CODEKS Tools program

Program for establishing communication
and changing the settings of Jantar devices
(Codeks Tools 9.8.48.2 version and newer)

User manual for the Codeks Tools program

Naklo, 2023

Table of Content

1. Codeks Tools

The ***Codeks Tools*** program is an additional program of the *Codeks software family* and is designed to be used for the initial setup of Jantar hardware devices before they are connected into the *Codeks* system for time attendance or access control. With the *Codeks Tools* program, you can set basic device parameters, establish, test and edit communication with devices, and download and update firmware on Jantar devices.

1.1. License information

- Logo "Hand" is registered at EUIPO (The European Union Intellectual Property Office) and is exclusively owned by Jantar d.o.o. You may not copy, imitate, rent, lease, sell, modify or otherwise use the "hand" logo, except as provided in this or any other agreement with Jantar d.o.o. Any such unauthorised use will result in immediate and direct termination of this license and may result in criminal and/or civil prosecution.

Codeks Tools software is distributed together with the Jantar hardware or separately as a replacement system for an existing access control system, which means:

- All copyrights of Codeks Tools are exclusively owned by the author, Jantar d.o.o.
- You may not use, copy, emulate, clone, rent, lease, sell, modify, decompile, disassemble, otherwise reverse engineer, or transfer the licensed program, or any subset of the licensed program, except as stated in this agreement. Any such unauthorised use shall result in immediate and automatic termination of this license and may result in criminal and/or civil prosecution.
- Codeks Tools binary code may NOT be used or reverse engineered to re-create the Codeks access control, time and attendance or communication algorithms which are proprietary and protected by copyright law.
- Codeks is distributed "as is". No warranty of any kind is expressed or implied. You use the Codeks şoftware at your own risk. Neither the author nor his authorised distributors will be liable for any data loss, damages, loss of profits or any other kind of loss while using, misusing or being unable to use this software.
- All rights not expressly granted here are reserved by Jantar d.o.o.
- By installing and using the Codeks Tools add-on you are accepting the terms and conditions of this license.
- If you do not agree with the terms of this license you must remove all Codeks Tools files from your storage devices and cease using the product.

1.2. Disclaimer and Warranty

Disclaimer

The information in this document is subject to change without notice. While the information contained herein is assumed to be accurate, Jantar d.o.o., assumes no responsibility for any errors or omissions. We also reserve the right to discontinue or change the specifications of products without prior notice. No claim can be made in the case of profit or loss from use or sale of any products bought or delivered by us. Errors reported will be corrected in new software releases.

Warranty

This manual comes "as is" - no warranty of any kind, expressed or implied. Jantar d.o.o. does not give any assurances or guarantee in connection with information in this document.

Although we strive to include accurate and up to date information, Jantar d.o.o., without prejudice to the generality of this paragraph does not guarantee that the information in this manual is complete, true, accurate and not misleading.

The information in this manual is designed for user purposes and not as a substitute for information from customer regulations, technical manuals/documents or other official documents. Customers using this manual can report errors or omissions, recommendations for improvement or other comments to Jantar d.o.o..

1.3. Contact information

Jantar d.o.o. has more than 30 years of experience in the development and production of access control, time attendance and visitor control systems. What sets us apart from our competitors is that we develop and manufacture all of our software and most of our hardware ourselves. Our systems are installed and utilized at airports, office buildings, financial institutions, factories, shopping centers, hospitals, etc. Our products are present virtually anywhere our clients need basic or advanced access control and time and attendance systems.

Jantar, elektronski sistemi, d.o.o.
Kranjska cesta 24, SI-4202 Naklo
SLOVENIA

VAT ID: SI34737332

E-mail: info@jantar.si
Web page: www.jantar.si

SUPPORT

For support contact our regional partner: https://jantar.si/en/contact/our-partners/

2. Description and installation

The ***Codeks Tools*** program is an additional program of the *Codeks software family* and is designed to be used for the initial setup of Jantar hardware devices before they are connected into the *Codeks* system for time attendance or access control. With the *Codeks Tools* program, you can set basic device parameters, establish, test and edit communication with devices, and download and update firmware on Jantar devices.

The Codeks Tools software package contains:

- **the Codeks Tools installation file and**
- **the user manual for the Codeks Tools.**

2.1. System requirements

System requirements for the successful operation of the program:

- a computer installed with the Windows 10 operating system or newer,
- installed Microsoft .NET Framework 4.8,
- internet access (to connect with devices in the local network and update the firmware of Jantar devices),
- PDF Reader software for displaying the program user manual.

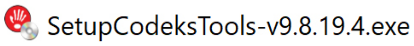
2.2. Software installation

ATTENTION

Before installing the software on your computer, please:

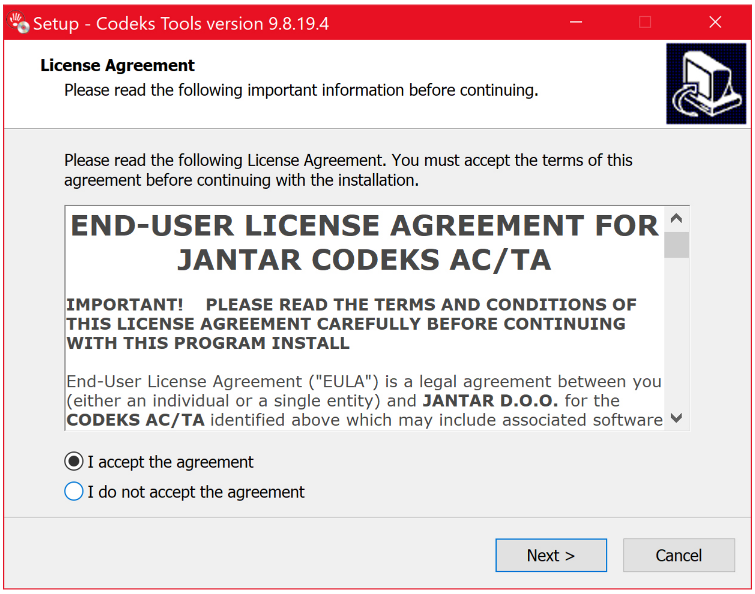
- check the system requirements 6,
- make sure the **.NET Framework at least version 4.8** is installed on your computer, otherwise, please, install it beforehand. (The Windows 8 operating system and newer already have the correct .NET Framework installed by default, however, with older operating systems manual installation of the .NET Framework may be required.)

To begin the program installation double-click the **SetupCodeksTools-v9.8.19.4.exe** file:



SetupCodeksTools-v9.8.19.4.exe

1. Read the terms of the license agreement. To continue select *I accept the agreement* and click ***Next***.



Setup - Codeks Tools version 9.8.19.4

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

END-USER LICENSE AGREEMENT FOR JANTAR CODEKS AC/TA

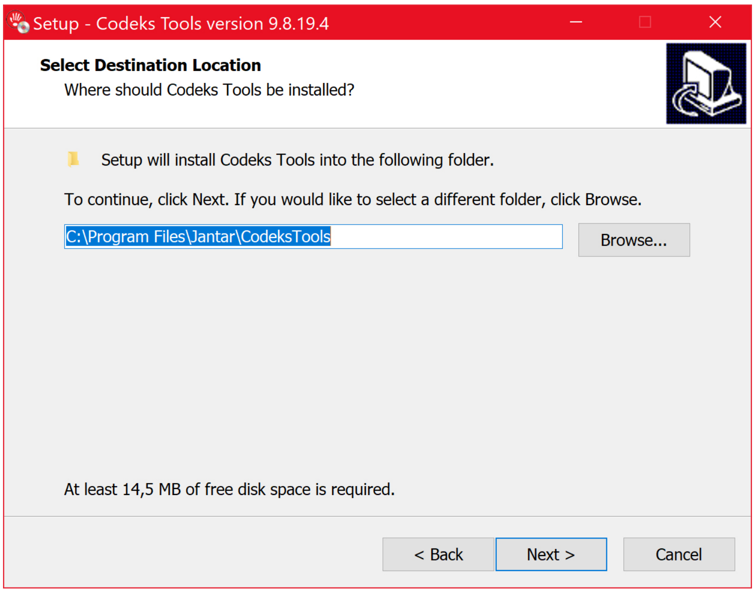
IMPORTANT! PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CONTINUING WITH THIS PROGRAM INSTALL

End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and **JANTAR D.O.O.** for the **CODEKS AC/TA** identified above which may include associated software

● I accept the agreement

○ I do not accept the agreement

2. Select the installation folder for the program and click ***Next***.



Setup - Codeks Tools version 9.8.19.4

Select Destination Location

Where should Codeks Tools be installed?

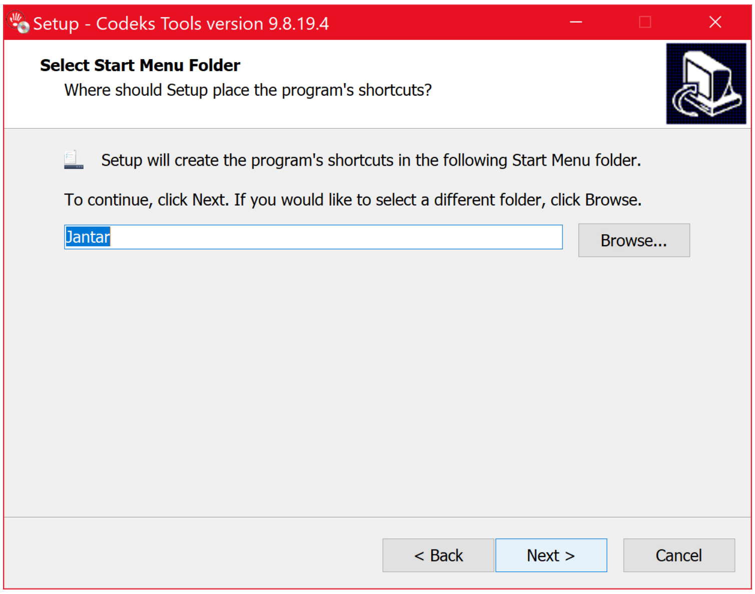
Setup will install Codeks Tools into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\Jantar\CodeksTools

At least 14,5 MB of free disk space is required.

3. You can also add a shortcut for the program in your *Start* menu. Click ***Next.***



Setup - Codeks Tools version 9.8.19.4

Select Start Menu Folder

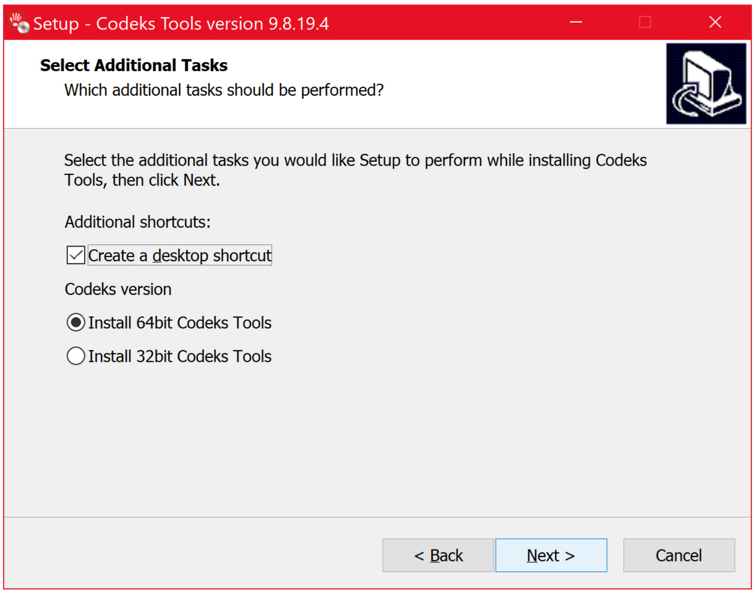
Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

Jantar

4. You can add the program icon to your desktop. Click ***Next***.



Setup - Codeks Tools version 9.8.19.4

Select Additional Tasks

Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing Codeks Tools, then click Next.

Additional shortcuts:

☑ Create a desktop shortcut

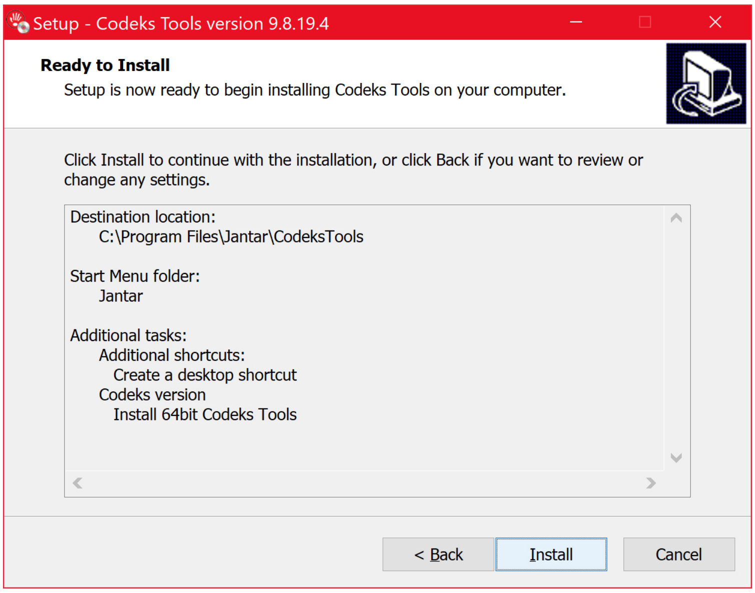
Codeks version

● Install 64bit Codeks Tools

○ Install 32bit Codeks Tools

5. Click ***Install***.

This process will take a few moments.



Setup - Codeks Tools version 9.8.19.4

Ready to Install

Setup is now ready to begin installing Codeks Tools on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

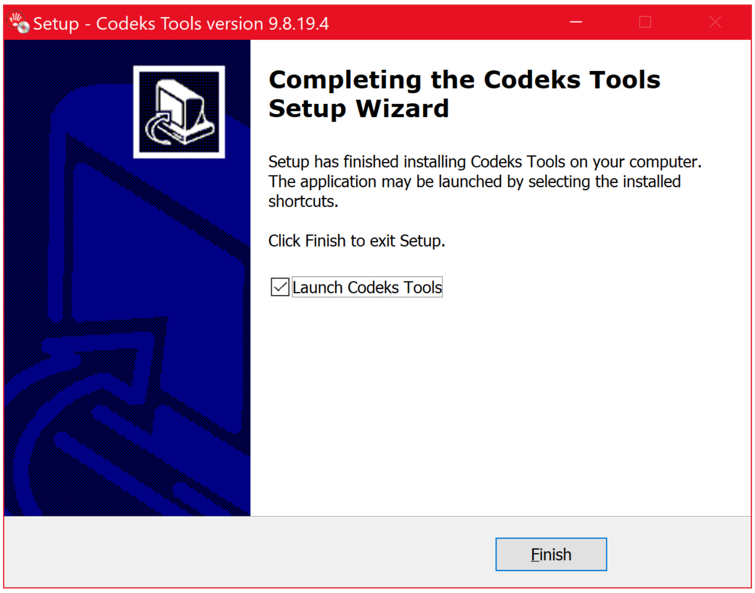
```
Destination location:
      C:\Program Files\Jantar\CodeksTools

Start Menu folder:
      Jantar

Additional tasks:
      Additional shortcuts:
         Create a desktop shortcut
      Codeks version
         Install 64bit Codeks Tools
```

6. After a successful installation the displayed message will appear. Click ***Finish***.

Thus you have successfully installed the *Codeks Tools* program.



Setup - Codeks Tools version 9.8.19.4

Completing the Codeks Tools Setup Wizard

Setup has finished installing Codeks Tools on your computer. The application may be launched by selecting the installed shortcuts.

Click Finish to exit Setup.

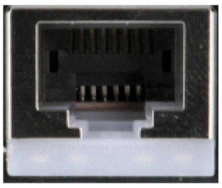
☑ Launch Codeks Tools

2.3. Firewall settings

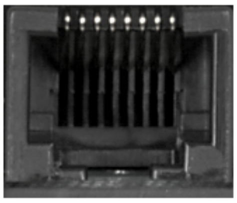
Incorrect firewall settings can cause problems when searching for NET communication lines.

You must enable the following:

- To enable communication with Spider NET devices allow communication on TCP port for older versions of the device and TCP port 1001 for new devices.
- To enable communication with controllers, with direct connection to your network, allow communication on TCP port 1001. This default value can be changed when editing hardware settings.
- To enable sending and receiving UDP packages (searching for communication lines), enable port 65535.



RJ45 connector for old Spiders with Tibbo: port 100

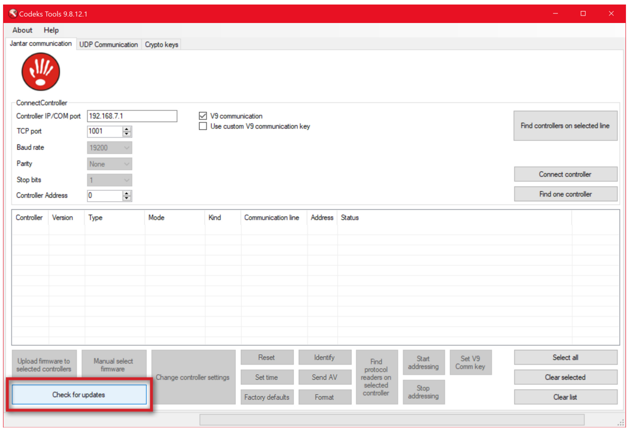


RJ45 connector for new Spiders without Tibbo: port 1001

2.4. Software update

You can check if a new update version for the *Codeks Tools* program is available by clicking the ***Check for updates*** button in the *Jantar communication* tab.
Jantar communication tab.
The existing version of the program does not need to be uninstalled from the computer before updating, as the new version of the *Codeks Tools* program will simply overwrite the existing version.

1. First, click the ***Check for updates*** button in the *Jantar communication* tab**.**
The program will check if a newer version of the program is available from our Jantar server.

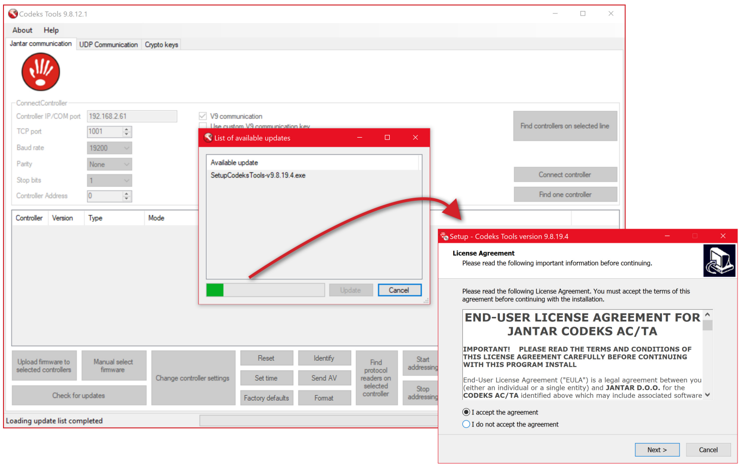


Controller IP/COM port: 192.168.7.1
TCP port: 1001
Baud rate: 19200
Parity: None
Stop bits: 1
Controller Address: 0
☑ V9 communication
☐ Use custom V9 communication key

2. Then, a new pop-up window will appear where all the newer versions of the program will be displayed. **Mark the newest version and click *Update.***

3. Select where you wish to save the installation file, and then, click ***Save***.

4. After the file download is complete the program installation 6 will start automatically.



Controller IP/COM port: 192.168.2.61
TCP port: 1001
Baud rate: 19200
Parity: None
Stop bits: 1
Controller Address: 0
☑ V9 communication
Use custom V9 communication key

SetupCodeksTools-v9.8.19.4.exe

Loading update list completed

License Agreement
Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

END-USER LICENSE AGREEMENT FOR JANTAR CODEKS AC/TA

IMPORTANT! PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CONTINUING WITH THIS PROGRAM INSTALL

End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and **JANTAR D.O.O.** for the **CODEKS AC/TA** identified above which may include associated software

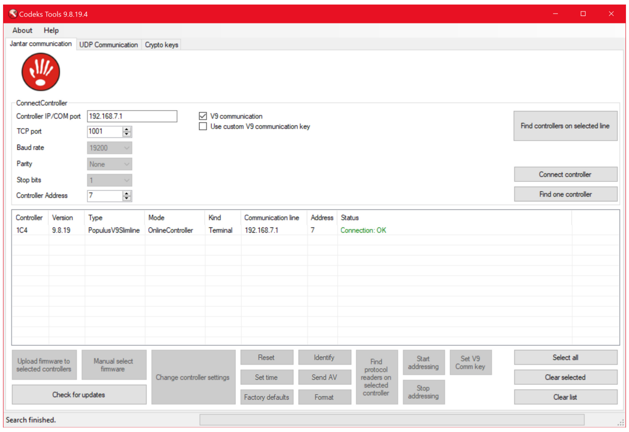
● I accept the agreement
○ I do not accept the agreement

3. Program interface

The Codeks Tools program consists of three tabs:

- **Jantar communication**

  In this tab, you can check the status and quality of the communication connection with individual controllers. Also, using specific tools you can update the firmware of devices, and change their basic parameters which affect their operation.



Controller IP/COM port: 192.168.7.1
TCP port: 1001
Baud rate: 19200
Parity: None
Stop bits: 1
Controller Address: 7
☑ V9 communication
☐ Use custom V9 communication key

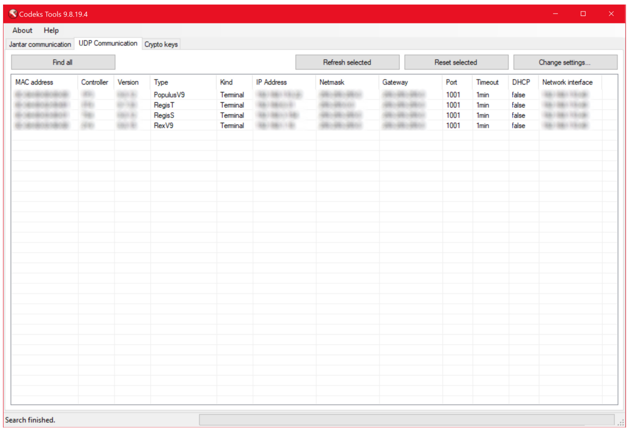
Controller	Version	Type	Mode	Kind	Communication line	Address	Status
1C4	9.8.19	PopulusV9Slimline	OnlineController	Terminal	192.168.7.1	7	Connection: OK

Search finished.

- **UDP Communication**

  In this tab, you can find all Jantar devices within your local network and also change their network settings.

  (UDP (User Datagram Protocol) communication differs from Jantar communication in that with this kind of communication you can find Jantar controllers within a system without the use of V9 encryption keys (because the connection does not use the V9 communication protocol), and also regardless of whether the devices are already communicating with another software. Because of this simple type of connection, however, the device settings you can change by using a UDP connection are limited (i.e. limited only to the device network settings).)

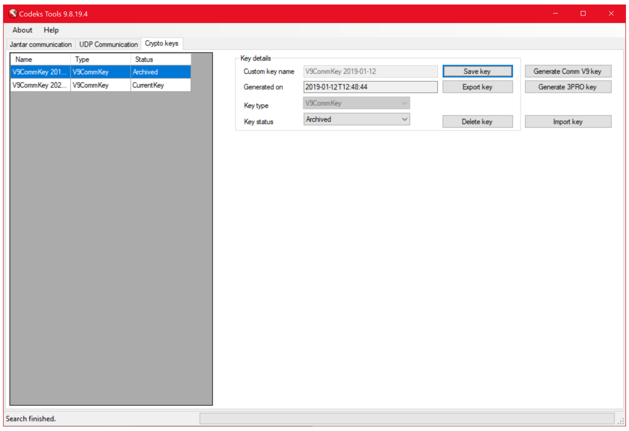


MAC address	Controller	Version	Type	Kind	IP Address	Netmask	Gateway	Port	Timeout	DHCP	Network interface
[redacted]	[redacted]	[redacted]	PopulusV9	Terminal	[redacted]	[redacted]	[redacted]	1001	1min	false	[redacted]
[redacted]	[redacted]	[redacted]	RegisT	Terminal	[redacted]	[redacted]	[redacted]	1001	1min	false	[redacted]
[redacted]	[redacted]	[redacted]	RegisS	Terminal	[redacted]	[redacted]	[redacted]	1001	1min	false	[redacted]
[redacted]	[redacted]	[redacted]	RexV9	Terminal	[redacted]	[redacted]	[redacted]	1001	1min	false	[redacted]

Search finished.

- **Crypto keys**

  In this tab, you can generate and manage encryption keys which are used to protect data transfer between the Codeks software server and controllers, and between controllers and user cards.



