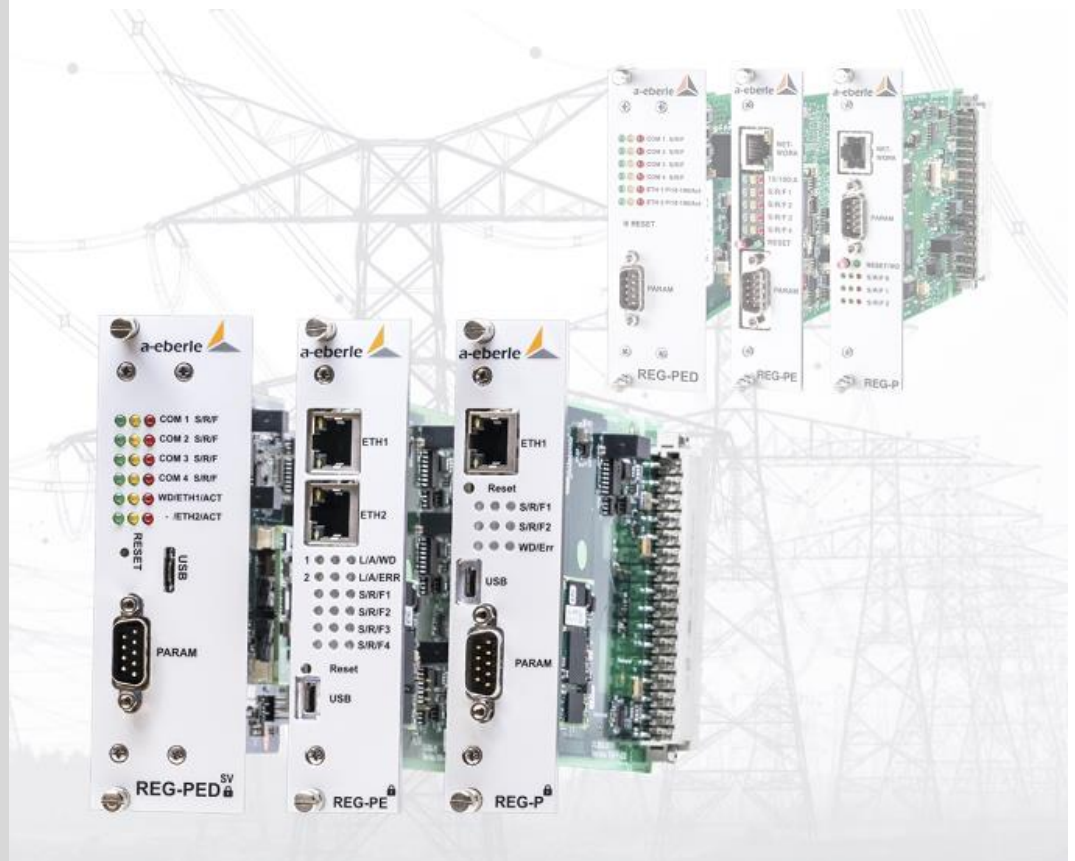


## Administrator Manual



**READ CAREFULLY BEFORE USE**

*KEEP FOR FUTURE REFERENCE*

The template was created based on DIN EN 82079-1: 2013-06.

[illegible]


## Table of Contents

<b>1.</b>	<b>User guidance .....</b>	<b>7</b>
1.1	Target group .....	7
1.2	Warnings .....	7
1.3	Tips .....	8
1.4	Other symbols .....	8
1.5	Applicable documentation .....	8
1.6	Keeping .....	8
1.7	Updated documentation .....	8
<b>2.</b>	<b>Scope of Delivery .....</b>	<b>9</b>
<b>3.</b>	<b>Safety instructions .....</b>	<b>9</b>
<b>4.</b>	<b>Security in REG-P, PE, PED, REG-PED<sup>SV</sup> card models TK28-x and TK102 .....</b>	<b>10</b>
4.1	User access methods and protocols summary .....	10
4.2	Rights assignment – roles access concept .....	11
4.3	Login modes .....	11
4.3.1	Login and Logout .....	11
4.3.2	RADIUS mode .....	14
4.3.3	Password mode .....	28
4.4	Management of the RBAC definition files .....	34
4.5	Management of security certificates .....	36
4.5.1	Security certificates in TK28-4, TK28-6 and TK102 telecontrol boards .....	37
4.6	Functionality concepts .....	37
<b>5.</b>	<b>Security in REG-PE and REG-PED telecontrol boards models TK8xx .....</b>	<b>42</b>
5.1	User access methods and protocols summary .....	42
5.2	Roles in TK8xx telecontrol boards .....	42
5.3	Login modes .....	43
<b>6.</b>	<b>WinConfig REG-P / REG-PE / REG-PED / REG-PED<sup>SV</sup> .....</b>	<b>44</b>
6.1	WinConfig Software introduction .....	44
6.1.1	Offline and online WinConfig .....	44
6.1.2	Offline WinConfig software solution .....	45
6.1.3	Online WinConfig software solution .....	47
6.1.4	Logging in TK28x and TK102 telecontrol boards .....	49
6.2	REG-PEX Loader software .....	58
6.3	Communication with REG-P(E)(D)(SV) telecontrol board in WinConfig 11 .....	59
6.3.1	Rules for higher security .....	60

6.3.2	Actions supported by firmware and their usage: .....	61
6.3.3	SSH access (REG-PEx, TK102, TK28x) .....	61
6.3.4	Menu and meaning of individual items: .....	62
6.3.5	Transfer of settings from / to a PC.....	66
6.4	Serial data transfer for REG-P telecontrol boards TK5xx, TK400 .....	69
6.4.1	Serial data transfer for REG-P telecontrol board TK28-4.....	71
6.5	Ethernet data transfer .....	72
6.5.1	TK400 telecontrol board: .....	72
6.5.2	REG-P (TK28-4), REG-PE (TK28-6, TK860) and REG-PED <sup>SV</sup> (TK102, TK 885) telecontrol boards:72	
6.5.3	Transfer settings from PC function .....	73
6.5.4	Transfer of settings from PC for TK28-4, TK28-6 and TK102 telecontrol boards.....	75
6.5.5	Change of IP settings for REG-PE(D) telecontrol boards .....	80
6.5.6	Change of IP settings for REG-PED <sup>SV</sup> (TK102) telecontrol boards.....	81
6.5.7	Submit certificates for TK28-4, TK28-6, TK860 and TK885, TK102 telecontrol boards .....	82
6.5.8	Bonding .....	84
6.5.9	PRP - Parallel Redundancy Protocol .....	84
7.	<b>Support for script-based upgrade procedure for TK28-4, TK28-6 and TK102 telecontrol boards and A-Eberle devices firmware .....</b>	<b>85</b>
7.1	Concepts .....	85
7.1.1	SW architecture .....	85
7.1.2	Concept of upgrade .....	85
7.1.3	Security concept .....	87
7.1.4	Hosting environment .....	87
7.2	Installation of upgrade support package .....	87
7.2.1	Windows .....	87
7.2.2	Linux.....	88
7.3	Preparation of upgrade.....	88
7.3.1	Windows .....	88
7.3.2	Linux.....	89
7.3.3	Digital signature of A-Eberle device firmware file .....	89
7.4	Upgrade process .....	89
7.4.1	Windows .....	89
7.4.2	Linux.....	90
7.4.3	Sequential upgrade.....	91
7.5	Hints .....	92
7.5.1	How to ensure compatibility .....	92

7.5.2	Output of scripts to console .....	92
7.5.3	Protection of production files.....	92
7.5.4	A-Eberle device firmware upgrade .....	92
<b>8.</b>	<b>Disassembly &amp; disposal .....</b>	<b>92</b>
<b>9.</b>	<b>Warranty .....</b>	<b>93</b>
10.	List of Figures .....	94
<b>11.</b>	<b>List of Tables .....</b>	<b>96</b>

# 1. User guidance

This Administrator Manual contains information about the WinConfig software intended for administrator purposes focused namely for secure access to telecontrol boards and security-related actions in WinConfig. For detailed information about configuration of telecontrol boards REG-P / REG-PE / REG-PED / REG-PED<sup>SV</sup> / PQI-DA see the WinConfig User Manual.

Read the Administrator Manual in its entirety and do not use the product unless you have understood the Administrator Manual.

## 1.1 Target group


The Administrator Manual is intended for skilled technicians as well trained.

The contents of this Administrator Manual must be accessible to people tasked with the installation and operation of the system.

## 1.2 Warnings


### Structure of the warnings


Warnings are structured as follows:


 <b>SIGNAL WORD</b>	<p><b>Nature and source of the danger.</b></p> <p>Consequences of non-compliance.</p> <p>Actions to avoid the danger.</p>
--	---

### Types of warnings

Warnings are distinguished by the type of danger they are warning against:

 <b>DANGER!</b>	Warns of imminent danger that can result in death or serious injuries if not avoided.
--	---

 <b>WARNING!</b>	Warns of a potentially dangerous situation that can result in death or serious injuries when not avoided.
---	---

 <b>CAUTION!</b>	Warns of a potentially dangerous situation that can result in fairly serious or minor injuries when not avoided.
---	--

<b>NOTICE:</b>	Warns of a potentially dangerous situation that if not avoided could result in material or environmental damage.
----------------	--

## 1.3 Tips



Tips on the appropriate device use and recommendations.

## 1.4 Other symbols

### Instructions

Structure of the instructions:



Instructions for an action.



Indication of an outcome, if necessary.

### Lists

Structure of unnumbered lists:

0 List level 1

— List level 2

Structure of numbered lists:

1) List level 1

2) List level 1

1. List level 2

2. List level 2

## 1.5 Applicable documentation

For the safe and correct use of the product, observe the additional documentation that is delivered with the system as well as the relevant standards and laws.

## 1.6 Keeping

Keep the user manual, including the supplied documentation, readily accessible near the system.

## 1.7 Updated documentation

The most recent versions of the documents can be obtained at <https://www.a-eberle.de/de/downloads>.



## **2. Scope of Delivery**

## **3. Safety instructions**

- Observe the operating instructions.
- Always keep the operating instructions with the unit.
- Make sure that the device is never operated in a damaged or compromised condition.
- Make sure that only specialized personnel operate the unit.
- The device must be connected according to the manufacturer's installation instructions.
- Make sure that the device is never operated beyond its stated ratings.
- Do not operate the unit in any hazardous environment where explosive gases, dust or fumes occur.
- Ensure that protective covers are always in place and are functional.
- Ensure that the five safety regulations according to DIN VDE 0105 are always observed.
- Clean the appliance only with commercially available detergents.

## 4. Security in REG-P, PE, PED, REG-PED<sup>SV</sup> card models TK28-x and TK102

- ➡ Please mind that the Cyber Security features are only available in telecontrol boards starting from manufacturing date 2018 (“TK28-4, TK28-6 and TK102”), not to predecessor boards (“TK517, TK509, TK400, TK860 and TK885”).
- ➡ The security needs in the above-mentioned card models are covered using role-based access control with the usage of Active Directory objects and RADIUS functionality. Only secured protocols with encryption are used for communication with card. The user is authenticated and then his authorization for each action is evaluated. This concept includes access methods with assigned protocols, roles of users and actions for which the authorization is evaluated according to the user role.

### 4.1 User access methods and protocols summary

- 0 WinConfig online (web access)
  - Internet browser client (like Internet Explorer) connects the web server embedded in the Linux OS inside the card.
  - Protocol HTTPS with direct authorization is used.
- 0 WinConfig console/shell menu (terminal access)
  - Terminal client (like PUTTY) connects the SSH server embedded in the Linux OS inside the card.
  - Protocol SSH with direct authorization is used
- 0 WinConfig offline (web access and transfer access)
  - Internet browser client (like Internet Explorer) connects the remote client-side proprietary web server (part of the WinConfig offline). A specialized server parts communicate with the card.
  - Data transfers use protocol HTTPS with direct authorization.
  - Network scan (broadcast functions) and system parameterization use UDP encrypted with AES256 with HTTPS preauthorization.
- 0 Remote script upgrade access (terminal access)
  - Command line SSH client (like PLINK) connects the SSH server embedded in the Linux OS inside the card.
  - Protocol SSH with direct authorization is used.

## 4.2 Rights assignment – roles access concept

The rights for particular actions defined in the system are assigned using role-based access control (RBAC) method.

### 0 Roles-to-user

- Dynamic assignment is done by Active Directory. Every role defined in the system is mapped to one user group.

### 0 Actions-to-roles

- Static assignment is hardcoded in the definition file inside the card firmware (provided to particular methods by request). This file can be changed by system administrators.

## 4.3 Login modes

There are 2 login modes implemented.

- 0 RADIUS mode uses the RADIUS server for authentication of the user and card and provides the information for authorization of actions via VSA strings. This mode has precedence.

- 0 The second emergency mode is Password mode. It uses the locally cached credentials for authentication, and then the user acts as embedded Admin user of the system. The Active Directory server is source of the cached credentials information.

### 4.3.1 Login and Logout

Logging ON can be done by dialog box that appears when a user attempts to access the tel-control board using internet browser and HTTPS access. The dialog box also shows the currently set Login mode.

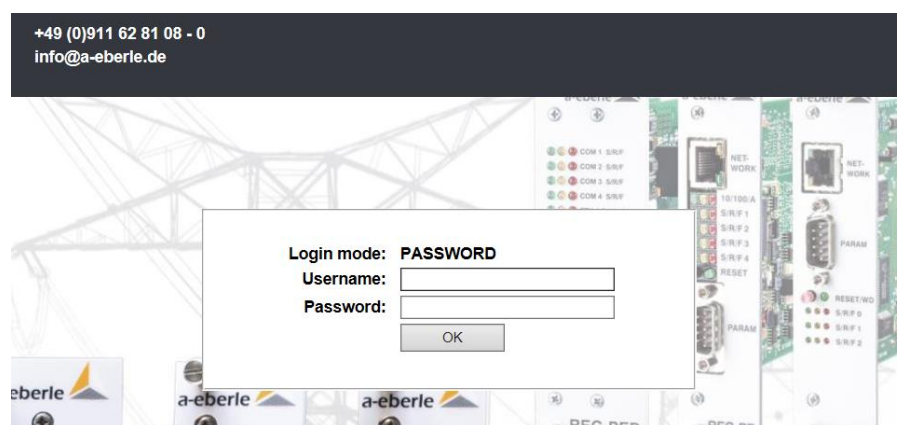
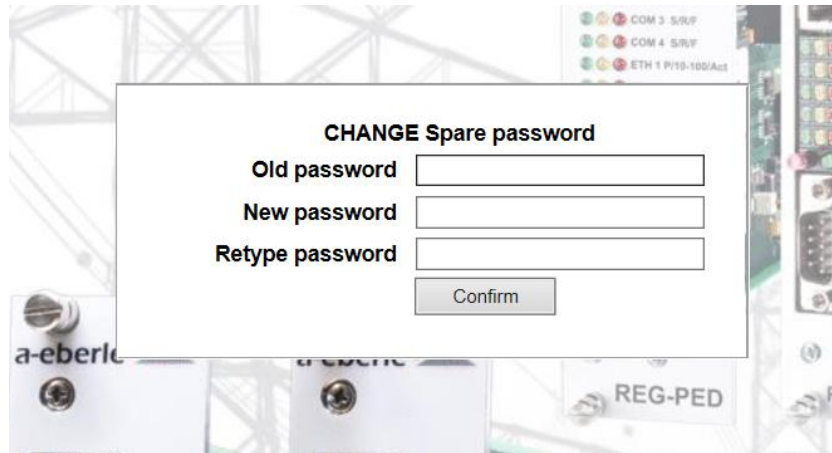


Figure 1: Login dialog

We take care of it.

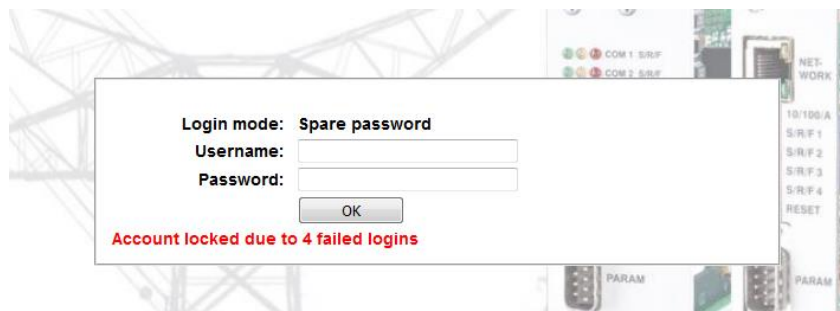
---

If the user makes a first time login in the board supplied from the factory, the program consequently forces the user to define a new password.



*Figure 2: Definition of new password*

If the login fails for 4 attempts, then the account is temporarily locked for 60 seconds. At the same, the message about locking appears on board. The locking refers only to the login name (user account) so it is never unlocked if a user tries login name that does not exist.



*Figure 3: Locking of account*

The users can logout using a special button in the left side of the window in the online Win-Config.



Figure 4: Logout button

#### 4.3.1.1 Special function for boards TK28x and TK102

The current setting of login mode is shown in the Regsys screen for a short period of time during the telecontrol board start.

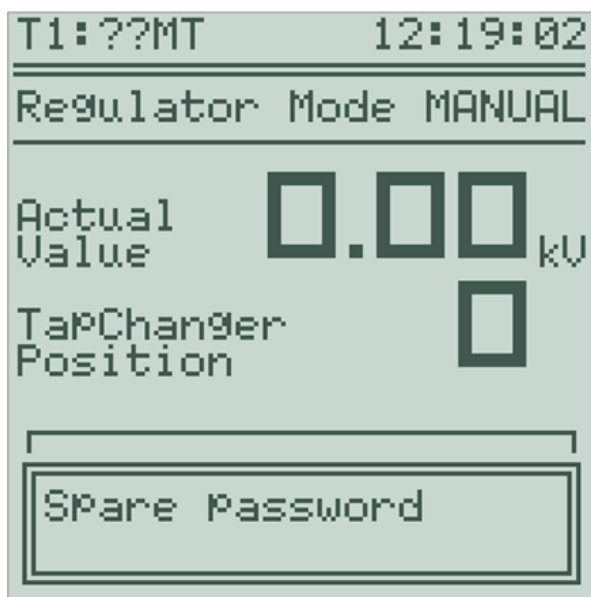


Figure 5: Information about login mode on Regsys screen

## 4.3.2 RADIUS mode

### 4.3.2.1 Roles and rights definition

According to the Rollenkonzept document the Active Directory objects and RADIUS server parameters should be implemented to achieve the desired WinConfig RADIUS functionality. There has to be a separate AD group for each role defined and every of these groups has to have the appropriate VSA string set. This is necessary because the same VSA strings are hardcoded and evaluated in the RADIUS client in the TK card. This means that the VSA strings count and values are mandatory; the underlying names of Security Groups are user-definable.

The access rules are defined in the file *rbac.def* located in the file system of the telecontrol boards. The elementary rules are composed of three objects in the format:

AccessMethod\_ActionType\_Role

where:

- 0 **AccessMethod** is a name selected from the set of the methods (applications) which are used for the data access. Possible values are:
  - OfflineWinConfig, OnlineWinConfig, ShellMenu, WebReg, ScriptBasedUpgrade
- 0 **ActionType** is a name selected from the set of actions defined for particular *AccessMethod*. Possible values are:
  - For OfflineWinConfig: transfer\_to, transfer\_from, set\_net, set\_services, set\_emergency\_pwd, set\_certificates
  - For OnlineWinConfig: change\_settings, save\_settings, set\_net, set\_services, security\_management, set\_emergency\_pwd, set\_certificates
  - For ShellMenu: shell\_access, get\_logs, set\_net, set\_services, security\_management
  - For WebReg: parameters\_read, parameters\_update, panel\_watch, panel\_setKey, terminal\_read, terminal\_update, RGL\_read, RGL\_update, log\_read, UTC\_read, UTC\_update, DST\_read, DST\_update, Communication\_read, Communication\_update, statistics\_read, simulation\_read, simulation\_start, simulation\_tapPos, simulation\_values, simulation\_monitor, IOMap\_read, IOMap\_update, basVal\_read, basVal\_update, autoMan\_read, autoMan\_update, time\_update, timeGroup\_update, features\_read, features\_update, ram\_read, ram\_backup, ram\_restore, firmware\_update, UDM\_update
  - For ScriptBasedUpgrade: no action is defined, the AccessMethod represents the ActionType so the rules are composed of two objects in the format:
    - AccessMethod\_Role
- 0 **Role** is the name of user role as defined in the RADIUS and AD according to the Rollenkonzept document. Possible values are:

- Administrator, ControlOperator, ProtectionOperator, TransmissionEquipmentOperator, UPSOperator, PDVOperator, BMSOperator, Extern, Observer, Manipulator, RemoteOperator

Each positive elementary rule (permission granted) is defined as one row of the *rbac.def* file. All other elementary rules are denied. The user with the corresponding rights can upload new definitions to the system or reset the definitions to the default factory state, which are defined in the following tables.

