iProtect - Release notes 10.3

Release notes | 10.3 **iProtect**	

Table of contents

1. Introduction

These release notes provide information about the latest features of iProtect, including required software versions and hardware installation and operating manuals.

2. System requirements

This chapter lists the required hardware and software for iProtect, including the licensing scheme of iProtect upgrades and other important information.

2.1 Supported servers

Below is a list of existing servers that can be updated to Ubuntu 20.04:

- TKH KP10
- DELL KP13
- DELL KP23
- DELL KP24
- DELL KP43
- DELL KP44
- IPT-S24
- IPH-S24
- IPH-S44
- IPH-S10

2.2 Hardware specification

The hardware specification depends on many variables, so the required specification is customer specific.

Guide lines for 2500 card users and 250 readers and 5 concurrent users*.

Version	CPU	Ram	Disk
10.3	>= 2.0 Ghz dual core	16 GB	>= 500GB
Test system (small)	1.6 Ghz dual core	4 GB	100GB

For large systems (>1000 readers, >20 concurrent users), a minimum of 32GB internal memory and 8 cores is recommended. *

Depending of the use of images (keymaps, photo's), the diskspace should be checked.

Deploying iProtect on a virtual environment, the performance of the disk read/write can be depended to the other virtual machine deployed on the same hypervisor.

2.3 Software

The minimum required operating system version for iProtect:

Version	O.S./ Firmware	Maintenance / serverbox	Internet connection required
iProtect 10.3	Ubuntu 20.04 LTS	>= 10.02.18	Yes, for installation and updates

For iProtect 10.03 and Ubuntu 20.04, there is a TKH repository with all needed files for installing and maintaining the setup files.

The operating system can be downloaded from Ubuntu's default repository.

It is highly recommended to ensure that iProtect is connected to the internet during installation. Permanent access to the internet is of course possible, but temporary internet access for updating the security packages is also possible.

On request there is an option to install iProtect without an internet connection but is not recommended.

2.4 Update policy

TKH security works non-stop to improve its products and their safety.
From iProtect version 10.4, the software version from which you update and the software version to which you update must be taken into account.

Why is this change? The security policy prevents newly installed software from working or communicating with software that does not meet these security requirements, so that a roll-back will no longer work.

2.4.1 Which iProtect version supports which Pluto rootFS

iProtect version	Pluto rootFS version	Comment
10.1	<= 5.68a	

10.2	<= 5.68a & 6.x	
10.3	<= 5.68a & 6.x	5.68 is supported but version 6 is automatically downloaded and after reboot version 6 becomes active
10.4	= > 6.x	5.68 is not supported. Controllers needs to be update to version = > 6 before starting the update procedure.

2.5 Software and firmware

Software versions of the connected hardware are managed from iProtect by default.
Below you will find an overview of the most used hardware and the **minimum** version that are installed (provisioned) when updating iProtect.

Hardware / Device	Software / Firmware	Note
Pluto (rootFS)	6.11.14	
Reader manager	5.03.57	
Orion	1.5.22	Keep using firmware **1.5.18** when a Sallis node is connected to the Orion!
iX-serie Reader firmware	2.8.2	
RIO firmware	1.2.25 / 2.4.2	

Release notes of the software/firmware are available on request.

If software/firmware versions have a lower number than shown in the table above, it will be automatically updated. Although this time is kept as short as possible, the customer may be inconvenienced for a short time.

When updating iProtect, all network controllers will be updated automatically to a new rootFS version. This update will be processed in the background and will take aprox 20 - minutes (depending on network speed).

During the preparation of the update, the customer will not experience any inconvenience.

When the update is complete, the system administrator must reboot the controller. Booting up the controller will take approximately 2 minutes (depending on network speed). During this time, the customer may experience problems opening the door.

2.6 Encrypted JDBC connection

From iProtect 10.3 an encrypted (sslmode) jdbc connection is required.

