTTP File Transfer 72
  IP Description 75
  Password 75
  Server Directory 75
  Server IP 76
  Server Port 76
  Server Type 76
  SNMP Access 73
  SSH CLI Access 73
  Transfer Protocol 77
  URI 74
  User Name 77
  Valid 74
  Web Access 73
User Group 102, 105
User Name 77, 92
Username 103, 105
Users and Passwords.....
  Authentication Priority 100
  Change Password 103
  Delete Account 102
  IP Description 100
  New Password 103
  Status 102
  TACACS+ 100
  TACACS+ Connect Timeout 100
  TACACS+ Receive Timeout 101
  TACACS+ Server 101
  TACACS+ Shared Secret 101
  User Group 102
  Username 103
Valid 74
Value 118
Vendor ID 125
Web Access 73
Web Access Mode 109
Web Configuration.....
  Download File Name 106
  File Transfer State 106
  Load Private Key 106
  Load Server Certificate 106
  Server Cert Issuer 107

Server Cert Key Status 107
Server Cert Parse Status 107
Server Cert Serial 107
Server Cert Subject 108
Server Cert Valid From 108
Server Cert Valid Till 108
Server Key Parse Status 108
Server Type 109
Server URI 109
Web Access Mode 109
Web_CLI Authen Traps 83
..... 24

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