Name	Type	Status
V9CommKey 201...	V9CommKey	Archived
V9CommKey 202...	V9CommKey	CurrentKey

Custom key name: V9CommKey 2019-01-12
Generated on: 2019-01-12T12:48:44
Key type: V9CommKey
Key status: Archived

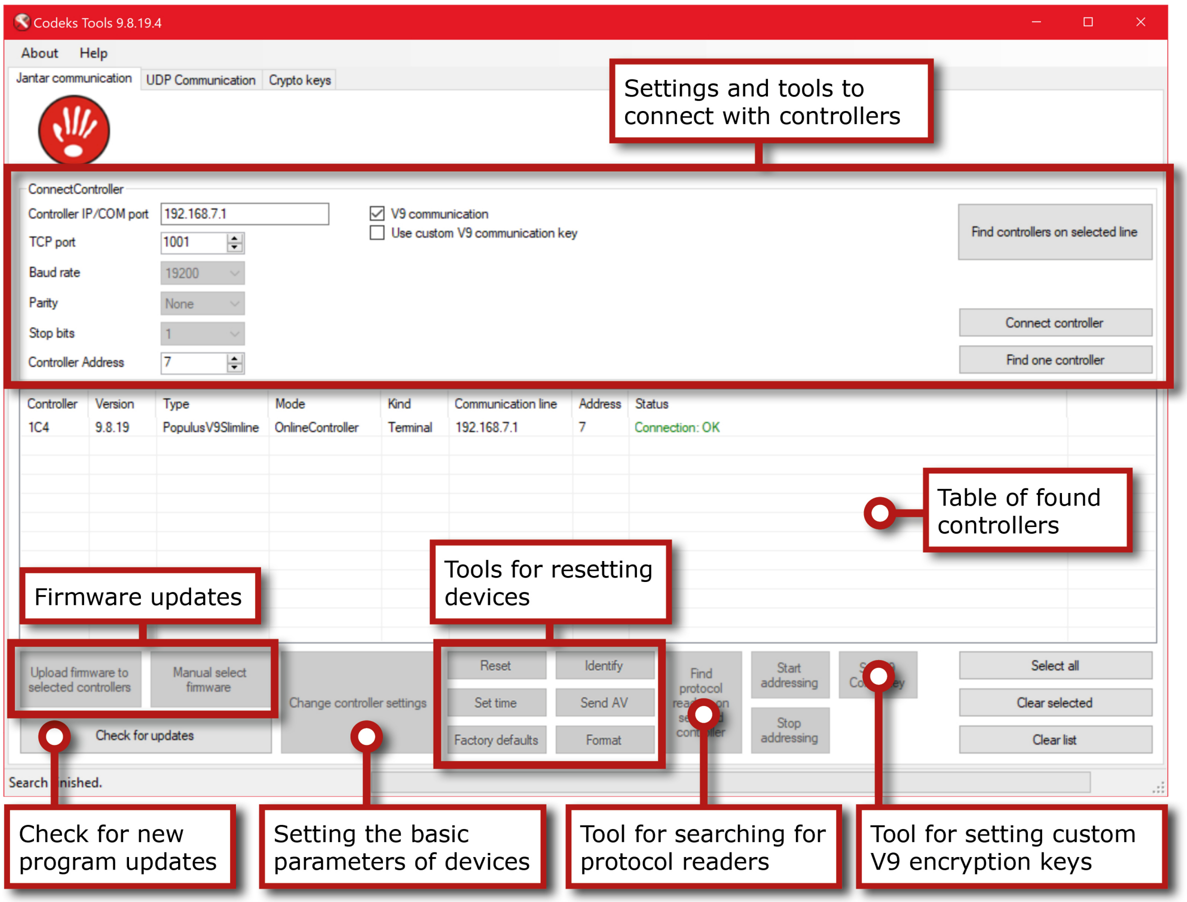
Search finished.

In the following chapters each individual tab is described in more detail.

3.1. Jantar communication

In the ***Jantar communication*** tab you can connect to a specific controller or search for all available controllers on a selected communication line by using the tools in the upper part of the window. You can then connect with the found controllers and perform different actions on them: update their firmware, change their basic device parameters, find protocol readers connected to it, etc.

NOTE!
Jantar devices can only actively communicate with one program (or program service)a at a time. If a device, with which you want to connect, is already actively communication with another program or service (e.g. the Codeks software), you must **first disable the communication between the device and this program.** Only after will you be able to find and connect with it using the Jantar communication tool.
(Alternatively, you can also use the UDP Communication search 28, to view the devices. However this connection offers limited options for device manipulation.)



Codeks Tools 9.8.19.4

ConnectController

Controller IP/COM port: 192.168.7.1
TCP port: 1001
Baud rate: 19200
Parity: None
Stop bits: 1
Controller Address: 7

☑ V9 communication
☐ Use custom V9 communication key

Controller	Version	Type	Mode	Kind	Communication line	Address	Status
1C4	9.8.19	PopulusV9Slimline	OnlineController	Terminal	192.168.7.1	7	Connection: OK

Search nished.

Settings and tools to connect with controllers

Table of found controllers

Firmware updates

Tools for resetting devices

Check for new program updates

Setting the basic parameters of devices

Tool for searching for protocol readers

Tool for setting custom V9 encryption keys

Settings and tools to connect with controllers	The tools at the top of the window allow you to search for and connect to a specific controller or search for all controllers on a specific communication line.
Table of found controllers	The table displays the controllers (and protocol protocols connected to them) that match the query at the top of the window.
Firmware updates	By using the ***Upload firmware to selected controllers*** or ***Manual select firmware*** buttons, you can update the firmware on the selected controllers or protocol readers.
Check for new program updates	Clicking the ***Check for updates*** button will trigger a query for new versions of the *Codeks Tools* program to update the program 10.
Setting the basic parameters of devices	Clicking the ***Change controller settings*** button brings up a window where you can change the basic parameters for the operation of the selected controller or protocol reader

Tools for resetting devices	With the device reset tools, you can either restart the selected controllers or reset them to the factory default settings.
Tool for searching for protocol readers	Clicking the ***Find protocol readers on selected controller*** button will initiate the search for any protocol readers connected to the selected controller.
Tool for setting custom V9 encryption keys	By clicking the ***Set V9 Comm key*** button, you can assign a new (custom-made) V9 encryption key to the selected controller, which will from now on encrypt the communication between the controller and Codeks software using this key.

In the following chapters the individual tools and how to use them are described in more detail.

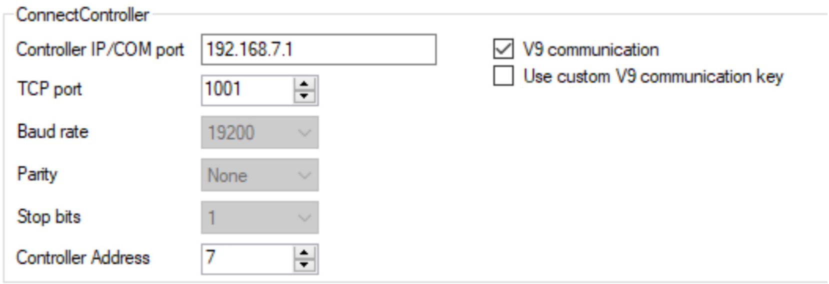
3.1.1. Finding controllers

By using the entry form in the upper part of the *Jantar communication* tab you can search and connect with controllers.

NOTE!
Jantar devices can only actively communicate with one program (or program service) at a time. If a device, with which you want to connect, is already actively communicating with another program or service (e.g. the Codeks software), you must **first disable the communication between the device and this program.** Only after will you be able to find and connect with it using the Jantar communication tool.
(Alternatively, you can also use the UDP Communication search 28, to view the devices. However, this connection offers limited options for device manipulation.)

NOTE!
The program will only display those controllers that you can access through your current (local) network.

1. To display a controller, first, **set appropriate values for these settings:**



ConnectController

Controller IP/COM port: 192.168.7.1
TCP port: 1001
Baud rate: 19200
Parity: None
Stop bits: 1
Controller Address: 7

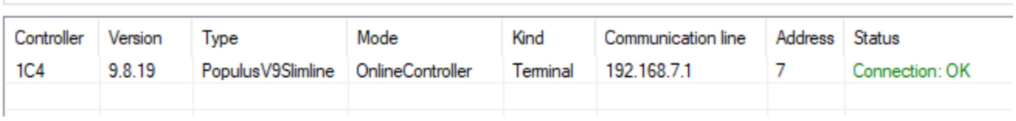
☑ V9 communication
□ Use custom V9 communication key

Controller info	
Controller IP/COM port	Enter the IP address of the communication line to which the controller is connected, or right-click the field and from the drop-down menu select the serial port (COM port) through which the controller is connected to your computer. **NOTE** **Each Jantar controller is assigned a default IP address during the manufacturing process. This information is written on the label of the device.** During the installation of the devices at the end locations, it is essential to record this information.
TCP port	The TCP port through which the controller communicates with the software.
Baud rate	The *Baud rate*, *Parity in* Stop *bits* settings only affect devices which are connected through a physical Com port (older devices). These settings do not affect devices connected through a LAN or USB connection. **NOTE** **We recommend that these settings only be changed by the IT system administrator or another suitably qualified person who knows and understands how these settings affect the communication with devices.**
Parity	
Stop bits	
Controller address	The controller's address is one of the key settings of controllers, as it defines the address through which the controller communicates with the Codeks software. You can choose values between 1 and 255. **NOTE** **All controllers which are connected through the same communication line must be assigned unique addresses.** This is because the Codeks software cannot communicate with controllers using the same address on the same communication line. **NOTE** **Each Jantar controller is assigned a default controller address during the manufacturing process. This information is written on the label of the device.** During the installation of the devices at the end locations, it is essential to record this information.
V9 communication	This setting enables communication with newer Jantar devices which use the V9 communication protocol.
Use custom V9 communication key	This setting enables communication with newer Jantar devices which use a custom V9 encryption key 32 to communicate with the software.

2. Then click one of the buttons on the right:

Find controllers on selected line	Clicking the ***Find controllers on selected line*** button will trigger a search for any controllers that are connected to the communication line specified in the *Controller IP / COM port* field. This action ignores the *Controller address setting* and returns data for all controllers found on the communication line, regardless of their controller address value.
Connect controller	Clicking on the ***Connect controller*** button will trigger a search action that will only return the controller which exactly matches the specified search parameters.
Find one controller	Clicking the ***Find one controller*** button will trigger the search for the first controller that is connected to the communication line specified in the *Controller IP / COM port* field. This action ignores the *Controller address* setting, and instead finds and returns information about the first controller it finds on the specified communication line (usually the first controller found is the one that has the lowest value entered as its controller address out of all controllers on the selected communication line).

3. The table below will show all the controllers that match the set parameters and the performed action (which depends on the button you selected).



Controller	Version	Type	Mode	Kind	Communication line	Address	Status
1C4	9.8.19	PopulusV9Slimline	OnlineController	Terminal	192.168.7.1	7	Connection: OK

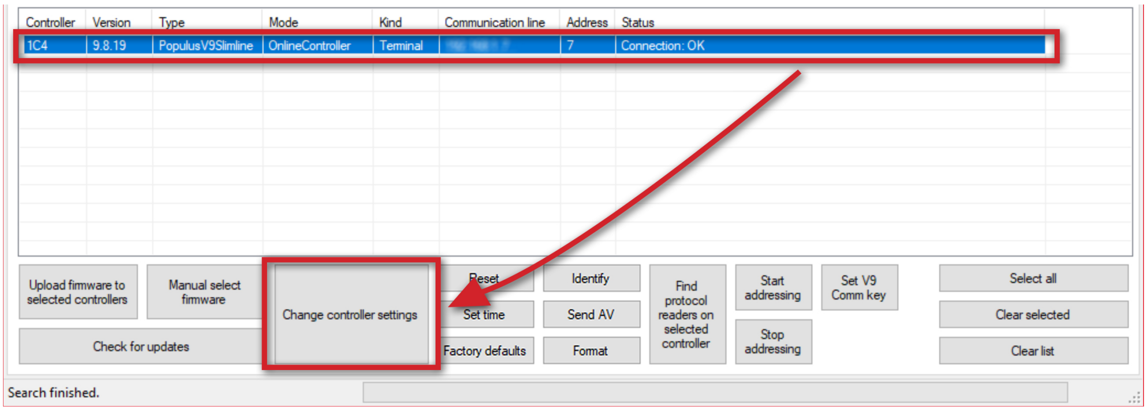
You can perform different actions on the controllers displayed in the table:

- update the controller's firmware 23,
- change the basic parameters of the controller 16,
- search for protocol readers 24 connected to a specific controller,
- assign a new custom V9 encryption key to a controller 38.

3.1.2. Editing controllers

Clicking on the ***Change controller settings*** button brings up a window where you can change the basic parameters which affect the operation of the selected controller.

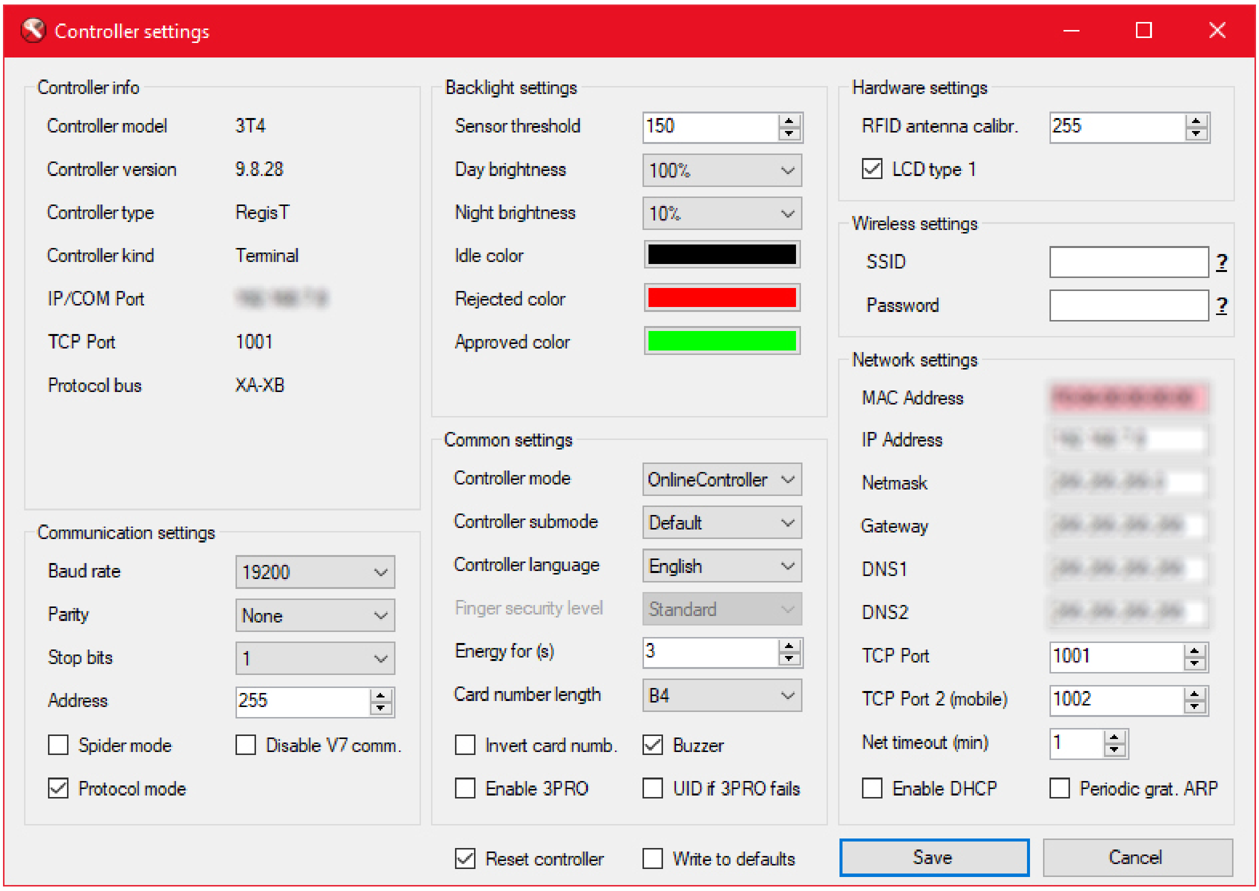
1. To change the controller settings, first, mark the appropriate controller in the table and click ***Change controller settings***.



Controller	Version	Type	Mode	Kind	Communication line	Address	Status
1C4	9.8.19	PopulusV9Slimline	OnlineController	Terminal	[redacted]	7	Connection: OK

Search finished.

2. A window will open where you can change the basic parameters of the controller.



Controller settings

Controller info

Controller model 3T4

Controller version 9.8.28

Controller type RegisT

Controller kind Terminal

IP/COM Port [redacted]

TCP Port 1001

Protocol bus XA-XB

Communication settings

Baud rate 19200

Parity None

Stop bits 1

Address 255

□ Spider mode □ Disable V7 comm.

☑ Protocol mode

Backlight settings

Sensor threshold 150

Day brightness 100%

Night brightness 10%

Idle color ■

Rejected color 🟥

Approved color 🟩

Common settings

Controller mode OnlineController

Controller submode Default

Controller language English

Finger security level Standard

Energy for (s) 3

Card number length B4

□ Invert card numb. ☑ Buzzer

□ Enable 3PRO □ UID if 3PRO fails

Hardware settings

RFID antenna calibr. 255

☑ LCD type 1

Wireless settings

SSID ?

Password ?

Network settings

MAC Address [redacted]

IP Address [redacted]

Netmask [redacted]

Gateway [redacted]

DNS1 [redacted]

DNS2 [redacted]

TCP Port 1001

TCP Port 2 (mobile) 1002

Net timeout (min) 1

□ Enable DHCP □ Periodic grat. ARP

☑ Reset controller □ Write to defaults

Controller info	
Controller model	An internal Jantar device identification label.
Controller version	The firmware version currently installed on the controller.
Controller type	The type of controller.
Controller kind	This setting defines if the device is acting like a controller (*Terminal*) or just a communication converter between the RS485 and LAN communication line (*Spider*).

Controller info	
IP/COM Port	The IP address or serial port (COM port) through which the controller is connected to your computer.
TCP Port	The TCP port through which the controller communicates with the software.
Protocol bus	This setting defines which of the physically present RS485 connectors is used as a protocol bus.

Communication settings	
Baud rate	These settings affect the communication of a device connected via the RS485 connection with the server and other connected devices. **You do not need to change these settings to use Jantar devices.** **NOTE** **We recommend that these settings only be changed by the IT system administrator or another suitably qualified person who knows and understands how these settings affect the communication with devices.** **NOTE** **If you are changing the settings of a controller to which other controllers or protocol readers are connected via the RS485 connection, you must first set the same settings on all connected controllers or protocol readers, starting with devices that are connected last on the RS485 line!** You must first set the settings for all devices connected to the master controller, then set the same settings to the master (initial) controller.
Parity	
Stop bits	
Address	The controller's address is one of the key settings of controllers, as it defines the address through which the controller communicates with the Codeks software. **NOTE** **All controllers which are connected through the same communication line must be assigned unique addresses.** This is because the Codeks software cannot communicate with controllers using the same address on the same communication line. **NOTE** The address of the controller (i.e. the numerical value between 1 and 249 or 255) must already be **assigned to the controllers during the installation process itself**. If you choose to manually add the controller to the Codeks application, you must **carefully record this device information**. If you add the controller using the *Add hardware wizard*, the wizard will automatically find and insert the correct controller address.
Spider mode	If this setting is enabled, the selected controller will operate similarly to the (Spider) communication converter, enabling other controllers to be connected through it (with an RS485 sequential connection) to the same communication line.
Disable V7 comm	If this setting is enabled, the controller's ability to communicate using the V7 protocol will be disabled. (Only older Jantar devices communicate using the V7 protocol. New devices communicate by using the V9 protocol, but they also have V7 communication capability for instances when they are installed in older existing systems.)
Protocol mode	This setting enables the use (connection and communication) of protocol readers on a selected controller.

Backlight settings	
Sensor threshold [1]	This setting defines the threshold value when the controller switches from day to night mode. You can select values between 0 and 255.
Day brightness [1]	The setting determines the brightness of the screen during the day. The value is given as a percentage.
Night brightness [1]	The setting determines the brightness of the screen at night. The value is given as a percentage.
Idle color [2]	The setting determines the backlight color when the controller is in idle mode.
Rejected color [2]	The setting determines the backlight color when the user is denied access.
Approved color [2]	The setting determines the backlight color when the user is allowed access.

[1] This setting is only relevant for older generation Jantar A-Line and H-line devices.

[2] This setting is only relevant for (newer) Jantar A-Line and H-line devices.

Common settings

Controller mode

Only change this setting if you want to change the controller's mode of operation otherwise leave the default value *Online controller*.

You can choose from values:

StandAlone	The controller acts as a standalone controller that is not connected to any software.
WiegandSingleKey	The operation of the controller is changed to that of a reader. (When the user approaches the card to the controller, the controller only reads the number and sends it forward. When the user enters the PIN on the controller, the controller promptly sends each number as it is entered.)
WiegandKeysAfterEntry	The operation of the controller is changed to that of a reader. (When the user approaches the card to the controller, the controller only reads the number and sends it forward. When the user enters the PIN on the controller, the controller only sends the number forward after the use clicks *Enter*.)
W72	Wiegand (72bit) functionality for compatibility with older devices.
OnlineController	The default (normal) operation of a controller (as a standard access controller).
KeyManager	The controller is defined to be the reader of the Jantar *Keymanager* system.
ElectronicPurse	This functionality has yet to be determined (TBD).
ElectronicPurseSetValue	This functionality has yet to be determined (TBD).
TableReader	This setting is used to define the Jantar USB Table Reader 21.
ProtocolReader	The controller will operate as a protocol reader.
Trap1	This functionality has yet to be determined (TBD).
Trap2	This functionality has yet to be determined (TBD).
CloudReader	This functionality has yet to be determined (TBD).
Switch	The controller will operate as a simple switch (e.g., light switch, switch for a fan).
Resistive Touch [3]	The controller uses a resistive touch screen.
Capacitive Touch [3]	The controller uses a capacitive touch screen.

[3] Nastavitev se uporablja samo za Jantar naprave Gumbi.

Controller sub mode

This setting more specifically defines the controller's mode of operation depending on the set ***Controller mode***.

StandAlone	**Pulse -** when a user registers at the controller, it connects the output to the mass for a short time (a pulse lasting a certain number of seconds) to temporarily unlock the door (lock). **Toggle -** when a user registers at the controller, it switches the status of the door (i.e., from locked to unlocked or vice versa). **CardHolder -** the controller or protocol reader is used as a cardholder (in hotel rooms) that turns on the electricity when the card is in the controller and turns it off when removed.
WiegandSingleKey	/
WiegandKeysAfterEntry	**Default** - the controller acts as a standard access controller. **BeepOnEnter** - the controller gives a sound signal when a user presses *Enter.*
W72	/
OnlineController	**Default** - the controller acts as a standard access controller. **CardHolder -** the controller acts as a cardholder (in hotel rooms) to turn on the electricity when the card is in the controller and turn it off when removed. **LEDOutput** - the controller maps LED outputs to Wiegand outputs so that external LEDs can be connected to the outputs to signal the controller status or operation.
KeyManager	/
ElectronicPurse	/
ElectronicPurseSetValue	/
TableReader	**ShortString** - the USB reader only reads and sends forward 3 bytes of the card number. **LongString** - the USB reader reads and sends forward 4 or more bytes of the card number.
ProtocolReader	**Default** - the controller or protocol reader acts as a regular card reader in the access control system. **CardHolder -** the controller or protocol reader acts as a cardholder (in hotel rooms) that turns on the electricity when the card is in the controller and turns it off when removed. **LEDOutput** - the controller maps LED outputs to Wiegand outputs so that external LEDs can be connected to the outputs to signal the controller status or operation.
Trap1	/
Trap2	/
CloudReader	/

<table>
<tr><th colspan="2">Common settings</th></tr>
<tr><td></td><td>
<table>
<tr><td><b><i>Switch</i></b></td><td><b>Pulse -</b> when the switch is pressed, the controller connects the output to the mass for a short time (a pulse lasting a certain number of seconds) to temporarily unlock the door (lock).
<b>Toggle -</b> when the switch is pressed, the controller switches the status of the door (i.e., from locked to unlocked or vice versa).</td></tr>
<tr><td><b><i>Resistive Touch</i></b> [3]</td><td><b>Regis -</b> the controller acts as a time attendance controller and displays a T&A keypad
<b>Status -</b> the controller acts as a reader without a keyboard and only signals the allowed or denied accesses
<b>CardHolder -</b> the controller or protocol reader acts as a cardholder (in hotel rooms) that turns on the electricity when the card is in the controller and turns it off when removed
<b>Numeric1 -</b> the controller acts as a card reader with a keyboard and displays the 1st version of the numeric keypad, which contains a numeric keypad and additional function keys
<b>Numeric2 -</b> the controller acts as a card reader with a keyboard and displays the 2nd version of the numeric keypad, which contains only a numeric keypad and additional function keys
<b>SwitchPulse -</b> the controller acts as a switch that opens the passage doors for a certain amount of time
<b>SwitchToggle -</b> the controller acts as a switch that changes the open state of the passage doors (i.e. if the door has been previously locked, pressing the switch unlocks it and vice versa)
<b>Info -</b> the controller acts as an information display with buttons to call up various services.
<b>Alarm -</b> the controller acts as an interface for turning the alarm on and off.
<b>Termostat -</b> the controller acts as a thermostat that controls the air condition devices of the room.</td></tr>
<tr><td><b><i>Capacitive Touch</i></b> [3]</td><td><b>Regis -</b> the controller acts as a time attendance controller and displays a T&A keypad
<b>Status -</b> the controller acts as a reader without a keyboard and only signals the allowed or denied accesses
<b>CardHolder -</b> the controller or protocol reader acts as a cardholder (in hotel rooms) that turns on the electricity when the card is in the controller and turns it off when removed
<b>Numeric1 -</b> the controller acts as a card reader with a keyboard and displays the 1st version of the numeric keypad, which contains a numeric keypad and additional function keys
<b>Numeric2 -</b> the controller acts as a card reader with a keyboard and displays the 2nd version of the numeric keypad, which contains only a numeric keypad and additional function keys
<b>SwitchPulse -</b> the controller acts as a switch that opens the passage doors for a certain amount of time
<b>SwitchToggle -</b> the controller acts as a switch that changes the open state of the passage doors (i.e. if the door has been previously locked, pressing the switch unlocks it and vice versa)
<b>Info -</b> the controller acts as an information display with buttons to call up various services.
<b>Alarm -</b> the controller acts as an interface for turning the alarm on and off.
<b>Termostat -</b> the controller acts as a thermostat that controls the air condition devices of the room.</td></tr>
</table>
[3] Nastavitev se uporablja samo za Jantar naprave Gumbi.</td></tr>
<tr><td><b>Controller language</b></td><td>The setting specifies the default language in which all messages on controllers with screens will be displayed.</td></tr>
<tr><td><b>Finger security level</b></td><td>The setting determines how closely the read fingerprint must match the user's stored fingerprint template.
* This setting is only relevant for controllers with a fingerprint reader.</td></tr>
<tr><td><b>Energy for (s)</b></td><td>The pulse duration when the controller connects the output to ground (for a specified number of seconds) to temporarily unlock the door (lock).</td></tr>
<tr><td><b>Card number length</b></td><td>This setting determines how many bytes of card number the controller should read and use. (Different programs and applications may read and process card numbers differently.)</td></tr>
<tr><td><b>Invert card numb.</b></td><td>If this setting is enabled, the controller will read the card number inverted (in reverse order of bytes). (This setting is usually used when newer Jantar devices are added to older systems that still use the V7 protocol.)</td></tr>
<tr><td><b>Buzzer</b></td><td>If this setting is enabled, the controller's sound (buzzer) will be turned on.</td></tr>
<tr><td><b>Enable 3 PRO</b></td><td>If this setting is enabled, the controller will not read the card's default serial number, but will instead search for an encrypted 3PRO card number located within the card's internal memory.
<b>If this 3PRO setting is enabled on a controller, you must also enable it on all the readers connected to this controller.</b></td></tr>
</table>

Common settings	
UID if 3PRO fails	This setting can only be used if the previous setting ***Enable 3PRO mode*** is also enabled. If this setting is enabled, the reader will first attempt to read the encrypted 3PRO card number (which is stored in a specific location within the card's internal memory), and if this fails, it will use the default serial number of the card.