Required .Jar files for iProtect v10.03.xx and higher:

- java-library-xx.x.x.jar
- keyprocessor-jdbc-xx.x.x.jar
- log4j-api-x.x.xx.jar
- log4j-core-x.x.xx.jar
- icu4j-73.1.jar
  - to ensure correct sort order for non ASCii characters (10.3.15+, 10.4+)
- tyrus-standalone-client-x.xx.jar

2.6.1 API documentation available (on request)

If desired, new API documentation is available:

- JDBC over SSL
- iProtect XML API v2.14

> Please contact TKH-Security for these API documents.

> TKH security tries to keep the links working at all times, but cannot guarantee this in case of an upgrade. When connecting third-party systems to Protect, it is strongly recommended to test for proper operation with a preset test system before upgrading.

2.6 License

When a major version number changes, it should be taken into account in advance that a new license is necessary. Please contact TKH Security service department or your account manager for this.

From version	To version	New license needed
10.01.x	10.3.x	Yes
10.02.x	10.3.x	Yes
10.3.x	10.3.x	No

2.7 Browser support

All tests are done with default browser settings, if some functionalities require changes to the settings, this will be mentioned in the specific manual. The following browsers are supported in iProtect:

Browser	Version
Google Chrome	>= 112
Mozilla Firefox	>= 102.9 ESR release
Mozilla Firefox	>=111
Microsoft Edge	>=111

> Microsoft internet explorer (IE) is not supported anymore.

3. End of support

- IBC-128 intrusion panel

3.1 Advance notice

- End of support HTA functionality. HTA is nowadays seen as a security risk, this function will be removed in iProtect 10.4.

4. iProtect server and application

This chapter describes the additions and/or changes of the application.

General improvements are:

- 64bit database.
- Log functionality by all services (for analyzing purposes).
- Sense maintenance: Reduce the amount of getdivalist calls.
- New date time format support carddata interpretation (DDxMMxYYYY where x could be any seperator).
- Output table increased form 8192 to 12280.

4.1 Highlights

4.1.1 iProtect Trails

> To enable this feauture, **iProtect Trails** license is needed

4.1.1.1 Walk route

Walking route allows a person to walk from A to B while the system checks whether they follow the specified walking route within a certain time. The system gives an alarm if there are deviations.

- Define a route for visitors/employees.
- Define a schedule for visitors/employees.
- Strict control over access areas.
- Define how to revoke the walk route (Time based or Error based)
- With one button, you can pause all walking routes, simplifying operational management.

4.1.1.1.1 Menu or items within the dialog have been added in

- General | Person (treeview)
  - Signed up activity list
  - Walk route list
- Access | Walk route schedule
  - Walk route schedule
  - Walk route schedule activity
- Access | Settings | Walk route
- Access | Settings | Walk route schedule
  - Walk route schedule

    - Walk route schedule activity
- Access | Overviews | Status | Active walk route
- Installation | Settings | System parameters | Hardware

4.1.1.2 Authorization user group and Workstation

In some situations, you want certain workstations to have limited rights from a security point of view. But you can also have an employee who works for department/location A today and for department/location B tomorrow. In this case, you want permissions to be determined by the login location.

- Restricted menu rights available, determined by location.
- Define the user group rights.
- You can define a type and location of the workstation.
- Login restriction (option). A person should be present in an area to login.

4.1.1.2.1 Menu or items within the dialog have been added in

Installation | Settings | Workstation | Workstation type

Installation | Authorization | Authorization user group

4.1.1.4 Free category type

In some cases it is important to indicate, for example, character traits or responsibilities of a person. For example, consider a manager who is responsible for several departments.
For example: John is Operations manager. Which departments are under his responsibilities:

- Service and support
- Projects
- Assembly
- .

4.1.1.4.1 Menu or items within the dialog have been added in

- General | Person (treeview)
    - Free category
- Installation | Settings | Free category type

4.1.2 Cosmos access, No Access token

For the doors you have access to, you will receive a token on your mobile device, and you can indicate the use of the mobile device per door.