Table 1: Definition of roles

Definition of roles	AD Security Group - example	VSA string - mandatory
Administrator	AE-Administrators	Administrator
Leittechnik-Operator	AE-ControlOperators	ControlOperator
Schutztechnik-Operator	AE-ProtectionOperators	ProtectionOperator
Übertragungstechnik-Operator	AE-TransmissionEquipmentOperators	TransmissionEquipmentOperator
USV-Operator	AE-UPSOperators	UPSOperator
PDV-Operator	AE-PDVOperators	PDVOperator
ZLT-Operator	AE-BMSOperators	BMSOperator
Dienstleister (extern)	AE-Externs	Extern
Beobachter	AE-Observers	Observer
Schaltpersonal (lokal)	AE-Manipulators	Manipulator
Netzleitstellen-Operator (Remote)	AE-RemoteOperators	RemoteOperator

Table 2: Offline WinConfig access method actions-to-role default rights

VSA string - mandatory	Online WinConfig actions rights - default					
	<i>transfer_to</i>	<i>transfer_from</i>	<i>set_net</i>	<i>set_services</i>	<i>set_emergency_pwd</i>	<i>set_certificates</i>
Administrator	yes	yes	yes	yes	yes	yes
ControlOperator	yes	yes	no	yes	yes	no
ProtectionOperator	yes	yes	no	yes	yes	no
Transmission-EquipmentOperator	yes	yes	no	yes	yes	no
UPSOperator	yes	yes	no	yes	yes	no
PDVOperator	yes	yes	no	yes	yes	no
BMSOperator	yes	yes	no	yes	yes	no
Extern	no	no	no	no	no	no
Observer	no	yes	no	no	no	no
Manipulator	no	yes	no	no	no	no
RemoteOperator	no	no	yes	no	no	no

Table 3: Online WinConfig access method actions-to-role default rights, part 1.

VSA string - mandatory	Online WinConfig actions rights - default				
	<i>change_settings</i>	<i>save_settings</i>	<i>set_net</i>	<i>set_services</i>	<i>security_management</i>
Administrator	yes	yes	yes	yes	yes
ControlOperator	yes	yes	no	yes	no
ProtectionOperator	yes	yes	no	yes	no
TransmissionEquipment-Operator	yes	yes	no	yes	no
UPSOperator	yes	yes	no	yes	no
PDVOperator	yes	yes	no	yes	no
BMSOperator	yes	yes	no	yes	no
Extern	no	no	no	no	no
Observer	no	yes	no	no	no
Manipulator	no	yes	no	no	no
RemoteOperator	no	no	yes	no	no



Table 4: Online WinConfig access method actions-to-role default rights, part 2.

VSA string - mandatory	Online WinConfig actions rights - default	
	<i>set_emergency_pwd</i>	<i>set_certificates</i>
Administrator	yes	yes
ControlOperator	yes	no
ProtectionOperator	yes	no
TransmissionEquipment-Operator	yes	no
UPSOperator	yes	no
PDVOperator	yes	no
BMSOperator	yes	no
Extern	no	no
Observer	no	no
Manipulator	no	no
RemoteOperator	no	no

Table 5: Shell menu access method actions-to-role default rights

VSA string - mandatory	Shell menu WinConfig actions rights - default				
	<i>shell_access</i>	<i>get_logs</i>	<i>set_net</i>	<i>set_services</i>	<i>security_management</i>
Administrator	yes	yes	yes	yes	yes
ControlOperator	no	yes	no	yes	no
ProtectionOperator	no	yes	no	yes	no
TransmissionEquipment-Operator	no	yes	no	yes	no
UPSOperator	no	yes	no	yes	no
PDVOperator	no	yes	no	yes	no
BMSOperator	no	yes	no	yes	no
Extern	no	no	no	no	no
Observer	no	yes	no	no	no
Manipulator	no	yes	no	no	no
RemoteOperator	no	no	yes	no	no

Table 6: Remote script-based upgrade access method actions-to-role default rights

VSA string - mandatory	remote script-based upgrade - default
Administrator	yes
ControlOperator	no
ProtectionOperator	no
TransmissionEquipment-Operator	no
UPSOperator	no
PDVOperator	no
BMSOperator	no
Extern	no
Observer	no
Manipulator	no
RemoteOperator	yes

Table 7: WebReg actions-to-role default rights, part 1.

We take care of it.

VSA string - mandatory	WebReg actions-to-role default rights									
	Parameters read	Parameters update	Panel - watching	Panel - set key	Terminal read	Terminal update	RGL read	RGL update	LOG read	UTC read
Administrator	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
ControlOperator	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Protection-Operator	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Transmission-Equipment-Operator	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
UPSOperator	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
PDVOperator	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
BMSOperator	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Extern	no	no	no	no	no	no	no	no	no	no
Observer	yes	no	yes	no	yes	no	yes	no	yes	yes
Manipulator	yes	no	yes	no	yes	no	yes	no	yes	yes
RemoteOperator	no	no	no	no	no	no	no	no	no	no

Table 8: WebReg actions-to-role default rights, part 2.

VSA string - mandatory	WebReg actions-to-role default rights								
	UTC update	Communication read	Communication update	Statistics read	Simulation read	Simulation start	Simulation TapPos	Simulation values	Simulation monitor
Administrator	yes	yes	yes	yes	yes	yes	yes	yes	yes
ControlOperator	yes	yes	yes	yes	yes	yes	yes	yes	yes
ProtectionOperator	yes	yes	yes	yes	yes	yes	yes	yes	yes
Transmission-Equipment-Operator	yes	yes	yes	yes	yes	yes	yes	yes	yes
UPSOperator	yes	yes	yes	yes	yes	yes	yes	yes	yes
PDVOperator	yes	yes	yes	yes	yes	yes	yes	yes	yes
BMSOperator	yes	yes	yes	yes	yes	yes	yes	yes	yes
Extern	no	no	no	no	no	no	no	no	no
Observer	no	yes	no	yes	yes	no	no	no	yes
Manipulator	no	yes	no	yes	yes	no	no	no	yes
RemoteOperator	no	no	no	no	no	no	no	no	no

Table 9: WebReg actions-to-role default rights, part 3.

VSA string - mandatory	WebReg actions-to-role default rights								
	I/O map read	I/O map update	Basic values read	Basic values update	Auto/man read	Auto/man update	Time update	Features read	Features update
Administrator	yes	yes	yes	yes	yes	yes	yes	yes	yes
ControlOperator	yes	yes	yes	yes	yes	yes	yes	yes	yes
ProtectionOperator	yes	yes	yes	yes	yes	yes	yes	yes	yes
Transmission-Equipment-Operator	yes	yes	yes	yes	yes	yes	yes	yes	yes
UPSOperator	yes	yes	yes	yes	yes	yes	yes	yes	yes
PDVOperator	yes	yes	yes	yes	yes	yes	yes	yes	yes
BMSOperator	yes	yes	yes	yes	yes	yes	yes	yes	yes
Extern	no	no	no	no	no	no	no	no	no
Observer	yes	no	yes	no	yes	no	no	yes	no
Manipulator	yes	no	yes	no	yes	no	no	yes	no
RemoteOperator	no	no	no	no	no	no	no	no	no

Table 10: WebReg actions-to-role default rights, part 4.

VSA string - mandatory	WebReg actions-to-role default rights				
	RAM read	RAM backup	RAM restore	Firmware update	UDM update
Administrator	yes	yes	yes	yes	yes
ControlOperator	yes	yes	yes	yes	yes
ProtectionOperator	yes	yes	yes	yes	yes
Transmission-Equipment-Operator	yes	yes	yes	yes	yes
UPSOperator	yes	yes	yes	yes	yes
PDVOperator	yes	yes	yes	yes	yes
BMSOperator	yes	yes	yes	yes	yes
Extern	no	no	no	no	no
Observer	yes	no	no	no	no
Manipulator	yes	no	no	no	no
RemoteOperator	no	no	no	no	no

#### 4.3.2.2 Actions-to-role hardcoded rights in A-Eberle device

Online WinConfig transfers the actions-to-role rights valid for the actual user and connection session also into the connected A-Eberle device (RegSys). WinConfig translates the RADIUS roles to the Regsys roles defined in external *Rollenmatrix..... XLSM* file. The external file creates a bitmask named CLIUM corresponding to the roles in the Regsys device. The hashtable with mapping of RBAC roles in the A-Eberle device to those of WinConfig can be seen below. It is mandatory to keep the names of Regsys roles exactly as they are defined in the hashtable. For more information see the A-Eberle device manual.

Regsys roles of A-Eberle device also include a special account of Panel-User intended to local access using device panel. The account of Panel-User has no relations to the RADIUS roles.

The A-Eberle device user rights are automatically switched to the default state when the predefined inactivity timeout expired.

Table 11: Definition of roles

Definition of roles	AD Security Group - example	Regsys roles
Administrator	AE-Administrators	Administrator
Leittechnik-Operator	AE-ControlOperators	<a href="#">Leittechnik-Operatoren</a>
Schutztechnik-Operator	AE-ProtectionOperators	Schutztechnik-Operator
Übertragungstechnik-Operator	AE-TransmissionEquipmentOperators	<a href="#">Übertragungstechnik-Operatoren</a>
USV-Operator	AE-UPSOperators	USV-Operator
PDV-Operator	AE-PDVOperators	PDVOperator
ZLT-Operator	AE-BMSOperators	ZLT-Operator
Dienstleister (extern)	AE-Externs	Dienstleister
Beobachter	AE-Observers	Beobachter
Schaltpersonal (lokal)	AE-Manipulators	<a href="#">Schaltpersonal</a>
Netzleitstellen-Operator (Remote)	AE-RemoteOperators	Netzleitstellen-Operator
Panel-User 1		Regsys role only for local panel user 1
Panel-User 2-5		Regsys role only for local panel user 2-5

#### 4.3.2.3 Windows Server R2 2008 and 2016 configuration step-by-step

Configuration of Windows Server R2 2008 to work as RADIUS server is used as implementation example. Configuration of Windows Server 2016 is similar; the same dialog boxes are used. The RADIUS server is called *Network Policy Server* in Windows. Configuration can be done in the Server Manager:

- 0 Roles->Network Policy And Access Services -> NPS in the Windows Server 2008,
- 0 Tools-> Network Policy Server in the Windows Server 2016.
- ➡ Add groups to the Active Directory according to the Roles and rights definition.

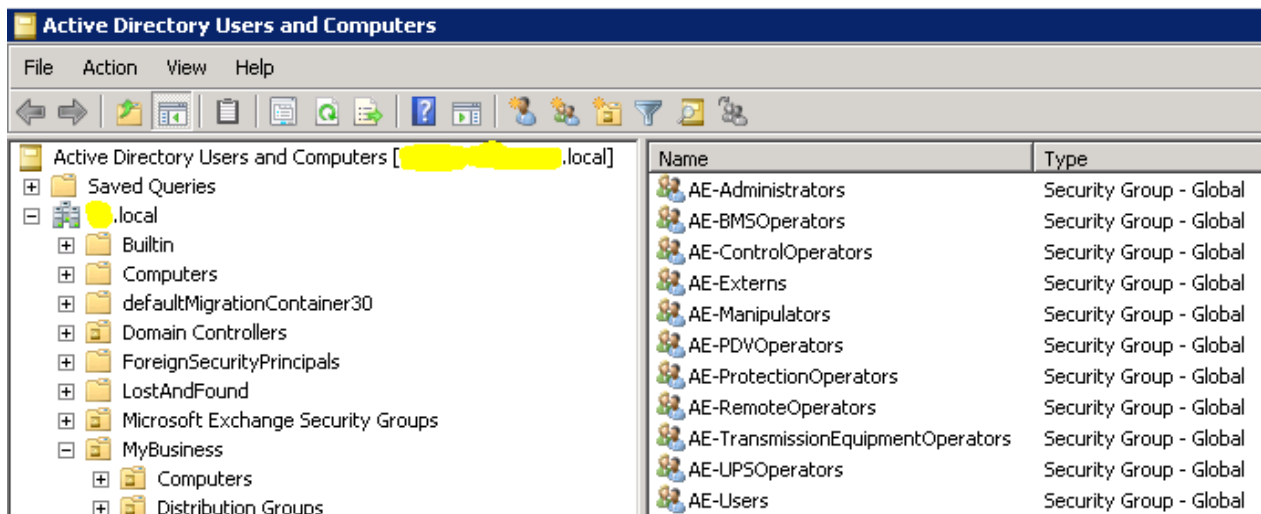


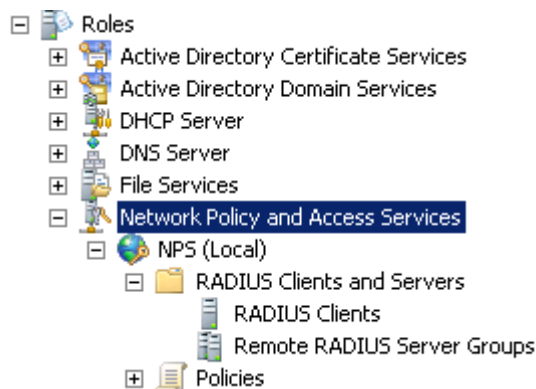
Figure 6: Adding groups

- ➡ Add domain users to one or more created groups.

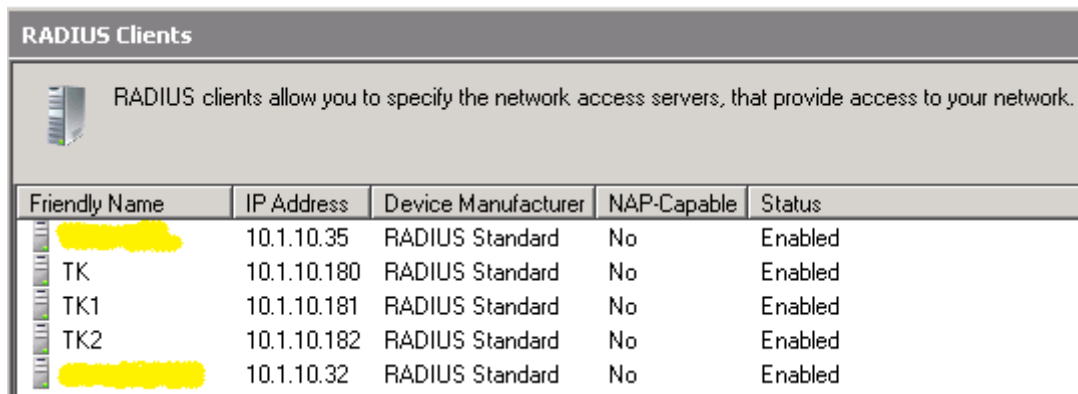
👉 There is some guide how to work with AD groups and users in this document:

<http://pc-addicts.com/create-ad-users-groups-server-2016/>

- ➡ Install RADIUS to the Windows Domain Controller (add NPS to the server roles via Server Manager).



👉 Add all TK cards (IP addresses) to the RADIUS clients group:



Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status
[Redacted]	10.1.10.35	RADIUS Standard	No	Enabled
TK	10.1.10.180	RADIUS Standard	No	Enabled
TK1	10.1.10.181	RADIUS Standard	No	Enabled
TK2	10.1.10.182	RADIUS Standard	No	Enabled
[Redacted]	10.1.10.32	RADIUS Standard	No	Enabled

Figure 7: Adding TK cards

- It is necessary to define the “shared secret” password for each client. It could be the same for all clients. This shared secret has to be set in the card using WinConfig:

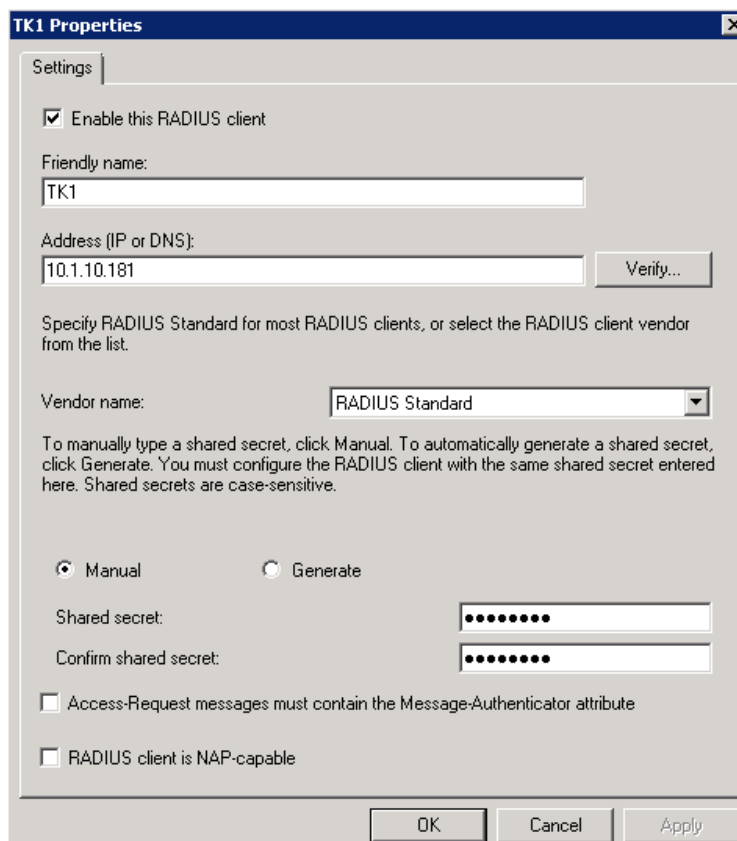


Figure 8: Shared secret

- ➡ Configure Network Policies and VSAs.

- The Network Policy has to be set for each Active Directory user group added at first step. The Server Manager is used for Network Policy:













Network Policies				
 Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can connect.				
Policy Name	Status	Processing Order	Access Type	Source
 AE-Administrator Secure Wired (Ethernet) Connections	Enabled	1	Grant Access	Unspecified
 AE-ControlOperator Secure Wired (Ethernet) Connections	Enabled	2	Grant Access	Unspecified
 AE-ProtectionOperator Secure Wired (Ethernet) Connections	Enabled	3	Grant Access	Unspecified
 AE-TransmissionEquipmentOperator Secure Wired (Ethernet) Connections	Enabled	4	Grant Access	Unspecified
 AE-UPSOperator Secure Wired (Ethernet) Connections	Enabled	5	Grant Access	Unspecified
 AE-PDOperator Secure Wired (Ethernet) Connections	Enabled	6	Grant Access	Unspecified
 AE-BMSOperator Secure Wired (Ethernet) Connections	Enabled	7	Grant Access	Unspecified
 AE-Manipulator Secure Wired (Ethernet) Connections	Enabled	8	Grant Access	Unspecified
 AE-User Secure Wired (Ethernet) Connections	Enabled	9	Grant Access	Unspecified
 AE-Extern Secure Wired (Ethernet) Connections	Enabled	10	Grant Access	Unspecified
 AE-RemoteOperator Secure Wired (Ethernet) Connections	Enabled	11	Grant Access	Unspecified

Figure 9: Network policies

#### NOTICE:

Note that the policies will be resolved in the processing order, when NPS finds the first policy with granted access, it uses it. So, the user group assignment will resolve within the first policy and only this corresponding VSA string will be returned to the requester (TK card).