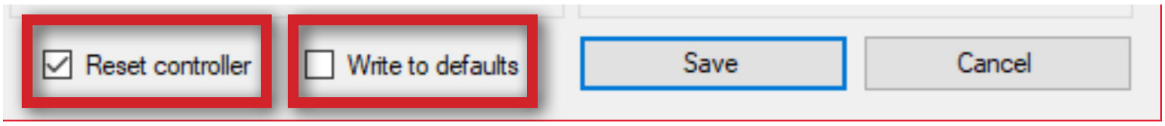
Hardware settings	
RFID antenna calibr.	With this setting, you can improve the card reading function of the reader. It is mainly used when the reader is mounted on a surface that causes interference when reading (e.g. metal surfaces). We recommend that you do not change the default value of this setting. Consult your system administrator or the Jantar Customer Support before making any changes.
LCD type 1	The setting for some older devices with screens, which value depends on some of the hardware components used in the device. We recommend that you do not change the default values of this setting.

Wireless settings	
SSID	The name of the wireless network to which the device will be connected. * This setting is relevant only if the controller has wireless connection capability.
Password	The password of the wireless network to which the device will be connected. * This setting is relevant only if the controller has wireless connection capability.

Network settings	
MAC Address	The hardware ID of each network device.
IP Address	Controller IP address that specifically defines it within the local area network.
Netmask	The network mask of the subnet that the controller can access.
Gateway	The IP address of the router that allows IP packets to be exchanged to and from the local network.
DNS 1	Primary DNS server address.
DNS 2	Secondary DNS server address.
TCP Port	TCP port through which the controller will communicate with the software.
TCP Port 2 (mobile)	TCP port through which the controller will communicate with mobile applications.
Net timeout (min)	The setting determines how long (in minutes) after a sudden or unwanted interruption of communication with the client, the device releases a communication port (port) so that another or the same client (e.g. server) can reconnect to it. (Example: A sudden disconnect of a cable somewhere on the network.)
Enable DHCP	If this setting is enabled, the controller will obtain its network settings from the router.
Periodic grat. ARP	If this setting is enabled, the controller terminal will regularly send *Periodic gratuitous ARP* packets to the network equipment. Enabling the function of sending *Periodic gratuitous ARP* packets helps the network equipment update the appropriate ARP (*Address Resolution Protocol*) entries in time. We recommend that you consult your system administrator or the Jantar Customer Support before changing the setting.

3. When you are finished setting basic controller parameters, click ***Save***.

However, before clicking, you can enable any of the following additional options:



Saving settings	
Reset controller	This setting initiates the restart of the controller (turns the controller off and on again) after the process of writing new parameters to the controller is complete.
Write to defaults	This setting saves all set parameters except the controller address as the default controller settings. This deletes and overwrites the factory default settings of the controller. (* The next time you perform the ***Factory defaults*** action on the same controller, the controller parameters will be set to these values and the controller address will be set to 255.)

3.1.2.1. Editing the USB Reader devices

Naprave Jantar USB Table Reader imajo drugačne možnosti nastavitev:

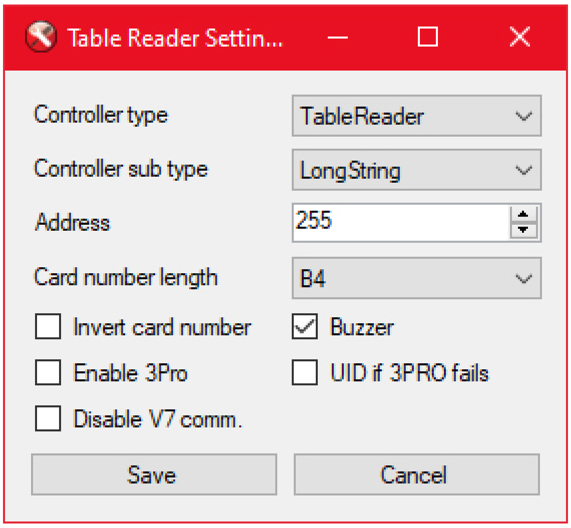


Table Reader Settin...

Controller type: TableReader

Controller sub type: LongString

Address: 255

Card number length: B4

□ Invert card number ☑ Buzzer

□ Enable 3Pro □ UID if 3PRO fails

□ Disable V7 comm.

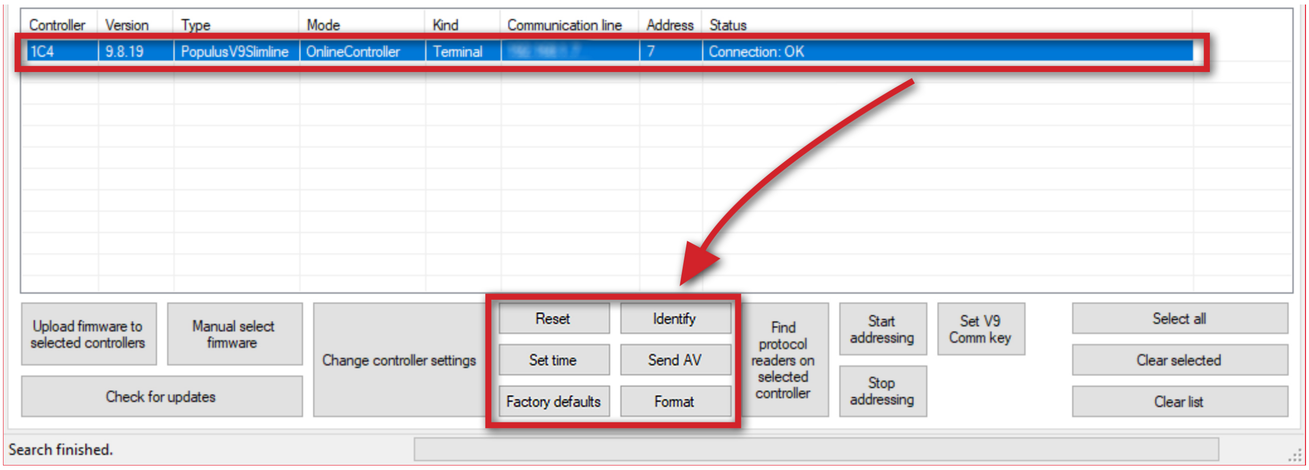
Settings	
Controller type	The default (and only possible) controller type setting is ***TableReader***. Other options for this setting do not make sense for Jantar USB Reader devices. Do not change the setting.
Controller sub type	The setting determines the length of the card number read. You can choose between ***ShortString***, which always limits the card number to 4 bytes, and ***LongString***, which allows you to read a longer card number. The length of the card number read is also affected by the **Card number length setting**, which determines more precisely what the length of the card read should be.
Address	This functionality has yet to be determined (TBD).
Card number length	The setting determines how many bytes of the card number the controller should read and use. (Different programs and applications can read and store card numbers differently.) You can choose between ***3B***, ***4B*** and ***Unlimited*** values. The length of the card number read is also affected by the ***Controller sub type*** 21 setting, which more generally limits the length of the card read. To use the *4B* and *Unlimited* setting values, the *Controller sub type* setting must be set to the *LongString* value.
Invert card numb.	If this setting is enabled, the controller will read the card number inverted (in reverse order of bytes). (This setting is usually used when newer Jantar devices are added to older systems that still use the V7 protocol.)
Buzzer	If this setting is enabled, the controller's sound (buzzer) will be turned on.
Enable 3 PRO	If this setting is enabled, the controller will not read the card's default serial number, but will instead search for an encrypted 3PRO card number located within the card's internal memory. **If this 3PRO setting is enabled on a controller, you must also enable it on all the readers connected to this controller.**
UID if 3PRO fails	This setting can only be used if the previous setting ***Enable 3PRO mode*** is also enabled. If this setting is enabled, the reader will first attempt to read the encrypted 3PRO card number (which is stored in a specific location within the card's internal memory), and if this fails, it will use the default serial number of the card.
Disable V7 comm.	If this setting is enabled, the controller's ability to communicate using the V7 protocol will be disabled. (Only older Jantar devices communicate using the V7 protocol. New devices communicate by using the V9 protocol, but they also have V7 communication capability for instances when they are installed in older existing systems.)

3.1.3. Reseting devices

With the device reset tools, you can either perform different resets of selected controllers.

> **NOTE!**
> **Some device reset actions clear the memory of the controllers, and also reset the network settings used to connect with the device to their factory default settings.**
> The device that was reset will now no longer be reachable using the previously entered parameters. To connect to it you must enter its factory default settings.

To reset a controller, first, mark the appropriate controller in the table, and then, click one of these options:



Controller	Version	Type	Mode	Kind	Communication line	Address	Status
1C4	9.8.19	PopulusV9Slimline	OnlineController	Terminal	[redacted]	7	Connection: OK

Search finished.

Reset	Clicking on the ***Reset*** button will restart the controller (turn the controller off and on again).
Identify	By clicking on the ***Identify*** button, the selected controller (or protocol reader) will start beeping. The *Identify* function makes it easier to search or identify devices already installed in various premises of the company.
Set time	Clicking the ***Set time*** button will send and reset the current time (clock) as set on your computer to the controller.
Send AV	Clicking on the ***Send AV files*** button will resend the image and audio files that are pre-uploaded to the controller by default (when it is still set to factory default).
Factory defaults	Clicking the ***Factory defaults*** button will reset the controller back to the factory default settings (the controller will be reset to the default IP address and controller address). (* If you have previously specified new defaults using the ***Write to defaults*** 20 function, the controller will be reset to these parameter values.)
Format	Clicking the ***Format*** button will reset the controller back to the factory settings (as with *Factory defaults*), and will also delete all image and audio files. Before using the controller again, we, therefore, suggest that you resend the image and audio files to the controller using ***Send AV files***.

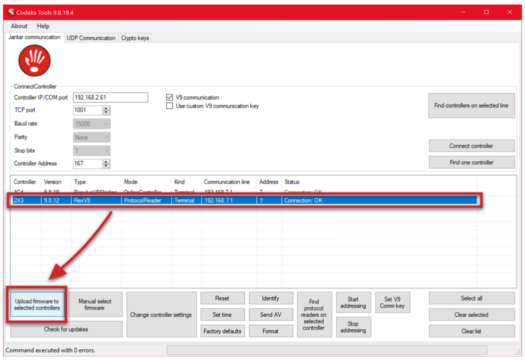
3.1.4. Updating the firmware

1. To upgrade the firmware of a controller of protocol reader, first, select the appropriate device in the table.

2. Then click one of the options:

2.a) *Upload firmware to selected controllers*

Clicking on the ***Upload firmware button to selected controllers*** will check if a newer version of the firmware is available for the selected device and **upgrade the device to the latest firmware version**.



ConnectController

Controller IP/COM port: 192.168.2.61

TCP port: 1001

Baud rate: 19200

Parity: None

Stop bits: 1

Controller Address: 167

☑ V9 communication

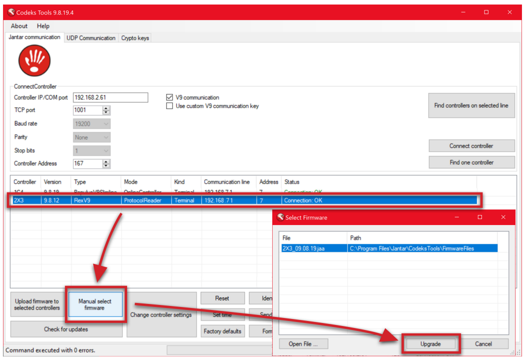
□ Use custom V9 communication key

Controller	Version	Type	Mode	Kind	Communication line	Address	Status
2X3	9.8.12	RexV9	ProtocolReader	Terminal	192.168.7.1	7	Connection: OK

Command executed with 0 errors.

2.b) *Manual select firmware.*

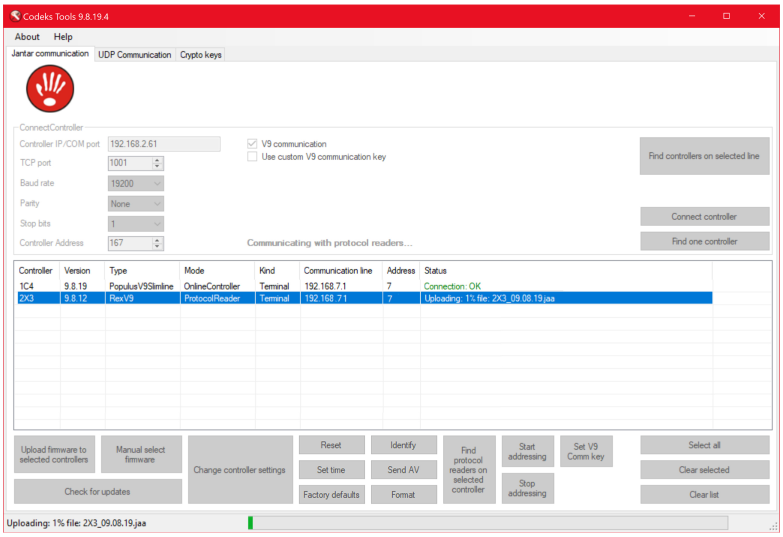
Clicking on the ***Manual select firmware*** button will open a new window showing all the firmware versions available for the selected device. Select the appropriate version and click ***Upgrade***.



File	Path
2X3_09.08.19.jaa	C:\Program Files\Jantar\CodeksTools\FirmwareFiles

Command executed with 0 errors.

3. Then the firmware will be transferred and download to the selected device. The process progress is visible at the bottom of the window and in the table at the end of the device's row.



ConnectController

Controller IP/COM port: 192.168.2.61

TCP port: 1001

Baud rate: 19200

Parity: None

Stop bits: 1

Controller Address: 167

☑ V9 communication

□ Use custom V9 communication key

Communicating with protocol readers...

Controller	Version	Type	Mode	Kind	Communication line	Address	Status
1C4	9.8.19	PopulusV9Slimline	OnlineController	Terminal	192.168.7.1	7	Connection: OK
2X3	9.8.12	RexV9	ProtocolReader	Terminal	192.168.7.1	7	Uploading: 1% file: 2X3_09.08.19.jaa

Uploading: 1% file: 2X3_09.08.19.jaa

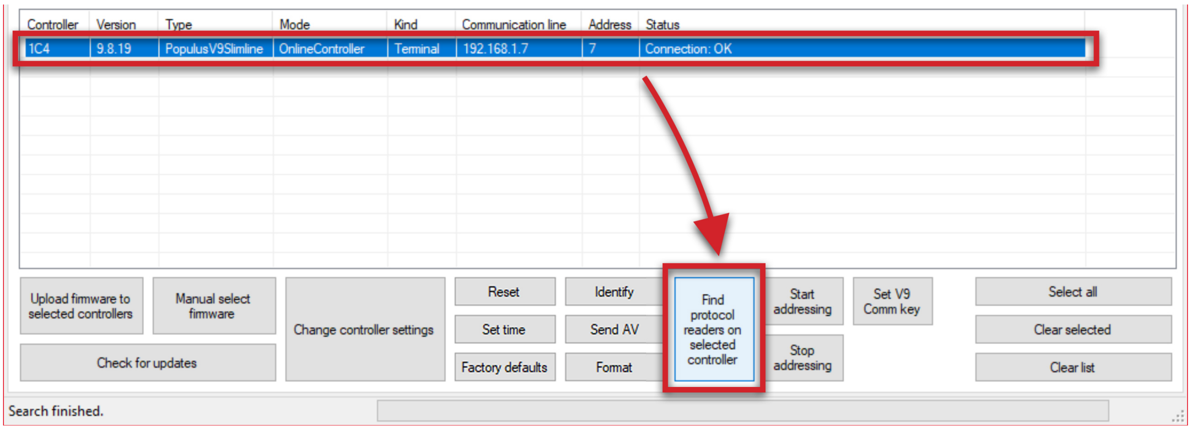
4. When the whole package is transferred the process is complete.

3.1.5. Finding and editing protocol readers on a selected controller

Using the *Codeks Tools* program you can also connect to and edit the protocol readers connected to controllers.

Find protocol readers on a selected controller

1. To search for protocol readers connected to a controller, **first select the controller for which you want to find protocol readers.**

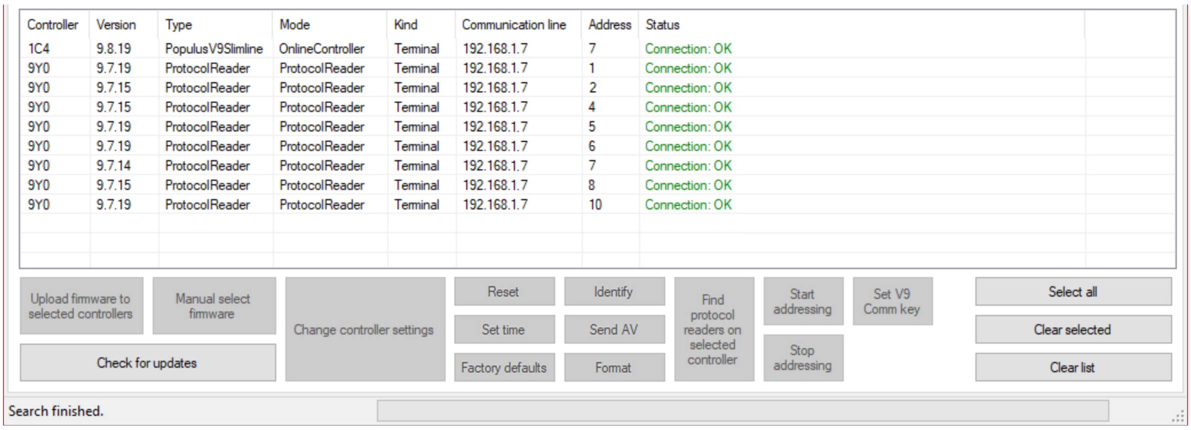


Controller	Version	Type	Mode	Kind	Communication line	Address	Status
1C4	9.8.19	PopulusV9Slimline	OnlineController	Terminal	192.168.1.7	7	Connection: OK

Search finished.

2. Then click the ***Find protocol readers on selected controller*** button.

The table below will show protocol readers connected to the selected controller.

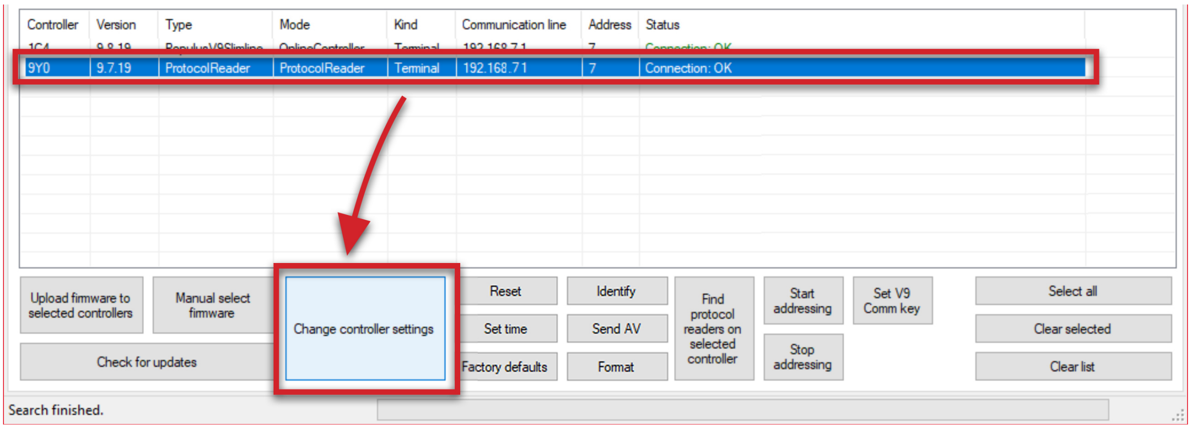


Controller	Version	Type	Mode	Kind	Communication line	Address	Status
1C4	9.8.19	PopulusV9Slimline	OnlineController	Terminal	192.168.1.7	7	Connection: OK
9Y0	9.7.19	ProtocolReader	ProtocolReader	Terminal	192.168.1.7	1	Connection: OK
9Y0	9.7.15	ProtocolReader	ProtocolReader	Terminal	192.168.1.7	2	Connection: OK
9Y0	9.7.15	ProtocolReader	ProtocolReader	Terminal	192.168.1.7	4	Connection: OK
9Y0	9.7.19	ProtocolReader	ProtocolReader	Terminal	192.168.1.7	5	Connection: OK
9Y0	9.7.19	ProtocolReader	ProtocolReader	Terminal	192.168.1.7	6	Connection: OK
9Y0	9.7.14	ProtocolReader	ProtocolReader	Terminal	192.168.1.7	7	Connection: OK
9Y0	9.7.15	ProtocolReader	ProtocolReader	Terminal	192.168.1.7	8	Connection: OK
9Y0	9.7.19	ProtocolReader	ProtocolReader	Terminal	192.168.1.7	10	Connection: OK

Search finished.

Editing protocol readers

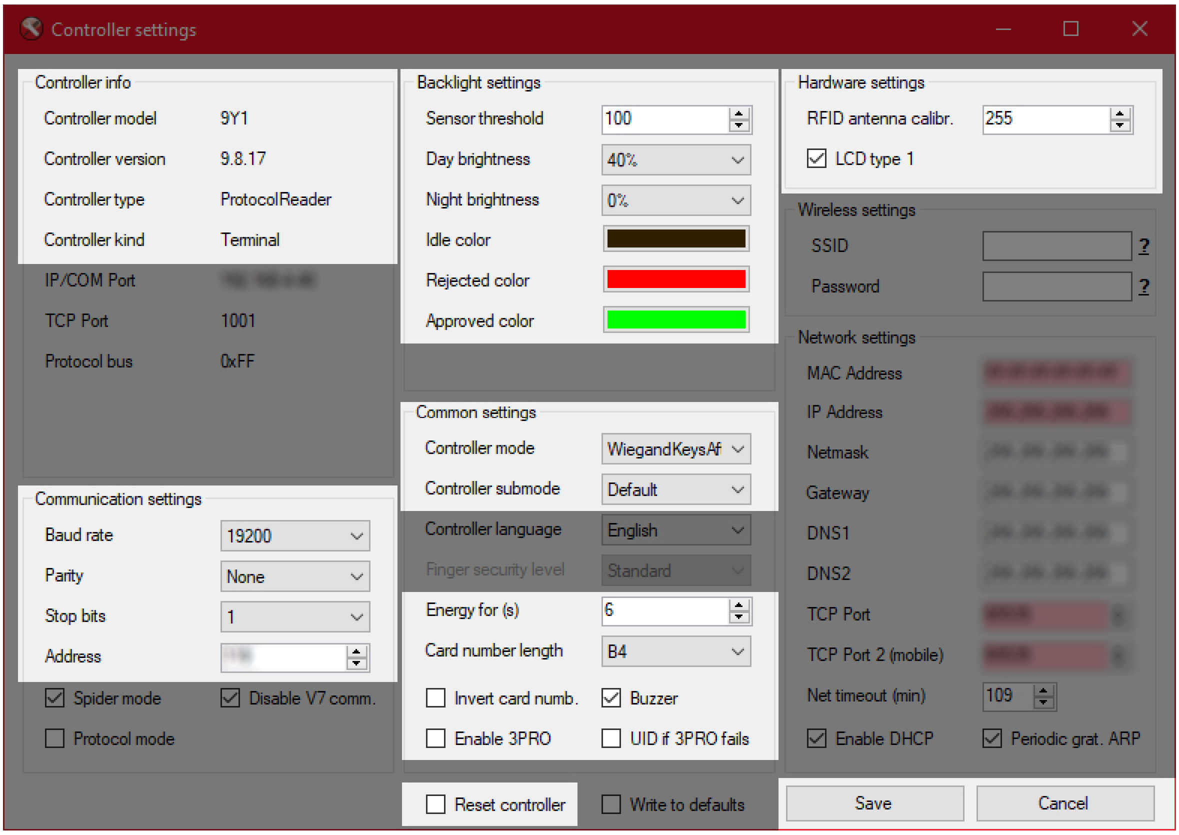
1. To edit the protocol reader, first, highlight the appropriate protocol reader in the table and click the ***Change controller settings*** button.



Controller	Version	Type	Mode	Kind	Communication line	Address	Status
1C4	9.8.19	PopulusV9Slimline	OnlineController	Terminal	192.168.7.1	7	Connection: OK
9Y0	9.7.19	ProtocolReader	ProtocolReader	Terminal	192.168.71	7	Connection: OK

Search finished.

2. A window will open where you can change the basic parameters of the protocol reader.



Controller settings

Controller info
Controller model 9Y1
Controller version 9.8.17
Controller type ProtocolReader
Controller kind Terminal
IP/COM Port [redacted]
TCP Port 1001
Protocol bus 0xFF

Communication settings
Baud rate 19200
Parity None
Stop bits 1
Address [redacted]
☑ Spider mode ☑ Disable V7 comm.
☐ Protocol mode

Backlight settings
Sensor threshold 100
Day brightness 40%
Night brightness 0%
Idle color
Rejected color 🟥
Approved color 🟩

Common settings
Controller mode WiegandKeysAf
Controller submode Default
Controller language English
Finger security level Standard
Energy for (s) 6
Card number length B4
☐ Invert card numb. ☑ Buzzer
☐ Enable 3PRO ☐ UID if 3PRO fails

Hardware settings
RFID antenna calibr. 255
☑ LCD type 1

Wireless settings
SSID
Password

Network settings
MAC Address [redacted]
IP Address [redacted]
Netmask [redacted]
Gateway [redacted]
DNS1 [redacted]
DNS2 [redacted]
TCP Port [redacted]
TCP Port 2 (mobile) [redacted]
Net timeout (min) 109
☑ Enable DHCP ☑ Periodic grat. ARP

☐ Reset controller ☐ Write to defaults

* Not all settings displayed in the window make sense for protocol readers. The picture shows only those settings that affect the operation of protocol readers, the rest are grayed out.