- Per system, a mobile device receives a No access token. This is necessary to give the user feedback when presenting the mobile device at the door where access cannot be granted (not allowed).
- Per reader it is possible to set how the Mobile device should be used. For example, does the phone have to be unlocked first, can you open doors within a certain distance by selecting the reader manually, or can you present your phone directly?
- Improvement user experience due faster response.
- To further improve user experiences. It is no longer necessary to unlock the mobile device in all cases before use.
- Improved no access feedback.

- An overview of tokens (by card and reader) are added for the root- and installer user.

4.1.2.1 Menu or items within the dialog have been added in

- Access | Card
- Installation | Hardware | Reader

4.1.3 Push transaction expanded

With the “JSON push transaction webservice” it is possible to send iProtect transactions in JSON format to an external system like a “Elastic Stack”. It is possible to specify precisely which transactions are send and what data is added.

- Defining which event type(s) needs be by send, only relevant data is stored.
- Defining which data of the events type(s) needs be by send, only relevant data is stored.
- End user is independent in choosing database type for storage events.
- End user is independent when making a choice of type of tooling for making overviews/reports.

4.1.3.1 Menu or items within the dialog have been added in

A profile can be created where a selection can be made on Event type(s) and/or on table(s).

- Installation | Settings | Services | Export profile

A link with an external database and a defined export profile can be created under:

- Installation | Settings | Services | Database link

4.1.4 Integration Ooperon pager management system

Effectiveness is important to prevent many 'expensive' pagers from remaining unused in the charging station.

When presenting a valid access card to a specific card reader, an event is sent automatically to the CM4 server containing the personal pager number, location and profile number (which are managed in iProtect). This immediately loads the profile of the employee into a charged available pager.

- The number of pagers in use is optimized as much as possible.
- Pager number and profile managed by iProtect.
- Pager requests logged in iProtect.

4.1.4.1 General information

- Supported pagers: Bodyguard 4g pagers
- Connection: RS232,
- Protocol: ESPA

4.1.4.2 Hardware setup

- Pluto
- Stacked Orion (USB connected)
- RS485 <=> RS232 converter

4.1.5 Intergration Deister Key management

Effective key management is crucial to prevent the consequences of misplaced, lost, or stolen mechanical keys

iProtect reads-in all linked Deister key management cabinets, including panels and key positions. It is therefore important that the key cabinet(s) are correctly created and configured within the Deister software.

By presenting an access card to the reader that is connected to the key cabinet, the cabinet is unlocked. In iProtect you can define which person can take out one or more KeyTags. Every handling will processed and registered in iProtect.

By leveraging Deister key cabinet, you can:

- Full control of user data and access rights
- Full traceability of the use of the Deister Key cabinets and KeyTags
- Add efficiency and time saving to your facility operations.
- Deny person(s) from exiting a building if in possession of a mechanical key.

4.1.5.1 Menu or items within the dialog have been added in

- Installation | Hardware | Key cabinet
- Installation | Overviews | Status | Key cabinet item status
- Installation | Settings | Services | Database link
- General | Person
- General | Person (treeview)
  - Key cabinet item access list
  - Key cabinet item group access list
- Access | Settings | Key cabinet item group

4.1.6 OSDP v2.2

Open Supervised Device Protocol (OSDP) is an access control communications standard developed by the Security Industry Association (SIA) to improve interoperability among access control and security products.
OSDP was approved as an international standard by the International Electrotechnical Commission in May 2020 and has been published as IEC 60839-11-5.

OSDP v2.2 with Secure Channel has an AES-128 encryption and authentication scheme with initialization messages and keys, to ensure communication takes place strictly between intended parties and to hide the data exchanged between the reader and the controller.

> When using the OSDP protocol, the keys to read the card are in the card reader itself. Using the TKH protocol the keys are stored in the controller itself and not in the card reader.