↪ Each Network Policy has to be configured this way (standard):

AE-ControlOperator Secure Wired (Ethernet) Connections	
Conditions - If the following conditions are met:	
Condition	Value
User Groups	AIS\AE-ControlOperators
Settings - Then the following settings are applied:	
Setting	Value
Ignore User Dial-In Properties	True
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Secured password (EAP-MSCHAP v2)
Authentication Method	EAP OR Unencrypted authentication (PAP, SPAP) OR Encryption authentication (CHAP) OR MS-CHAP v1 OR MS-CHAP v2
NAP Enforcement	Allow full network access
Update Noncompliant Clients	True
Vendor-Specific	ControlOperator
Framed-Protocol	PPP
Service-Type	Framed

Figure 10: Network policy configuration

✎ The Conditions – Authentication methods should be set for all policies like this:

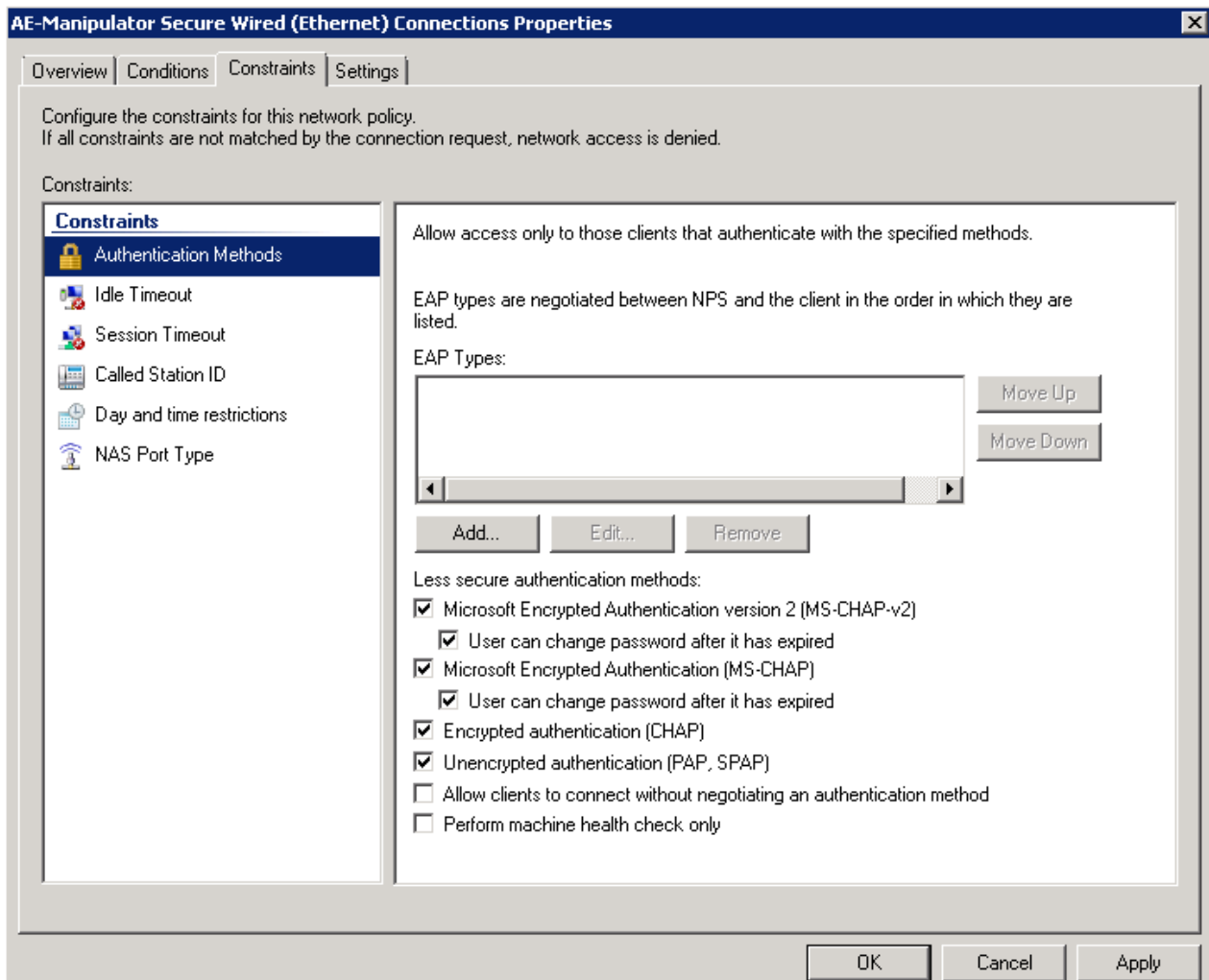
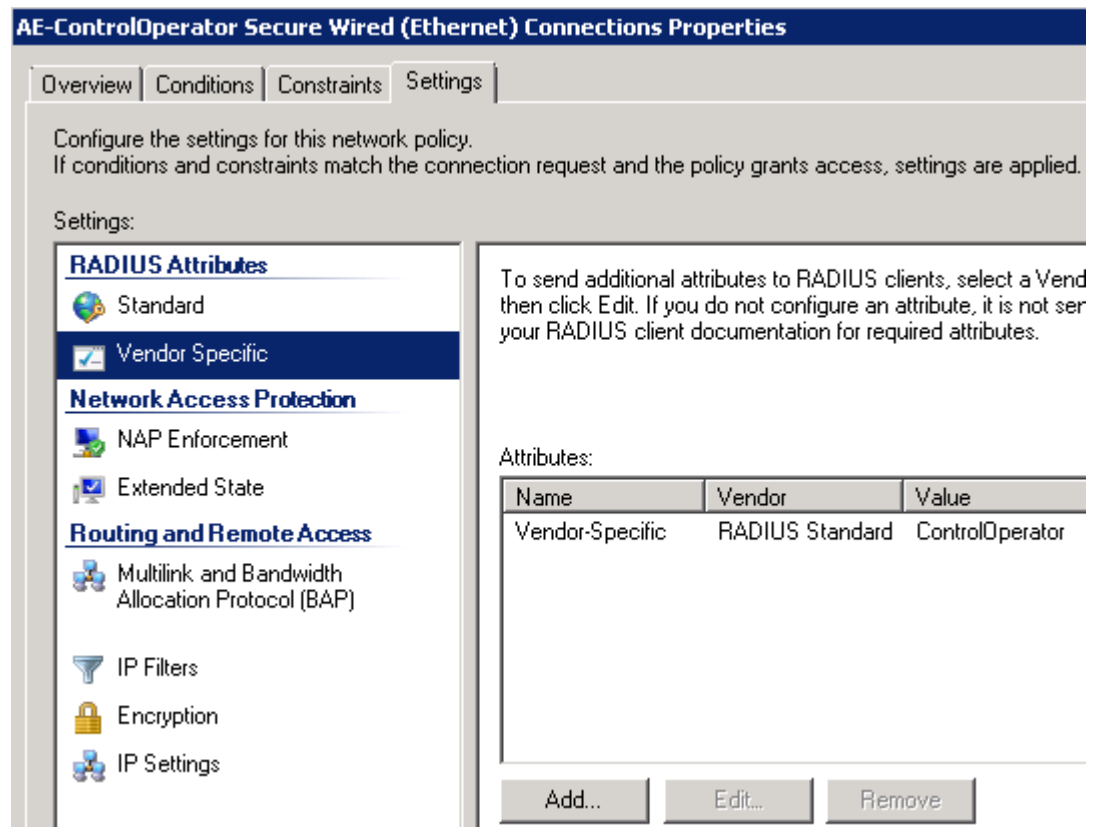


Figure 11: Authentication methods

✎ The Vendor-Specific attribute has be set to the desired mandatory value according to the Active Directory user group:





*Figure 12: Vendor specific attributes*

- This Vendor-Specific attribute should be set by the following way (Vendor Code value doesn't matter):

We take care of it.

---

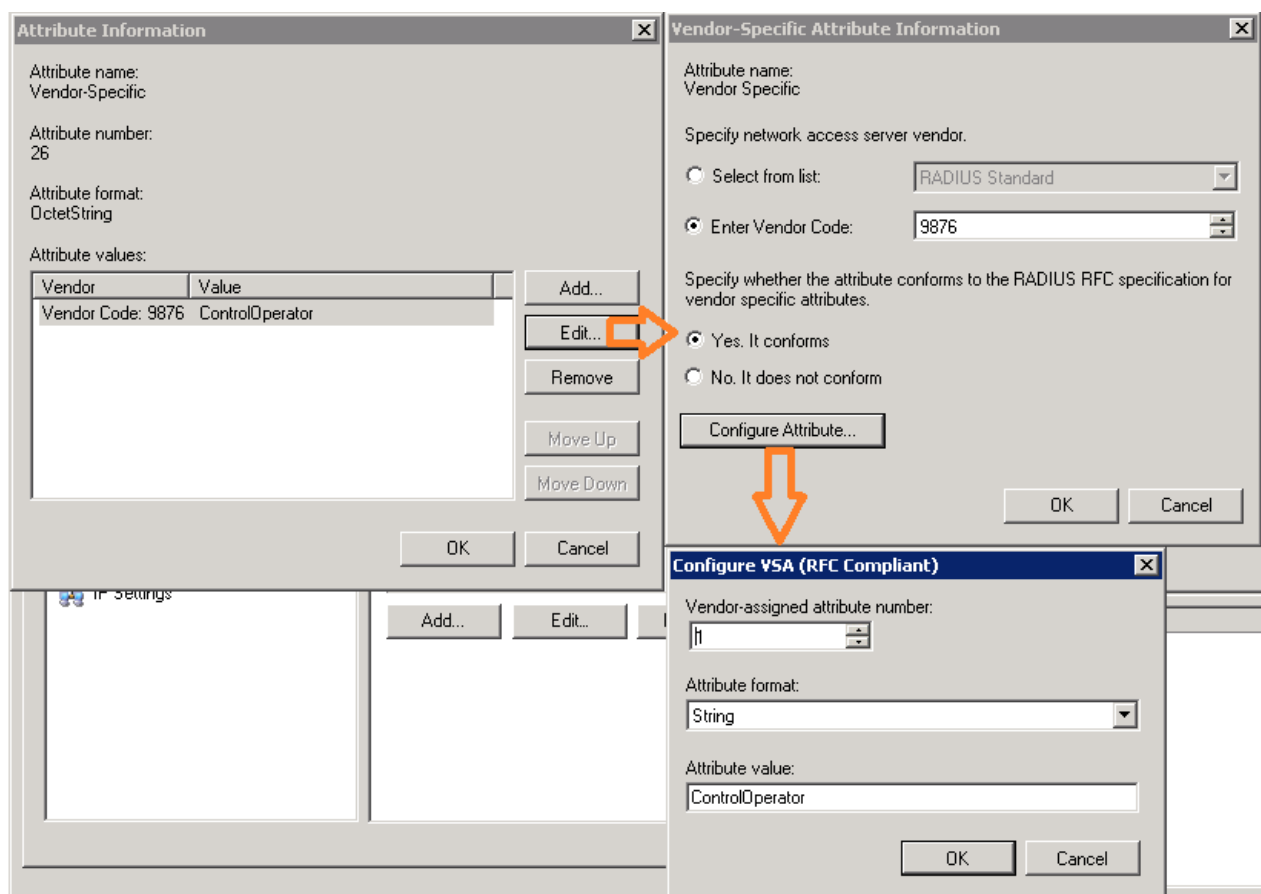


Figure 13: Vendor specific attribute setting

#### 4.3.2.4 RADIUS mode settings in WinConfig

✎ The RADIUS mode properties can be set in the *Security* page of online WinConfig:

Login mode: ☐ Password ☒ RADIUS

RADIUS settings

☐ RADIUS address is same as AD

IP address

Port

Secret

Table 12: Radius mode settings

Setting	Value
RADIUS address is the same as AD	The RADIUS server could be implemented on the same PC as Active Directory server.
RADIUS IP address	IP address of the RADIUS server (TK cards have no DNS client implemented, so IP address is mandatory)
Port	TCP port of RADIUS server service
Secret	Share secret configured for this TK card on the server

### 4.3.3 Password mode

The embedded *Admin* account is used for authorization of actions in password mode. The password of this account (so-called emergency password) is stored locally in the OS of the card, but is periodically cached from the Active Directory (caching is done by system daemon). The version of this password using the same method is also cached. This mechanism allows to login to the card in the case when no RADIUS server is connectable. This version of password is shown for a short period of time to the user on the connected REGSYS device display after reset of the TK card and system administrator could provide the right password for this version.

The *Admin* account in password mode uses the same rights as *Administrator* role in Radius mode.

It is necessary to modify the AD to provide the right information supporting this login mode.

If the telecontrol board is switched to RADIUS mode and the RADIUS server is not available, the board automatically switches to the Password mode after unsuccessful attempt to login in RADIUS mode. However, the telecontrol board makes periodical attempts to connect the RADIUS server. When the RADIUS server becomes available then the telecontrol board switches back to RADIUS mode on background. So if the Password mode is desirable from operating reasons, it is necessary to switch the board to password mode by using the *Security* settings.

The user has the possibility to switch to the RADIUS mode *on demand* by using the *Try to switch to Radius* button in the login dialog. If the RADIUS is still unavailable, the attempt has no effect and the user can continue in the *Password mode*.

Login mode: **Spare password mode**

	<input type="button" value="Try to switch to RADIUS"/>
Username:	<input type="text"/>
Password:	<input type="password"/>
	<input type="button" value="OK"/>

#### NOTICE:

The name of Password mode is user-definable with *Spare password mode* as default. Both mode name and password can be changed in the *Security* settings.

#### 4.3.3.1 AD server and schema preparation step-by-step

New mandatory AD attributes:

It is mandatory to add two new attributes to the AD schema with the following common names / display names:

- 0 ae-WinConfig-AdminEmergencyPassword / aeWinConfigAdminEmergencyPassword
- 0 ae-WinConfig-AdminEmergencyPasswordVersion / aeWinConfigAdminEmergencyPasswordVersion

The recommended method how to add extend AD schema by Windows Server embedded AD attributes editor is described here:

<https://social.technet.microsoft.com/wiki/contents/articles/20319.how-to-create-a-custom-attribute-in-active-directory.aspx>

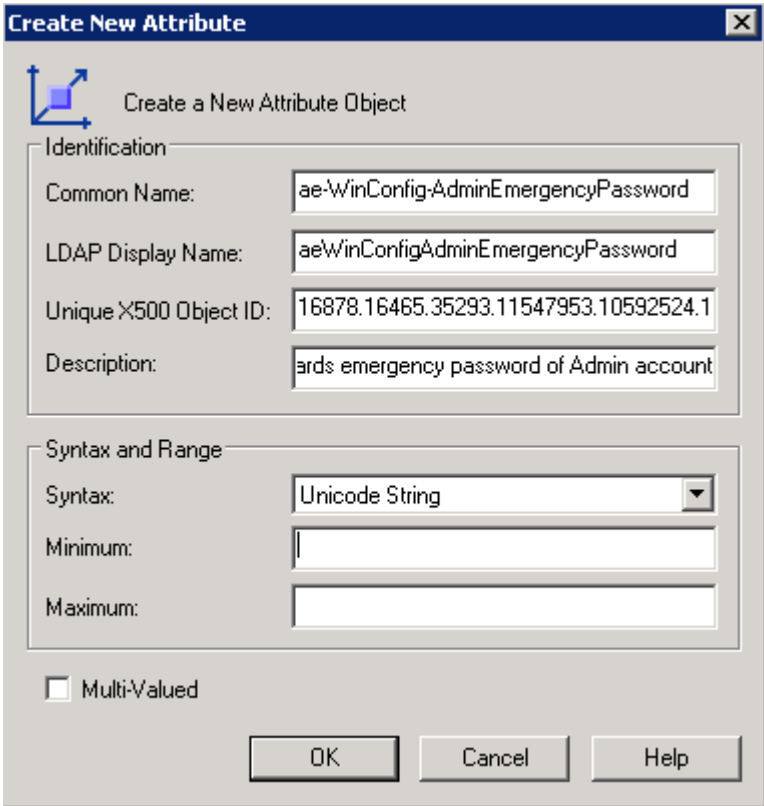


Figure 14: Example how Administrator has to fill the unique OID property of each new attribute

The efficiency and fast way of generating the right IOD is described here:

<https://gallery.technet.microsoft.com/scriptcenter/56b78004-40d0-41cf-b95e-6e795b2e8a06>

These two new parameters have to be mapped to the User class as described in the above mentioned document.

To ensure the propagation of the new parameters to all desired AD objects, it is recommended to restart the Active Directory service or Windows.

AD user with mandatory display name:



The following user has to exist in the Users group of the AD with this Display name (it is recommended to create new user with this property. Good practice is to leave Last and First Name empty and enter desired Display name to the Full name):

*Admin for A-Eberle cards*

A screenshot of a Windows-style dialog box titled "Admin for A-Eberle cards Properties". The dialog has a tabbed interface with tabs for "Published Certificates", "Member Of", "Password Replication", "Dial-in", "Object", "Security", "Environment", "Sessions", "Remote control", "Terminal Services Profile", "COM+", "UNIX Attributes", "Attribute Editor", "General", "Address", "Account", "Profile", "Telephones", and "Organization". The "General" tab is selected. Inside the dialog, there is a user icon and the name "Admin for A-Eberle cards". Below this, there are several text input fields: "First name:", "Last name:", "Display name:" (which contains the text "Admin for A-Eberle cards"), "Description:", "Office:", "Telephone number:", "E-mail:", and "Web page:". There are also "Initials:" and "Other..." buttons. At the bottom, there are "OK", "Cancel", "Apply", and "Help" buttons.

*Figure 15: Admin for A-Eberle cards*

The *Admin for A-Eberle cards Properties* user object works as container for appropriate attributes. The LDPAS client from the TK cards caches login attributes from this object. This is also the place where to set the following attributes (this operation should be automated by AD administrator):

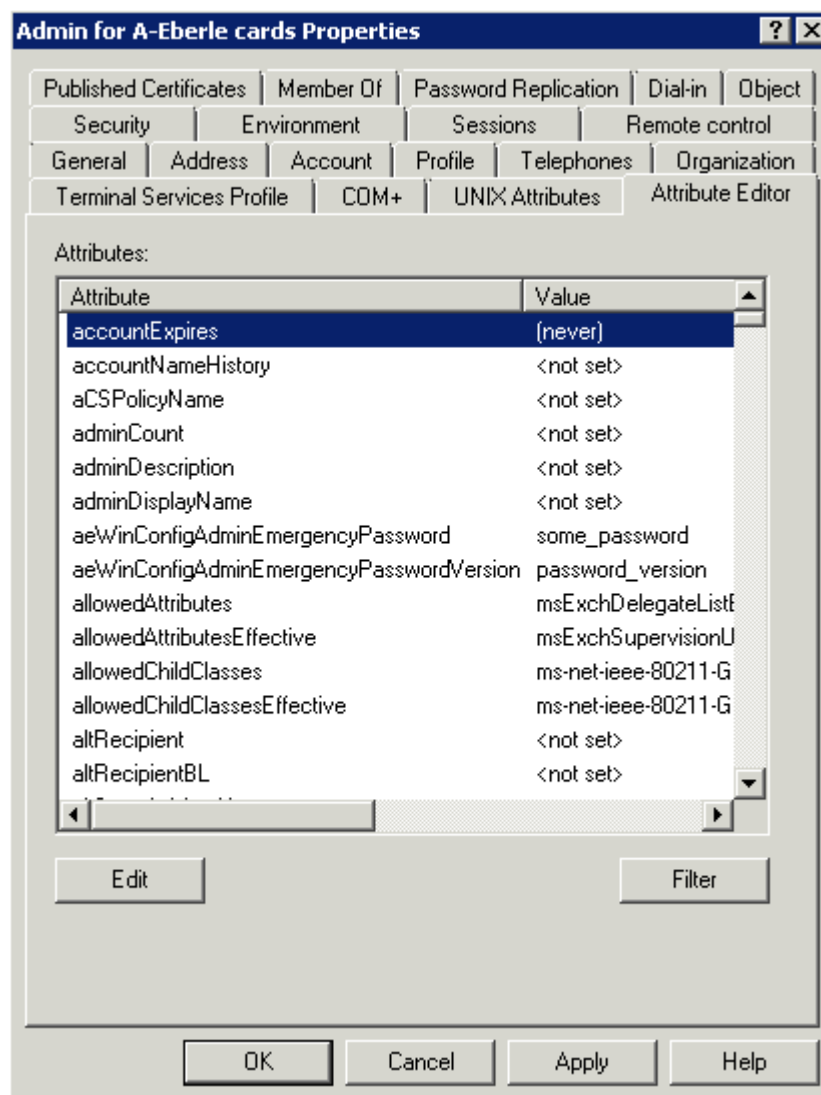


Figure 16: Configuration of attributes

It is mandatory to install appropriate server certificate on the AD server named exactly as FQDN of the server to ensure right authorization using LDAPS.



Good practice is to use locally installed Certification Services, create certificate request, issue the certificate and install it locally.

For details please refer to Microsoft documentation, for example: <https://gallery.technet.microsoft.com/Windows-Server-2016-Active-165e88d1>.

#### 4.3.3.2 Limitation of user names



Use letters (A ....Z, a....z) and/or numbers (0...9) in user names.

Avoid usage of special characters (non-letters). The only allowed special characters are stated below.

We take care of it.

---

Allowed special characters:    - \_

#### 4.3.3.3 Password mode settings in WinConfig



The image shows a web-based configuration interface for WinConfig. At the top, there is a 'Login mode' section with two radio buttons: 'Password' (which is selected) and 'RADIUS'. Below this is a 'Password settings' section. It contains a label 'Name of password mode' followed by a text input field containing the text 'Spare password'. Directly below the input field is a button labeled 'Change password'. At the bottom of the form, there are two buttons: 'Save' and 'Reload'.

*Figure 17: Password mode setting, RBAC and other security settings*



**Security**

**Common settings**

AD server IP address	<input style="width: 90%;" type="text" value="0.0.0.0"/>
LDAPS port	<input style="width: 90%;" type="text" value="636"/>
AD server FQDN	<input style="width: 90%;" type="text"/>
AD user name FQDN	<input style="width: 90%;" type="text"/>
AD user password	<input style="width: 90%;" type="password"/>
CA certificate	<div style="border: 1px solid #ccc; height: 150px; width: 100%; margin-top: 5px;"></div>

Login mode: ☒ Password ☐ RADIUS

**Password setting**

Name of password mode	<input style="width: 60%;" type="text" value="Spare password"/>
<input type="button" value="Change password"/>	

**RBAC and CLIUM definitions**

RBAC file:	<input type="button" value="Browse..."/> No file selected.	<input type="button" value="Transfer RBAC definition to card"/>
		<input type="button" value="Transfer RBAC definition from card"/>
		<input type="button" value="Reset RBAC definition"/>
CLIUM file:	<input type="button" value="Browse..."/> No file selected.	<input type="button" value="Transfer CLIUM definition to card"/>
		<input type="button" value="Transfer CLIUM definition from card"/>
		<input type="button" value="Reset CLIUM definition"/>
Password for Panel user 1:	<input style="width: 100%;" type="password"/>	<input type="button" value="Set"/>
Password for Panel user 2:	<input style="width: 100%;" type="password"/>	<input type="button" value="Set"/>
Password for Panel user 3:	<input style="width: 100%;" type="password"/>	<input type="button" value="Set"/>
Password for Panel user 4:	<input style="width: 100%;" type="password"/>	<input type="button" value="Set"/>
Password for Panel user 5:	<input style="width: 100%;" type="password"/>	<input type="button" value="Set"/>

Figure 18: Password mode setting, RBAC and other security settings

Table 13: AD server settings

Setting	Value
AD server IP address	IP address of the AD server (TK cards have no DNS client implemented, so IP address is mandatory)
LDAPS port	TCP port of LDAPS server service running on the AD server – usually 636
AD server FQDN	TK card uses LDAPS protocol to communicate with AD, in this case is mandatory to know the FQDN name AD server. This name has to be the same as the name of the certificate used for LDAPS
AD Username FQDN	Name of the AD user which has rights to read the cached ae... attributes (it is stored encrypted locally with standard PAM security procedures). It is mandatory to use FQDN user name. It is good practice to utilize the user created according to the procedure described in chapter 4.3.3.1, because this user is owner of desired attributes and has surely access.
AD user password	Password of this user (it is stored encrypted locally with standard PAM security procedures)
CA certificate	The certificate of the authority which issued the certificate for the LDAPS server

The login mode can be selected as Password or Radius, however the name of password mode can be also user-defined. Default mode name is *Spare password*. Also the password for this mode can be later changed using the *Change password* button.