Controller info	
Controller model	An internal Jantar device identification label.
Controller version	The firmware version currently installed on the reader.
Controller type	The type of reader.
Controller kind	This setting defines if the device is acting like a controller (*Terminal*) or just a communication converter between the RS485 and LAN communication line (*Spider*).

Communication settings	
Baud rate	These settings affect the communication of a device connected via the RS485 connection with the server and other connected devices. **You do not need to change these settings to use Jantar devices.** **NOTE** **We recommend that these settings only be changed by the IT system administrator or another suitably qualified person who knows and understands how these settings affect the communication with devices.** **NOTE** **If you are changing the settings of a controller to which other controllers or protocol readers are connected via the RS485 connection, you must first set the same settings on all connected controllers or protocol readers, starting with devices that are connected last on the RS485 line!** You must first set the settings for all devices connected to the master controller, then set the same settings to the master (initial) controller.
Parity	
Stop bits	
Address	The address of a protocol reader is one of the key settings for the communication between a protocol reader and the controller to which it is connected. In the setting's field insert a number between 1 and 255. **NOTE** **Protocol readers connected to the same controller must be assigned unique reader addresses.** The controller is not able to communicate with readers assigned with the same address. **NOTE** The protocol reader address (i.e. the numerical value between 1 and 255) is already **assigned to the readers during the installation process itself**. Therefore, you must **carefully record this device information**.

Backlight settings	
Sensor threshold [1]	This setting defines the threshold value when the controller switches from day to night mode. You can select values between 0 and 255.
Day brightness [1]	The setting determines the brightness of the screen during the day. The value is given as a percentage.
Night brightness [1]	The setting determines the brightness of the screen at night. The value is given as a percentage.
Idle color [2]	The setting determines the backlight color when the controller is in idle mode.
Rejected color [2]	The setting determines the backlight color when the user is denied access.
Approved color [2]	The setting determines the backlight color when the user is allowed access.

[1] This setting is only relevant for older generation Jantar A-Line and H-line devices.
[2] This setting is only relevant for (newer) Jantar A-Line and H-line devices.

Common settings	
Controller mode	Only change this setting if you want to change the reader's mode of operation otherwise leave the default value *Protocol reader*. You can choose from values:

StandAlone	This functionality has yet to be determined (TBD).
WiegandSingleKey	A Wiegand reader. (When the user approaches the card to the reader, the reader only reads the number and sends it forward. When the user enters the PIN on the reader, the reader promptly sends each number as it is entered.)
WiegandKeysAfterEntry	A Wiegand reader. (When the user approaches the card to the reader, the reader only reads the number and sends it forward. When the user enters the PIN on the reader, the reader only sends the number forward after the use clicks *Enter*.)
ProtocolReader	The default (normal) operation of a protocol reader.
Switch	The reader will operate as a simple switch (e.g., light switch, switch for a fan).

Controller sub mode	This setting more specifically defines the reader's mode of operation depending on the set ***Controller mode***.	
	StandAlone	/
	WiegandSingleKey	/
	WiegandKeysAfterEntry	**Default** - the protocol reader acts as a standard access controller. **BeepOnEnter** - the protocol reader gives a sound signal when a user presses *Enter.*
	ProtocolReader	**Default** - the protocol reader acts as a regular card reader in the access control system. **CardHolder -** the protocol reader is used as a cardholder (in hotel rooms) that turns on the electricity when the card is in the protocol reader and turns it off when removed. **LEDOutput** - the protocol reader maps LED outputs to Wiegand outputs so that external LEDs can be connected to the outputs to signal the protocol reader status or operation.
	Switch	**Pulse -** when the switch is pressed, the protocol reader connects the output to the mass for a short time (a pulse lasting a certain number of seconds) to temporarily unlock the door (lock). **Toggle -** when the switch is pressed, the protocol reader switches the status of the door (i.e., from locked to unlocked or vice versa).
Energy for (s)	The pulse duration when the reader connects the output to ground (for a specified number of seconds) to temporarily unlock the door (lock).	
Card number length	This setting determines how many bytes of card number the reader should read and use. (Different programs and applications may read and process card numbers differently.)	
Invert card numb.	If this setting is enabled, the reader will read the card number inverted (in reverse order of bytes). (This setting is usually used when newer Jantar devices are added to older systems that still use the V7 protocol.)	
Buzzer	If this setting is enabled, the reader's sound (buzzer) will be turned on.	
Enable 3 PRO	If this setting is enabled, the reader will read the encrypted 3PRO card number located within the card's internal memory. **This setting must be enabled for all readers connected to a controller using the 3PRO functionality.**	
UID if 3PRO fails	This setting can only be used if the previous setting ***3PRO mode*** is also enabled. If this setting is enabled, the reader will first attempt to read the encrypted 3PRO card number (which is stored in a specific location within the card's internal memory), and if this fails, it will use the default serial number of the card.	

Hardware settings	
RFID antenna calibr.	With this setting, you can improve the card reading function of the reader. It is mainly used when the reader is mounted on a surface that causes interference when reading (e.g. metal surfaces). We recommend that you do not change the default value of this setting. Consult your system administrator or the Jantar customer support before making any changes.
LCD type 1	The setting for some older devices with screens, which value depends on some of the hardware components used in the device. We recommend that you do not change the default values of this setting.

3. When you have finished editing the basic settings of a reader, click ***Save***.

Before saving, you can enable the ***Reset controller*** option, which, after writing new parameters to the reader, restarts the reader (turns the reader off and on).

3.2. UDP Communication

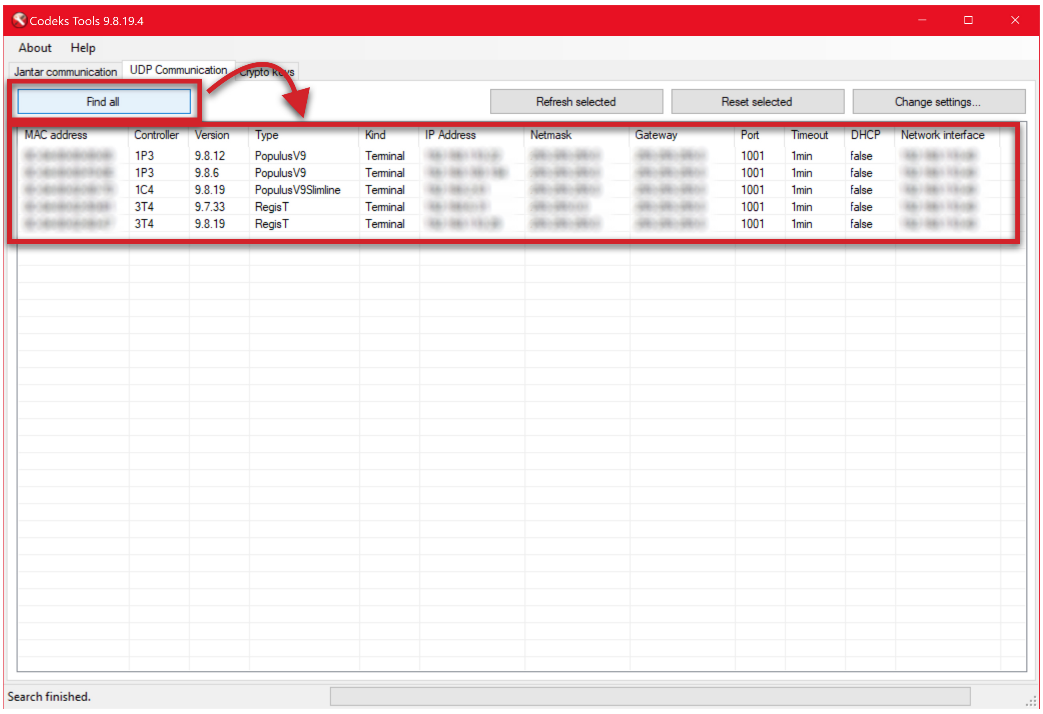
In the ***UDP Communication*** tab, you can find all Jantar devices within your local network and also change their network settings.

(UDP (User Datagram Protocol) communication differs from Jantar communication in that with this kind of communication you can find Jantar controllers within a system without the use of V9 encryption keys (because the connection does not use the V9 communication protocol), and also regardless of whether the devices are already communicating with another software. Because of this simple type of connection, however, the device settings you can change by using a UDP connection are limited (i.e. limited only to the device network settings).)

Find all controllers

1. To find all controllers click the ***Find all controllers*** button.

2. In the table below all controllers found in the local network will be displayed.



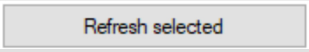
MAC address	Controller	Version	Type	Kind	IP Address	Netmask	Gateway	Port	Timeout	DHCP	Network interface
[redacted]	1P3	9.8.12	PopulusV9	Terminal	[redacted]	[redacted]	[redacted]	1001	1min	false	[redacted]
[redacted]	1P3	9.8.6	PopulusV9	Terminal	[redacted]	[redacted]	[redacted]	1001	1min	false	[redacted]
[redacted]	1C4	9.8.19	PopulusV9Slimline	Terminal	[redacted]	[redacted]	[redacted]	1001	1min	false	[redacted]
[redacted]	3T4	9.7.33	RegisT	Terminal	[redacted]	[redacted]	[redacted]	1001	1min	false	[redacted]
[redacted]	3T4	9.8.19	RegisT	Terminal	[redacted]	[redacted]	[redacted]	1001	1min	false	[redacted]

Search finished.

Refresh and reset controllers

1. To refresh or restart a controller, first, select the appropriate controllers on the list.

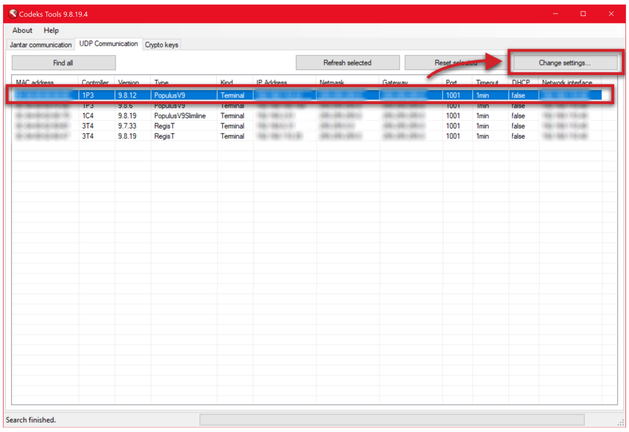
2. Then, select the appropriate button:

 Refresh selected	Clicking on the ***Refresh selected*** button will refresh the data of the selected controllers.
Reset selected	Clicking on the ***Reset selected*** button will restart the selected controllers (turn the controller off and on again).

Editing the controllers' network settings

1. To edit the network setting of a controller, first, select the appropriate controller on the list.

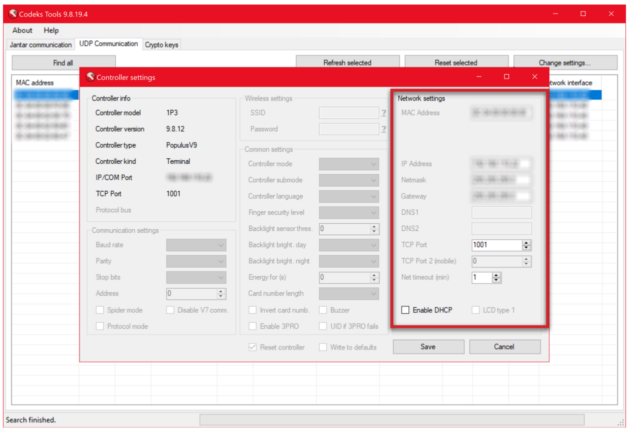
2. Then click the ***Change settings*** button.



MAC address	Controller	Version	Type	Kind	IP Address	Netmask	Gateway	Port	Timeout	DHCP	Network interface
[redacted]	1P3	9.8.12	PopulusV9	Terminal	[redacted]	[redacted]	[redacted]	1001	1min	false	[redacted]
[redacted]	1P3	9.8.6	PopulusV9	Terminal	[redacted]	[redacted]	[redacted]	1001	1min	false	[redacted]
[redacted]	1C4	9.8.19	PopulusV9Slimline	Terminal	[redacted]	[redacted]	[redacted]	1001	1min	false	[redacted]
[redacted]	3T4	9.7.33	RegisT	Terminal	[redacted]	[redacted]	[redacted]	1001	1min	false	[redacted]
[redacted]	3T4	9.8.19	RegisT	Terminal	[redacted]	[redacted]	[redacted]	1001	1min	false	[redacted]

Search finished.

3. A new window will open where you change the network settings of the selected controller.



Controller info

Controller model 1P3

Controller version 9.8.12

Controller type PopulusV9

Controller kind Terminal

IP/COM Port [redacted]

TCP Port 1001

Protocol bus

Communication settings

Baud rate

Parity

Stop bits

Address 0

□ Spider mode □ Disable V7 comm.

□ Protocol mode

Wireless settings

SSID

Password

Common settings

Controller mode

Controller submode

Controller language

Finger security level

Backlight sensor thres. 0

Backlight bright. day

Backlight bright. night

Energy for (s) 0

Card number length

□ Invert card numb. □ Buzzer

□ Enable 3PRO □ UID if 3PRO fails

☑ Reset controller □ Write to defaults

Network settings

MAC Address [redacted]

IP Address [redacted]

Netmask [redacted]

Gateway [redacted]

DNS1

DNS2

TCP Port 1001

TCP Port 2 (mobile) 0

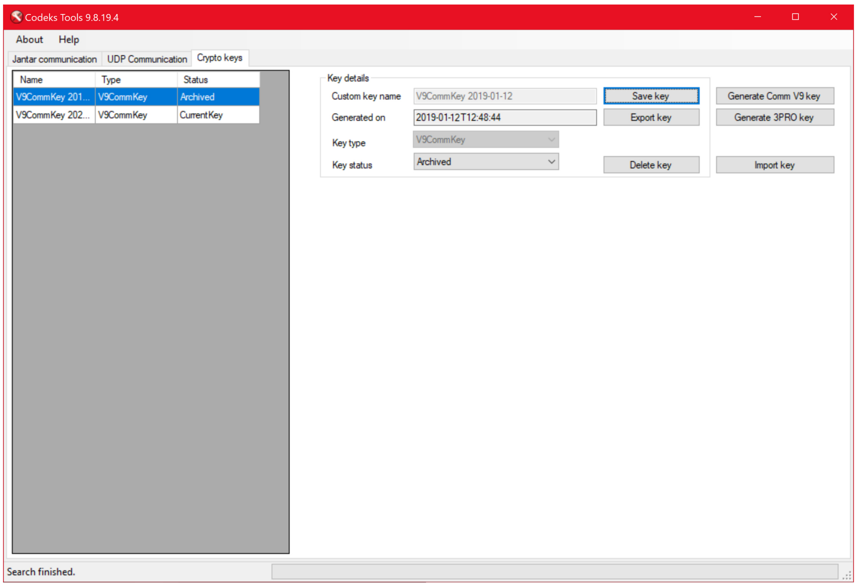
Net timeout (min) 1

□ Enable DHCP □ LCD type 1

Search finished.

3.3. Crypto keys

In the ***Crypto keys*** tab, you can create and manage custom encryption keys generated at your request.



Name	Type	Status
V9CommKey 201...	V9CommKey	Archived
V9CommKey 202...	V9CommKey	CurrentKey

Custom key name: V9CommKey 2019-01-12

Generated on: 2019-01-12T12:48:44

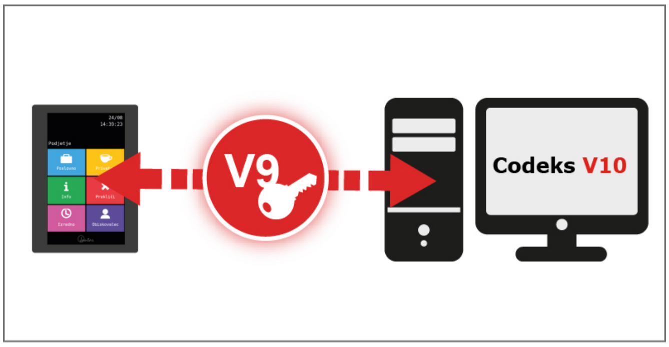
Key type: V9CommKey

Key status: Archived

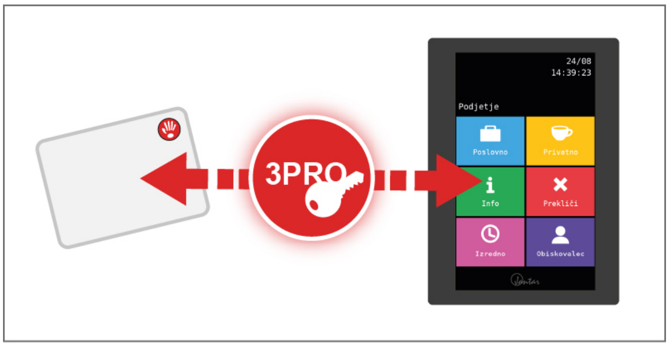
Search finished.

You can generate different encryption keys:

- **V9 encryption keys** which are used to protect the data transfer between the Codeks software server and controllers in the system.



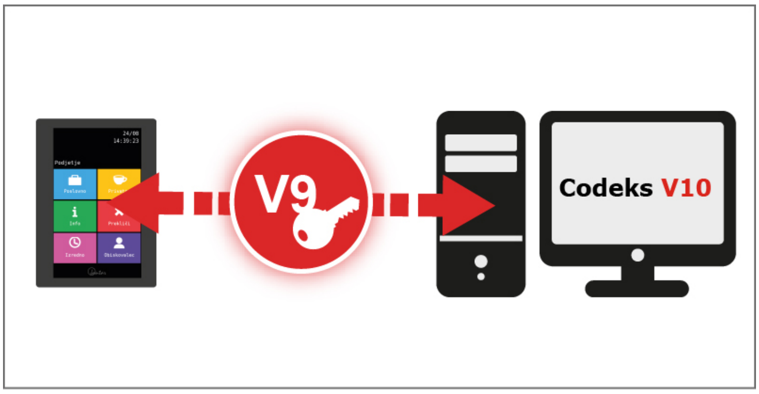
- **3PRO encryption keys** are used to protect the data transfer between the controllers and user cards.



3.3.1. Generating and using the custom V9 encryption key

V9 encryption keys are used to protect the data transfer between the Codeks software server and controllers.

Newer Jantar controllers that use the V9 protocol for communication already encrypt the communication between Codeks software and devices by using the factory default V9 encryption key for the encryption. However, you can protect the communication between the software and devices even better by using a new V9 encryption key, made especially for your system.



NOTE!
Only controllers using the **firmware version 9.6.15 or newer** enable the use of custom V9 encryption keys.

ATTENTION!
The following chapters describe the process of generating a new custom V9 encryption key.
By changing the factory default encryption key you run the risk of permanently disabling the communication with your controllers in the event that you lose your custom encryption key. We recommend that this procedure is only performed by professionally qualified persons (administrators).

The following steps are necessary to correctly and successfully implement a new custom V9 encryption key:

1. Generating a new V9 encryption key 32.
2. Assigning a custom V9 encryption key to a selected controller 38.
3. Importing the new custom V9 encryption key into the Codeks software 40.
4. Assigning the new V9 encryption key to all communication lines 43 that connect controllers which have been assigned the new key.

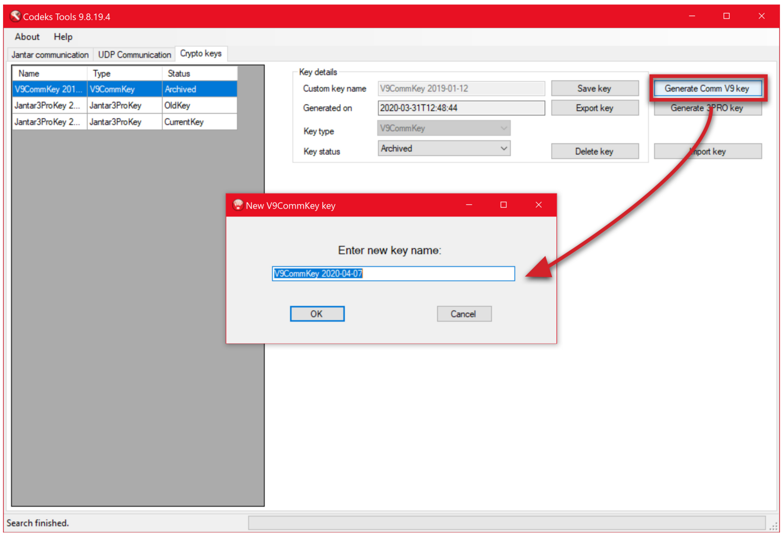
3.3.1.1. Generating, editing and managing the custom V9 encryption key

In the ***Crypto key*** tab, you can generate new, edit, export and import encryption keys and delete them if needed.

Generating a new V9 encryption key

1. To generate a new V9 encryption key click the ***Generate Comm V9 key*** button.

2. A new window will open, where you can **enter a new name for your key**, then **click *OK***.

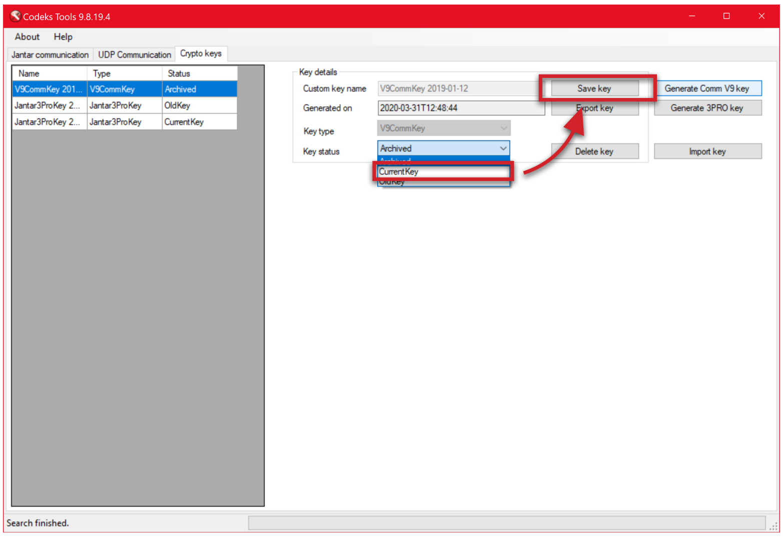


Name	Type	Status
V9CommKey 201...	V9CommKey	Archived
Jantar3ProKey 2...	Jantar3ProKey	OldKey
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey

Custom key name: V9CommKey 2019-01-12
Generated on: 2020-03-31T12:48:44
Key type: V9CommKey
Key status: Archived

Enter new key name: V9CommKey 2020-04-07

3. Then, in the entry form, set the *Key status* setting to ***Current key*** and click the ***Save key*** button.

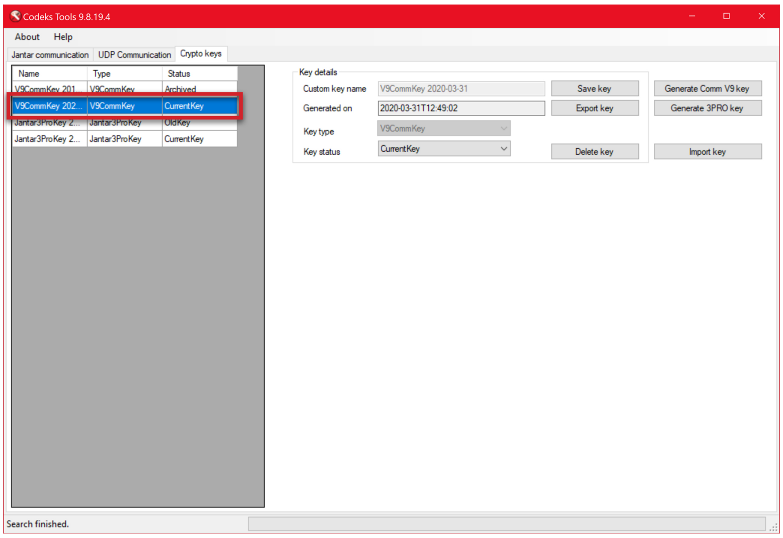


Name	Type	Status
V9CommKey 201...	V9CommKey	Archived
Jantar3ProKey 2...	Jantar3ProKey	OldKey
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey

Custom key name: V9CommKey 2019-01-12
Generated on: 2020-03-31T12:48:44
Key type: V9CommKey
Key status: Archived

Key status	
Archived	The V9 encryption key is archived, meaning it is only stored in the *Codeks Tools* program. Before you can assign it to the selected controllers, you must first change its status to *Current key*. A key with an *Archived* status may have been used in the past or may have been left waiting to be used.
Current key	The encryption key is the currently selected (active) V9 encryption key, ready to be assigned to the selected controllers using the ***Set V9 Comm key*** function.
Old key	The encryption key is a direct predecessor to the currently selected (active) V9 encryption key. The tag is important for tracking the order of key usage in a given *Codes* system.

4. The new encryption key will be added to the list on the left.



Name	Type	Status
V9CommKey 201...	V9CommKey	Archived
V9CommKey 202...	V9CommKey	CurrentKey
Jantar3ProKey 2...	Jantar3ProKey	OldKey
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey

Key details
Custom key name: V9CommKey 2020-03-31
Generated on: 2020-03-31T12:49:02
Key type: V9CommKey
Key status: CurrentKey

Search finished.

Your custom V9 encryption key has now been generated and is ready to use. However, in this step, it is not yet used for communicating with any of your controllers. To use your custom V9 encryption key, you need to **write the new encryption key to the selected controller** 38, **import the encryption key into Codeks software** 40, and **assign a new encryption key to the selected communication lines** 43.

Information for Jantar partners and distributors

All V9 encryption keys created with *Codeks Tools* are written in the *CodeksCommunicationCryptoKey.txt* file, which is stored in the *... Program Files\Jantar\CodeksTools* folder.