> Because the readers must be configured, TKH-Security has prepared a number of readers to communicate with iProtect. If there is any uncertainty as to whether a configuration exists for the card reader, please contact your account manager.

Supported readers with TKH-Security configurations:

- Tagmaster
- Nedap
- TM
- PHG
- IDESCO

- IE / GEO

4.1.6.1 Menu or items within the dialog have been added in

- Installation | Hardware | Node

4.1.7 Threat management (access levels)

Situations change daily and the threat management level of your facility needs to be appropriately set for different times. With Threat Management Level, functionalities can be adjusted when the situation is appropriate.

A person can only access an access area if his personal access level is equal(=) to or higher (>) than the access level set for the area. Examples of environments and applications are:

1. Company emergency services, if an incident happens, all EROs can have instant access to certain areas.
2. International Ship & Port Facility Security (ISPS).
3. Access to areas restrictions based on conditions other than default rights on the card.
4. Governmental buildings.

With Access levels Level, functionalities can be adjusted when the situation is appropriate.

For example:

- Whether or not to use a pin code.
- Changing normal access to remote access through the intervention of a control room (video verification).
- Being able to block certain groups of people, for example, visitors or even employees.

4.1.7.1 Menu or items within the dialog have been added in

- General | Person
- Access | Settings | Area
- Access | Settings | Access level

4.1.8 Dutch Government Service Card: Framework of standards version 8 add-on

The following functionalities and improvements have been implemented:

- Function: Update compartment status (Access levels)
- Function: pass movement notification
- Option: Strict card group policy (for new rijkspas profiles)
- Fix: default card group should not be added by a “status update”
- Fix: when a Rijkspas user changes to another CMSID, is now supported
- Rijkspas support without endpoint support (only if the Rijkspas hub is used)
- Rijkspas WSDL support V4.9

4.1.8.1 Menu or items within the dialog have been added in

- Installation | Hardware | Reader
- Installation | Hardware | Area
- General | Person
- Access | Settings | Area
- Access | Settings | Access level

- Installation | Settings | Services | Database link

4.1.9 OSS major release change

The supported OSS version is changed from version A1 to B1. By updating the OSS version, add signature option is added.

The system that creates an XML file must sign this file and the system that imports the XML file
must verify the signature before further processing. To support this feature, OSS version B1 is implemented.

How does it work?

If the Host System creates a new Configuration.xml file, the host System must digitally sign the file. The Configuration Tool that processes the resulting file must check the digital signature. If the signature verification pro-cess fails, the input XML file should be rejected.

Similarly, in the case where the Configuration Tool creates a ConfigurationResult.xml file, the Configuration Tool must sign the file and the Host System must verify the signature.

> Use of a signature option is a setting on/off. Import without signature results in a popup message to proceed anyway without signature yes/no. Importing with a wrong signature will popup a message with the question, proceed anyway without wrong signature yes/no.

4.2 Other improvements / changes

4.2.1 WebSocket TLS/SSL

In addition to the existing communication protocol, WebSocket communication has been added.

WebSocket is a computer communications protocol, providing full-duplex communication channels over a single TCP connection:

- Default port: 20200
- Optional port: 443

4.2.1.1 Menu or items within the dialog have been added in

- Installation | Settings | System parameters | Communication

4.1.2 Provisioner improvements

A number of things have been adjusted. This can be security related or an improvement of the product.

- Speed-up provisioner.
- Show/hide provisioner group

4.1.3 Update of Pluto rootFS by provisioner

The Pluto root file system (named **rootfs** in our sample error message) is the most basic component of Linux. A root file system contains everything needed to support a full Linux system. It contains all the applications, configurations, devices, data, and more. Without the root file system, your Linux system cannot run.

iProtect **10.3** will be the last version of iProtect which supports rootfs versions < 6.xx.xx.