## 4.4 Management of the RBAC definition files

There are 2 files with definitions of actions-to-role rights – WinConfig RBAC and CLIUM definition files. The CLIUM definition file contains rules for A-Eberle device (RegSys), see chapter 4.3.2.2.

The basic security behavior of CLIUM definition file:

- 0 The security policies defined by the CLIUM file are active only when a user logged in the online WinConfig.
- 0 The role of logged user is used to set the appropriate matrix of security policies (see regulator documentation).
- 0 If a user logged out of the online WinConfig, then the RegSys security policies are returned back to the default state after a defined timeout inside the RegSys. The *padlock* symbol appears in the regulator display and no operations on the regulator are permitted.
- 0 In the case of upload of a new CLIUM definition file to the regulator, it is necessary to log out and login again in the online WinConfig to use the newly defined matrix of effective security policies.

The WinConfig RBAC definition file is described in the chapter 4.3.2.1. This file can be transferred to the card in the online and offline WinConfig modes. The action *set\_certificates* is used for authorizing the transfer.

The RBAC definition file can be reset to the factory default state described in this documentation. This operation is reserved for Administrator role only and is not present in RBAC definitions to avoid deadlock in the case of corrupted RBAC file in the card.

## Certificates and RBAC

---

Transfer of files

*All certificate and key files are expected in PEM format.*

Certificate file:

Key file:

RBAC file:

CLIUM file:

---

Authorization - password mode

Password:

## Certificates and RBAC

Transfer of files

All certificate and key files are expected in PEM format.

Certificate file:

Browse...

Key file:

Browse...

Transfer certificates to card

RBAC file:

Browse...

Transfer RBAC definition to card

Reset RBAC definition

CLIUM file:

Browse...

Transfer CLIUM definition to card

Reset CLIUM definition

Authorization - standard mode

User name:

Admin

Password:

Use last login values

Forget login values

Operation

Progress: 

0%

Status:

Activity:

Figure 19: Offline WinConfig management of RBAC definition files

## 4.5 Management of security certificates

Work with certificates is subject to Public Key Infrastructure (PKI). The certificate is issued by *certification authority* after obtaining the *certificate request*. Such certificate can be used e.g. for encrypting of HTTPS as described in the column 1) below.

According to the PKI rules, a new certificate is necessary in the case, when:

- 0 The original certificate validity expired.

- 0 The certificate has been revoked either by *certification authority* (suspicion of unauthorized use etc.) or by certificate owner request (disclosure of private key etc.).

#### 4.5.1 Security certificates in TK28-4, TK28-6 and TK102 telecontrol boards

- 1) The certificate used for encrypting of HTTPS communication in online and offline WinConfig:

This certificate with key is pre-installed and supplied with the WinConfig system on boards. The certificate is issued for the purpose of WinConfig for regped.tele-data.de with the validity till 2050. A user can replace the certificate with his own pair of *certificate/private key* using the offline WinConfig after detection and board selection using the *Submit certificates* option.

- 2) The CA certificate for verification of encrypted communication using LDAPS protocol:

This certificate is necessary for the automatic change of the emergency password from the Active Directory storage. All certificates, of certification authorities obtained in the end of 2017 from Windows™ system, are supplied with the WinConfig system on the boards. These certificates can be replaced by other CA certificates using the *User management* option in online WinConfig.

### 4.6 Functionality concepts

The password login mode applies if the RADIUS server is not available.

This appears in the following situation:

- 0 There was an unsuccessful login in the RADIUS mode because the RADIUS server is not accessible. The telecontrol board automatically switches to the password mode.

To get the right information about the login mode in such case, a user has to do the following:

- ➡ Online mode: Make a new login attempt.

↳ The PASSWORD mode appears after browser refresh.

- ➡ Offline mode: A new detection has to be done after unsuccessful login to refresh the card login mode information.

↳ Password mode appears after the detection.

- ➡ Serial console

↳ Password mode appears after unsuccessful login to RADIUS.

- ➡ SSH console

- ✎ The same behaviour as serial console but login mode information is not visible to the user.

Unsuccessful login in RADIUS mode can also appear in the situation when a user forgot his password or the RADIUS settings is accidentally damaged in the telecontrol board. The following steps can be done in such situation:

- ➡ Disconnect the board from network.
- ✎ RADIUS becomes inaccessible.
- ➡ Connect the board locally using notebook.
- ➡ Follow one of the scenarios above.

**NOTICE:**

Note: In such case the board is switched to the PASSWORD mode only temporarily and the board software makes periodical attempts with 1 hour period to connect to the RADIUS server again. So the board will be switched to RADIUS mode automatically if a user logs off and RADIUS server becomes available.

The factory delivery includes a default password which is strongly recommended to be changed at the end of the SAT.

The emergency password is set by the online WinConfig web server or by the central Active Directory.

The emergency password can be also set by the offline WinConfig in the case when the RADIUS is not available and the password was not previously changed by the online WinConfig, so the user is not forced to use the online WinConfig for the first time. The HTTPS access is used for the transfer of the new password to the card to keep a secure transfer of the important data.

Basic assumptions:

- 1) Functionality of the WinConfig offline:
  - The WinConfig offline could be started according to the standard Windows rules.
  - The work with settings and card detection could be performed by everyone who has the according rights to the connected PC.
  - These actions will be preauthenticated after the card selection: transfer data from/to card, services settings and IP settings.
  - The preauthentication will be made by the connected online WinConfig web server according to the card settings – using the RADIUS or emergency online WinConfig account. User of the offline WinConfig will be informed which credentials to use (offline WinConfig will obtain this info during detect process, the same way as other services information).
  - The user has to set the emergency password if it is not set yet and the RADIUS is not used.

- 2) The card initially contains only the RADIUS client without the RADIUS server connection information (IP address etc.). There is an initial online WinConfig web access account contained in the card (Admin/teledata) and the user will be allowed only to change the initial password of this login to the emergency one (the program will apply rules to that). The term "emergency password" means the password of the standard Admin account of the online WinConfig web server. This Admin account with the emergency login will work only after the factory default online WinConfig web access password change to emergency one.
- 3) The emergency password could be set by using the online or offline WinConfig within the first login. This operation will recreate the Admin account in the online WinConfig web server with emergency password. User will set the RADIUS connection information in the online WinConfig.
- 4) The emergency password is cached from the AD in the case the AD server is visible on the LAN. This method has priority over the local assignment method.
- 5) Unsuccessfully login tries are logged to MicroSD and to the remote SYSLOG server.

Basic scenarios on *REG-P (TK28-4)*, *REG-PE (TK28-6)* and *REG-PED<sup>SV</sup> (TK102)* telecontrol boards:

- 1) End-user will access A-Eberle device equipped with the above mentioned telecontrol boards locally (WinConfig online method) for the first time and RADIUS is not available.
- 2) End-user will access A-Eberle device equipped with the above mentioned telecontrol boards locally (WinConfig online method) for the next times and RADIUS is available.
- 3) End-user will access A-Eberle device equipped with the above mentioned telecontrol boards locally (WinConfig online method) for the next times and RADIUS is not available.
- 4) End-user will access A-Eberle device equipped with the above mentioned telecontrol boards remotely (WinConfig offline method) for the card which uses RADIUS authentication.
- 5) End-user will use A-Eberle device equipped with the above mentioned telecontrol boards remotely (WinConfig offline method) for the first time for the card without RADIUS authentication.
- 6) End-user will use A-Eberle device equipped with the above mentioned telecontrol boards remotely (WinConfig offline method) for the next time for the card without RADIUS authentication

Scenarios 2,3,4,6 could be used after 1 or 5 (end-user have to initiate authentication on the cards).

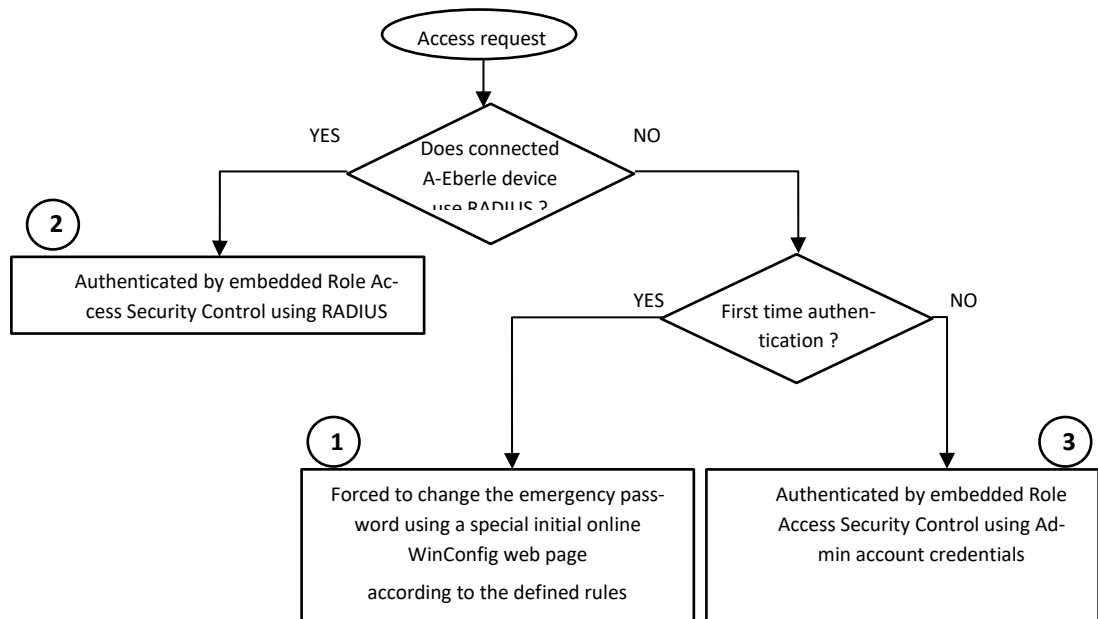


Figure 20: Online WinConfig access method – first/next authentication

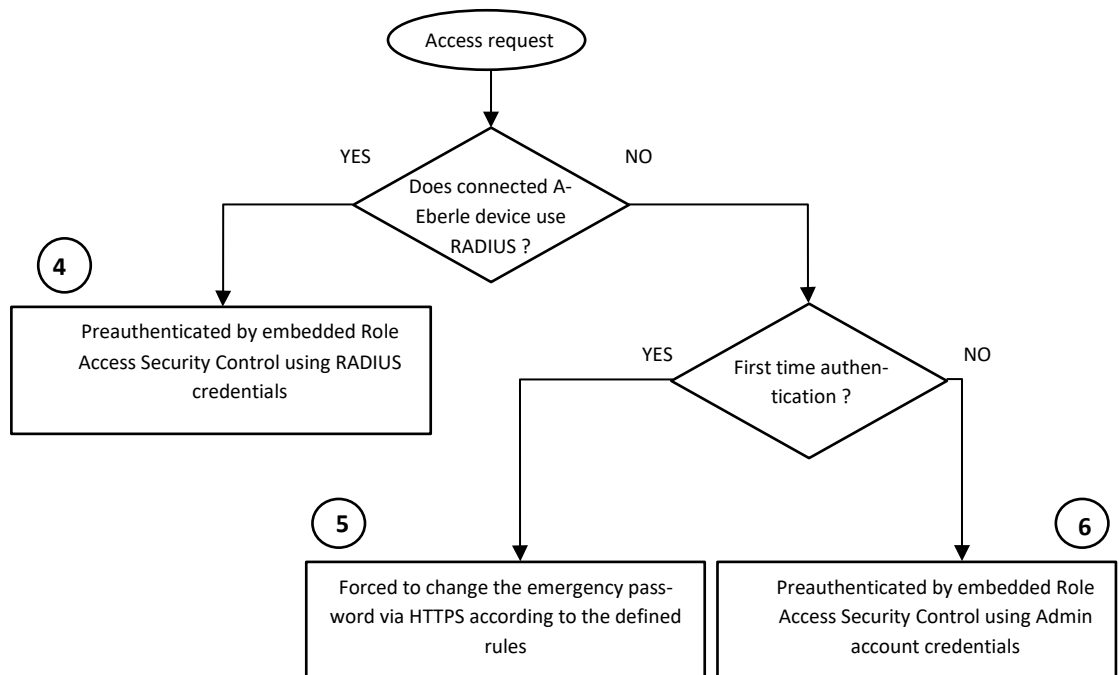


Figure 21: Offline WinConfig access method – first/next time authentication



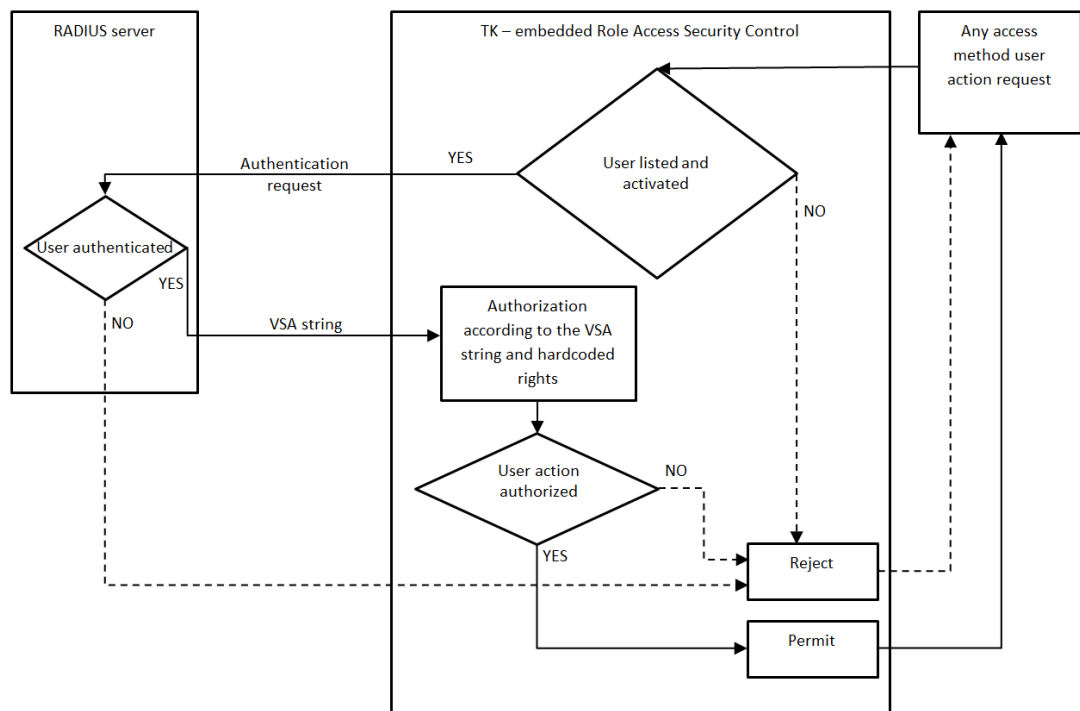


Figure 22: User action authorization scenario - RADIUS login mode

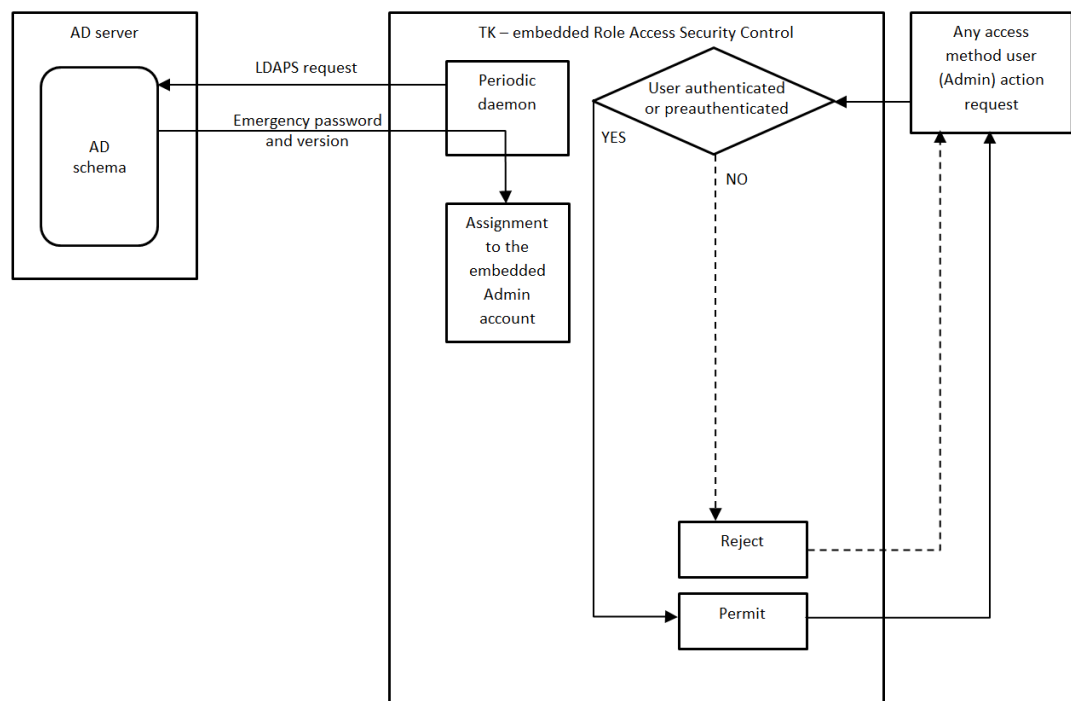


Figure 23: User action authorization scenario - password login mode

## 5. Security in REG-PE and REG-PED telecontrol boards models TK8xx

### 5.1 User access methods and protocols summary

#### 0 WinConfig online (web access)

- Internet browser client (like Internet Explorer) connects the web server embedded in the Linux OS inside the card.
- Protocol HTTPS with direct authorization is used.

#### 0 WinConfig console/shell menu (terminal access)

- Terminal client (like PUTTY) connects the SSH server embedded in the Linux OS inside the card.
- Protocol SSH with direct authorization is used

#### 0 WinConfig offline (web access and transfer access)

- Internet browser client connects the remote client-side proprietary web server (part of the WinConfig offline). A specialized server parts communicate with the card. It is recommended to use Internet Explorer as other browsers can have problems with displaying the web server pages.
- Data transfers use protocol HTTPS with direct authorization.
- Network scan (broadcast functions) and system parameterization use UDP with HTTPS preauthorization.

### 5.2 Roles in TK8xx telecontrol boards

Security system in telecontrol boards TK8xx uses two roles – *Administrator* and *User*. *Administrator* and *User* roles use rights as defined for *Administrator* and *Observer* in RBAC definitions. Default user is *Admin/teledata* and belongs to *Administrator* role.

Management of users can be done via online Winconfig, page *User Management (Security)* invoked by button with padlock symbol.

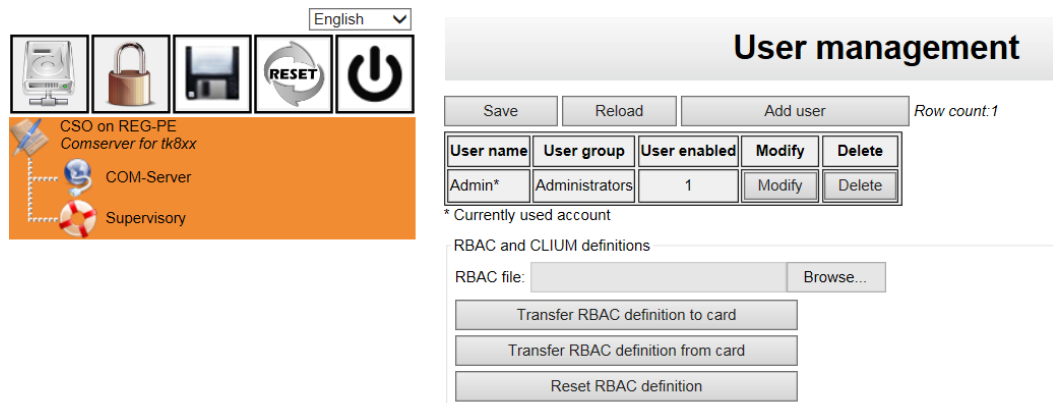


Figure 1: User management in the boards TK8xx (TK860)

## 5.3 Login modes

The TK8xx boards doesn't support *RADIUS mode*, there is only the *Password mode* implemented. The logged user has rights according to the current role.



Figure 1: Login example for boards TK8xx in http mode

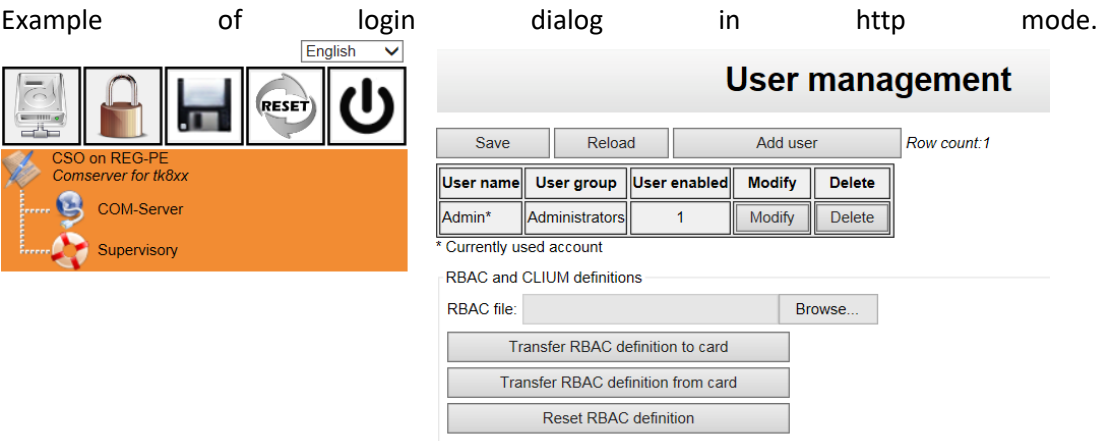


Figure 2: Login example for boards TK8xx in https mode (TK860)

Figure 3:

## 6. WinConfig REG-P / REG-PE / REG-PED / REG-PED<sup>SV</sup>

### 6.1 WinConfig Software introduction

WinConfig is software for managing of firmware and communication protocol settings of telecontrol boards and modules placed into A-Eberle device racks. WinConfig consists of of-line and online parts.