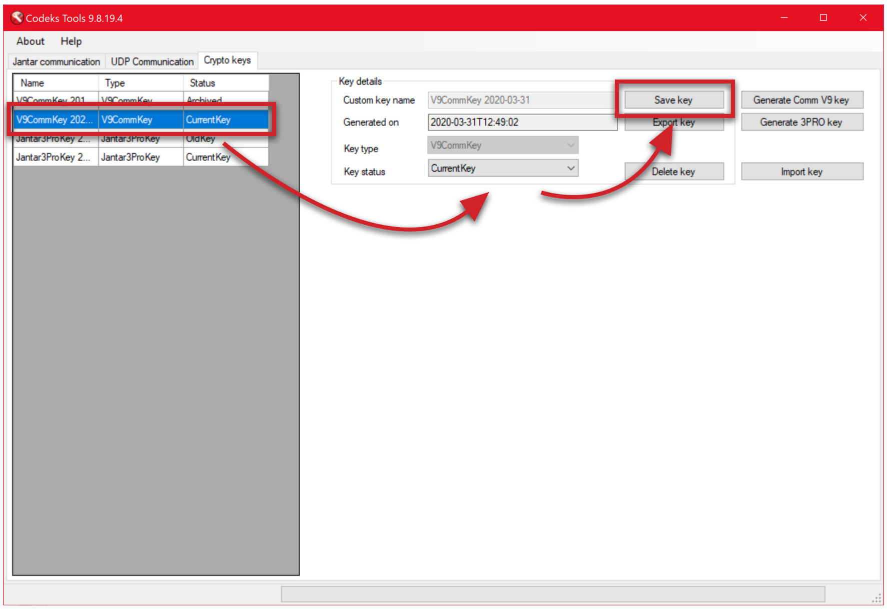
ATTENTION!
The **CodeksCommunicationCryptoKey.txt** file contains all the V9 encryption keys you have created with your copy of the *Codeks Tools* program for end-users' Codeks systems. This means that the file contains highly sensitive security information. **Therefore, the file must be protected against theft or destruction!**

ATTENTION!
Make sure you back up the file containing the V9 encryption keys and save it in a safe place. Pay particular attention to security when transferring the file to another computer.
If a specific V9 encryption key is ever lost, it will be necessary to find the appropriate encryption key again to restore communication with the device or reset the device to factory default settings. Unfortunately, in cases where this is not possible, a device with a lost encryption key can no longer be used.

Editing the V9 encryption key

1. To edit a V9 encryption key, first, mark the appropriate key on the list on the left.

2. The key data will appear in the form where you can now make the changes you want.



Codeks Tools 9.8.19.4

Name	Type	Status
V9CommKey 201...	V9CommKey	Archived
V9CommKey 202...	V9CommKey	CurrentKey
Jantar3ProKey 2...	Jantar3ProKey	OldKey
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey

Key details

Custom key name: V9CommKey 2020-03-31

Generated on: 2020-03-31T12:49:02

Key type: V9CommKey

Key status: CurrentKey

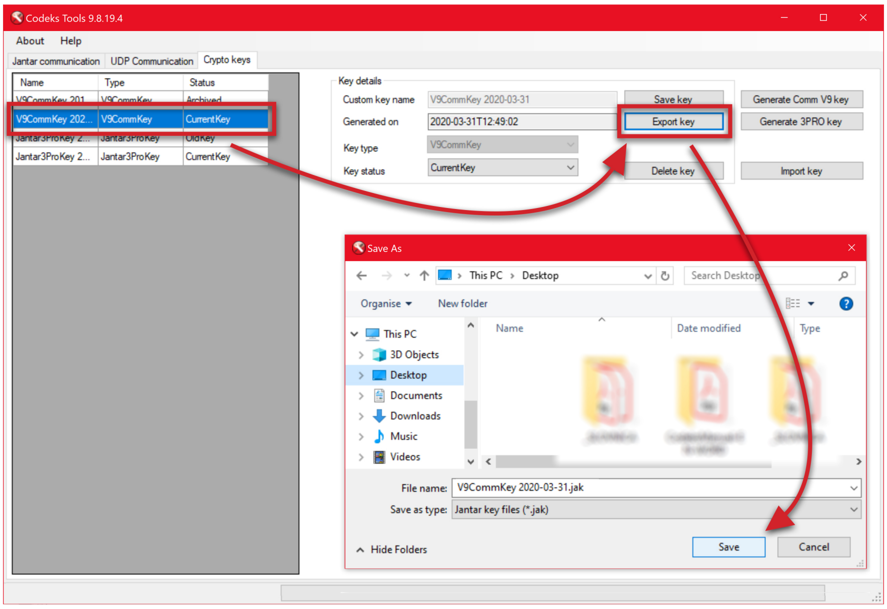
3. When you are finished making changes, click the ***Save key*** button***.***

Exporting the V9 encryption key

1. To export a V9 encryption key, first, mark the appropriate key on the list on the left.

2. Then click the ***Export key*** button***.***

3. A new window will open where you can select where you want to save the file to. Click ***Save.***



Name	Type	Status
V9CommKey 201...	V9CommKey	Archived
V9CommKey 202...	V9CommKey	CurrentKey
Jantar3ProKey 2...	Jantar3ProKey	OldKey
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey

Key details

Custom key name: V9CommKey 2020-03-31

Generated on: 2020-03-31T12:49:02

Key type: V9CommKey

Key status: CurrentKey

File name: V9CommKey 2020-03-31.jak

Save as type: Jantar key files (*.jak)

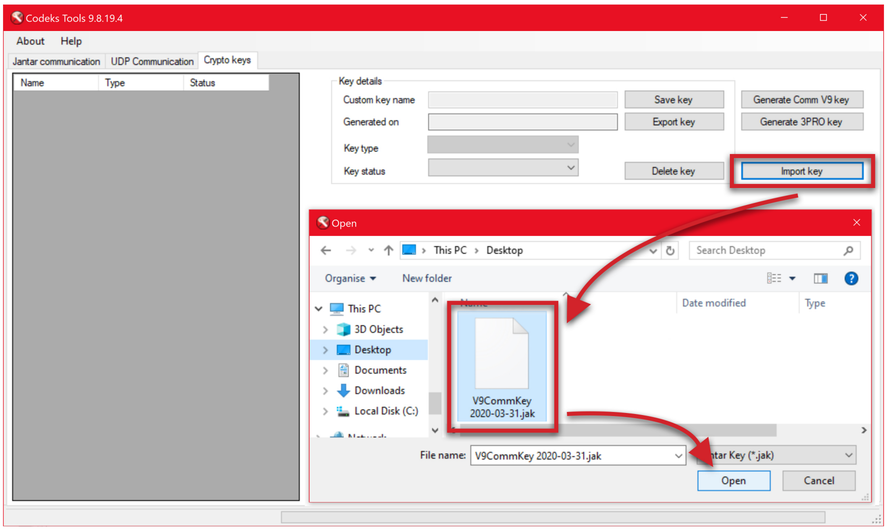
NOTE
The file you just exported contains your custom V9 encryption key, which will be used to encrypt the communication with controllers in your system. This means that the file contains highly sensitive security information. Therefore, the file must be protected against theft or destruction.

ATTENTION!
Make sure you back up the file you just exported and save it in a safe place. Pay particular attention to security when transferring the file to another computer.
If a specific V9 encryption key is ever lost, it will be necessary to find the appropriate encryption key again to restore communication with the device or reset the device to factory default settings. Unfortunately, in cases where this is not possible, a device with a lost encryption key can no longer be used.

Importing the V9 encryption key

1. To import a V9 encryption key (e.g. when transferring it to a new computer), first, click the *Import key* button.

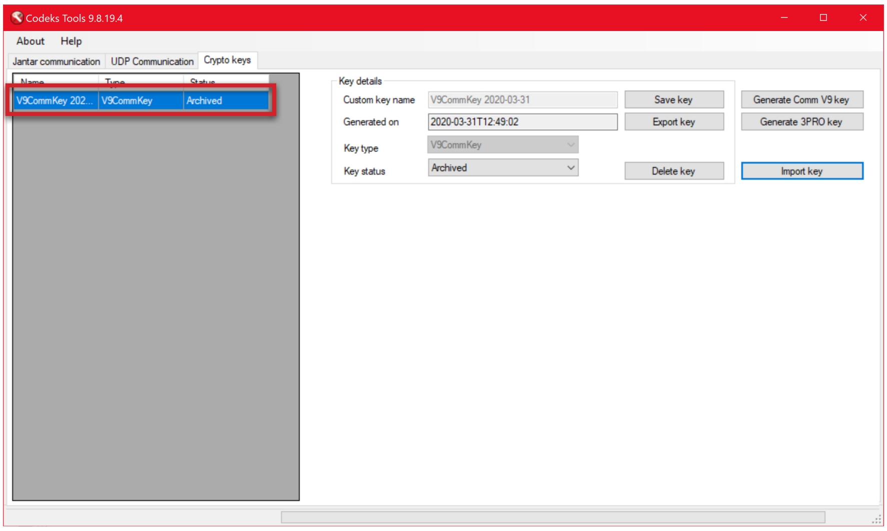
2. A new window will open where you can navigate to and select the file you wish to import. Click ***Open.***



File name: V9CommKey 2020-03-31.jak

…tar Key (*.jak)

3. The newly imported V9 encryption key will be displayed on the list on the left.



Name	Type	Status
V9CommKey 202...	V9CommKey	Archived

Custom key name: V9CommKey 2020-03-31

Generated on: 2020-03-31T12:49:02

Key type: V9CommKey

Key status: Archived

NOTE
Be extremely careful when transferring the file containing your V9 encryption key. The file contains highly sensitive security information and must, therefore, be protected against theft or destruction.

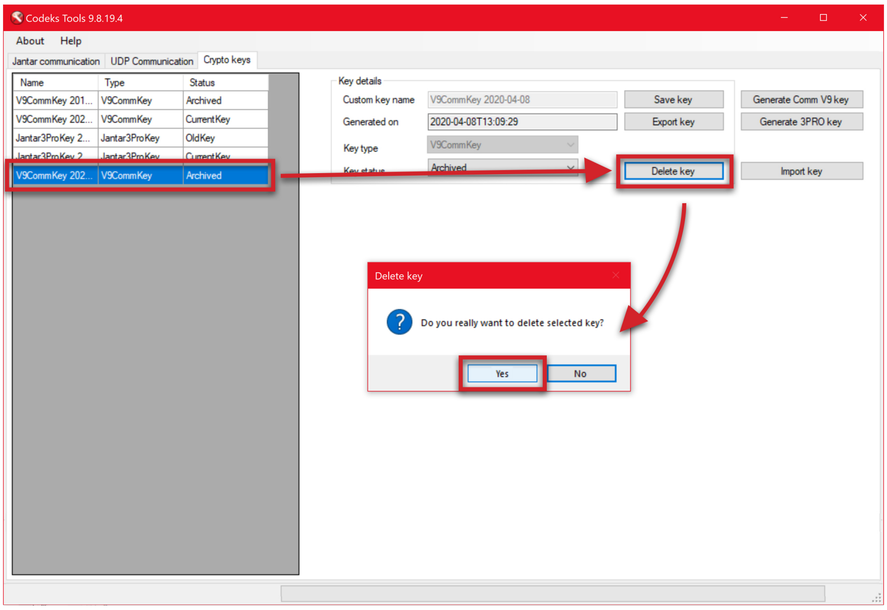
Deleting the V9 encryption key

NOTE
Before deleting a V9 encryption key, make sure that the key is no longer used to communicate with devices!
If a specific V9 encryption key is ever lost, it will be necessary to find the appropriate encryption key again to restore communication with the device or reset the device to factory default settings. Unfortunately, in cases where this is not possible, a device with a lost encryption key can no longer be used.

1. To delete a V9 encryption key, first mark the appropriate key on the list on the left.

2. Then click the ***Delete key*** button***.***

3. The system will request confirmation of the deletion. **Click *Yes* to permanently delete the key.**



Name	Type	Status
V9CommKey 201...	V9CommKey	Archived
V9CommKey 202...	V9CommKey	CurrentKey
Jantar3ProKey 2...	Jantar3ProKey	OldKey
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey
V9CommKey 202...	V9CommKey	Archived

Key details
Custom key name: V9CommKey 2020-04-08
Generated on: 2020-04-08T13:09:29
Key type: V9CommKey
Key status: Archived

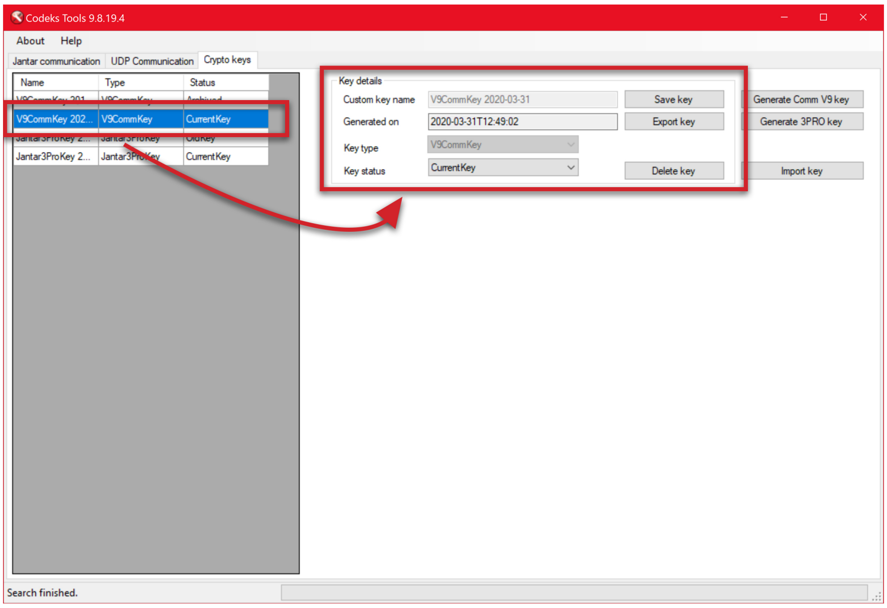
Do you really want to delete selected key?

3.3.1.2. Assigning a custom V9 encryption key to a selected controller

By using the ***Set V9 Comm key*** function you **will assign the V9 encryption key which is currently set to the *Current key* status as the new communication encryption key for all selected controllers**.

ATTENTION!
A custom V9 encryption key can only be assigned to devices that have **firmware version 9.6.15 or newer**.

1. In the *V9 Communication key* tab, first, check that the appropriate key is set as the current V9 key (i.e. its status is set to *Current key*).



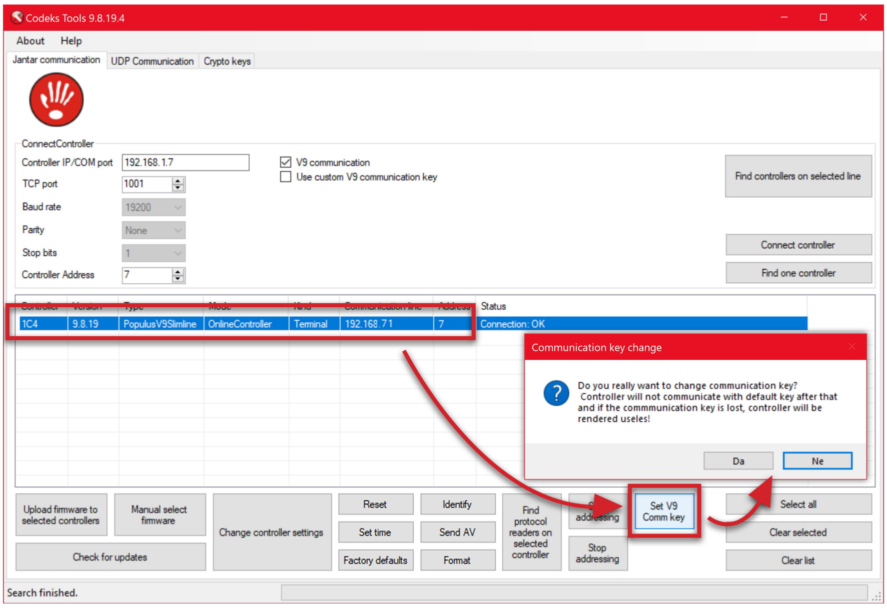
Name	Type	Status
V9CommKey 201...	V9CommKey	Archived
V9CommKey 202...	V9CommKey	CurrentKey
Jantar3ProKey 2...	Jantar3ProKey	OldKey
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey

Key details
Custom key name: V9CommKey 2020-03-31
Generated on: 2020-03-31T12:49:02
Key type: V9CommKey
Key status: CurrentKey

Search finished.

2. Then, in the ***Jantar communication*** tab, **find the appropriate controller and mark it in the table.**

3. To assign the custom V9 encryption key to the selected controller click the *Set V9 Comm key* button.



ConnectController
Controller IP/COM port: 192.168.1.7
TCP port: 1001
Baud rate: 19200
Parity: None
Stop bits: 1
Controller Address: 7
☑ V9 communication
☐ Use custom V9 communication key

Controller	Version	Type	Mode	Kind	Communication line	Address	Status
1C4	9.8.19	PopulusV9Slimline	OnlineController	Terminal	192.168.7.1	7	Connection: OK

Communication key change

Do you really want to change communication key?
Controller will not communicate with default key after that and if the commmunication key is lost, controller will be rendered useles!

Da Ne

Search finished.

4. A warning will appear informing you that you are about to change the way you communicate with the controllers and that communication with the factory default key will no longer be possible. If you are not quite sure that you want to change the encryption key, you can still cancel the process without changes at this point (click **No**). If you want to assign your own V9 encryption key to the device, click **Yes**.

5. The controller will confirm the allocation of the new V9 encryption key with a single audio signal (1 beep).

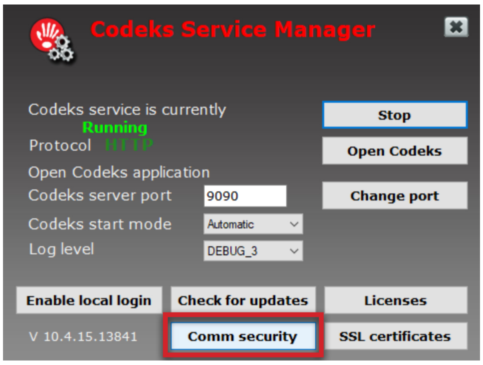
ATTENTION!
By allocating a new custom V9 encryption key to selected controllers, you can no longer communicate with it using the default factory encryption key.
In order to restore communication with the controller in the *Codeks Tools* program, enable the *Use custom V9 communication key* 24 function.
In order to communicate with the selected controller using the *Codeks* application, it is first necessary to *import the new custom V9 encryption key into the Codeks system* 40 and then also assign the key to all communication lines 38 that connect the controllers using the new encryption key.

3.3.1.3. Importing the new custom V9 encryption key into the Codeks software

You can import the newly generated custom V9 encryption key into your *Codeks* system by using the ***Codeks Servis Manager*** program. To perform the process described in this chapter you will need access to the Codeks server.

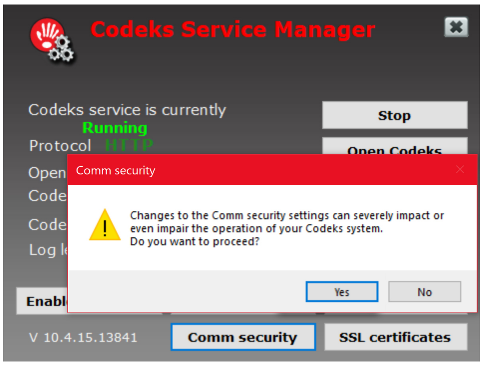
1. First, launch the **Codeks Service Manager** program.

2. Then click the ***Comm security*** button.



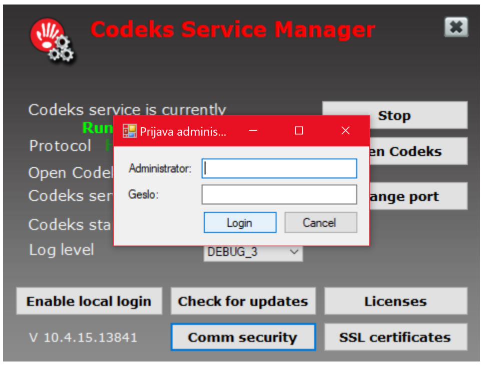
Codeks service is currently Running
Protocol HTTP
Open Codeks application
Codeks server port 9090
Codeks start mode Automatic
Log level DEBUG_3
V 10.4.15.13841

3. The system will then warn you that changes to *Comm security* can critically affect or even impair the functioning of your *Codeks* system. **Click *Yes*.**



Changes to the Comm security settings can severely impact or even impair the operation of your Codeks system.
Do you want to proceed?

4. Next, the system will ask for **your super admin username and password.** Enter the relevant information and click ***Login*.**



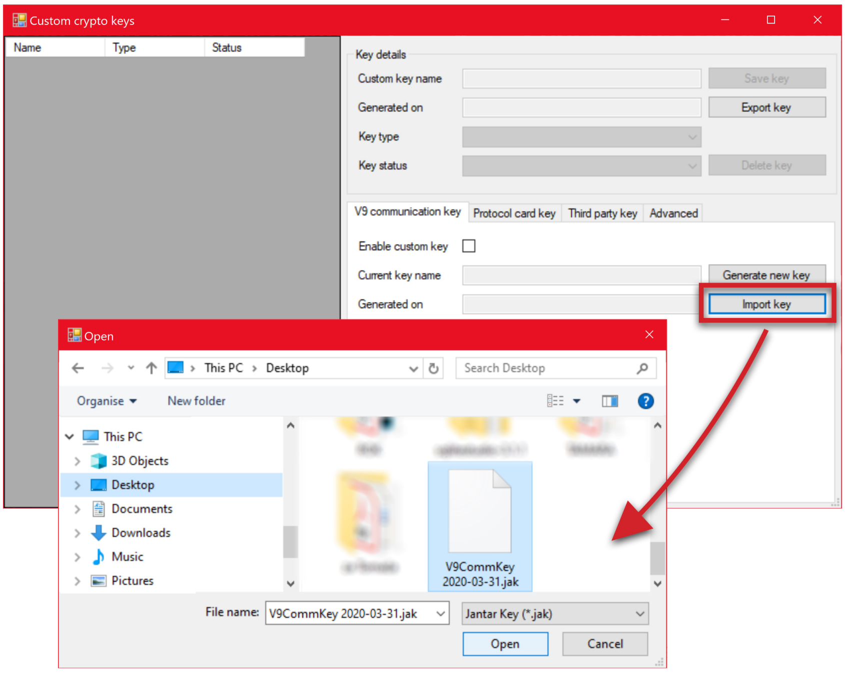
Administrator:
Geslo:

5. A new window will open.

In the ***V9 communication key*** tab, click the ***Import key*** button.

In the new window, **locate the file with your V9 encryption key** that you exported from *Codeks Tools*.

Click ***Open***.



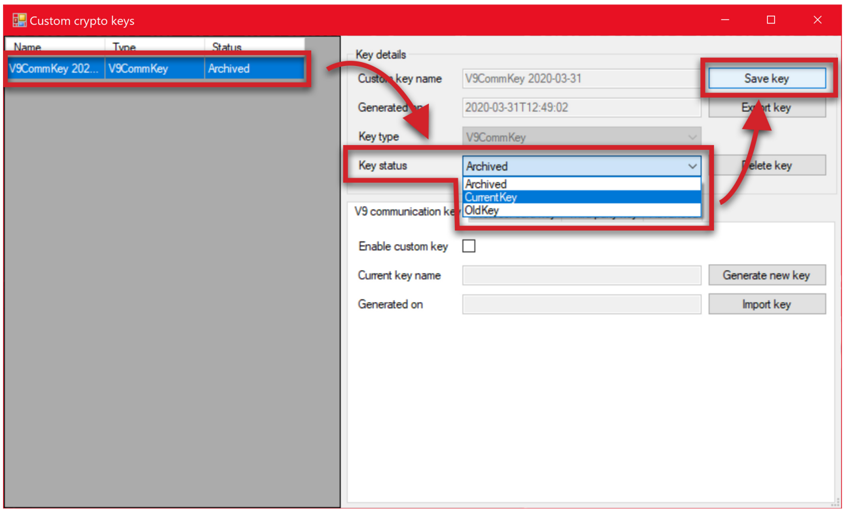
File name: V9CommKey 2020-03-31.jak

Jantar Key (*.jak)

6. The newly imported key will be displayed on the list on the left and its status set to ***Archived***.

The status of the key must be changed to ***Current key*** for further use.

Then click ***Save.***



Name	Type	Status
V9CommKey 202...	V9CommKey	Archived

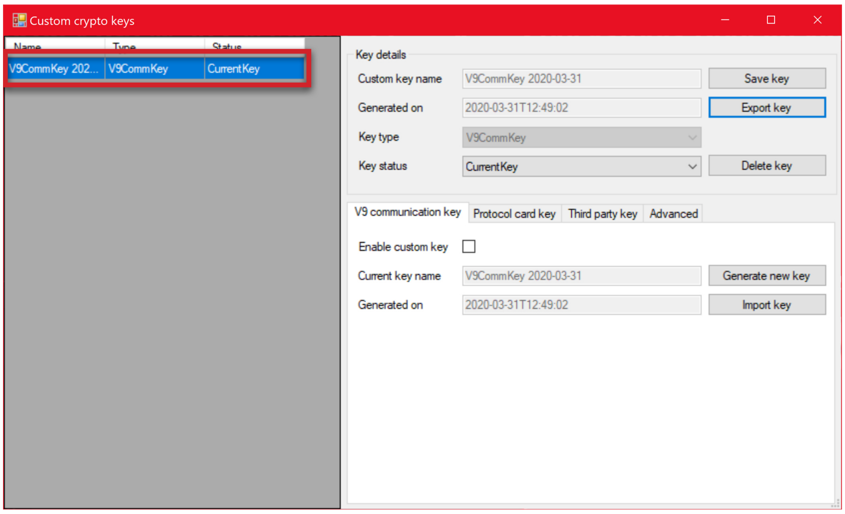
Custom key name: V9CommKey 2020-03-31

Generated on: 2020-03-31T12:49:02

Key type: V9CommKey

Key status: Archived

7. The key on the list on the left is now set to *Current key* and is now ready to use.


Custom crypto keys

Name	Type	Status
V9CommKey 202...	V9CommKey	CurrentKey

Key details

Custom key name: V9CommKey 2020-03-31

Generated on: 2020-03-31T12:49:02

Key type: V9CommKey

Key status: CurrentKey

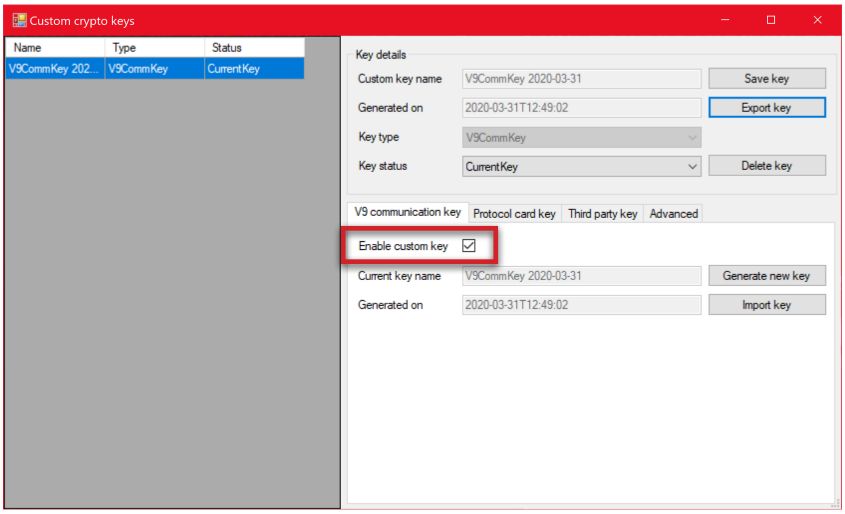
V9 communication key

Enable custom key ☐

Current key name: V9CommKey 2020-03-31

Generated on: 2020-03-31T12:49:02

8. Enable the global setting for using V9 encryption keys for communication between the Codeks software and controllers by enabling the ***Enable custom key*** setting in the *V9 communication key* tab of the *Codeks Service Manager*.