In iProtect a default provisioner element is added with the latest version of rootfs. This element is added to the default provisioner group. After updating the iProtect system to version 10.3 and activating the line, after installing all needed updates (e.g. Nodemanager and Reader manager) the rootfs will be uploaded in the background. The controller is fully functional during this upload. When the upload is finished, the Pluto must be restarted manually (controlled). After this restart, the Pluto is provided with the new rootfs.

A reboot may take a few minutes!

4.1.3.1 Menu or items within the dialog have been added in

- Installation | Hardware | Line (Treeview)
- Installation | Hardware | Line

4.2.4 Stand-by functionality improvements

- VRRP service in combination with firewall settings.
- Server priorities improved. To prevent that two server are active at the same time.
- Document is updated: See: *iProtect™ Stand-by Server

4.2.5 Maintenance language support

- Improved handling of sorting methods for several languages

4.2.6 OSDP support ApolloN

In order to meet market demands, the use of an OSDP reader on an ApolloN has been made possible. For example, a card reader with support of Legic technology.

4.2.6.1 Menu or items within the dialog have been added in

- Installation | Hardware | Node
- Access | Settings | Access level
- Access | Settings | Area

4.2.7 Keymap widget definition filter

To be able to show only what is relevant on a keymap (interactive floorplan), an extra filter has been added to Widget definition.

For example:

- an overview of the doors that are in Office mode. You only want to see those doors.
- and overview of controllers / locations that have a problem. Everything for which there is no problem does not have to be shown.

A Widget definition filter column can only be created when the Widget definition includes a table.

Added values are:

- Selection: Column

- Potition in filter: <number>
- Compare: !=, <, <=, ==, >, >=
- Value: <table dependency, functionality>

4.2.7.1 Menu or items within the dialog have been added in

- General | Settings | Keymap | Widget definition

4.2.8 TANlock rack handle improvements

A number of things have been adjusted. This can be security related or an improvement of the product.

- Improvements provisioner
- Improvements key data interpretation

4.2.9 Database operation statistics

Menu: Installation | Database | Connection database operation statistics

Function: Give an overview of database operation statistics

4.2.10 Service restore

Menu: Installation | Database restore | Services restore

Function: After an upgrade of iProtect the services can be enabled manually

4.2.11 Secure communication type

Menu: Installation | Hardware | Security communication type

Function: Make settings for the server- and client endpoint

4.2.12 Provisioner group

Menu: Installation | Settings | Provisioner group

Function: Makes it possible to hide the provisioner group in a list

4.2.13 Visitor location

Menu: Visitors | Settings | Location

Function: Makes it possible to set the location of the visitor

4.2.14 New input option

Menu: Installation | Hardware | Input

- Manual reset input
  - The Input mode “active until manual reset” is expanded with an option to reset the input also with an other input.
  - The Input mode “active until manual reset” is expanded with an option to reset the input by following "Access Granted" through Person class and reader.

4.2.15 Confirm ending office mode

Menu: Installation | Hardware | Reader

When office mode is de-activated and the door is not closed, the office mode will be activated for this reader again.

4.2.16 Validity update VCN/OSS

When a card with offline data is re-used in the system, the offline validity of this card will be disabled by default at the update reader.

4.2.17 Node dialog, Pluto Reader manager

The IP address of the reader manager can only be localhost. Due to security improvement the reader manager does not except other addresses then:

- 127.0.0.1
- Empty (Leave the input field empty)

> During the update to iProtect version 10.3, the IP address field is automatically emptied if the above condition is not met.

4.2.18 Upload a non signed autostartup at line or as provisioner media element

Now it is not possible anymore to upload a non signed autostartup at line or as provisioner media element.

> Uploading a non-signed reader configuration file from the line dialog is no longer possible. The file must be uploaded as a media item and sent through the provisioner.

4.2.19 Expiration check format extended for QR Barcode

In version 10.3.17 a check on the QR Barcode format is added.

Menu: Access | Settings| Card data interpretation

- Expire date format added: DxMxYYYY