#### 6.1.1 Offline and online WinConfig

Offline WinConfig is a web-based program for the creation and management of files containing protocol settings, for two-way transfer of settings and firmware from a user PC to REG-P / REG-PE / REG-PED / REG-PEDSV boards and modules, and for identification of REG-P / REG-PE / REG-PED / REG-PEDSV devices connected to the network. Additionally, offline WinConfig can be used also for configuration of network and security parameters of connected telecontrol board.

Offline WinConfig splits into two main parts: the local web server and the local Web site with application libraries. WinConfig launches a local web server and a default web browser on your PC.

Settings may be prepared, stored and retrieved for various configurations without a direct link to the telecontrol board. Settings are saved in .xml file types.

Online Winconfig is also transferred to the telecontrol board together with settings and communication firmware. This software provides management of communication protocol settings and system functions focused to the management of telecontrol board system software, user management etc. with high level of security.

Telecontrol boards REG-P type TK400 are not equipped with online WinConfig. Such boards have to be equipped with COM-Server to identify itself within the network. COM-Server is part of all IEC101, IEC103 protocols installed as firmware and accessible by the offline Win-Config. COM-Server cannot work in TK519 and TK509 REG-P types without Ethernet connection.

Should one of the expressions used in this document be unclear to you, you may refer to the glossary at the end of this document for an explanation of it. Otherwise please feel free to contact us with your technical questions at this email address: [info@a-eberle.de](mailto:info@a-eberle.de).

## 6.1.2 Offline WinConfig software solution

Offline WinConfig program equipment consists of web server Mohican equipped with active pages for GUI and libraries developed in C# .NET software development environment for communication with telecontrol boards, file services and additional auxiliary functions.

Offline WinConfig prepares settings for REG-P / REG-PE / REG-PED with IEC101, IEC103, IEC104, DNP3 and Modbus protocols and COM-Server on a local host (local web server) and stores them in a standard file format - .XML file. The settings file can then be transferred via HTTPS to board flash memory in the case of REG-P / REG-PE / REG-PED / REG-PEDSV board type's models TK8xx, TK28x and TK102. WinConfig creates binary data files in Intel HEX format and transfers them into the board memory in the case of REG-P boards model TK400, TK509, TK519. Serial transfer via A-Eberle device or Ethernet transfer can be used according to the REG-P type. Firmware is always transferred together with settings, WinConfig use the latest firmware, which is part of its package.

### 6.1.2.1 Offline WinConfig processes, resources and security

There is only one Windows process called *WinConfig.exe* covering the entire functionality, internally realized as in-process components. The security behaviour of this process (access right, integrity, etc.) has to be set via standard Microsoft Windows methods depending on the host environment. The resources (free space on disk, usage of RAM, TCP/UDP connections) management is based on standard Windows and .NET methods.

### 6.1.2.2 Offline WinConfig - Mohican server TCP port management and logging

The default TCP port used by Mohican web server is port 8080. To avoid conflict in the case when this port is occupied, WinConfig always tests whether TCP port 8080 is free. If not, then WinConfig tries to increment the port number and finds the first free port. Such port number is written in the WinConfig configuration file and this number is consequently used for the WinConfig operation. The described test is performed always when WinConfig is launched.

The WinConfig software creates two log files:

#### 0 The log files created by C# libraries

These files are created in the WinConfig installation folder and are named according to the format *YYYY.MM.DD.WinConfig.log*, where YYYY.MM.DD is date of the log file creation. The maximum depth of the log files is 10 days; older files are deleted when WinConfig is launched.

#### 0 The log files created by Mohican web server

The logging created by Mohican web server is switched off by default. The logging can be switched on by editing the following line in the *Mohican.conf* configuration file placed in the WinConfig installation folder:

```
<Logging state="off">../log/httpserver.log</Logging>
```

To switch the logging on, change the *Logging state* option to "on". The option allows also setting of the log file name and folder. In the above stated example, the log file name is *httpserver.log* and will be created in the */log* subfolder of the WinConfig installation folder.

Remark:

Due to security reasons the embedded WEBserver always restricts multiple logins to online WinConfig and also login conflicts between online and offline WinConfig (data transfers). So it is good practice to ensure that there is nobody logged in the online WinConfig when the board is managed by offline WinConfig as an access conflict may appear in such cases.

### 6.1.3 Online WinConfig software solution

The software of the telecontrol board's type TK28x and TK102 is based on Embedded Linux operation system assembled for the appropriate hardware. The functionality of online WinConfig is ensured by configuration of Linux system parts - services and components (daemons) completed by processes ensuring the WinConfig functions.

The security behaviour of online WinConfig covering access rights, integrity, etc. is set via Linux settings and parameters and by implementation of Role Based Access Control (RBAC).

The resources (free space on flash, usage of RAM, TCP/UDP connections) management is based on standard Linux configurations, which are optimized as needed (e.g. behaviour of TCP connections).

RBAC access rules ensure only authorized access the telecontrol board system in offline and online WinConfig. Only authorized personnel can login, change parameters and properties of the system. Unauthorized access is excluded and high level of security is guaranteed.

WinConfig also checks user inputs for correctness and completeness and thus possibility of invalid user input is excluded. However, a special care should be taken and deep knowledge is necessary when changing important system parameters as careless change can cause unexpected malfunctions.

#### 6.1.3.1 Online WinConfig processes and daemons

System processes completing the Linux operational system by WinConfig functionality:

- 0 *goahead* - online WinConfig web server with modifications for WebREG,
- 0 *prp\_pcap\_tap\_userspace* – management of PRP redundancy network,
- 0 *txrx\_ledd* - daemon for management of LED diodes for indication of serial ports activity,
- 0 *udpsrv* - UDP daemon for management of communication with offline WinConfig and Reg-P-Loader,
- 0 *dropbear* - SSH server (version 2015.71),
- 0 *regploader* - for TK28-8 board type only, communication with REG-P-Loader (Windows based program),
- 0 *regsysupgrader* – software for communication with regulator for transfer of firmware and UDM files,
- 0 *viaregysloader* – for TK28-4 board type only, transfer of communication protocol settings using RegSys device with bootloader software,
- 0 */bin/sh* – various scripts for support of WinConfig functionality.
- 0 *TLS* version 1.2

Table 14: Protocol-based daemons and their usage

	<i>CSO</i>	<i>DNP3</i>	<i>IEC101</i>	<i>IEC104</i>	<i>IEC61850</i>
<i>ser2net</i>	yes	yes	yes	yes	yes
<i>dnp3xreg</i>	-	yes	-	-	-
<i>regx101</i>	-	-	yes	-	-
<i>iec104</i>	-	-	-	yes	-
<i>regx850</i>		-	-	-	yes
<i>regxsv</i>	-	-	-	-	yes



## 6.1.4 Logging in TK28x and TK102 telecontrol boards

There are several different parts of telecontrol board software that make logging independently – system parts of software, WebReg and application firmware. The application logging setting can be found in the supervisory part of the protocol settings.

Table 15: Logging in TK28x and TK102 - system

Logging in TK28x and TK102 - system				
<i>Target - format</i>	<i>Logger (logread) to RAM – Linux like text file</i>	<i>UDP SYSLOG server - syslog</i>	<i>MicroSD - Linux like log text file</i>	<i>Linux console - text</i>
<i>WinConfig part / where to set</i>	<i>hardcoded</i>	<i>set in online web (Supervisory)</i>	<i>set in online web (Supervisory)</i>	<i>hardcoded</i>
WinConfig system scripts	yes	no	no	yes
System login/logout (ssh, console, online WinConfig web server)	yes	yes	yes	no
REG-P-LOADER (TK28-8 CSO application remote loader)	yes	yes	yes	no
PTP operations	no	yes	yes	no
Upgrade of firmware/settings	yes	yes	yes	yes
REGSYS upgrade (A-Eberle device firmware or UDM upgrade)	yes	yes	yes	yes
Security operations (RBAC, CLIUM, CERTIFICATE, RADIUS)	no	yes	yes	no
Change of settings	no	yes	yes	no
Change of network parameters	no	yes	yes	no
CPU and memory thresholds	no	yes	yes	no
Viaregysloader (TK28-4 tele-control board settings upload via A-Eberle device)	no	no	no	yes
WebREG	no	yes	yes	no

Table 16: Logging in TK28x and TK102 – protocol applications, WebREG

Logging in TK28x and TK102 - protocol application, WebREG				
<i>target - format</i>	<i>logger (logread) to RAM - Linux like log text file</i>	<i>UDP SYSLOG server - syslog</i>	<i>Raw TCP - text</i>	<i>Linux console - text</i>
<i>WinConfig part / where to set</i>	<i>hardcoded</i>	<i>set in online web (Security GUI)</i>	<i>hardcode - if MicroSD with FAT32 partition present</i>	<i>hardcoded</i>
protocol applications	no	Some*	no	all (excl. CSO)

\* all applications excluding IEC104 and DNP3

#### Notes to logging:



- 1) Logger (local logging) represents standard Linux logging to text file. The tele-control boards use ramdisk for application operation, so local logs disappear after reboot. Local log file can be read using the shell user menu or using logread command.
- 2) The system and WebReg syslog works in the case when the IP setting of Syslog Server is not 0.0.0.0 or empty in the online WinConfig.
- 3) The unsuccessful login attempt is logged locally in any case and logged in the syslog when the IP setting of the Syslog Server is not 0.0.0.0 or empty in the online WinConfig.
- 4) The unsuccessful login attempt is logged to the microSD if it is present. The log has the form of permanent log file, which could be read using the shell user menu or via cat or other commands. It can be also read externally in Windows.
- 5) All log files are organized as round buffer and read as FIFO (listing shows the oldest as uppermost on the screen).

#### 6.1.4.1 Storage of log files in MicroSD

The TK28x and TK102 telecontrol boards can be equipped with microSD memory card for the purpose of local storage of log files.

The board system allows also first system initialization using MicroSD. The MicroSD can be equipped with boot partition and Linux partition for such purpose. The logging software of online WinConfig at first checks the MicroSD for presence of partitions. The following situations can appear:


- 0 If there is no partition present in the MicroSD, the logging software tries to create the logging partition.
- 0 If there is one partition present, the logging software tries to use it for the logging purposes.

- 0 If there are two partitions present, the logging software tries to create a third partition for the logging purposes.
- 0 If there are three or more partitions present, the logging software tries to use the third partition the logging purposes.

All successful or unsuccessful attempts are logged to syslog server.

The log records are stored in log files with fixed capacity and automatic way of creation.

If the logging file is full, the logging software stores it with actual date and starts logging to a new file.

If the logging partition is almost full, a warning message is sent to the syslog server. The threshold can be set in *Supervisory* settings in online WinConfig using the  icon.

If the entire logging partition is full then the oldest log file is deleted.

#### 6.1.4.2 Logging settings in online WinConfig


The logging settings are available in the *Supervisory* settings in online WinConfig using the  icon. Logging settings are available for Syslog and CD card logging. Default values of logging options are set to the most common values.

Table 17: Supervisory settings in online WinConfig

Setting	Format	Range	Default	Description
IP address of Syslog	IP address	4x 0 to 255	0.0.0.0	IP address of remote syslog
Syslog port		0 to 65535	514	Port of remote syslog
Login/logout		checkboxes	checked	Logging of login/logout to Syslog and/or SD card
PTP		checkboxes	checked	Logging of PTP operations to Syslog and/or SD card
Change of firmware/parameters		checkboxes	checked	Logging of firmware/parameters change to Syslog and/or SD card
Change of REGSYS firmware		checkboxes	checked	Logging of upgrade REGSYS firmware to Syslog and/or SD card
Security (RBAC, CLIUM, CERTIFICATE, RADIUS)		checkboxes	checked	Logging of security operations (RBAC, CLIUM, CERTIFICATE, RADIUS) to Syslog and/or SD card
Change of parameters		checkboxes	checked	Logging of change of parameters to Syslog and/or SD card
Change of network parameters		checkboxes	checked	Logging of change of network parameters to Syslog and/or SD card
Threshold values for CPU, memory and disk		checkboxes	checked	Logging of Threshold values for CPU, memory and disk to Syslog and/or SD card
Webreg		checkboxes	checked	Logging of Webreg to Syslog and/or SD card
Log temperature measurement		checkboxes	checked	Logging of temperature measurement to Syslog and/or SD card
Log memory of processes		checkboxes	checked	Logging memory of processes to Syslog and/or SD card
Inactivity timeout settings: Console timeout	[s]	30 to 7200	180	Console inactivity timeout
Inactivity timeout settings: Web timeout	[min]	5 to 120	30	Web inactivity timeout

Setting	Format	Range	Default	Description
Inactivity timeout settings: RADIUS period	[s]	60 to 7200	300	RADIUS period
Setting of thresholds: Period	[s]	30 to 1800	60	Period of thresholds check
Setting of threshold values: Threshold value for CPU	[%]	50 to 99	90	CPU threshold
Setting of threshold values: Threshold value for memory	[%]	50 to 99	90	Memory threshold
SD Card settings: Size of log file	[MB]	1 to 3000	1	Capacity of log file
SD Card settings: Limit for Log saving	[days]	1 to 30	30	Log saving limit
SD Card settings: Limit of used space	[%]	50 to 99	90	Limit of used space for warning
SNMP: Activate at startup		checkbox	checked	SNMP activation at startup
Port		0 to 65535	161	Port of SNMP client
User		Textbox 8-32		Identification of user
Authentication key		8 to 32 characters Listbox (MD5, SHA)	SHA	Authentication key Encryption method
Encryption key		8 to 32 characters Listbox (DES, AES)	AES	Encryption key Encryption method

#### NOTICE:

##### Notes:

The CPU load in Linux system is calculated as a usage of processor by processes. This value is recalculated to one processor core in Win-Config. The value includes active processes and also processes waiting in a queue so value over 100% can also appear and represents valid number.

For more information concerning the thresholds in Linux system see the following references:

<https://www.tecmint.com/understand-linux-load-averages-and-monitor-performance/>

<http://www.brendangregg.com/blog/2017-08-08/linux-load-averages.html>

#### Usage of SNMP:

The implementation of Simple Network Management Protocol (SNMP) supports version v3. The available nodes and data are defined in an internal configuration file (snmpd.conf). The data can be read (get) from the board e.g. using the Mib Browser tool.

The SNMP is disabled by default. Use online WinConfig to enable SNMP on the board and to set user, encryption methods and keys. The changes are written internally to the configuration file. Reset the board when required changes are done.

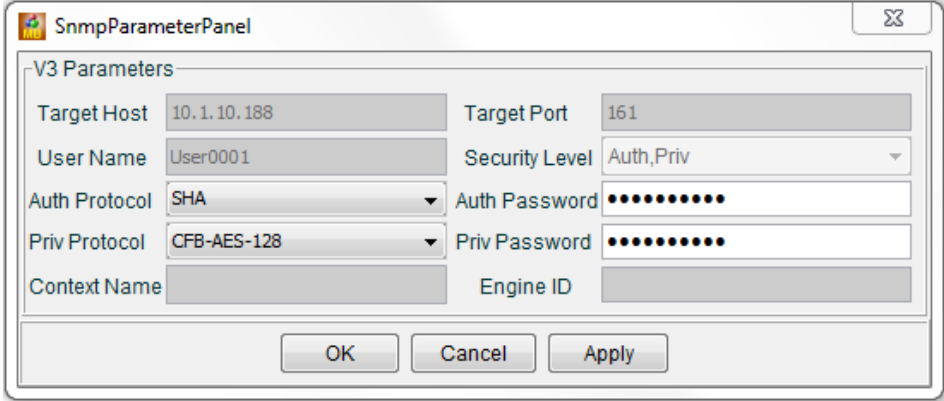
The available data can be read from the following MIB classes:

0 system from SNMPv2-MIB [.1.3.6.1.2.1.1]

0 interfaces from IF-MIB [.1.3.6.1.2.1.2]

For more information see e.g.

<http://www.net-snmp.org/docs/man/snmpd.conf.html>



The screenshot shows a dialog box titled "SnmpParameterPanel". Inside, there is a section labeled "V3 Parameters". The parameters are arranged in two columns:

- Target Host: 10.1.10.188
- Target Port: 161
- User Name: User0001
- Security Level: Auth,Priv (dropdown menu)
- Auth Protocol: SHA (dropdown menu)
- Auth Password: masked with dots
- Priv Protocol: CFB-AES-128 (dropdown menu)
- Priv Password: masked with dots
- Context Name: (empty field)
- Engine ID: (empty field)

At the bottom of the dialog, there are three buttons: OK, Cancel, and Apply.

Figure 4: Definition of SNMP connection parameters in the Mib Browser

We take care of it.

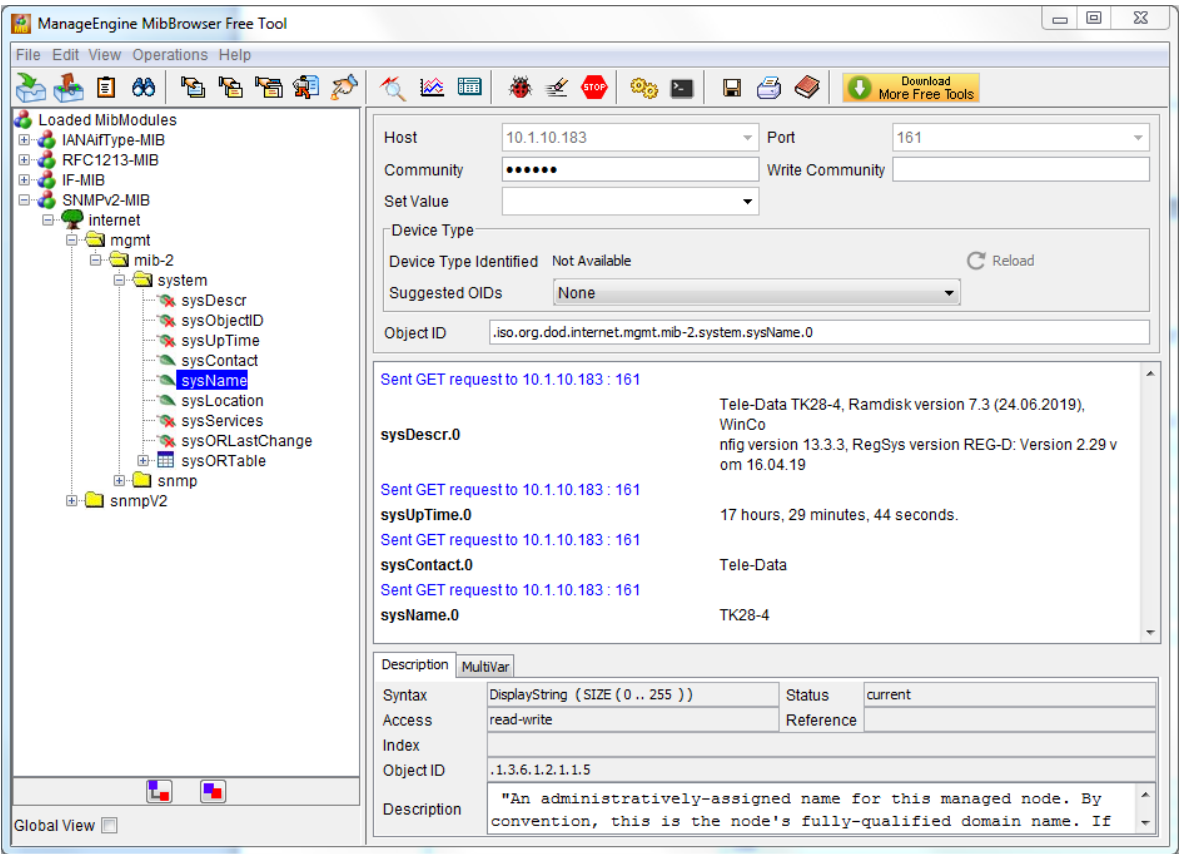


Figure 5: Getting the SNMP data in the Mib Browser



## Supervisory

Setting of Syslog a logging

IP adress of Syslog: 10.1.10.51
Syslog port: 514

	Syslog	SD card
Login/Logout:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
PTP:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Change of firmware/parameters:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Change of firmware for REGSYS:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Security (RBAC, CLIUM, CERTIFICATE, RADIUS):	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Change of parameters:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Change of network parameters:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Threshold values for CPU, memory and disk:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Webreg:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Log temperature measurement	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Log memory of processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Parameters of inactivity timeouts

Console timeout [s]: 180
Web timeout [min]: 30
Period of RADIUS server check [s]: 300

Setting of threshold values

Period [s]: 60
Threshold value for CPU [%]: 90
Threshold value for memory [%]: 90

SD card parameters

Size of log file [MB]: 1
Limit for log saving [days]: 30
Limit of used space [%]: 90

SNMP setting

Activate at startup: ☐
Port: 161
User:
Authentication key: SHA
Encryption key: AES

Save
Reset

Figure 6: Supervisory settings in online WinConfig

## 6.2 REG-PEX Loader software

The REG-PEX loader (RPL) is a software tool for transfer of Linux Kernel and RAM disk into the REG-PE(D) (TK8xx models only) and PQI-DA telecontrol boards equipped only with U-Boot software. Such boards cannot cooperate directly with WinConfig. The RPL also allows change of board IP settings and selection of kernel with/without the bonding feature.