Custom crypto keys

Name	Type	Status
V9CommKey 202...	V9CommKey	CurrentKey

Key details

Custom key name: V9CommKey 2020-03-31

Generated on: 2020-03-31T12:49:02

Key type: V9CommKey

Key status: CurrentKey

V9 communication key

Enable custom key ☑

Current key name: V9CommKey 2020-03-31

Generated on: 2020-03-31T12:49:02

9. Finally, stop and restart the Codeks application in the Codeks Service Manager program.

In order to finally enable communication between the *Codeks* software and the selected controllers, it is still necessary to set the new V9 encryption key also to the communication lines 38 that connect the controllers to the new encryption key.

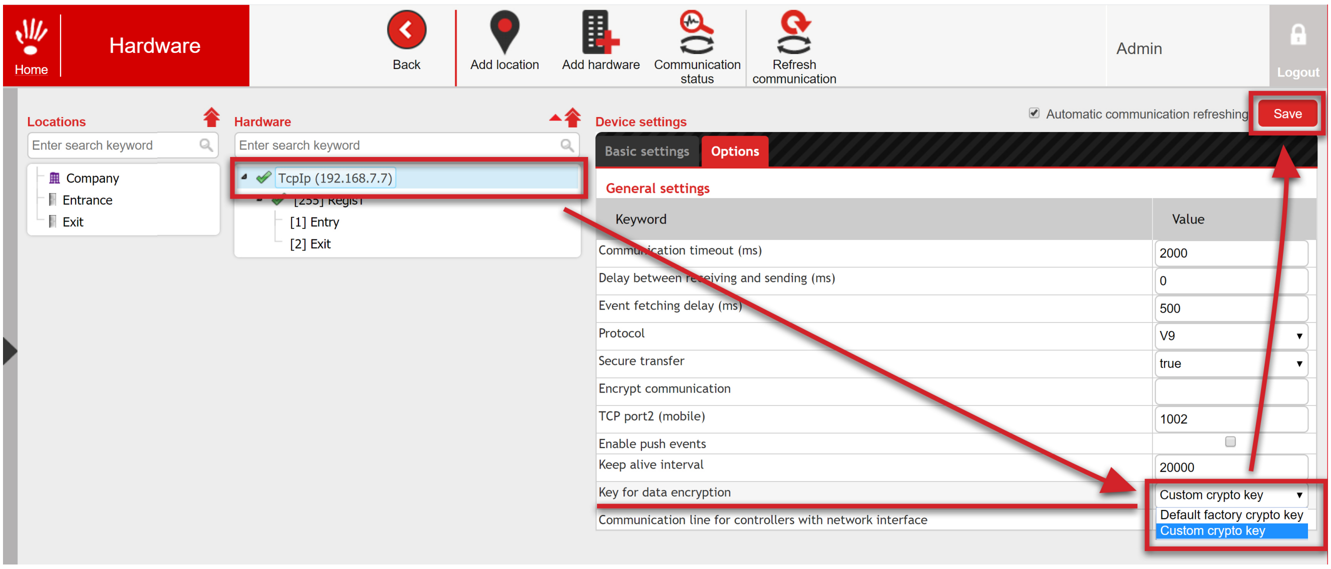
3.3.1.4. Setting the custom V9 encryption key on the communication lines

NOTE!
In the Codeks application, communication with the V9 encryption key can only be set at the communication line level. Controllers and readers connected to the same communication line, therefore, use the same encryption key.
In order to enable communication, the same encryption key as assigned to the communication line must also be sent to each controller or reader attached to that communication line.

1. Open the *Codeks* application and sign in with your administrator username and password.

2. In the *Hardware* editor, **in the hardware list, locate and mark the communication line that you want to change the V9 encryption key for**.

3. In the device settings, select the ***Options*** tab and look for the ***Data encryption key*** setting. By default, this setting is set to ***Default factory crypto key***, and you must enable the use of your new custom V9 encryption key by selecting ***Custom crypto key*** from the setting's drop-down menu.



☑ Automatic communication refreshing

Keyword	Value
Communication timeout (ms)	2000
Delay between receiving and sending (ms)	0
Event fetching delay (ms)	500
Protocol	V9
Secure transfer	true
Encrypt communication	
TCP port2 (mobile)	1002
Enable push events	□
Keep alive interval	20000
Key for data encryption	Custom crypto key Default factory crypto key Custom crypto key
Communication line for controllers with network interface	

4. Save your changes by clicking ***Save.***

5.* In the same way, set the new V9 encryption key to other communication lines that connect controllers with the new encryption key.

6. Finally, you also need to send tables to controllers or at least refresh the communication with them!

3.3.2. Generating and using the custom 3PRO encryption key

NOTE!
3PRO encryption can only be performed on Mifare® DESFire® cards, which were 3PRO encrypted by Jantar when purchased (or subsequently). Encrypted 3PRO cards can only be bought from Jantar or our distributors.

NOTE!
Changing the 3PRO encryption key can only be performed on controllers with firmware version 9.8.1 or newer.

3PRO is a means for protecting the (Mifare® DESFire®) user card and its contents in communication with our Jantar controllers. The name derives from triple protection (3 protection) with encryption:

- **protected card content;**
  The card's content is encrypted, which means that the card number and the data contained on the card cannot be easily read. Only the controller with an appropriate encryption key can decipher the data.
- **the content access is encrypted;**
  The cards have a memory component divided into several parts and access to each part is protected by a different encryption key. This allows the user to use the same card in different systems and for different services, while data in different memory parts of the card remain separate and protected.
- **communication between the card and the controller is encrypted;**
  Data packages which are exchanged during communication between the card and the controller are also encrypted. This means that the exchanged messages are unrecognisable to the unauthorised "listener" since they do not know the key that deciphers the code.

3PRO
24/08
14:39:23
Podjetje
Poslovno
Privatno
Info
Prekliči
Izredno
Obiskovalec

The 3PRO key is stored on all user cards and is also used by controllers in the system in order to communicate with the user cards.
The 3PRO cards you buy from Jantar already use the factory default 3PRO encryption key to protect data transfer with controllers. However, you can protect the communication between the controllers and user cards even better by using a new 3PRO encryption key, made especially for your system.

The following steps are necessary to correctly and successfully implement a new custom 3PRO encryption key:

1. Generating a new 3PRO encryption key 45.
2. Importing the new custom 3PRO encryption key into the Codeks software 52.
3. Setting the 3PRO encryption key in the Codeks software 55.
4. Changing the 3PRO encryption keys on user cards 57.

3.3.2.1. Generating, editing and managing the custom 3PRO encryption key

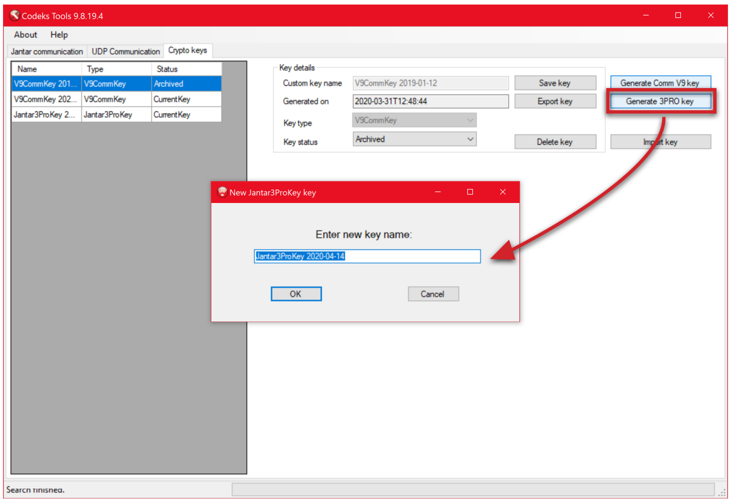
In the ***Crypto key*** tab, you can generate new, edit, export and import encryption keys and delete them if needed.

Generating a new 3PRO encryption key

NOTE!
3PRO encryption keys cannot be assigned to user cards using the *Codeks Tools* program. Changing 3PRO encryption keys is only possible using the main Codeks application.

1. To generate a new 3PRO encryption key click the ***Generate 3PRO key*** button.

2. A new window will open, where you can **enter a new name for your key**, then **click *OK***.



Name	Type	Status
V9CommKey 201...	V9CommKey	Archived
V9CommKey 202...	V9CommKey	CurrentKey
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey

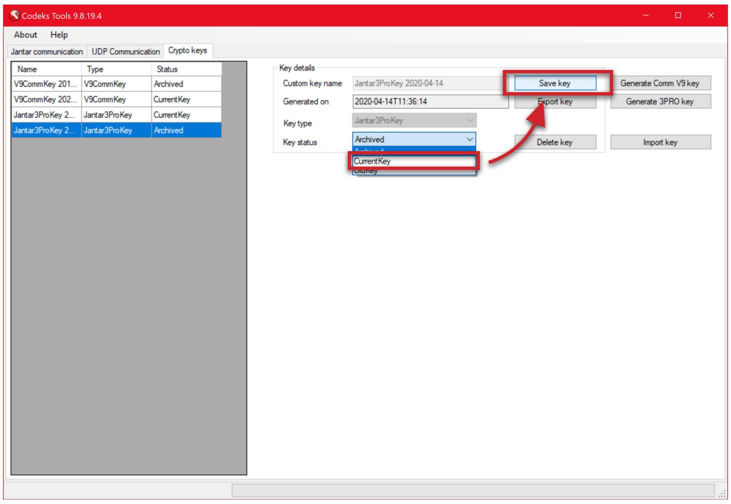
Custom key name: V9CommKey 2019-01-12
Generated on: 2020-03-31T12:48:44
Key type: V9CommKey
Key status: Archived

Enter new key name:
Jantar3ProKey 2020-04-14

Search finished.

3. Then, in the entry form, set the *Key status* setting to ***Current key*** and click the ***Save key*** button.

(If you are already using a custom 3PRO encryption key, you MUST set the status of your previous 3PRO encryption key to *Old key.*)

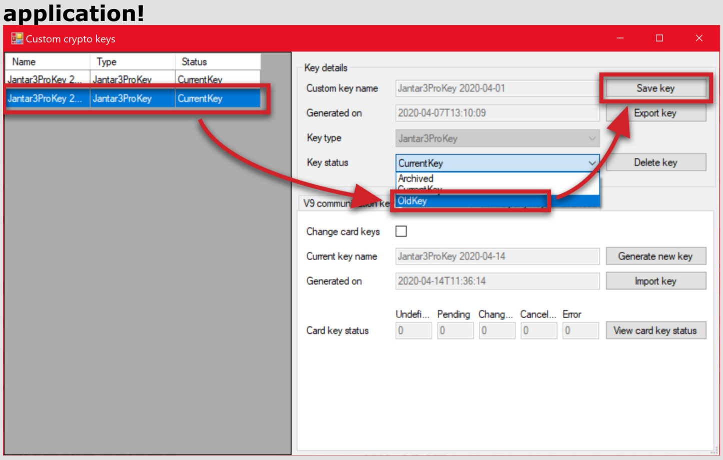


Name	Type	Status
V9CommKey 201...	V9CommKey	Archived
V9CommKey 202...	V9CommKey	CurrentKey
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey
Jantar3ProKey 2...	Jantar3ProKey	Archived

Custom key name: Jantar3ProKey 2020-04-14
Generated on: 2020-04-14T11:36:14
Key type: Jantar3ProKey
Key status: Archived
Archived
CurrentKey
OldKey

Key status	
Archived	The 3PRO encryption key is archived, meaning it is only stored in the *Codeks Tools* program. A key with an *Archived* status may have been used in the past or may have been left waiting to be used.
Current key	The encryption key is the currently selected (active) 3PRO encryption key. The tag is important for tracking the order of key usage in a given *Codes* system.
Old key	The encryption key is a direct predecessor to the currently selected (active) 3PRO encryption key. The tag is important for tracking the order of key usage in a given *Codes* system.

NOTE!
We recommend that you consistently mark old 3PRO keys, which are the direct predecessors of the current 3PRO key, with the *Old key* status, **because the correct marking of 3PRO key statuses is crucial in the Codeks application!**



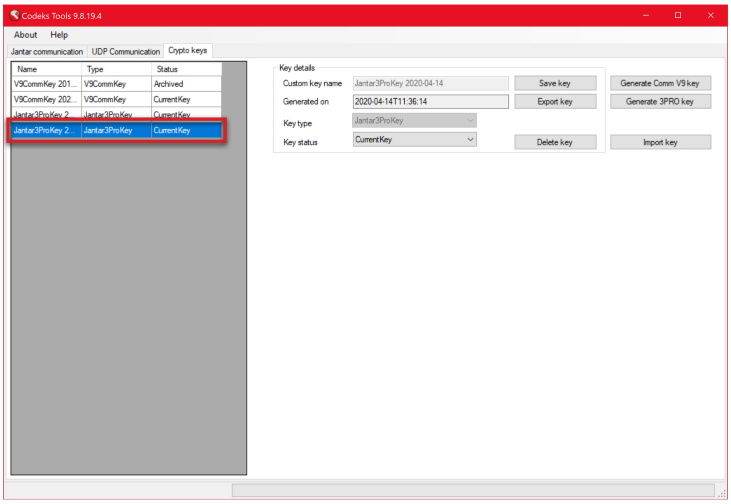
Name	Type	Status
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey

Custom key name: Jantar3ProKey 2020-04-01
Generated on: 2020-04-07T13:10:09
Key type: Jantar3ProKey
Key status: CurrentKey (Archived, CurrentKey, OldKey)
Change card keys: □
Current key name: Jantar3ProKey 2020-04-14
Generated on: 2020-04-14T11:36:14

	Undefi...	Pending	Chang...	Cancel...	Error
Card key status	0	0	0	0	0

This is because the Codeks software uses the *Old key* and *Current key* statuses in the process of changing the key on user cards, always changing only the 3PRO key labeled *Old key* with the 3PRO key labeled *Current key*.
You can read more about the import and 3PRO key statuses in chapter Changing the 3PRO encryption keys on user cards 57.

4. The new encryption key will be added to the list on the left.



Name	Type	Status
V9CommKey 201...	V9CommKey	Archived
V9CommKey 202...	V9CommKey	CurrentKey
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey

Custom key name: Jantar3ProKey 2020-04-14
Generated on: 2020-04-14T11:36:14
Key type: Jantar3ProKey
Key status: CurrentKey

Next, you still need to import your new custom 3PRO key into the Codeks application 52, properly set the controllers and readers within your system 55 and start the process of changing the 3PRO encryption keys on user cards 57.

Information for Jantar partners and distributors

All 3PRO encryption keys created with *Codeks Tools* are written in the *CodeksCommunicationCryptoKey.txt* file, which is stored in the *... Program Files\Jantar \CodeksTools* folder.

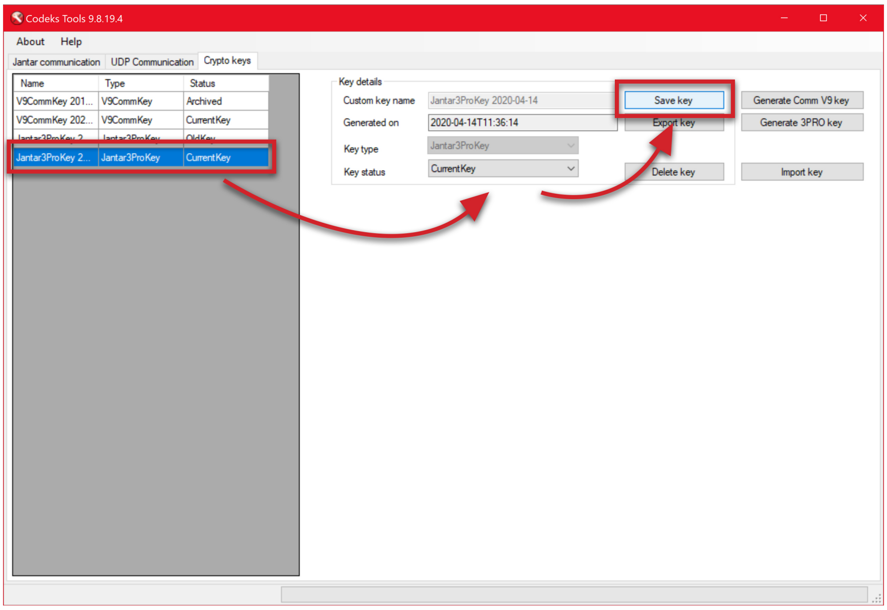
ATTENTION!
The **CodeksCommunicationCryptoKey.txt** file contains all the 3PRO encryption keys you have created with your copy of the *Codeks Tools* program for end-users' Codeks systems. This means that the file contains highly sensitive security information. **Therefore, the file must be protected against theft or destruction!**

ATTENTION!
Make sure you back up the file containing the 3PRO encryption keys and save it in a safe place. Pay particular attention to security when transferring the file to another computer.
If a specific 3PRO encryption key is ever lost, it will be necessary to find the appropriate encryption key again to restore communication between the devices and user cards. or reset the device to factory default settings. In cases where this is not possible, the user cards can, unfortunately, no longer be used.

Editing the 3PRO encryption key

1. To edit a 3PRO encryption key, first, mark the appropriate key on the list on the left.

2. The key data will appear in the form where you can now make the changes you want.



Name	Type	Status
V9CommKey 201...	V9CommKey	Archived
V9CommKey 202...	V9CommKey	CurrentKey
Jantar3ProKey 2...	Jantar3ProKey	OldKey
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey

Key details

Custom key name: Jantar3ProKey 2020-04-14

Generated on: 2020-04-14T11:36:14

Key type: Jantar3ProKey

Key status: CurrentKey

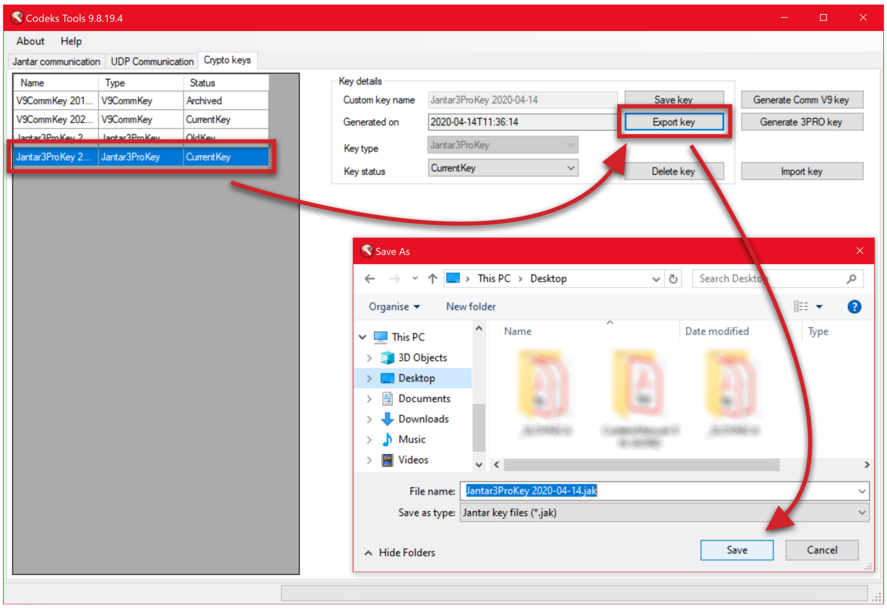
3. When you are finished making changes, click the ***Save key*** button***.***

Exporting the 3PRO encryption key

1. To export a 3PRO encryption key, first, mark the appropriate key on the list on the left.

2. Then click the ***Export key*** button***.***

3. A new window will open where you can select where you want to save the file to. Click ***Save.***



Name	Type	Status
V9CommKey 201...	V9CommKey	Archived
V9CommKey 202...	V9CommKey	CurrentKey
Jantar3ProKey 2...	Jantar3ProKey	OldKey
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey

Key details

Custom key name: Jantar3ProKey 2020-04-14

Generated on: 2020-04-14T11:36:14

Key type: Jantar3ProKey

Key status: CurrentKey

File name: Jantar3ProKey 2020-04-14.jak

Save as type: Jantar key files (*.jak)

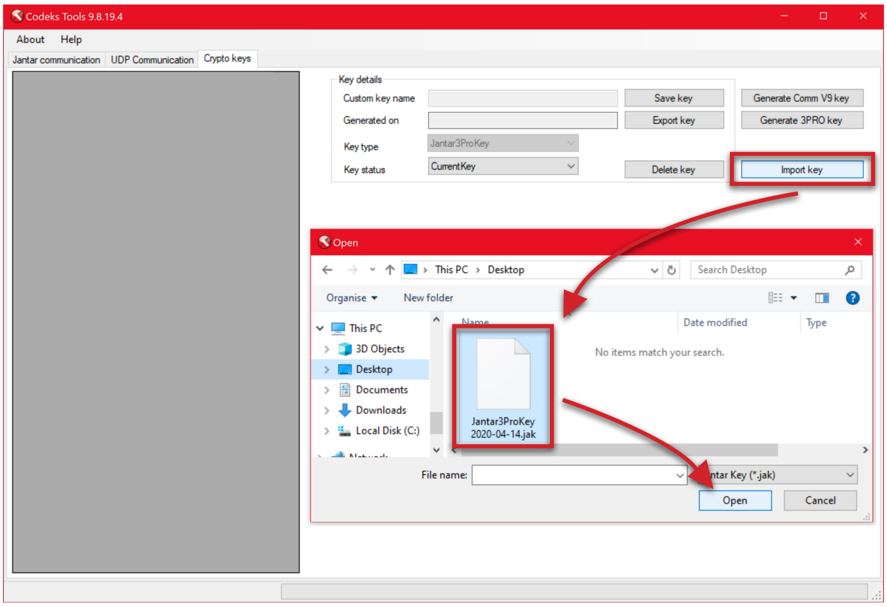
NOTE
The file you just exported contains your custom 3PRO encryption key, which will be used to encrypt the communication with controllers in your system. This means that the file contains highly sensitive security information. Therefore, the file must be protected against theft or destruction.

ATTENTION!
Make sure you back up the file containing the 3PRO encryption keys and save it in a safe place. Pay particular attention to security when transferring the file to another computer.
If a specific 3PRO encryption key is ever lost, it will be necessary to find the appropriate encryption key again to restore communication between the devices and user cards. or reset the device to factory default settings. In cases where this is not possible, the user cards can, unfortunately, no longer be used.

Importing the 3PRO encryption key

1. To import a 3PRO encryption key (e.g. when transferring it to a new computer), first, click the *Import key* button.

2. A new window will open where you can navigate to and select the file you wish to import. Click ***Open.***



Key type: Jantar3ProKey

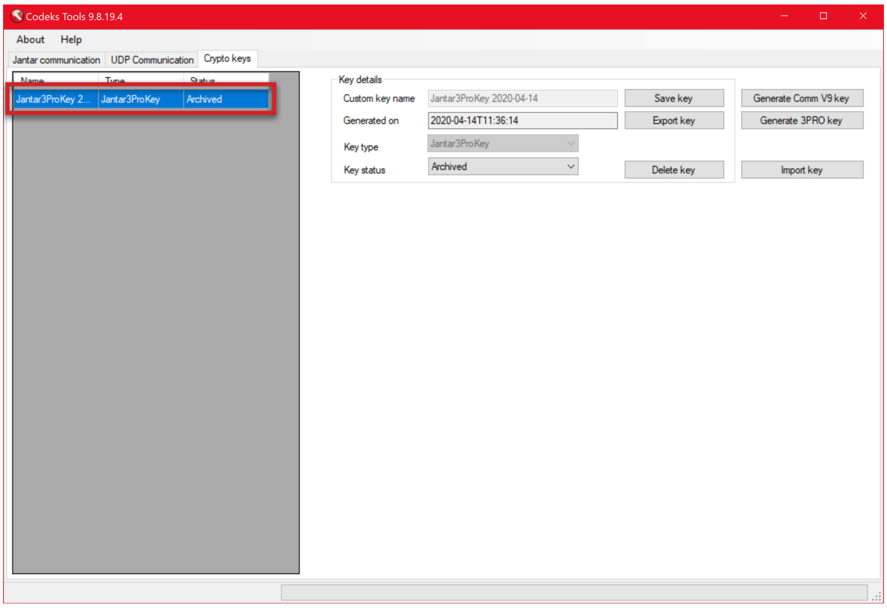
Key status: CurrentKey

No items match your search.

Jantar3ProKey 2020-04-14.jak

Jantar Key (*.jak)

3. The newly imported 3PRO encryption key will be displayed on the list on the left.



Name	Type	Status
Jantar3ProKey 2...	Jantar3ProKey	Archived

Custom key name: Jantar3ProKey 2020-04-14

Generated on: 2020-04-14T11:36:14

Key type: Jantar3ProKey

Key status: Archived

NOTE
Be extremely careful when transferring the file containing your 3PRO encryption key. The file contains highly sensitive security information and must, therefore, be protected against theft or destruction.