The RPL is a low-level software tool and should be used by advanced users only.

The RPL software is contained in the WinConfig installation package and can be launched from *Transfer from PC* page by the *Run RPL* button. The WinConfig also offers launch of RPL in the case when no REG-PE(D) telecontrol board is detected.

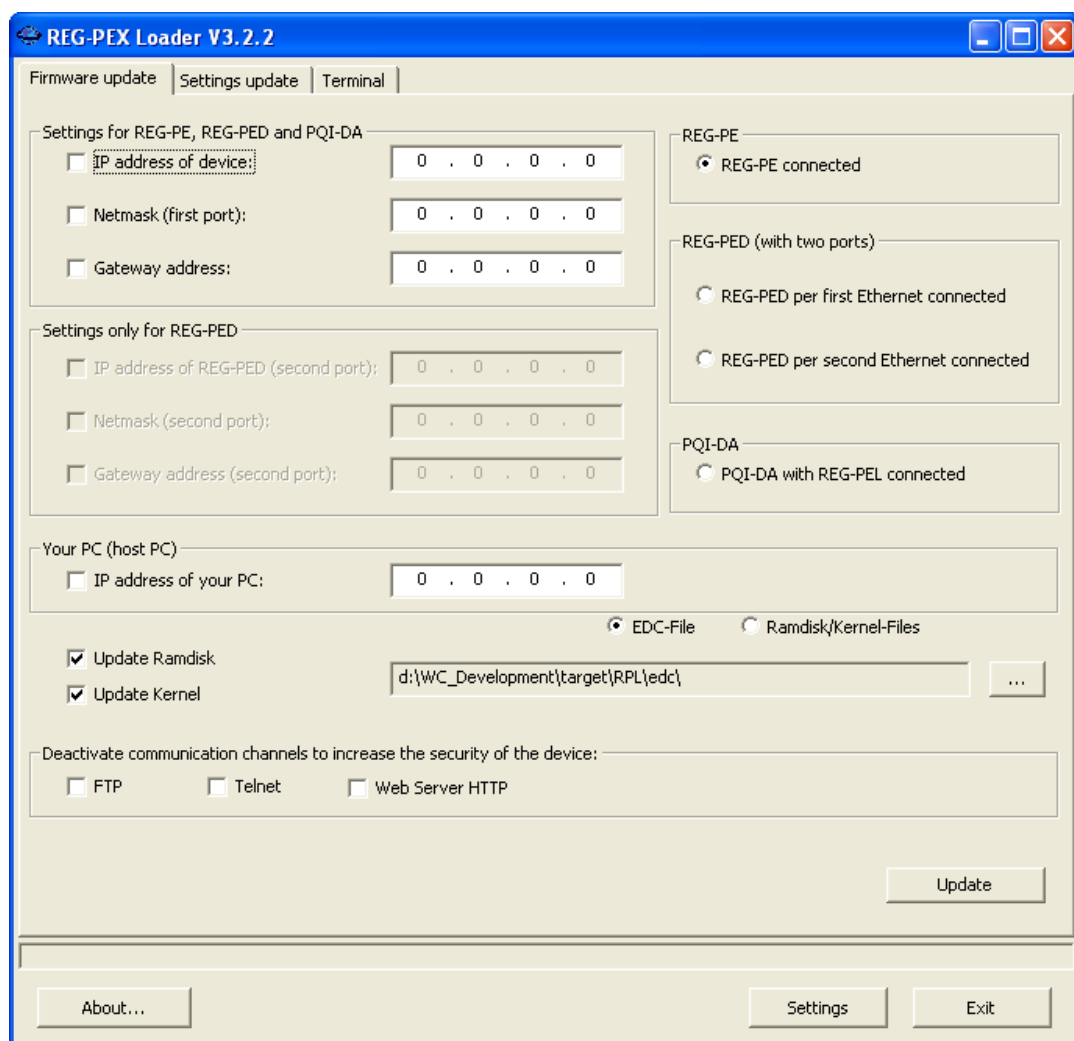


Figure 7: The RPL window

To transfer Linux Kernel and RAM disk into the REG-PE(x) follow these steps:

- ➡ Connect the PARAM connector of REG-PE(x) board and your computer with the RS232 cable supplied with the A-Eberle device or with any serial null modem cable.
- ➡ Connect your computer and the REG-PE(x) board by Ethernet cable. Some Ethernet adapters do not switch to the correct mode automatically, so please use preferably a crosslink patch cable.
- ➡ Fill the IP address lines in RPL window.
- ➡ Use the (...) button to browse the edc file placed in the WinConfig installation folders. There are two edc files distributed in the WinConfig setup, the difference is in the versions of Kernel - with/without support of bonding. Select whatever of the two files as bonding and related features can be set later using the *Change of IP settings for REG-PE(D) telecontrol boards* WinConfig function.
- ➡ Press the *Update* button.

➡ The update process can be seen in the RPL tab Terminal.

## 6.3 Communication with REG-P(E)(D)(SV) telecontrol board in WinConfig 11

A higher level of security for data transfer and communication with REG-PE(D) telecontrol board is used in WinConfig v.11. The online WinConfig (www pages placed in the board memory) can be disabled in the *Transfer settings from PC* page in offline WinConfig or in the *REG-PE(D) board IP settings* page in online WinConfig or in user menu.

The new firmware supports several functions as described below.

The following secured communication technologies are used in WinConfig 11:

- 0 SSH is used for remote access to console. This access is typically used for basic board configuration. A SSH client (e.g. PUTTY) is necessary for this type of connection.
- 0 HTTPS (HTTP over SSL) together with SSL certificates is used for communication between off-line WinConfig and telecontrol board.

**NOTICE:**

Note on HTTPS accounts functionality when upgrading/downgrading from/to WinConfig 10

When user upgrades from WinConfig 10 to 11 using offline WinConfig, one of the HTTPS accounts (username and password) from version 10 (passwords coded by XOR, not by SHA2 hash) is used. The accounts defined in the version 10 coded by XOR remain in the upgraded version 11. The individual account is changed to the new SHA2 coding version in the moment when user changes this account in the WinConfig 11.

The file with SHA2 coded accounts remains in the telecontrol board when downgrading from version 11 to version 10. Offline WinConfig 10 using XOR password coding will not work in such case. To solve such situation, the user can change the accounts using FTP or serial PARAM port or to delete the account file `/mnt/jffs2/config/webs_users.conf`. When the file is deleted, the default account will be used.

### 6.3.1 Rules for higher security



It is strongly recommended to switch off at least the online WinConfig and change the factory default passwords to get highest security concerning data and software stored in telecontrol board.

User should also disable all network services that are not necessary for the board operation and management, namely SSH and HTTPS (WinConfig).

**NOTICE:**

When creating a new user password, keep also in mind the basic rules for secure passwords:

- ➡ Password should be at least 10 characters long
- ➡ Use at least one uppercase and at least one lowercase letters (A...Z, a...z)
- ➡ Use at least one number (0...9)
- ➡ Use at least one special character `@%.,/!,:;=^~_-`. Other characters are not allowed.



For more information about secure and strong passwords we recommend the BSI web pages in the Internet (<https://www.bsi.bund.de/EN>).

## 6.3.2 Actions supported by firmware and their usage:

### Restart of board

- Prepare empty file named *reboot* and copy it in the */xload/new* folder.
- Wait approx. 20s for the automatic restart of board.

### Installation of new XML settings and ICD file

- Prepare new settings file named *settings.xml* and copy it in the */xload/new* folder.
  - Prepare new ICD file (if ICD change is required) and copy it to the folder.
  - Prepare empty file named *move* and copy it.
  - Wait approx. 20s for the automatic move and installation of the files.
  - Prepare empty file named *reload* and copy it.
  - Wait approx. 20s for the automatic reload of files transferred in the previous sequence.
- Reload can be used if there was change in the supervisory parameters only. Otherwise use *restart*, see item 1.

### Installation of new certificates

- Prepare device certificate in the *cert.pem* file and copy in the */xload/new* folder. The certificate has to be in the PEM format.
  - Prepare and copy also the key as *key.pem* file.
  - If required, prepare and copy also the intermediate certificates as *intercert.pem* file.
- The certificates must be in PEM format and must be sorted starting with the certificate to the highest level (root CA).
- Alternatively, the CA certificate can also be copied as the *cacert.pem* file.
  - Prepare empty file named *cert\_move* and copy it in the */xload/new* folder.
  - Restart the board, see item 1.

## 6.3.3 SSH access (REG-PEx, TK102, TK28x)

SSH is used for remote access to console. The file transfer is encrypted and protected by user login and password.

The *remoteuser* login can be used with the *remoteuser* password in the case of REG-PE(D) telecontrol boards.

The access is driven by sequence of user menu that allow user to show and/or change the board settings of to show logs of kernel, system and applications.

The menu sequence is modified according to the current user role and rights.

### 6.3.4 Menu and meaning of individual items:

#### Main menu

##### Network menu

- ➡ *Go to menu for network setting and diagnostic*

##### Services menu

- ➡ *Go to menu administration of network services (SSH/SFTP, HTTPS)*

##### Log menu

- ➡ *Go to menu showing logs*

##### Change terminal password

- ➡ *Change of SSH and SFTP passwords. Change is applied to the currently logged user. Program asks for entering of old password and two times new password. Attention, a change is applied immediately.*

##### Change Spare password

- ➡ *This option allows an additional possibility to change Spare password. The name **Spare password** also reflects possible change of the mode name i.e. correct name appears in this option if the name was changed.*

##### HTTPS user's management

- ➡ *Go to administration of HTTPS users (off-line WinConfig)*

##### Logout

- ➡ *Terminal logout*

##### Reboot

- ➡ *Restart telecontrol board*

##### Recovery menu

- ➡ *Go to recovery mode. This menu item is shown only in the case of access via local serial port. Another condition is that the board has to be prepared for the recovery mode (the R key is pressed in the moment or recovery notification during the card restart).*

##### Start root shell

- ➡ *The root shell is determined only for administrators and is not available for remoteuser and localuser.*

#### Network menu

##### Ping ICMP

- ➡ *The ICMP ping is determined for the diagnostic of network connection. The system asks for counterparty IP. The ICMP echo-request packet is used. The user network interface is determined by routing table.*

#### Ping ARP

- *The ARP ping is determined for the diagnostic of network connection within one subnet. The system asks for counterparty IP and, if there are more network interfaces (TK885), it asks also for the interface to be used. This ping usually passes through firewall. The ARP protocol is not routed to other networks.*

#### Show routing table

- *Shows current routing table.*

#### Show interfaces

- *Shows current list of network interfaces with parameters (IP address, mask, MAC address and statistics of sent and received data).*

#### Show saved network parameters (IP addresses, bonding)

- *Shows network parameters (IP address, mask, gateway, state of bonding) saved in the flash memory. These parameters will be used after board restart.*

#### Set network parameters (IP addresses, bonding)

- *Setting of network parameters (IP address, mask, gateway, state of bonding) solved as a series of questions and answers. Possible options of bonding parameters:*

1. *Disabled*
2. *PRP V1*
3. *Broadcast mode*
4. *Bridge with RSTP*

#### Back

- *Go to main menu.*

### Services menu

#### Services state

- *Shows the state of SSH/SFTP and HTTPS services (enabled or disabled).*

#### Enable SSH/SFTP

- *Enables SSH/SFTP service. The change takes effect after board restart.*

#### Disable SSH/SFTP

- *Disables SSH/SFTP service. The change takes effect after board restart.*

#### Enable WinConfig (https, network detect)

- *Enables services necessary for the communication with off-line WinConfig. The change takes effect after board restart.*

#### Disable WinConfig (https, network detect)

- ➡ *Disables services necessary for the communication with off-line WinConfig. The change takes effect after board restart.*

Enable WinConfig WWW pages

- ➡ *Enables WinConfig WWW pages.*

Disable WinConfig WWW pages

- ➡ *Disables WinConfig WWW pages.*

Back

- ➡ *Go to main menu.*

#### NOTICE:

Attention:

When both SSH/SFTP and HTTPS accesses are disabled, it is not possible to connect the board remotely. The local access via PARAM port only is possible in such case.

### Log menu

Application and system log

- ➡ *Shows log with messages from system and from user applications.*

Kernel log

- ➡ *Shows log with messages from system kernel.*

Back

- ➡ *Go to main menu.*

### HTTPS user's management menu

List users

- ➡ *Shows list of user accounts for HTTPS service (users of off-line WinConfig).*

Change user password

- ➡ *Changes user password. The service asks for old password and two times for the new password.*

↪ The change takes effect after board restart.

Add new user

- ➡ *Adds a new user account. The service asks for new account name and two times password.*

↪ The change takes effect after board restart.

Delete user

- ➡ *Deletes existing user account. The service asks for existing user account name.*



↩ The change takes effect after board restart.

Back

➡ Go to main menu.

### Recovery menu

Reboot and format applications part of firmware

➡ Sets the formatting flag and performs board reset.

#### NOTICE:

Attention:

This service formats the jffs2 area without the possibility of a recovery. This service is determined for emergency situations only, when the board stuck and there is no other possibility of fix. The off-line WinConfig can be consequently used for transfer of new firmware.

Back

➡ Go to main menu.

### 6.3.5 Transfer of settings from / to a PC

The following ways of data transfer are available:

- 0 Serial transfer via A-Eberle device (for example a REG-D regulator) using serial booter firmware saved in the telecontrol board memory (available for boards TK5xx, TK400 and TK28-4)
- 0 Ethernet TCP transfer using Ethernet booter firmware saved in the telecontrol board memory (available for TK400 boards). Ethernet transfer can be used in local mode with manual board reset or in remote mode with automatic reset (available for TK400 telecontrol boards with COM-SERVER or CSO firmware installed).
- 0 Ethernet HTTPS transfer (available for TK8xx, TK28x and TK102 telecontrol boards) in offline and online modes too.

#### Transfer communication protocol settings from PC

Transfer from PC to telecontrol board can be performed in the following ways depending upon the types of telecontrol board and application program:

- 0 Transfer via a serial connection of A-Eberle device for telecontrol board types TK28-4, TK517, TK509 and TK400 via *Manual transfer from PC button*. User has to enter COM port number of connected PC and manually set the A-Eberle device and telecontrol board to the serial down/upload state before transfer can begin.
- 0 Transfer via local Ethernet connection for TK400 board type by *Manual transfer from PC button*. Telecontrol board has to be manually reset by reset button on TK400 board to run Ethernet booter so this way of data transfer is usable only if user has access to the A-Eberle device rack. WinConfig performs automatic detection of manual reset event of telecontrol board and automatically chooses free IP address within the given subnet if the current IP address of telecontrol board cannot be used for connection with the Ethernet booter. IP settings for TCP connection with Ethernet booter are used only for the current TCP session. In the case of manual Ethernet transfer, the WinConfig function has to be started first and then the TK400 board has to be reset so that the WinConfig program can detect start of Ethernet booter program.
- 0 Transfer via remote via Ethernet connection using COM-Server on remote PC and Ethernet booter application programs for TK400 by *Remote transfer from PC button*. If the current IP address of telecontrol board is out of the visible subnet the Program automatically chooses free IP address within the given subnet for connection with the Ethernet booter. Board reset is performed automatically in this case so this way of data transfer is intended for remote usage. IP settings for TCP connection with Ethernet booter are used only for the current TCP session. This method is not available for the DNP protocol. Detection of available boards has to be performed before the remote transfer function can be activated.
- 0 Transfer remotely from PC via Ethernet using HTTPS protocol for REG-P (TK28-4), REG-PE (TK28-6) and REG-PED<sup>SV</sup> (TK102) telecontrol boards by *Remote transfer from PC button*.

Detection of available boards has to be performed before the remote transfer function can be activated. The detection of available telecontrol boards is done by UDP broadcast telegrams using UDP port 12000 and proprietary protocol developed for the

detection purposes. Remote data transfers are done via HTTPS protocol after successful user pre-authentication according to the login mode.

The detection table contains more information about the detected board like IP and Mask, MAC, PRP activity and others.

UDP communication is encrypted by AES256 for telecontrol boards type TK28x and TK102.

The detection algorithm finds out if the IP address and mask of the telecontrol board can be accessed from some of the active Network Interface Controllers (NIC) on the user PC, if it is possible to connect the board using HTTPS and if it is first connection to the board after factory initialization (for board types TK28x and TK102).

For more information see chapter 6.5.4 Transfer settings from PC function for telecontrol boards type REG-PE(D), TK28 and TK102

Progress bar, operation step and status information are displayed on screen in all cases of data transfer.

#### Transfer from telecontrol board to PC

Transfer to PC (reading of settings from telecontrol board) can be performed in similar ways to transfer from PC:

- 0 Transfer manually via serial line of A-Eberle device for board types TK28-4, TK517, TK509 and TK400
- 0 Transfer manually and locally via Ethernet for TK400 board type
- 0 Transfer remotely via Ethernet using *COM-Server* and *Ethernet booter* application programs for TK400
- 0 Transfer remotely via Ethernet using HTTPS protocol for TK8xx, TK28x and TK102 board types.

User actions for transfer to PC are similar to those for transfer from PC.

Card type, name	Firmware type, version	Version of settings, date	Name of settings	Device IP address	Net Mask	MAC address	PRP active	Port types
REG-PE (TK28-6), TK28-6	SPABUS, 3.2.0.39234 (r.d0c7009)	13.4.6, 2018-12-15	REG-DxSPA-Bus Standard Configuration	10.1.10.184	255.255.255.0	00D09344FE87	yes	copper, 100BASE-FX

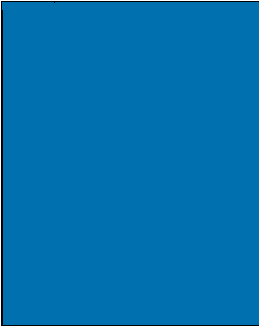
Figure 8: Example of detection table, REG-PE type TK28-6

#### NOTICE:

Important note:

When settings are transferred from PC to telecontrol board, they are always transferred together with appropriate application (protocol converter, firmware), with online WinConfig (web pages etc.) for REG-PE(D) boards and also together with RAMdisk and kernel for REG-PE(D) boards (can be selected as option).

Thus, the remote detection (Detect on LAN) performed by WinConfig after successful transfer of data shows version of application (proto-



col, firmware) and also version of WinConfig that was also transferred to telecontrol board. The settings file has the same version number as WinConfig.

If verification of digital signature for boards TK28x and TK102 fails during transfer of settings from offline WinConfig, the failure is logged to syslog via the connected telecontrol board. Correct setting of logging to syslog in the telecontrol board settings is required for this functionality.

## 6.4 Serial data transfer for REG-P telecontrol boards TK5xx, TK400

The line type *Serial via A-Eberle device* and *Serial port number* has to be selected to run the serial data transfer. Use a full modem cable and follow the instructions on the screen.

### Transfer settings to PC

Transfer settings from telecontrol board to PC

Board type: REG-P, PQI-DA (TK400) ▼

Line type: Serial via Eberle device ▼

Serial port number: 1

Operation

Progress:  0%

Status:

Activity:

*Put the device in loader mode according to the manual, press reset button of telecontrol board, wait until serial booter runs and click the 'Manual transfer to PC' button. Wait cca 30s after restart for TK400 REG-P type.*

Manual transfer to PC

Compare with selected settings

Figure 9: Serial data transfer, REG-P



In the case of problems with serial transfer when USB/Serial converter is used in your PC, hints for possible solution of the problem can be shown in another browser window after clicking the Hints button.

The most important thing is to set the Latency timer parameter to 1.

Operation

Progress:  100%

Status: Finished

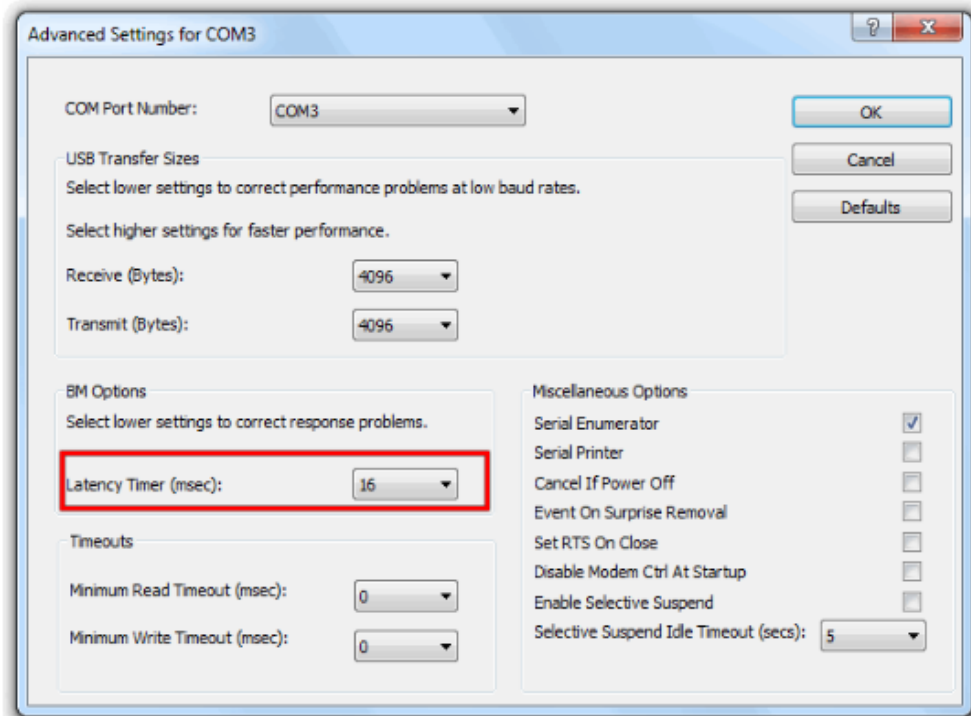
Activity: Error: No response

Hints

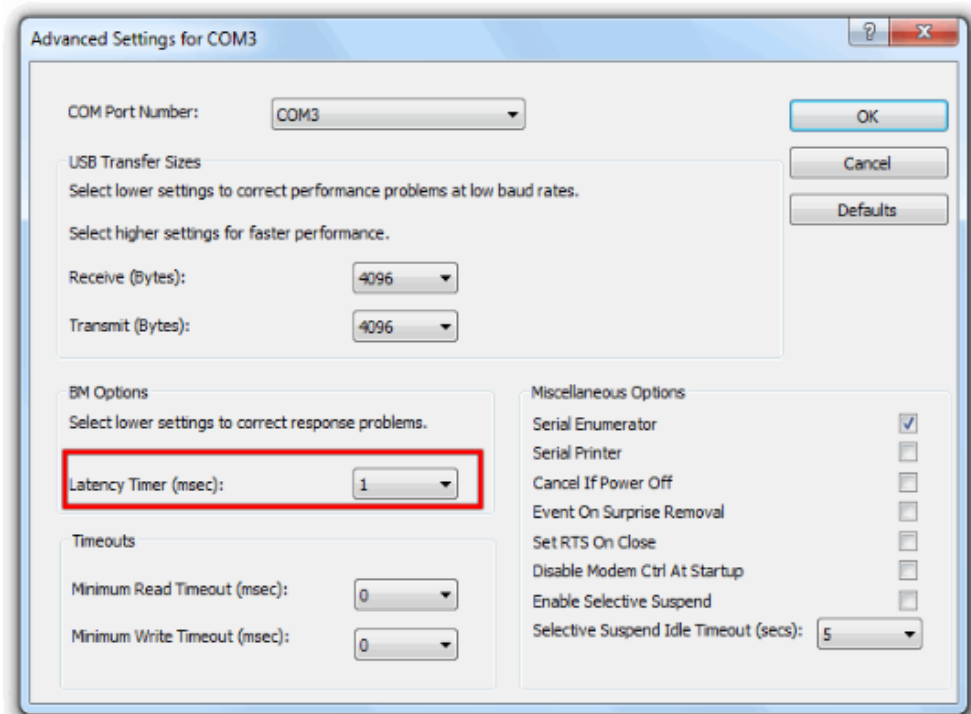
Figure 10: Hints button

We take care of it.

---



**Select Latency parameter**



**Change value to 1**

*Figure 11: Serial transfer hints*

### 6.4.1 Serial data transfer for REG-P telecontrol board TK28-4

Serial data transfer for the TK28-4 board consists of more options due to the Linux operating system.

- 0 The transfer of Linux system files and default application (CSO) can be time consuming depending on the type of device processor.
- 0 The transfer of application and settings is the most common transfer with ensured compatibility of both files.
- 0 The transfer of settings should be used only in the case when it is sure that the protocol application recorded in the board is compatible with the new settings.

**Transfer settings from PC**

Transfer settings from PC to telecontrol board

Line type: Serial via Eberle device ▼

Transfer of Linux system files and default application: ☐

Transfer of application and settings: ☒

Transfer of settings only: ☐

Serial port number: 1

Operation

Progress:  0%

Status:

Activity:

Bring the A-Eberle device into the loader mode (described in the manual), press reset button of telecontrol board, wait until the serial loader is active (with REG-P type TK400 approx. 30s and with REG-P type TK28-4 approx. 60s) and press the 'Manual Transfer from PC' button. The activity of the serial loader can also be detected by the LEDs on protocol cards with LEDs. With the REG-P TK400 the serial loader is active when the green and yellow LED in line S/R/F 1 flash in common mode. In addition, the LEDs of the Ethernet socket also flash in common mode. With the REG-P TK28-4 the activity of the serial loader is indicated by the simultaneous flashing of the green and yellow LED in line S/R/F 2.

Manual transfer from PC

Run RPL

Cancel

Figure 12: Serial data transfer, TK28-4



If the update of Linux files (ramdisk) is desirable, choose first the 1st option and consequently 2nd option with required protocol application.

## 6.5 Ethernet data transfer

### 6.5.1 TK400 telecontrol board:

Detection of board is performed by COM-Server program (CS or CSO) that has to be enabled and running in board memory. Remote operations without running CS cannot be performed while manual Ethernet transfer is still available.

Ethernet operations are not available for DNP3 protocol.

Data transfer from/to the board is done via Ethernet booter program NBOOT which runs after card reset. Temporary change of IP settings applies also to NBOOT.

### 6.5.2 REG-P (TK28-4), REG-PE (TK28-6, TK860) and REG-PED<sup>SV</sup> (TK102, TK885) telecontrol boards:

It is recommended to change the IP address of the PC in the case when the board IP address is out of range of addresses accessible for the PC.

However, for the TK8xx telecontrol boards it is also possible to let the WinConfig to change temporarily the address of telecontrol board. The temporary change of IP settings can apply to one or two board interfaces according to the IP configuration of the board and connected PC. Original board IP settings are automatically renewed after successful data transfer or after approximately 5 minutes timeout in the case of connection breakage during transfer. Note that this option is valid for TK8xx boards only.

The Application protocol running on board is interrupted during transfers.

The Data transfers from/to TK8xx, TK28x and TK102 boards are done via secured HTTPS protocol.

#### **Survey of cases when Ethernet data transfers cannot be performed:**

- 0 Telecontrol board is connected via LAN with router or firewall, which prevents telegrams used by WinConfig from passing through.
- 0 PC with running WinConfig has two or more Ethernet interfaces connected to the same subnet.
- 0 There is no free IP address in the connected subnet to be used for re-addressing of telecontrol board Ethernet interface.
- 0 Ethernet interface of PC with running WinConfig has the same IP address as connected telecontrol board Ethernet interface.



### 6.5.3 Transfer settings from PC function

To transfer selected settings please click the  icon which can be found in the main menu. The following Data transfer now appears on the right side of the settings tree.

Transfer settings from PC

Transfer settings and firmware from PC to telecontrol board

Line type: Ethernet

Transfer mode

Manual transfer: ☐

Remote transfer: ☒

Operation

Progress: 0%

Status:

Activity:

Detect on LAN

Remote transfer from PC

Figure 13: Remote transfer from PC, REG-P

#### Available controls:

- 0 *Line type* – selection of the way of data transfer (Ethernet or serial via A-Eberle device)
- 0 *Transfer Mode: Manual transfer or Remote transfer* – selection of the way of data transfer
- 0 *Detect on LAN* – function of the automatic detection of telecontrol boards with CSO or COM-SERVER firmware connected to LAN. List of detected boards can be seen in the above placed table after successful detection.
- 0 *Remote transfer from PC* – execution button for activating remote transfer function.

Transfer settings from PC

Transfer settings and firmware from PC to telecontrol board

Line type: Serial via Eberle device

Serial port number: 1

Operation

Progress: 0%

Status:

Activity:

Put the device in loader mode according to the manual, press reset button of telecontrol board, wait until serial booter runs and click the 'Manual transfer from PC' button. Wait cca 30s after restart for TK400 REG-P type.

Manual transfer from PC

*Figure 14: Manual transfer from PC*

If the manual transfer function is selected, the user has to prepare A-Eberle device rack for data transfer manually.

**Ethernet transfer** – click the *Manual transfer from PC* button **first** and **then** reset the telecontrol board. WinConfig waits until Ethernet booter runs, changes temporarily its topical IP settings, establishes TCP connection and performs required data transfer. All actions are performed automatically.

**Serial transfers** – put the A-Eberle device in the loader mode, reset telecontrol board and wait until the serial booter runs. Then click the *Manual transfer from PC* button.

**NOTICE:**

Serial null modem cable with modem signals (RTS/CTS) has to be used to enable hardware handshaking during data transfer.

## 6.5.4 Transfer of settings from PC for TK28-4, TK28-6 and TK102 telecontrol boards

HTTPS data transfer is used for the transfer of settings, optionally with or without firmware (Linux Kernel and Ramdisk) in the case of TK8xx, TK28x and TK102 telecontrol board types. In the case of REG-PED (TK885), the correct REG-PED version has to be selected using radio buttons when the telecontrol board firmware (Linux Kernel and TK8xx RAM disk) is also transferred. The Login information has to be entered to transfer data successfully.

**Transfer settings from PC**

Transfer settings and firmware from PC to telecontrol board

Automatic firmware transfer: ☒

Forced firmware transfer: ☐

Please choose your application case

☒ Usage of max. 3 COM ports

☐ Usage of max. 4 COM ports (forbidden in case of double optic Ethernet)

Authorization - standard mode

User name:

Password:

Transmission protocol

Transmission protocol is set to HTTP

HTTPS protocol is recommended for improved security of data transfers.

Services

Enable www pages: ☒      Unlock UBoot: ☒

Enable SSH/SFTP: ☒      Unlock Console: ☒

For more information about board services see tooltips.

Card type, name	Firmware type, version	Version of settings, date	Name of settings	Device IP address	MAC address
REG-PED (TK885), Lojza	IEC103, 4.10.0	13.0.1, 20120911	IEC103_REG-D Standard Configuration	10.1.10.205, 10.2.10.206	00D09322DF32, 00D09322DF33

Operation

Progress:  100%

Status: Finished

Activity: Completed detecting devices

Steps to transfer settings

1. Detect board on LAN
2. Select board in the table
3. **Transfer from PC to device**

States of detected boards

HTTPS transfer possible

HTTPS transfer blocked

IP unreachable (click for hint)

Unknown state

Figure 15: Transfer from PC for telecontrol boards type REG-PE(D)(SV)

**Special controls:**

- 0 *Automatic firmware transfer/Forced firmware transfer* radio button – selection whether WinConfig is supposed to decide about necessity to transfer also kernel, RAM disk or both (*Automatic firmware transfer*) or whether kernel and RAM disk will be transferred in any case (*Forced firmware transfer*).
- 0 *Selection of application case* – selection of the correct version of the REG-PED board concerning usage of COM ports. This selection affects the version of telecontrol board firmware.
- 0 *User name* – user login for HTTPS access The *Admin* account in password mode
- 0 *Password* – user password for HTTPS access
- 0 *Use last login values* – used last remembered login values
- 0 *Forget login values* – don't remember the entered login values
- 0 *Transmission protocol*:
  - Set HTTPS - use HTTPS protocol for data transfers to ensure security of transferred data,
  - Set HTTP - use standard unsecured HTTP protocol.
- 0 *Available board services: Enable WWW pages, Enable SSH/SFTP, Unlock UBoot, Unlock Console* – options are dedicated to advanced user and allow to modify behaviour of telecontrol board to achieve security of data transfers by enabling/disabling the corresponding services or by performing the indicated actions.
- 0 *Change board IP settings* – this button switches to the *REG-PE(D) board IP settings* page.
- 0 *Run RPL* – this button runs the *REG-PEX loader* configuration software that can be used to configure a REG-PE(D) board in the case when the firmware on board is insufficient for the detection by WinConfig. The usage of RPL requires serial connection between the PC and board being configured.
- 0 *Submit certificates* – this button switches to the *Submit certificates* page.
- 0 *Available board services* – check buttons to enable/disable board services
  - *Enable www pages* – this option enables/disables online WinConfig installed in the board. If www pages are disabled, user can manage the board by menu system.
  - *Enable SSH/SFTP* – this option enables the online console (access to board via menu system).
  - *Unlock UBoot* – option to enable/disable user access by interrupting the boot process before the UBoot is executed.
  - *Unlock Console* – This option unlocks SSH access to console instead of user menu. This option is not available for telecontrol boards TK28x and TK102 where the console access is always locked.
- 0 *States of detected boards*

- *HTTPS transfer possible* – the board is ready for data transfer.
- *HTTPS transfer blocked* – The transfer is not possible. Probable reason of this is setting of firewalls in user PC or unavailable WEB server in the board.
- *IP unreachable* – If the board IP address is out of range of IP addresses visible from the user PC. Click this item to show hints to solve this problem by changing the IP address of PC. Another possibility is to let the WinConfig to change temporarily the address of telecontrol board; this option is valid for TK8xx telecontrol boards only.
- The *IP unreachable state* can appear also when there is Ethernet interface with correct IP address present in the user PC, but this interface is disconnected or connected to wrong network. In such cases please check correct connection of Ethernet interfaces.
- *Unknown state* – The board cannot be read by *Detect* function.

#### 6.5.4.1 REG-P (TK28-4), REG-PE (TK28-6) and REG-PED<sup>SV</sup> (TK102) telecontrol boards detected for the first time

As it is stated in the *Functionality concepts* chapter above, the user has to change the emergency password in the case of first detection of the board. The state of detected board is marked with the colour *Password has to be changed* board state.

Card type, name	Firmware type, version	Version of settings, date	Name of settings	Device IP address	MAC address
REG-PE (TK28-6), TK28-6	unknown,	unknown	unknown	192.168.55.36, 192.168.1.214	000F6BFAE022, 000F6BFAE023
REG-PE (TK28-6), TK28-6	CSO, 3.2.0	11.2.5, 20120422	Comserver for tk8xx	10.3.10.185, 192.168.1.214	000F6BFAE00C, 000F6BFAE00D

Operation

Progress:  100%

Status: Finished

Activity: Completed detecting devices

Detect on LAN

Transfer from PC to device

Change board IP settings

Steps to transfer settings

1. Detect board on LAN
2. Select board in the table
3. Transfer from PC to device

States of detected boards

HTTPS transfer possible

Password have to be changed

HTTPS transfer blocked

IP unreachable (click for hint)

Unknown state

Figure 16: First detection of TK28x and TK102 boards

#### 6.5.4.2 REG-P (TK28-4), REG-PE (TK28-6) and REG-PED<sup>SV</sup> (TK102) telecontrol boards with online WinConfig connected for the first time

The same rule is valid also for the online WinConfig connected for the first time in the case when the emergency password was not changed before using offline WinConfig. In such a case the following dialog appears:

Emergency password

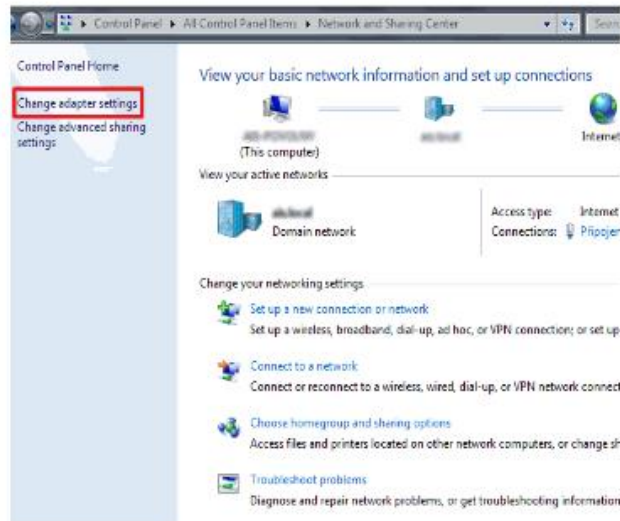
Password:

Retype password:

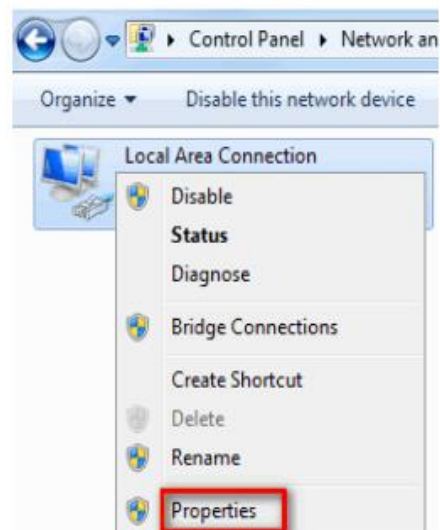
Figure 17: First connection with online WinConfig

## Hints for 'IP unreachable' problem

Hints in the case of 'IP unreachable' problem



Go to Control Panel - change adapter settings



Select adapter properties

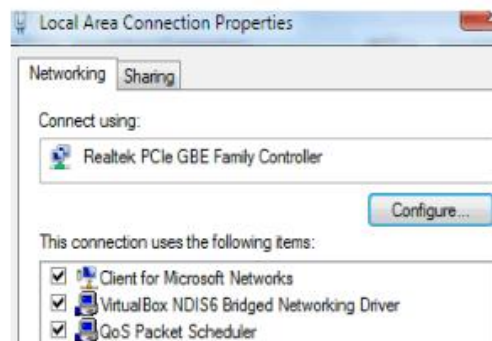


Figure 18: Hints for "IP unreachable" problem

### 6.5.5 Change of IP settings for REG-PE(D) telecontrol boards

To change the IP settings for telecontrol board type REG-PE(D) (TK8xx TK28-x) click the *Change board IP settings* button, which appears on the screen when successful detection of the board on LAN is performed and the particular board is selected. The detection can be done before the data transfer either from or to PC. The IP setting of the telecontrol board is protocol-independent. The following window appears on screen:

## REG-PE(D)(SV) board IP settings

Set IP settings to telecontrol board

Board type: REG-PE (TK28-6)

Board name:

Couple of 1. and 2. Ethernet

Use PRP V1 (Parallel Redundancy Protocol): ☐

Use Ethernet interfaces bonding (Broadcast): ☐

Use Ethernet interfaces independently: ☒

Enable RSTP according to IEEE 802.1D: ☐

1. Ethernet interface

MAC: 000F6BFAE022

IP address:

Subnet mask:

Gateway IP address:  ☒ Gateway used

☐ Use VLAN with ID:

2. Ethernet interface

MAC: 000F6BFAE023

IP address:

Subnet mask:

Gateway IP address:  ☐ Gateway used

☐ Use VLAN with ID:

Authorization - password mode

Password:

Operation

Progress:

Status:

Activity:


Go to "Transfer to PC" page 

Figure 19: REG-PE(D) board IP settings

Enter new values and click the *Set* button to change IP settings of the Ethernet interfaces.



If you want to prevent an Ethernet interface fail, click the *Use Ethernet interfaces bonding* option box to bond Ethernet interfaces and to use 'Active backup' policy.

The 2<sup>nd</sup> Ethernet interface is available only for REG-PED (TK885) board type. One of the defined gateways can be selected as default gateway by the radio button *Gateway used*.

To switch off the bonding of Ethernet interfaces check the *Use Ethernet interfaces independently* checkbox.

To use PRP V1(Parallel Redundancy Protocol) check the *Use PRP* checkbox.

To enable RSTP defined according to the IEEE 802.1D check the *Enable RSTP* checkbox.

To enable usage of Ethernet interface in VLAN check the *Use VLAN with ID* checkbox and enter the VLAN ID number.

### 6.5.6 Change of IP settings for REG-PED<sup>SV</sup> (TK102) telecontrol boards

The TK102 board can be equipped with extension module that contains another couple of Ethernet ports. Such extension can be detected during the detection process. The *REG-PE(D) IP settings page* is extended by parameters of 3<sup>rd</sup> and 4<sup>th</sup> Ethernet ports in such a case.

There is a limitation of configurations of the two pairs of Ethernet ports. If the 1<sup>st</sup> couple is set to Parallel Redundancy Protocol (PRP) or Ethernet bonding then the second couple has to be set as two independent Ethernet ports.

Couple of 3. and 4. Ethernet

Use PRP V1 (Parallel Redundancy Protocol): ☐

Use Ethernet interfaces bonding (Broadcast): ☐

Use Ethernet interfaces independently: ☒

Enable RSTP according to IEEE 802.1D: ☐

3. Ethernet interface

MAC: 000F6BFAEC08

IP address: 192.168.2.214

Subnet mask: 255.255.255.0

Gateway IP address: 0.0.0.0 ☐ Gateway used

☐ Use VLAN with ID: 0

4. Ethernet interface

MAC: 000F6BFAEC09

IP address: 192.168.3.214

Subnet mask: 255.255.255.0

Gateway IP address: 0.0.0.0 ☐ Gateway used

☐ Use VLAN with ID: 0

Figure 20: Couple of 3. and 4. Ethernet (TK102)

### 6.5.7 Submit certificates for TK28-4, TK28-6, TK860 and TK885, TK102 tele-control boards

Security certificates are used for HTTPS communication with REG-PEx telecontrol board. Telecontrol boards are supplied with default factory certificates that can be rewritten by user certificates.

The user certificate can be obtained from the Certification Authority (CA) or generated by a special program (e.g. OpenSSL). The certificates have to be in the PEM (Privacy Enhanced Mail) format; other formats can be converted to the PEM using appropriate program.

The certificate typically consists of a *certificate file* and a *key file*. If the certificate is issued by the CA, then there is also the *CA certificate file* and possibly also an *intermediate certification file*, in the case that the Intermediate certification authority is used by the CA. The *key file* must not be password protected to be accepted by the REG-PEx.