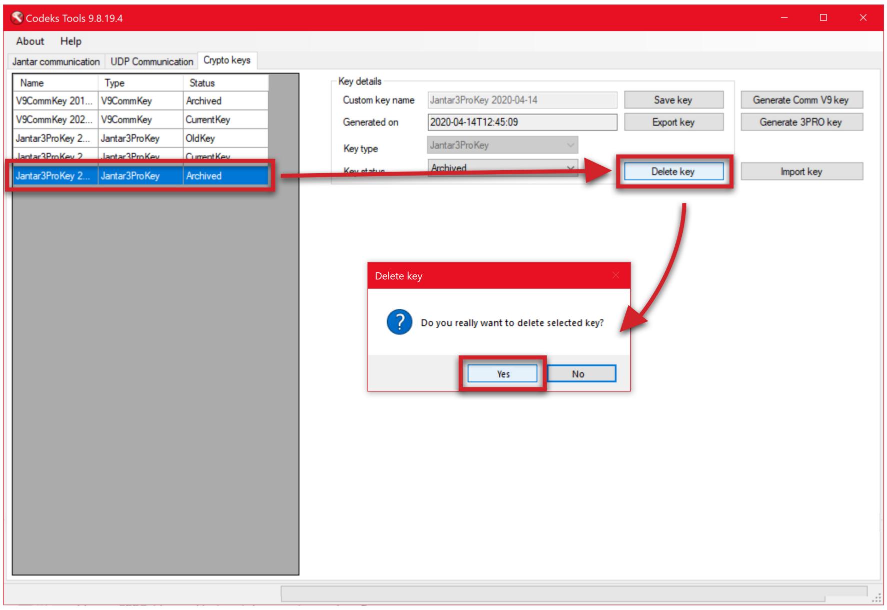
Deleting the 3PRO encryption key

NOTE
Before deleting a V9 encryption key, make sure that the key is no longer used to communicate with devices!
If a specific 3PRO encryption key is ever lost, it will be necessary to find the appropriate encryption key again to restore communication between the devices and user cards. or reset the device to factory default settings. In cases where this is not possible, the user cards can, unfortunately, no longer be used.

1. To delete a 3PRO encryption key, first mark the appropriate key on the list on the left.

2. Then click the ***Delete key*** button***.***

3. The system will request confirmation of the deletion. **Click *Yes* to permanently delete the key.**



Codeks Tools 9.8.19.4

Name	Type	Status
V9CommKey 201...	V9CommKey	Archived
V9CommKey 202...	V9CommKey	CurrentKey
Jantar3ProKey 2...	Jantar3ProKey	OldKey
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey
Jantar3ProKey 2...	Jantar3ProKey	Archived

Key details
Custom key name: Jantar3ProKey 2020-04-14
Generated on: 2020-04-14T12:45:09
Key type: Jantar3ProKey
Key status: Archived

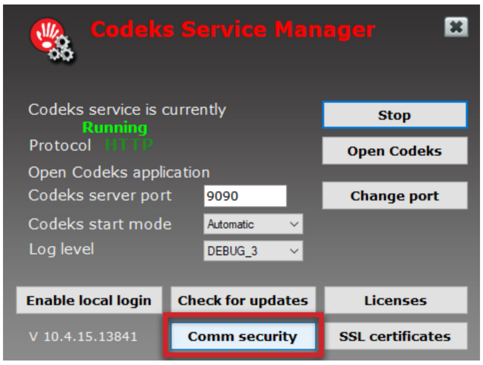
Delete key
Do you really want to delete selected key?

3.3.2.2. Importing the new custom 3PRO encryption key into the Codeks software

You can import the newly generated custom 3PRO encryption key into your *Codeks* system by using the ***Codeks Servis Manager*** program. To perform the process described in this chapter you will need access to the Codeks server.

1. First, launch the **Codeks Service Manager** program.

2. Then click the ***Comm security*** button.



Codeks Service Manager

Codeks service is currently Running

Protocol HTTP

Open Codeks application

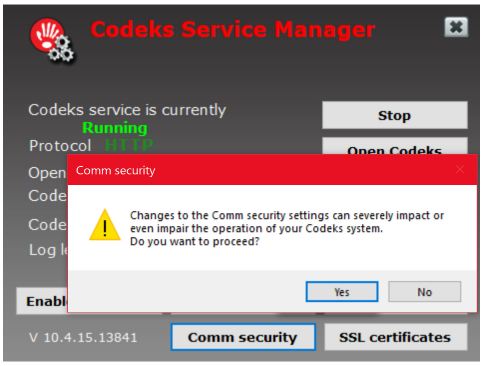
Codeks server port 9090

Codeks start mode Automatic

Log level DEBUG_3

V 10.4.15.13841

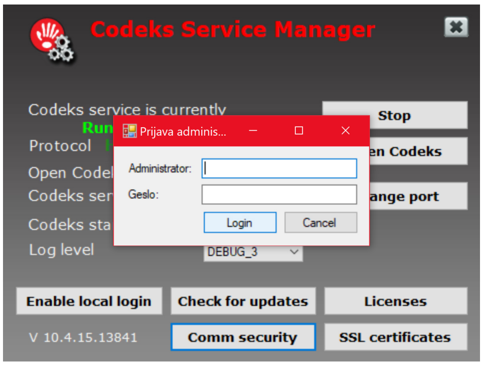
3. The system will then warn you that changes to *Comm security* can critically affect or even impair the functioning of your *Codeks* system. **Click *Yes*.**



Comm security

Changes to the Comm security settings can severely impact or even impair the operation of your Codeks system.
Do you want to proceed?

4. Next, the system will ask for **your super admin username and password.** Enter the relevant information and click ***Login.***



Prijava adminis...

Administrator:

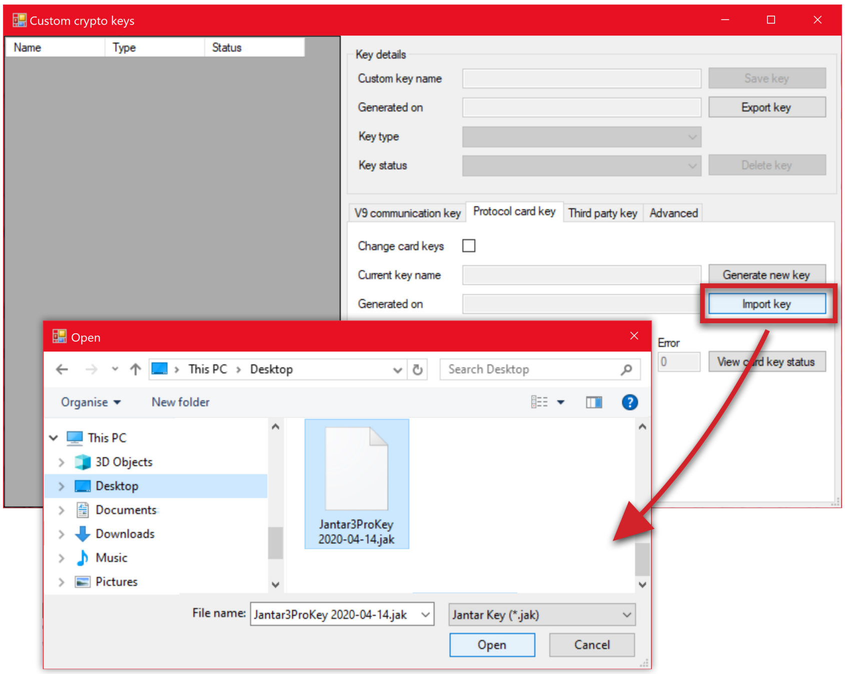
Geslo:

5. A new window will open.

In the ***3PRO communication key*** tab, click the ***Import key*** button.

In the new window, **locate the file with your 3PRO encryption key** that you exported from *Codeks Tools*.

Click ***Open***.



File name: Jantar3ProKey 2020-04-14.jak

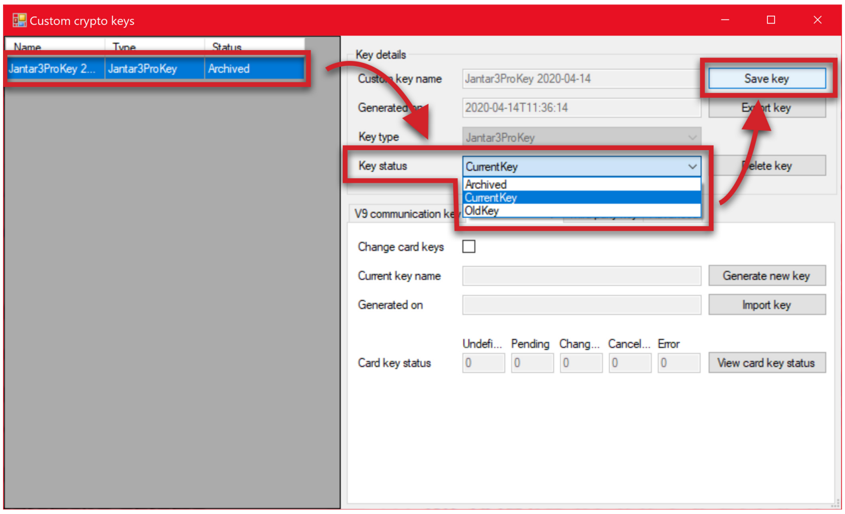
Jantar Key (*.jak)

6. The newly imported key will be displayed on the list on the left and its status set to ***Archived***.

The status of the key must be changed to ***Current key*** for further use.

Then click ***Save.***

(If you are already using a custom 3PRO encryption key, you MUST set the status of your previous 3PRO encryption key to *Old key.*)



Name	Type	Status
Jantar3ProKey 2...	Jantar3ProKey	Archived

Custom key name: Jantar3ProKey 2020-04-14

Generated on: 2020-04-14T11:36:14

Key type: Jantar3ProKey

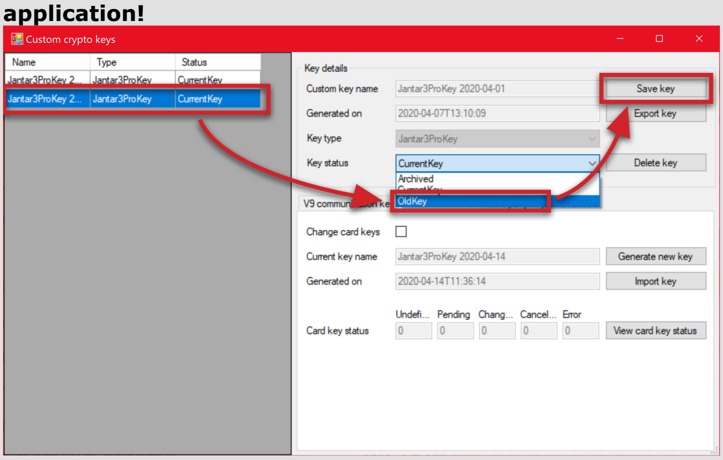
Key status: CurrentKey

Card key status: 0 0 0 0 0

Key status	
Archived	The 3PRO encryption key is archived, meaning it is only stored in the *Codeks* application. A key with an *Archived* status may have been used in the past or may have been left waiting to be used.
Current key	The encryption key is the currently selected (active) 3PRO encryption key that will be written onto the users' cards as the new 3PRO key in the process of changing the 3PRO encryption keys.

Old key	The encryption key is a direct predecessor to the currently selected (active) 3PRO encryption key. In the process of changing 3PRO encryption keys, this key will be replaced on the user cards with the new currently selected 3PRO key.

NOTE!
We recommend that you consistently mark old 3PRO keys, which are the direct predecessors of the current 3PRO key, with the *Old key* status, **because the correct marking of 3PRO key statuses is crucial in the Codeks application!**



Custom crypto keys

Name	Type	Status
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey

Key details

Custom key name: Jantar3ProKey 2020-04-01

Generated on: 2020-04-07T13:10:09

Key type: Jantar3ProKey

Key status: CurrentKey

Change card keys □

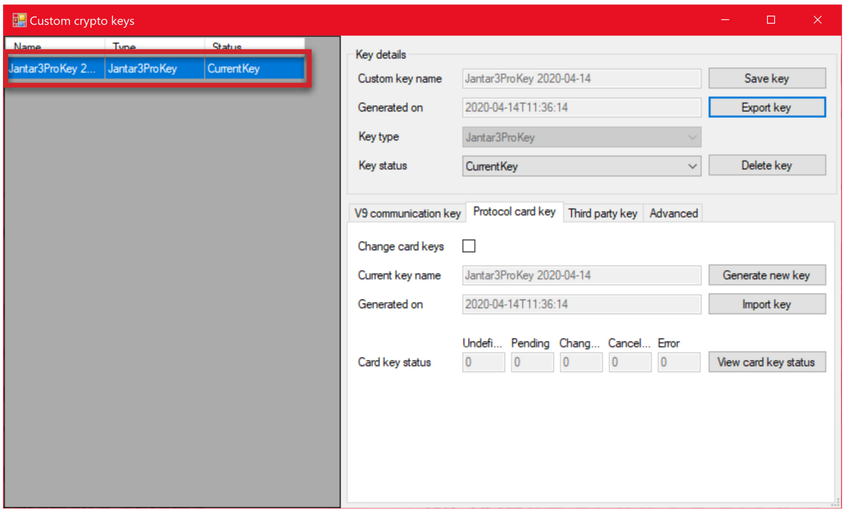
Current key name: Jantar3ProKey 2020-04-14

Generated on: 2020-04-14T11:36:14

	Undefi...	Pending	Chang...	Cancel...	Error
Card key status	0	0	0	0	0

This is because the Codeks software uses the *Old key* and *Current key* statuses in the process of changing the key on user cards, always changing only the 3PRO key labeled *Old key* with the 3PRO key labeled *Current key*.
You can read more about the import and 3PRO key statuses in chapter Changing the 3PRO encryption keys on user cards 57.

7. The key on the list on the left is now set to *Current key* and is now ready to use.



Custom crypto keys

Name	Type	Status
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey

Key details

Custom key name: Jantar3ProKey 2020-04-14

Generated on: 2020-04-14T11:36:14

Key type: Jantar3ProKey

Key status: CurrentKey

Change card keys □

Current key name: Jantar3ProKey 2020-04-14

Generated on: 2020-04-14T11:36:14

	Undefi...	Pending	Chang...	Cancel...	Error
Card key status	0	0	0	0	0

In order to finally enable communication between the *Codeks* software and the selected controllers, it is still necessary to properly set the controllers and reader in your Codeks system 55 and also start the 3PRO key change process 57.

3.3.2.3. Settings for using the 3PRO encryption key in the Codeks software

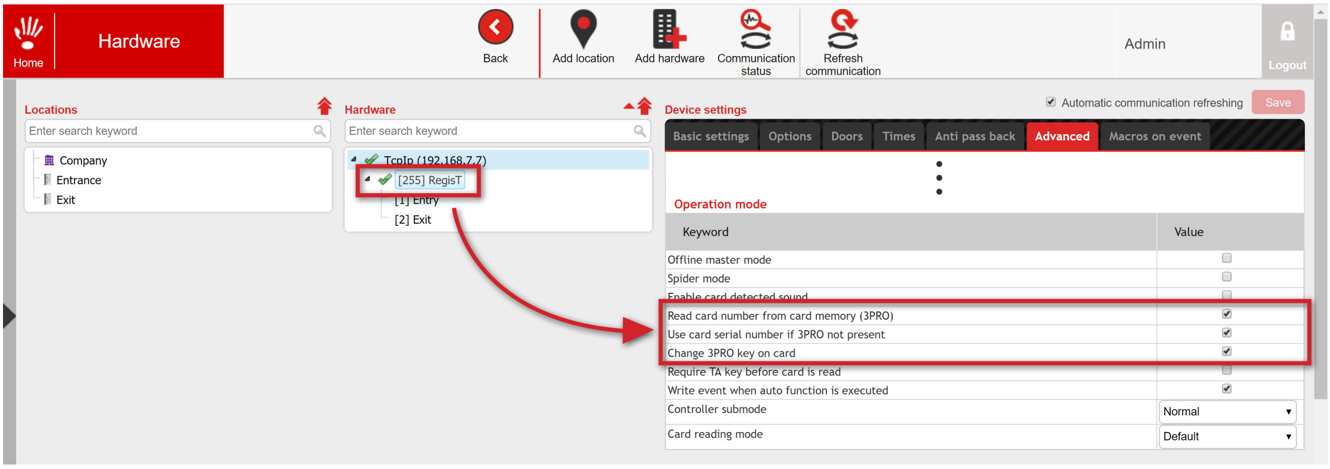
To use the new 3PRO encryption key, you have to set (or check) the controller and reader settings for reading user cards using the 3PRO encryption key in the Codeks application.

Controller settings

1. To edit the controller setting, first, **find and mark the appropriate controller on the *list of hardware*** in the *Hardware* editor.

2. Then, on the left side of the window, select the *Advanced* tab and find the *Operation mode* section.

3. To enable the reading of the card's 3PRO number, first, enable the *Read card number from card memory (3PRO)* setting.



Operation mode

Keyword	Value
Offline master mode	☐
Spider mode	☐
Enable card detected sound	☐
Read card number from card memory (3PRO)	☑
Use card serial number if 3PRO not present	☑
Change 3PRO key on card	☑
Require TA key before card is read	☐
Write event when auto function is executed	☑
Controller submode	Normal
Card reading mode	Default

3PRO settings	
Read card number from card memory (3PRO)	If this setting is enabled, the controller will not read the card's default serial number, but will instead search for an encrypted card number located within the card's internal memory. **If this 3PRO setting is enabled on a controller, you must also enable it on all the readers connected to this controller.**
Use card serial number if 3PRO not present	This setting can only be used if the previous setting ***Read card number from card memory (3PRO)*** is also enabled. If this setting is enabled, the controller will first attempt to read the encrypted 3PRO card number (which is stored in a specific location within the card's internal memory), and if this fails, it will use the default serial number of the card.
Change 3PRO key on card	If this setting is enabled, then users will be able to change the 3PRO encryption key on their cards by registering on this controller during the process of changing the 3PRO keys. You can read more about the process of changing the 3PRO encryption keys on user cards in chapter The process of changing the 3PRO encryption keys 61.

4.* If you wish, you can also enable the ***Use card serial number if 3PRO not present***. If you enable this setting, controllers will also be able to read the default serial number of the card when they cannot access the 3PRO number (e.g. because of an outdated 3PRO key on the card).

5.* In the process of changing 3PRO keys on users' cards 61, you must enable the *Change 3PRO key on card* setting on all controllers where users will be able to replace the 3PRO key on their cards.

NOTE!
Changing the 3PRO encryption key can only be performed on controllers with firmware version 9.8.1 or newer.

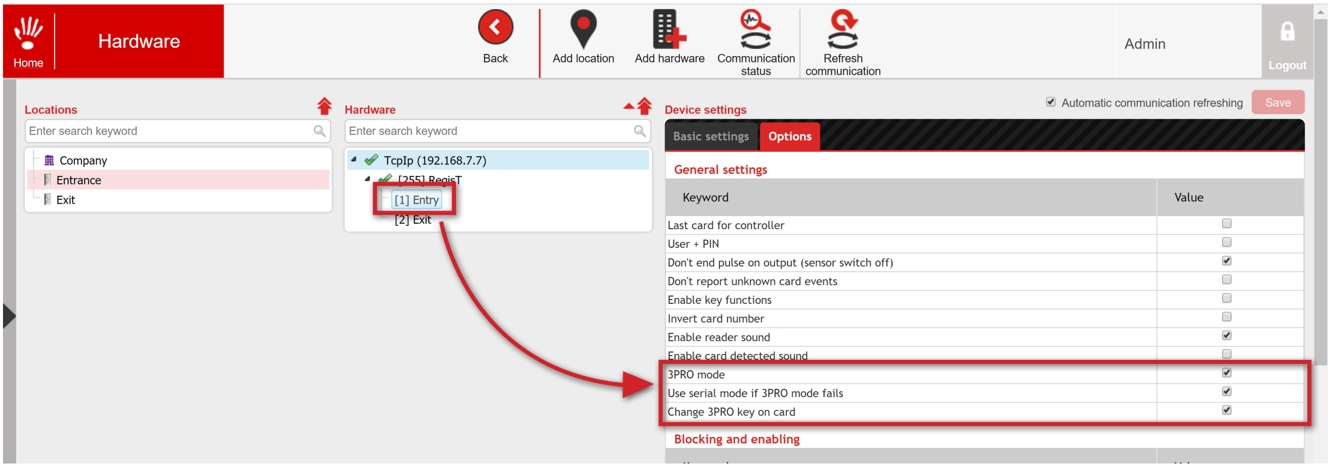
6. When you are finished do not forget to send tables to controllers.

Reader settings

1. To edit the reader setting, first, **find and mark the appropriate reader on the *list of hardware*** in the *Hardware* editor.

2. Then, on the left side of the window, select the *Options* tab and find the *General settings* section.

3. To enable the reading of the card's 3PRO number, first, enable the *3PRO mode* setting.



☑ Automatic communication refreshing

General settings

Keyword	Value
Last card for controller	□
User + PIN	□
Don't end pulse on output (sensor switch off)	☑
Don't report unknown card events	□
Enable key functions	□
Invert card number	□
Enable reader sound	☑
Enable card detected sound	□
3PRO mode	☑
Use serial mode if 3PRO mode fails	☑
Change 3PRO key on card	☑

Blocking and enabling

3PRO settings	
3PRO mode	If this setting is enabled, the reader will read the encrypted 3PRO card number located within the card's internal memory. **This setting must be enabled for all readers connected to a controller using the 3PRO functionality.**
Use serial mode if 3PRO mode fails	This setting can only be used if the previous setting ***3PRO mode*** is also enabled. If this setting is enabled, the reader will first attempt to read the encrypted 3PRO card number (which is stored in a specific location within the card's internal memory), and if this fails, it will use the default serial number of the card.
Change 3PRO key on card	If this setting is enabled, then users will be able to change the 3PRO encryption key on their cards by registering on this reader during the process of changing the 3PRO keys. You can read more about the process of changing the 3PRO encryption keys on user cards in chapter The process of changing the 3PRO encryption keys 61.

4.* If you wish, you can also enable the ***Use serial mode if 3PRO fails***. If you enable this setting, readers will also be able to read the default serial number of the card when they cannot access the 3PRO number (e. g. because of an outdated 3PRO key on the card).

5.* In the process of changing 3PRO keys on users' cards 61, you must enable the *Change 3PRO key on card* setting on all readers (of a controller set in the same way) where users will be able to replace the 3PRO key on their cards.

6. When you are finished do not forget to send tables to controllers.

3.3.2.4. Changing the 3PRO encryption keys on user cards

To successfully implement a new 3PRO encryption key, it must also be replaced on all cards used by the users in your system. Changing the 3PRO encryption key is performed on specific controllers and readers in the system. **After defining a new 3PRO encryption key in your Codeks system and initiating the key change process, it will take some time for all users to change the encryption keys on their cards. This means that all users must register at least once at least one of the controllers where the encryption key change is performed.**

From the moment you change the encryption key on the controllers (i.e. when you send tables to the controllers), users will no longer be able to move through your system with the old encryption key (they will be denied access), but will first need to register at a controller which enables them to replace the old 3PRO encryption key with the new one. The process of changing the encryption keys usually takes some time (in some cases maybe even days). Before you finish the process of changing the 3PRO encryption keys, we suggest that you check that the keys on the user cards have been replaced by all users (or at least most), or even check which users have not updated the encryption key. You can find the tools to track the number of encryption keys already replaced in the *Codeks Service Manager* program.

For user cards that did not update the encryption key during the process of changing the 3PRO key, the 3PRO encryption key can also be replaced at a later time using the tools in the main *Codeks* application. You can read more about this in the documentation of the main *Codeks* application.

3.3.2.4.1 Ways of carrying out the 3PRO key change process

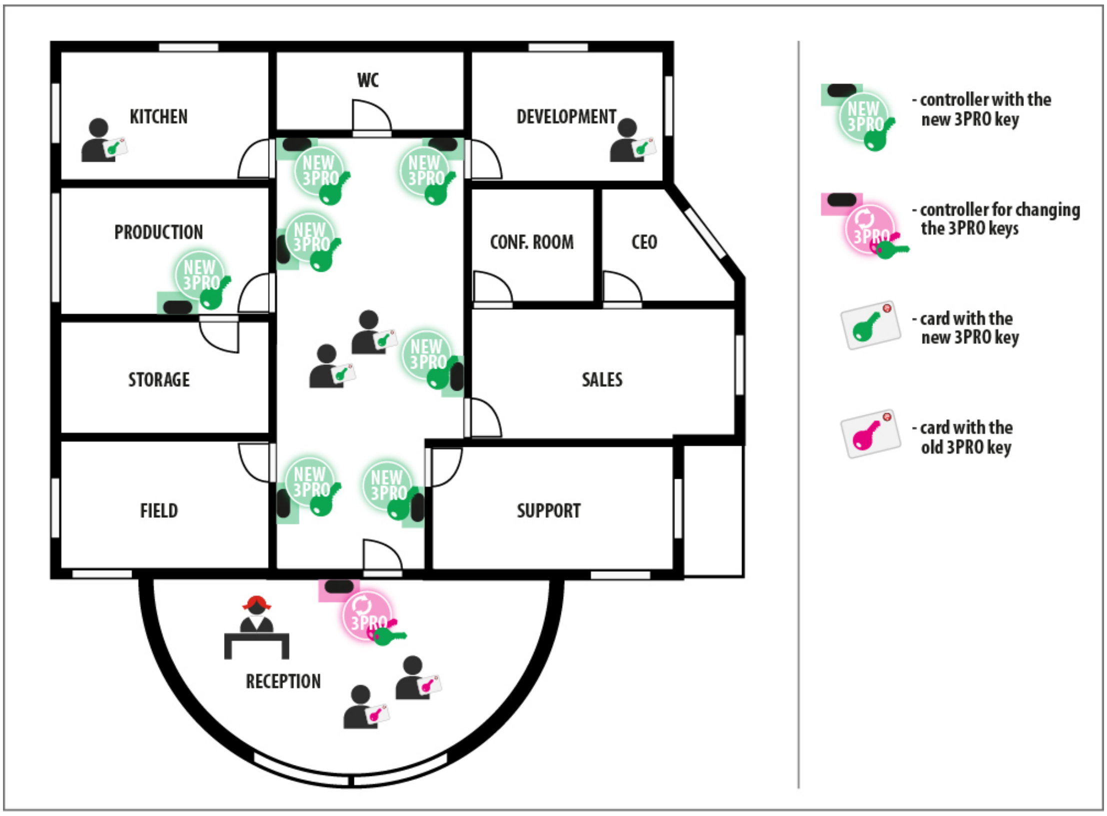
NOTE!
During the process of changing the 3PRO encryption keys, your Codeks system is more vulnerable.
Because controllers, where the 3PRO encryption keys change, is taking place can communicate with two 3PRO encryption keys (i.e., the *Old key* and the *Current key*), unauthorized entry of persons or attempts to steal the new encryption key can occur.
It is therefore advisable to use a limited number of controllers to change the 3PRO encryption keys or temporarily increase the security of the object when changing keys.

The process of changing 3PRO keys can be performed in many ways. The following chapters describe two different ways to perform the 3PRO key replacement process, as well as the advantages and disadvantages of each system.

Changing keys at only one specific location

Users can only change the key in one location (e.g., at the HR office or the corporate reception desk), and the process of changing the key is monitored and directed by trained personnel (e.g. the HR staff or the reception staff).

All controllers except the controller on which the keys are changed only communicate with the new 3PRO encryption key. The controller on which the key exchange takes place communicates with both the *Old key* and the *Current key*.

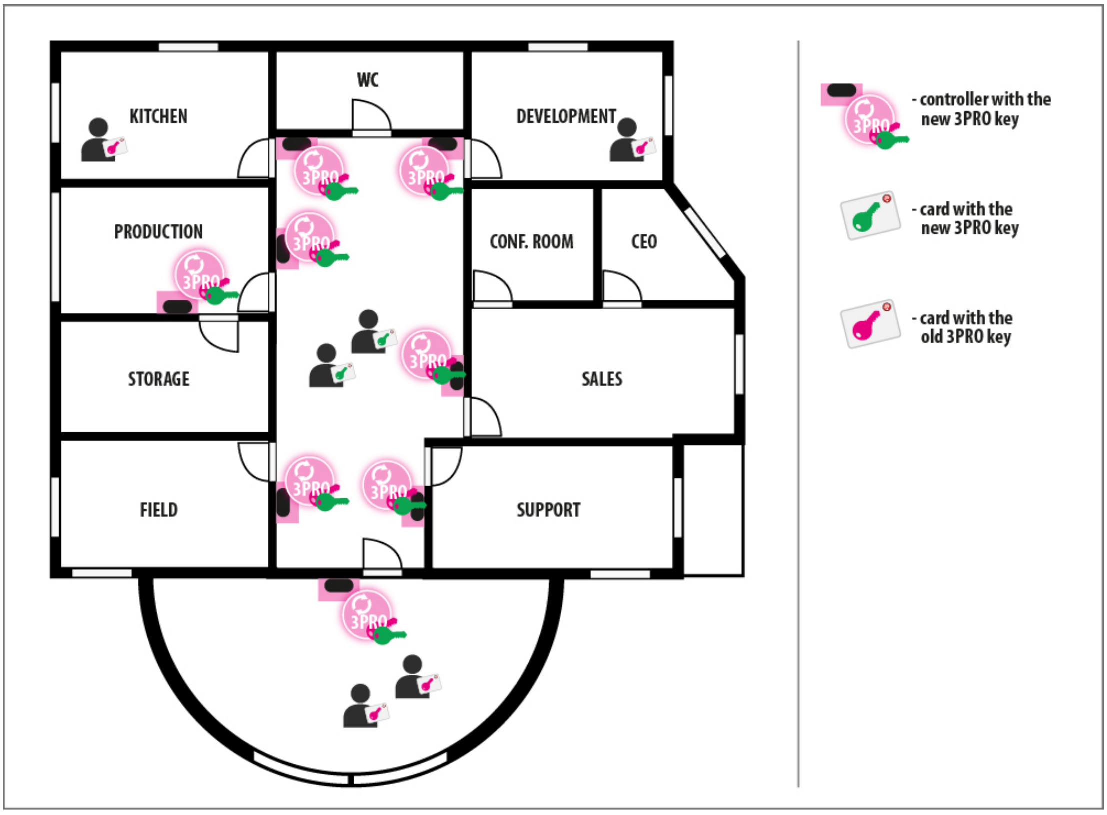


KITCHEN
WC
DEVELOPMENT
PRODUCTION
CONF. ROOM
CEO
STORAGE
SALES
FIELD
SUPPORT
RECEPTION
NEW 3PRO
3PRO
- controller with the new 3PRO key
- controller for changing the 3PRO keys
- card with the new 3PRO key
- card with the old 3PRO key

Advantages	Disadvantages
• a limited number of locations for key exchange, • less potential for abuse or unauthorized entry, • controlled key exchange (trained personnel).	• until they replace the old 3PRO key, users will not be able to navigate the system, • slow change of 3PRO keys, • the additional workload of the staff overseeing the key exchange.

Changing keys at any location

Users can change the key on their cards on any controller in the system. All controllers in the system communicate with both the *Old key* and the *Current key*.


KITCHEN
WC
DEVELOPMENT
PRODUCTION
CONF. ROOM
CEO
STORAGE
SALES
FIELD
SUPPORT
3PRO
- controller with the new 3PRO key
- card with the new 3PRO key
- card with the old 3PRO key

Advantages	Disadvantages
• quick change of 3PRO keys, • there is no need for additional work by the staff overseeing the key exchange, • user traffic between locations is not hindered.	• during the key change process, the system security is compromised because all controllers communicate with two keys, • possible need for additional (physical) security of company access points by security staff.

3.3.2.4.2 The process of changing the 3PRO encryption keys

PREPARATION

Before performing the process of changing the 3PRO encryption keys described below, make sure you have the following settings already in place:

- **imported 3PRO keys and properly set 3PRO key statuses**

  Import the new 3PRO encryption key into your Codeks system using the *Codeks Service Manager* program. The process of importing a 3PRO key is described in chapter Importing the new custom 3PRO encryption key into the Codeks software 52.

  Also, make sure you have the 3PRO key statuses set up correctly 53. The status of the new key must be set to *Current key*, and if you are already using your own custom 3PRO encryption key, be sure to change the status of the old 3PRO key to *Old key*.

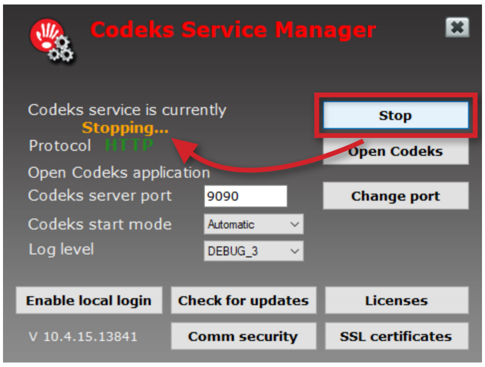
- **enabled settings for changing the 3PRO keys on specific controllers**

  You must enable the ***Change 3PRO key on card*** 55 setting on all controllers and readers where users will be able to replace the 3PRO key on their cards.

A. Starting the process of changing keys in the *Codeks Service Manager* program

1. To start the process of changing the 3PRO keys, first, open the **Codeks Service Manager** program.

2. Next, stop the Codeks service by clicking the ***Stop*** button.



Codeks Service Manager

Codeks service is currently Stopping...

Protocol HTTP

Open Codeks application

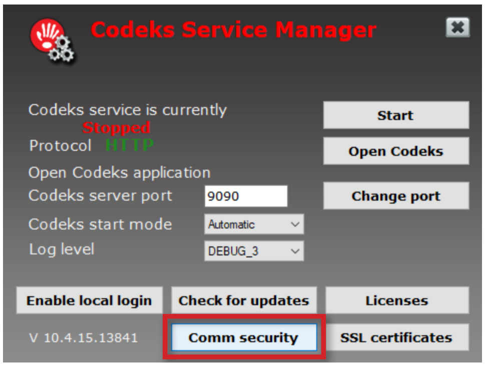
Codeks server port 9090

Codeks start mode Automatic

Log level DEBUG_3

V 10.4.15.13841

3. Then click the ***Comm security*** button.



Codeks Service Manager

Codeks service is currently Stopped

Protocol HTTP

Open Codeks application

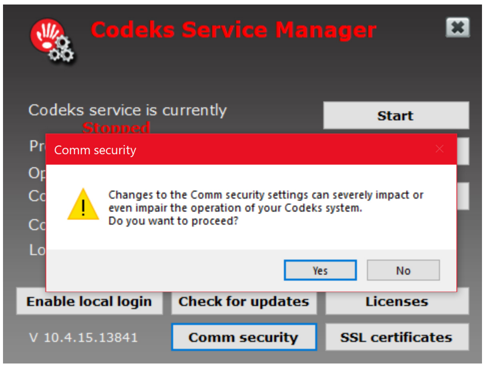
Codeks server port 9090

Codeks start mode Automatic

Log level DEBUG_3

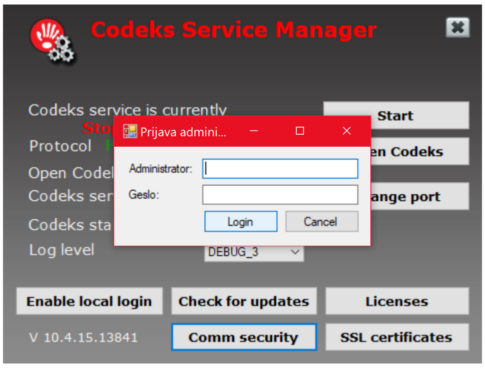
V 10.4.15.13841

4. The system will first warn you that changes to *Comm security* can critically affect or even impair the functioning of your Codeks system. **Click *Yes***.



Changes to the Comm security settings can severely impact or even impair the operation of your Codeks system.
Do you want to proceed?

5. Then the system will ask for **the username and password of a super admin of your system**. Enter the relevant information and click ***Sign in***.

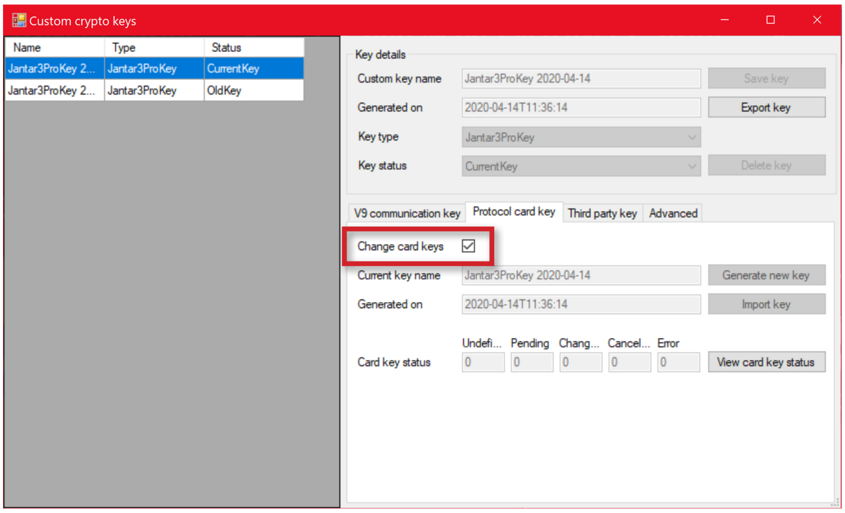


Administrator:
Geslo:
Log level: DEBUG_3

6. A new window will open.

In the ***Protocol card key*** tab, enable the ***Change card keys*** function.

With this, you will allow 3PRO keys to be changed on all selected controllers.



Name	Type	Status
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey
Jantar3ProKey 2...	Jantar3ProKey	OldKey

Key details

Custom key name: Jantar3ProKey 2020-04-14

Generated on: 2020-04-14T11:36:14

Key type: Jantar3ProKey

Key status: CurrentKey

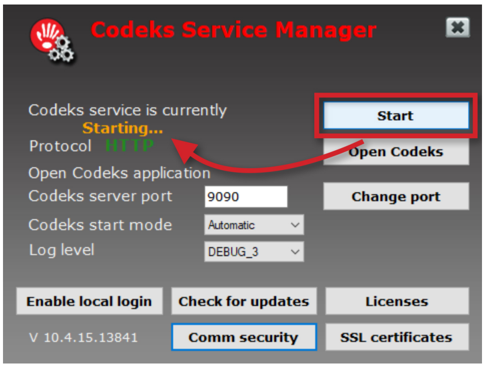
Change card keys ☑

Current key name: Jantar3ProKey 2020-04-14

Generated on: 2020-04-14T11:36:14

	Undefi...	Pending	Chang...	Cancel...	Error
Card key status	0	0	0	0	0

7. Finally, restart the Codeks service by clicking the ***Start*** button in the *Codeks Service Manager* program.

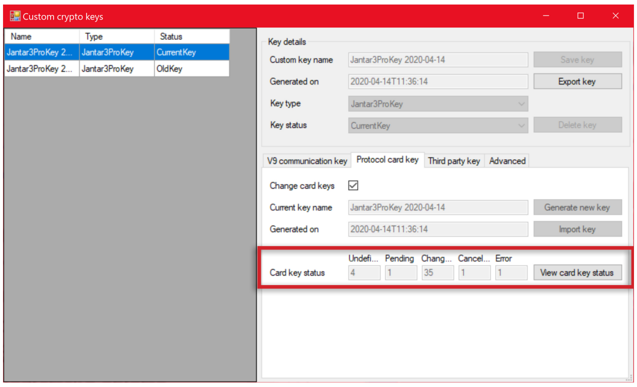


Codeks service is currently Starting...
Protocol HTTP
Open Codeks application
Codeks server port 9090
Codeks start mode Automatic
Log level DEBUG_3
V 10.4.15.13841

B. Waiting - monitoring the key change process in the *Codeks Service Manager* program

The process of changing the encryption keys usually takes some time (sometimes days).

The current number of keys replaced on user cards can be tracked at the bottom of the *Protocol card key* tab.



Custom crypto keys

Name	Type	Status
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey
Jantar3ProKey 2...	Jantar3ProKey	OldKey

Key details

Custom key name: Jantar3ProKey 2020-04-14

Generated on: 2020-04-14T11:36:14

Key type: Jantar3ProKey

Key status: CurrentKey

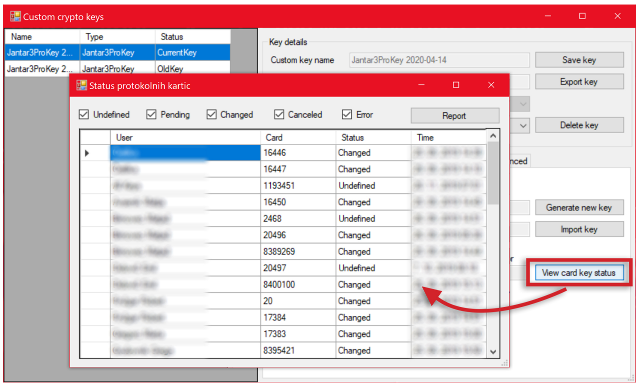
Change card keys ☑

Current key name: Jantar3ProKey 2020-04-14

Generated on: 2020-04-14T11:36:14

	Undefi...	Pending	Chang...	Cancel...	Error
Card key status	4	1	35	1	1

By clicking the ***View card key status*** button, you can open a window with more detailed information.



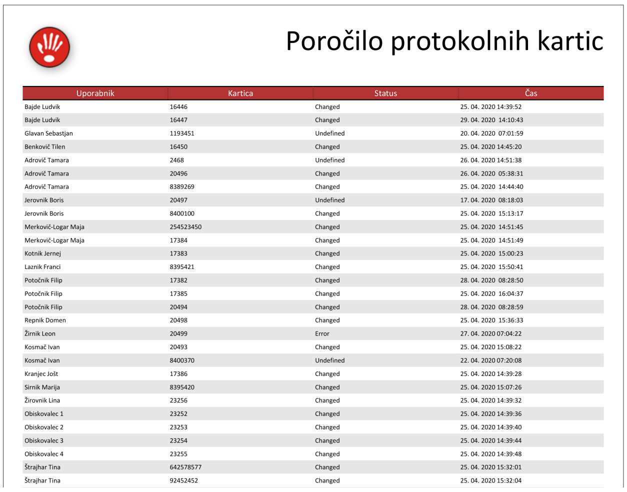
Custom crypto keys

Status protokolnih kartic

☑ Undefined ☑ Pending ☑ Changed ☑ Canceled ☑ Error

User	Card	Status	Time
[redacted]	16446	Changed	[redacted]
[redacted]	16447	Changed	[redacted]
[redacted]	1193451	Undefined	[redacted]
[redacted]	16450	Changed	[redacted]
[redacted]	2468	Undefined	[redacted]
[redacted]	20496	Changed	[redacted]
[redacted]	8389269	Changed	[redacted]
[redacted]	20497	Undefined	[redacted]
[redacted]	8400100	Changed	[redacted]
[redacted]	20	Changed	[redacted]
[redacted]	17384	Changed	[redacted]
[redacted]	17383	Changed	[redacted]
[redacted]	8395421	Changed	[redacted]

You can also export the displayed information in the form of a report by clicking the ***Report*** button.



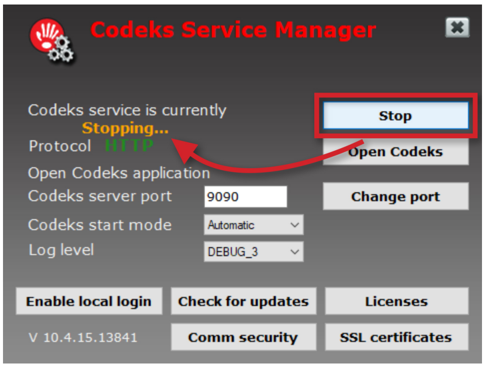
Poročilo protokolnih kartic

Uporabnik	Kartica	Status	Čas
Bajde Ludvik	16446	Changed	25. 04. 2020 14:39:52
Bajde Ludvik	16447	Changed	29. 04. 2020 14:10:43
Glavan Sebastjan	1193451	Undefined	20. 04. 2020 07:01:59
Benkovič Tilen	16450	Changed	25. 04. 2020 14:45:20
Adrovič Tamara	2468	Undefined	26. 04. 2020 14:51:38
Adrovič Tamara	20496	Changed	26. 04. 2020 05:38:31
Adrovič Tamara	8389269	Changed	25. 04. 2020 14:44:40
Jerovnik Boris	20497	Undefined	17. 04. 2020 08:18:03
Jerovnik Boris	8400100	Changed	25. 04. 2020 15:13:17
Merkovič-Logar Maja	254523450	Changed	25. 04. 2020 14:51:45
Merkovič-Logar Maja	17384	Changed	25. 04. 2020 14:51:49
Kotnik Jernej	17383	Changed	25. 04. 2020 15:00:23
Laznik Franci	8395421	Changed	25. 04. 2020 15:50:41
Potočnik Filip	17382	Changed	28. 04. 2020 08:28:50
Potočnik Filip	17385	Changed	25. 04. 2020 16:04:37
Potočnik Filip	20494	Changed	28. 04. 2020 08:28:59
Repnik Domen	20498	Changed	25. 04. 2020 15:36:33
Žirnik Leon	20499	Error	27. 04. 2020 07:04:22
Kosmač Ivan	20493	Changed	25. 04. 2020 15:08:22
Kosmač Ivan	8400370	Undefined	22. 04. 2020 07:20:08
Kranjec Jošt	17386	Changed	25. 04. 2020 14:39:28
Sirnik Marija	8395420	Changed	25. 04. 2020 15:07:26
Žirovnik Lina	23256	Changed	25. 04. 2020 14:39:32
Obiskovalec 1	23252	Changed	25. 04. 2020 14:39:36
Obiskovalec 2	23253	Changed	25. 04. 2020 14:39:40
Obiskovalec 3	23254	Changed	25. 04. 2020 14:39:44
Obiskovalec 4	23255	Changed	25. 04. 2020 14:39:48
Štrajhar Tina	642578577	Changed	25. 04. 2020 15:32:01
Štrajhar Tina	92452452	Changed	25. 04. 2020 15:32:04

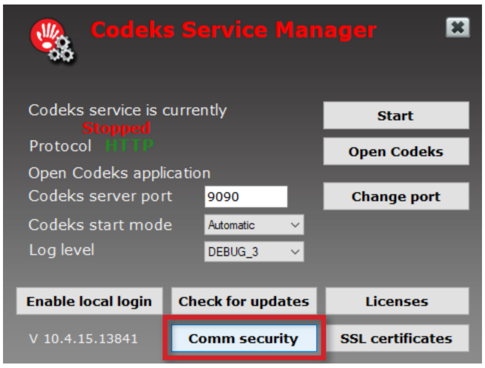
C. Stop the process of changing keys in the *Codeks Service Manager* program

1. To stop (switch off) the process of changing the 3PRO keys, again open the **Codeks Service Manager** program.

2. Next, stop the Codeks service by clicking the ***Stop*** button, and then, click ***Comm security***.

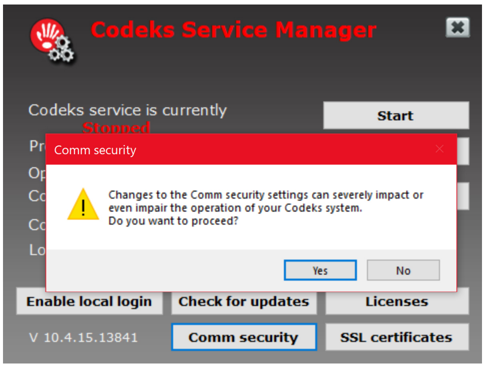


Codeks service is currently Stopping...
Protocol HTTP
Open Codeks application
Codeks server port 9090
Codeks start mode Automatic
Log level DEBUG_3
V 10.4.15.13841



Codeks service is currently Stopped
Protocol HTTP
Open Codeks application
Codeks server port 9090
Codeks start mode Automatic
Log level DEBUG_3
V 10.4.15.13841

3. Log in to the system.

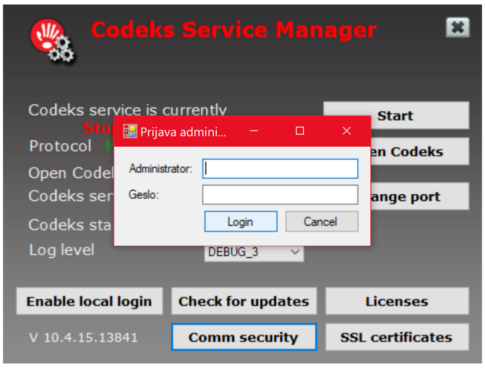


Codeks service is currently Stopped

Comm security

Changes to the Comm security settings can severely impact or even impair the operation of your Codeks system.
Do you want to proceed?

V 10.4.15.13841



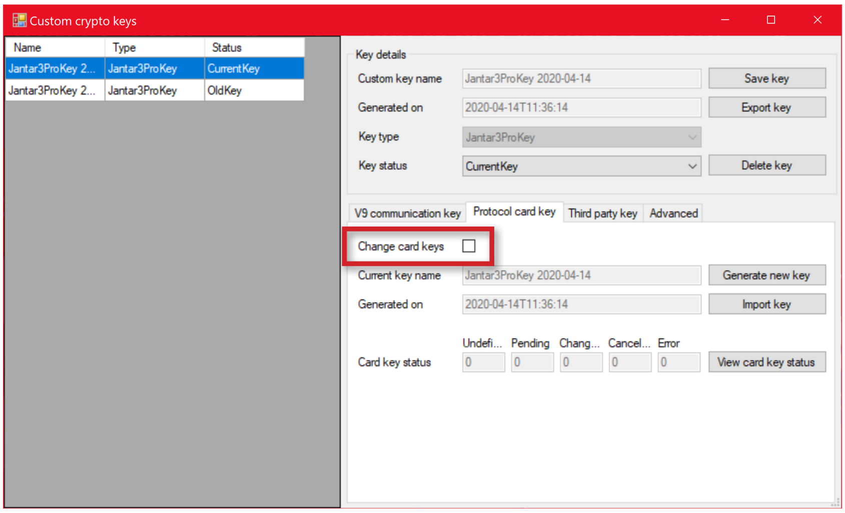
Prijava admini...

Administrator:

Geslo:

V 10.4.15.13841

4. In the new window, in the ***Protocol card key*** tab, disable the ***Change card keys*** function. This will switch off the process of changing the 3PRO keys.



Name	Type	Status
Jantar3ProKey 2...	Jantar3ProKey	CurrentKey
Jantar3ProKey 2...	Jantar3ProKey	OldKey

Key details

Custom key name Jantar3ProKey 2020-04-14

Generated on 2020-04-14T11:36:14

Key type Jantar3ProKey

Key status CurrentKey

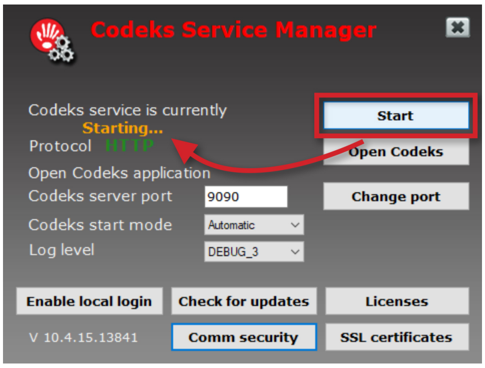
Change card keys □

Current key name Jantar3ProKey 2020-04-14

Generated on 2020-04-14T11:36:14

	Undefi...	Pending	Chang...	Cancel...	Error
Card key status	0	0	0	0	0

5. Finally, restart the Codeks service by clicking the ***Start*** button in the *Codeks Service Manager* program***.***



Codeks Service Manager

Codeks service is currently Starting...

Protocol HTTP

Open Codeks application

Codeks server port 9090

Codeks start mode Automatic

Log level DEBUG_3

V 10.4.15.13841

NOTE!
For user cards that did not update the encryption key during the process of changing the 3PRO key, the 3PRO encryption key can also be replaced at a later time using the tools in the main *Codeks* application. You can read more about this in the documentation of the main *Codeks* application.