In the case when a special program is used for generation of certificate, it is possible to generate the CA or to use the CA that is already available (3 created files) or to generate a self-signed certificate (2 created files).

For more information about certificates please consult the publicly available information in the Internet.

All necessary actions for rewriting the default certificates can be done on the *Certificates and RBAC* page where also RBAC and CLIUM definition files can be transferred to the board.

To submit user certificates, browse the certificate files and transfer them to the telecontrol board by *Submit* button.

## Certificates and RBAC

Transfer of files

*All certificate and key files are expected in PEM format.*

Certificate file:  [Browse...](#)

Key file:  [Browse...](#)

[Transfer certificates to card](#)

---

RBAC file:  [Browse...](#)

[Transfer RBAC definition to card](#) [Reset RBAC definition](#)

---

CLIUM file:  [Browse...](#)

[Transfer CLIUM definition to card](#) [Reset CLIUM definition](#)

---

Authorization - standard mode

User name:

Password:

[Use last login values](#) [Forget login values](#)

---

Operation

Progress:

Status:

Activity:

---


Go to "Transfer from PC" page 

Figure 21: REG-PE(D) board certificates, RBAC and CLIUM files

### 6.5.8 Bonding

The Ethernet interface bonding is a software feature to achieve higher security. If the feature is activated then have the Ethernet interfaces the same MAC and IP addresses. This leads to redundancy in the case of an broken Ethernet cable.

When the bonding option is switched ON, the firmware uses the Ethernet interface via which the connection was established and in the case of connection breakage (link is down because of broken or disconnected Ethernet cable), the firmware automatically switches to the second bonded interface that works as backup.

The *Use Ethernet interface bonding* option and the dual Ethernet ports are available only for the TK885 board type, the TK860 and TK885-1 card types have only one Ethernet interface available.

Furthermore, there are more conditions in connection with the bonding option:

The TK885 board with 2x fibre optic COM ports has always the COM 4 port disabled and bonding available.

Other versions of the TK885 board use two different firmware's (Linux Kernels), in according to the bonding function. The checkbox *Use Ethernet interfaces bonding* in the REG-PE(D) board IP settings page of WinConfig is enabled/disabled according to the Kernel version of the REG-PED board detected and selected in the previous Transfer settings from the PC page.

If the bonding is required but not supported by the current Kernel loaded in the board, go to the Transfer settings from the PC page and transfer the settings together with the firmware and the correct version of the REG-PED board.

If the bonding option is available in the firmware then the COM 4 port cannot be used.

When using the bonding feature, always keep in mind that the correct version of the firmware with bonding option has to be selected for boards with electric or electric/fiber optics Ethernet interfaces and the bonding option has to be switched ON in the RED-PED board IP settings page. Also keep in mind that the COM4 serial port cannot be used in the case of firmware with the bonding option.

### 6.5.9 PRP - Parallel Redundancy Protocol

A network redundancy means to have two independent active paths between two devices. The sender REG-PED (TK885) and REG-PED<sup>SV</sup> (TK102) use two independent network interfaces that transmit the same data simultaneously. Then the redundancy monitoring protocol makes sure that the recipient uses only the first data packet and discards the second. If only one packet is received, the recipient knows that a failure has occurred on the other path. The parallel redundancy protocol is described in the IEC 62439-3 standard.

The REG-PED<sup>SV</sup> (TK102) telecontrol board can be equipped with two pairs of network interfaces. There is a limitation in such a case. Only one pair of network interfaces can be set to PRP protocol or other available bonding features. Another pair of network interfaces has to be operated as two independent ports. For more information see chapter 6.5.6 *Change of IP settings for REG-PED<sup>SV</sup> (TK102) telecontrol boards*.

## 7. Support for script-based upgrade procedure for TK28-4, TK28-6 and TK102 telecontrol boards and A-Eberle devices firmware

### 7.1 Concepts

#### 7.1.1 SW architecture

The REG-P(E)(D)(SV) of type TK28-x or TK102 telecontrol boards (cards) have Embedded Linux based operation system. The supported upgradeable parts are:

- 0 SYSTEM.FIT image – filesystem of the operating system (sometimes called rootfs or ramdisk in the Linux environment). It includes for example an embedded web server binaries, SSH server binaries etc.
- 0 TKxxxxx.TGZ – application tarball. It includes applications (protocols) binaries and Win-Config online files (scripts, web pages etc.). It does not include settings files.
- 0 YYY.XML – settings file (also called template) – parameterization file for applications. It is distributed in the pair with corresponding ICD file in the case of IEC61850 application type.

#### 7.1.2 Concept of upgrade

The supported upgrade method works in the following steps:

- 0 The User prepares *distribution scripts* by using the provided *preparation script* (*distribution scripts* include desired files to upgrade, digital signature and prepared script-based upgrading code).
- 0 The User runs the *upgrade script* with the appropriate parameters towards one target card.
- 0 The *Upgrade script* connects the SSH server on the card and copies the *distribution scripts* to the card.
- 0 The *Upgrade script* runs remotely the *distribution scripts* that start the upgrade process. The process typically consists of the following steps:
  - Verification of the digital signature of distribution script.
  - Checking of target HW compatibility.
  - Stopping and blocking actually running applications.
  - Restart.
  - Transfer of the distribution script.
  - Parsing the distribution script to the zipped upgrade files and upgrade script.
  - Upgrade.

We take care of it.

---

- Restart.
- 0 Two restarts appear during the entire upgrade process.
- 0 The process can be automated by the user as needed.

### 7.1.3 Security concept

The following security issues are implemented:

- 0 The distribution script is digitally signed using certificate issued especially for this purpose. This private key is distributed in the upgrade support package. There is also an appropriate public key distributed as part of the TK card system. It is used for verification of signature in the start of upgrading procedure.
- 0 The User has to use the right credentials to connect the SSH server on the target card. Both RADIUS and password modes are supported.
- 0 The upgrade process uses the backup/upgrade/restore method of workflow so the original state is restored if the upgrade fails.
- 0 The A-Eberle device firmware file in **mot** format is digitally signed by A-Eberle and the end user uses this signed file for the upgrade. The TK card system checks signature and verifies that the firmware is authorized by A-Eberle. The appropriate public key is distributed as part of the TK card system, the private key remains at A-Eberle Company for signing purposes.

### 7.1.4 Hosting environment

The two versions of upgrade support packages for Windows and Linux environments are distributed. Both packages include similar tools and use identical methods for preparation and upgrade.

## 7.2 Installation of upgrade support package

### 7.2.1 Windows

The installation package should be unpacked or copied to the desired folder. The package includes all necessary binaries (7z.exe, plink.exe, openssl.exe, tee.exe, wget.exe), static libraries (7z.dll, libeay32.dll, ssleay32.dll, libiconv2.dll, libintl3.dll, libssl32.dll), scripts (preparation.bat, run\_upgrade.bat), templates (upg\_restart.tpl, upg\_system.tpl, upg\_application.tpl, upg\_settings.tpl, upg\_firmware.tpl), key (fd.key) and subfolders (/UPG\_RESTART, /UPG\_SYSTEM, /UPG\_APPLICATION, /UPG\_SETTINGS, /UPG\_FIRMWARE). No other installation steps are needed and no other software has to be installed. The installation package is compatible with Windows 7 and higher, 64-bit.

## 7.2.2 Linux

The installation package should be unpacked or copied to the desired folder. The package includes all necessary scripts (preparation.sh, run\_upgrade.sh), templates (upg\_restart.tpl, upg\_system.tpl, upg\_application.tpl, upg\_settings.tpl, upg\_firmware.tpl), key (fd.key) and subfolders (/UPG\_RESTART, /UPG\_SYSTEM, /UPG\_APPLICATION, /UPG\_SETTINGS, /UPG\_FIRMWARE). The following software packages have to be installed:

- 0 ssh
- 0 sshpass
- 0 wget

## 7.3 Preparation of upgrade

### 7.3.1 Windows

The preparation script is *preparation.bat*. It has to run with the parameter "MODE", indicating what to prepare. The parameter valid values are following:

- 0 "MODE=s" (example: C:\Upgrade\preparation.bat "MODE=s") for preparation of tele-control board system upgrade.
- 0 "MODE=a" (example: C:\Upgrade\preparation.bat "MODE=a") for preparation of tele-control board applications upgrade.
- 0 "MODE=x" (example: C:\Upgrade\preparation.bat "MODE=x") for preparation of tele-control board settings upgrade.
- 0 "MODE=f" (example: C:\Upgrade\preparation.bat "MODE=f") for preparation of A-Eberle device firmware upgrade.

Appropriate files have to be copied in the preparation folders before running the preparation script:

- 0 For system upgrade – folder /UPG\_SYSTEM, system.fit and testimage.tgz are needed.
- 0 For application upgrade – folder /UPG\_APPLICATION, applications.tgz is needed, settings.xml (and corresponding ICD file in the case of IEC61850 application) is recommended.
- 0 For settings upgrade – folder /UPG\_SETTINGS, settings.xml (and corresponding ICD file in the case of IEC61850 application) is needed.
- 0 For A-Eberle firmware upgrade – folder /UPG\_FIRMWARE, firmware. smot is needed (digitally signed mot firmware file).

Various temporary text files (\*.txt) are created in the installation folder during the preparation process.



## 7.3.2 Linux

The preparation script is `preparation.bat`. It has to run with the parameter "MODE", indicating what to prepare. The parameter valid values are following:

- 0 "MODE=s" (example: `\upgrade\preparation.sh "MODE=s"`) for preparation of telecontrol board system upgrade.
- 0 "MODE=a" (example: `\upgrade\preparation.sh "MODE=a"`) for preparation of telecontrol board applications upgrade.
- 0 "MODE=x" (example: `\upgrade\preparation.sh "MODE=x"`) for preparation of telecontrol board settings upgrade.
- 0 "MODE=f" (example: `\upgrade\preparation.sh "MODE=f"`) for preparation of A-Eberle device firmware upgrade.

Appropriate files have to be copied in the preparation folders before running the preparation script:

- 0 For system upgrade – folder `/UPG_SYSTEM`, `system.fit` and `testimage.tgz` are needed.
- 0 For application upgrade – folder `/UPG_APPLICATION`, `applications.tgz` is needed, `settings.xml` (and corresponding ICD file in the case of IEC61850 application) is recommended.
- 0 For settings upgrade – folder `/UPG_SETTINGS`, `settings.xml` (and corresponding ICD file in the case of IEC61850 application) is needed.
- 0 For A-Eberle device firmware upgrade – folder `/UPG_FIRMWARE`, `firmware.smot` is needed (digitally signed mot firmware file).

Various temporary text files (\*.txt) are created in the installation folder during the preparation process.

## 7.3.3 Digital signature of A-Eberle device firmware file

The files necessary for support of digital signatures of A-Eberle device firmware files are distributed in the folder `/EBERLE`. This folder is not intended for distribution to the end user. The folder contains scripts `sign_mot_udm.bat` for digital signing. The file name of mot file is used as parameter of the script; result is the file `filename.smot` which should be copied to the folder `/UPG_FIRMWARE` and renamed to `firmware.smot`. The script uses private key file "fd.key".

## 7.4 Upgrade process

### 7.4.1 Windows

The upgrade script is `run_upgrade.bat`. It has to run with 5 parameters "MODE", "SERVER", "USER", "PWD", "HW" indicating what to upgrade and connection parameters.

The parameter "MODE" range of values is:

- 0 "MODE=s" for telecontrol board system upgrade.
- 0 "MODE=a" for telecontrol board applications upgrade.

- 0 "MODE=x" for telecontrol board settings upgrade.

- 0 "MODE=f" for A-Eberle device firmware upgrade.

The parameter "SERVER" is IP address or host name of the target TK card.

The parameters "USER" and "PWD" are user name and password for login to the target TK card according to the security model – RADIUS or password. All security models provide users, who have rights to perform script-based remote upgrade.

The parameter "HW" indicates the target card type. Range of permitted values is "HW=TK28-4", "HW=TK28-6", "HW=TK28-8", "HW=TK102" and "HW=". The last blank value should be used in the case when unexpected state of upgrade occurs – for example unattended interruption of upgrade process after first stage etc. In such cases the card remains without appropriate HW version info available. The value of "HW=" disables checking of HW version compatibility and forces the upgrade without compatibility check. Such upgrade can be risky and should be use carefully only in the situations when the HW info from the card is not available. The value of "HW=" cannot be used in the system upgrade and A-Eberle device firmware upgrade modes.

Example:

```
run_upgrade.bat "MODE=a" "SERVER=10.1.10.185" "PWD=password2" "USER=scripter"
"HW=TK28-6"
```

Various temporary text files (\*.txt) are created in the installation folder during the upgrade process. Some temporary "sedxxx" files are also created and can be occasionally deleted.

## 7.4.2 Linux

The upgrade script is run\_upgrade.sh. It has to run with 5 parameters "MODE", "SERVER", "USER", "PWD", "HW" indicating what to upgrade and connection parameters.

The parameter "MODE" range of values is:

- 0 "MODE=s" for telecontrol board system upgrade.

- 0 "MODE=a" for telecontrol board applications upgrade.

- 0 "MODE=x" for telecontrol board settings upgrade.

- 0 "MODE=f" for A-Eberle device firmware upgrade.

The parameter "SERVER" is IP address or host name of the target TK card.

The parameters "USER" and "PWD" are user name and password for login to the target TK card according to the security model – RADIUS or password. All security models provides user, which have the rights to perform script-based remote upgrade.

The parameter "HW" indicates the target card type. Range of permitted values is "HW=TK28-4", "HW=TK28-6", "HW=TK28-8", "HW=TK102" and "HW=". The last blank value should be used in the case when unexpected state of upgrade occurs – for example unattended interruption of upgrade process after first stage etc. In such cases the card remains without appropriate HW version info available. The value of "HW=" disables checking of HW version compatibility and forces the upgrade without compatibility check. Such upgrade can be risky and should be use carefully only in the situations when the HW info from

the card is not available. The value of "HW=" cannot be used in the system upgrade and A-Eberle device firmware upgrade modes.

Example:

```
\upgrade\run_upgrade.sh "MODE=a" "SERVER=10.1.10.185" "PWD=password2" "USER=scripter" "HW=TK28-6"
```

Various temporary text files (\*.txt) are created in the installation folder during the upgrade process.

### 7.4.3 Sequential upgrade

The upgrade process allows also sequential upgrade of several TK boards. In such case the user runs the preparation script, creates the *IP.txt* file in the folder with scripts and modifies the script file *sample\_loop.bat*.

The *IP.txt* file will contain IP addresses of boards prepared for upgrade. The *sample\_loop.bat* contains loop with *run\_upgrade.bat* activation, where the appropriate parameters has to be entered (MODE, USER, PWD, HW). The script takes the IP addresses from the *IP.txt* file. The tee redirection can be used for record of all console outputs from entire loop to output text file.

Example:

0 *IP.txt* file structure:

- 10.1.10.55
- 10.1.10.78
- 10.1.10.48
- .
- .

0 Modification of *sample\_loop.bat* (parameters to modify marked as **bold**)

```
for /f %x in (ip.txt) do call run_upgrade.bat "MODE=f" "SERVER=%x" "PWD=password"
"USER=User" "HW=TK28-6" | tee output.txt
```

## 7.5 Hints

### 7.5.1 How to ensure compatibility

The only tool which ensures the compatibility between application and settings is Windows based WinConfig offline program. It is necessary to use its functionality to ensure the compatibility between uploaded application package and settings xml file.

Best practice to do it is to open the desired xml settings file in the WinConfig and save it back to the new file. WinConfig makes necessary background changes in the settings file to ensure compatibility with the application version included in its package. Opening and saving the settings file ensures application of necessary changes to get the same correct settings file, which WinConfig use for downloading.

It is recommended to use the application upgrade mode with prepared settings xml file (and corresponding ICD file in the case of IEC61850 application) included in the UPG\_APPLICATION folder (as "settings.xml"). Such procedure is close to the way how WinConfig makes upgrade.

### 7.5.2 Output of scripts to console

It is good practice to analyze the console output produced by upgrade scripts in the case of problem and in other cases as well.

### 7.5.3 Protection of production files

The text scripts and templates should remain marked as read-only in the file system to avoid some accidental overwriting. The scripts targeting to Linux (all shell scripts, templates on Linux) should be transferred and copied carefully to avoid changing of EOL characters and leave them UNIX styled.

### 7.5.4 A-Eberle device firmware upgrade

The firmware upgrade takes quite a long time (minutes).

Note:

- 0 There is a long timeout (approx. 15 minutes) before resetting the A-Eberle device to the default working state in the case of failed transfer of firmware to the A-Eberle device. The device is not working and interacting during this interval.
- 0 COM3 port (telecontrol board) and COM1S port (A-Eberle device) are used for firmware update.

## 8. Disassembly & disposal

The disposal of the LVRSys™ is carried out by A. Eberle GmbH & Co. KG.

➡ Send all components to:

A. Eberle GmbH & Co. KG  
Frankenstraße 160  
D-90461 Nuremberg



## 9. Warranty

A. Eberle GmbH & Co. KG. warrants that this product and accessories will be free from defects in materials and workmanship for a period of three years from the date of purchase.

Warranty does not apply to damage caused by:

- 0 Accidents
- 0 Misuse
- 0 Abnormal operating conditions

To make a warranty claim, please contact your local A.Eberle distributor or alternatively contact A. Eberle GmbH & Co KG in Nuremberg, Germany

## 10. List of Figures

Figure 1:	Login dialog.....	11
Figure 2:	Definition of new password .....	12
Figure 3:	Locking of account.....	12
Figure 4:	Logout button.....	13
Figure 5:	Information about login mode on Regsys screen.....	13
Figure 6:	Adding groups.....	21
Figure 7:	Adding TK cards .....	22
Figure 8:	Shared secret.....	22
Figure 9:	Network policies.....	23
Figure 10:	Network policy configuration.....	23
Figure 11:	Authentication methods.....	24
Figure 12:	Vendor specific attributes .....	25
Figure 13:	Vendor specific attribute setting.....	26
Figure 14:	Example how Administrator has to fill the unique OID property of each new attribute.....	29
Figure 15:	Admin for A-Eberle cards .....	30
Figure 16:	Configuration of attributes.....	31
Figure 17:	Password mode setting, RBAC and other security settings.....	32
Figure 18:	Password mode setting, RBAC and other security settings.....	33
Figure 19:	Offline WinConfig management of RBAC definition files.....	36
Figure 20:	Online WinConfig access method – first/next authentication.....	40
Figure 21:	Offline WinConfig access method – first/next time authentication .....	40
Figure 22:	User action authorization scenario - RADIUS login mode .....	41
Figure 23:	User action authorization scenario - password login mode.....	41
Figure 1:	User management in the boards TK8xx (TK860) .....	43
Figure 1:	Login example for boards TK8xx in http mode.....	43
Figure 2:	Login example for boards TK8xx in https mode (TK860).....	44
Figure 3:	.....	44
Figure 4:	Definition of SNMP connection parameters in the Mib Browser .....	55
Figure 5:	Getting the SNMP data in the Mib Browser.....	56
Figure 6:	Supervisory settings in online WinConfig.....	57
Figure 7:	The RPL window .....	58
Figure 8:	Serial data transfer, REG-P .....	69
Figure 9:	Hints button.....	69
Figure 10:	Serial transfer hints .....	70
Figure 11:	Serial data transfer, TK28-4 .....	71
Figure 12:	Remote transfer from PC, REG-P .....	73
Figure 13:	Manual transfer from PC.....	74
Figure 14:	Transfer from PC for telecontrol boards type REG-PE(D)(SV) .....	75
Figure 15:	First detection of TK28x and TK102 boards.....	78
Figure 16:	First connection with online WinConfig.....	78

Figure 17:	Hints for “IP unreachable” problem .....	79
Figure 18:	REG-PE(D) board IP settings .....	80
Figure 19:	Couple of 3. and 4. Ethernet (TK102) .....	81
Figure 20:	REG-PE(D) board certificates .....	83

## 11. List of Tables

Table 1:	Definition of roles .....	15
Table 2:	Offline WinConfig access method actions-to-role default rights .....	16
Table 3:	Online WinConfig access method actions-to-role default rights, part 1.....	16
Table 4:	Online WinConfig access method actions-to-role default rights, part 2.....	17
Table 5:	Shell menu access method actions-to-role default rights.....	17
Table 6:	Remote script-based upgrade access method actions-to-role default rights.....	17
Table 7:	WebReg actions-to-role default rights, part 1. ....	17
Table 8:	WebReg actions-to-role default rights, part 2. ....	18
Table 9:	WebReg actions-to-role default rights, part 3. ....	19
Table 10:	WebReg actions-to-role default rights, part 4. ....	19
Table 11:	Definition of roles .....	20
Table 12:	Radius mode settings .....	27
Table 13:	AD server settings.....	34
Table 14:	Protocol-based daemons and their usage.....	48
Table 15:	Logging in TK28x and TK102 - system.....	49
Table 16:	Logging in TK28x and TK102 – protocol applications, WebREG.....	50
Table 17:	Supervisory settings in online WinConfig.....	52





## Notes

[illegible]

[illegible]

[illegible]



A. Eberle GmbH & Co. KG

Frankenstraße 160  
D-90461 Nuremberg  
Germany

Tel.: +49 (0) 911 / 62 81 08-0  
Fax: +49 (0) 911 / 62 81 08 96  
E-Mail: [info@a-eberle.de](mailto:info@a-eberle.de)

<http://www.a-eberle.de>

Presented by:

---

**Copyright 2018 by A. Eberle GmbH & Co. KG**

Subject to change without prior notice.