PRODUCT SHEET

SYNGUARD PLATFORM

V.3.05- 21/12/2024

ALWAYS WITH YOU

SYNGUARD

Synguard is a developer and manufacturer of access management hardware and software solutions. The development of software and intelligent controllers is done entirely in-house, in Belgium.

The Synguard software offers a complete solution for access control, visitor registration, parking management, security management and graphic management.

In terms of both software links/integrations and hardware devices, Synguard brings together the best of the market according to the best-of-breed principle in 1 open management platform.

Synguard is a complete & highly configurable access management solution

- 100% web-based
- Cloud or on-premise, and easily migratable
- End-to-end secure
- Unified web interface for management, use & configuration, without client software installation
- Application developed for multisite & -user environments
- Unlimited scalability
- All-in-one software with various modules to be activated through licences

The main modules within the Synguard platform:

- Access control
- Visitor registration
- Parking and mobility management
- Biometrics
- Digital key management

- Locker management
- Lift management
- Camera surveillance
- Intrusion & fire detection
- Security management & alarm processing
- Indoor positioning
- Reservation management

Synguard uses open standards & open source development tools allowing us to track and integrate integrations, new technology trends and security updates.

Synguard has a wide range of software modules that can be flexibly activated (by means of licence keys) according to the customer's needs. No additional applications need to be installed when you want to add an additional module. The software modules are available for both the cloud solution and the on-premise solution.

We use our expertise to work with the partner and customer to see which modules are needed to provide a solution that fully meets the customer's needs.

1. FUTURE PROOF

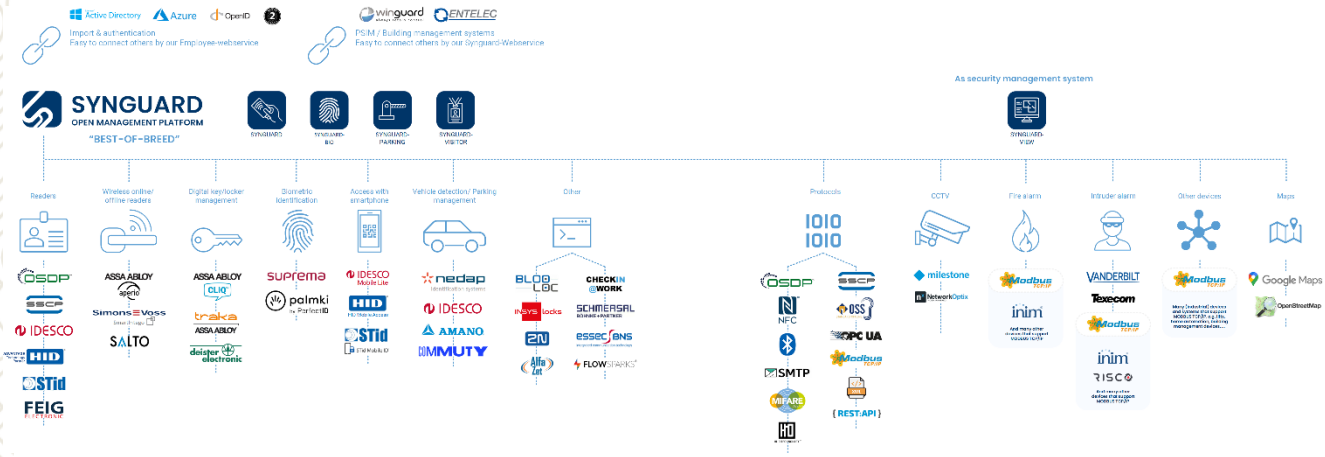
Synguard's own, in-house development team develops both our hardware and software solutions based on open standards and open source development tools. Open standards (or norms) establish a certain way of working, allowing suppliers to
that use it can all share data in the same way. This makes it easy to fully integrate other solutions into the Synguard solution. We also do not write browser-specific software, so new versions of web browsers are immediately supported. Moreover, we follow and integrate new, reliable technology trends on the market to offer our customers a complete and future-proof solution.

Through our many in-house developments, we therefore ensure that a 'vendor lock-in' is avoided for our customers. So you are never stuck with 1 vendor, system or product, but can opt for a best-of-breed solution.

In a best-of-breed solution, each manufacturer has a strong focus on its own core business (products), only they can be 'best-of-class' in what they do. We bring like this solution together in our platform. Our platform gets our full focus. So Synguard is above all an open access management platform, built according to the best-of-breed principle, and together with the best technology partners in the world of access management/security.
Synguard counted more than 100 integrations in 2024.

This is not the only reason why Synguard is future-proof. Also because Synguard is highly configurable, it fits

in any environment and changing customer needs. Think free fields, event rule engine, personal dashboards, operating scenarios, etc....



2. INTEGRATION INTO THE IT ENVIRONMENT

To address growing cyber security risks, you need to comply with all the latest cyber and Information security standards. In addition, important integrations into existing IT environment that contribute to a secure, well-managed, user-friendly environment.

Have you thought about the following issues?

- Are all persons in the access management system still all employed?
- Are there any logins from employees who are no longer active?
- Does a new employee need to be created and managed in different systems?
- Can the right people log into the application?
- Does everyone log in with a unique user and a secure password?
- Do those logging in have the right rights in the software?

To provide a solution to these, and numerous other problems, integrations are available so that Synguard works flawlessly within the IT environment. There are authentication - and synchronisation capabilities thanks to our integrations with Microsoft Active Directory and Azure. Synguard is even compatible with various Single Sign On solutions for authentication. Such as Active directory Single Sign On, OpenID and OAuth 2.0.

Need integrations with other (in-house) applications?
No problem! Synguard has several import, export, linking and integration options.
Loading employees via an Excel? A daily automatic CSV exchange between Synguard and another system? Need an intelligent bidirectional link
No problem, Synguard can do it all.

3. SYNGUARD ACCESS CONTROL

3.1. 1 platform for small and large solutions

The basics of access control are about who (what identifier) can access where (what door or other obstacle) when (during what hours).
The access control solutions market has continued to evolve today with all kinds of new technologies and applications, but the 'who-where-when' always remains the basis of any solution

Who **Where** **When**

Synguard is a global concept, perfectly scalable to anyone's size. From solutions with one door to complex installations spread over several sites. With Synguard, you easily manage who gets access where and when. For smaller systems, the built-in software, accessible via the local network, is sufficient. We speak of small installations when we stay within the same IP controller, without special modules. For larger systems (from more than 1 IP controller and/or the use of special functions such as visitor management), a Synguard with server must be provided. This is possible as a cloud service or as an installation on your own hardware/server.

Security
Alarm follow-up, history, evacuation reports, graphical overviews, floor plans, ...

Reception
An efficient reception desk ensures a customer-friendly receptive. Possibility of visitor self-service.

IT
Easy management: configurable user roles, access profiles, schedules, ...

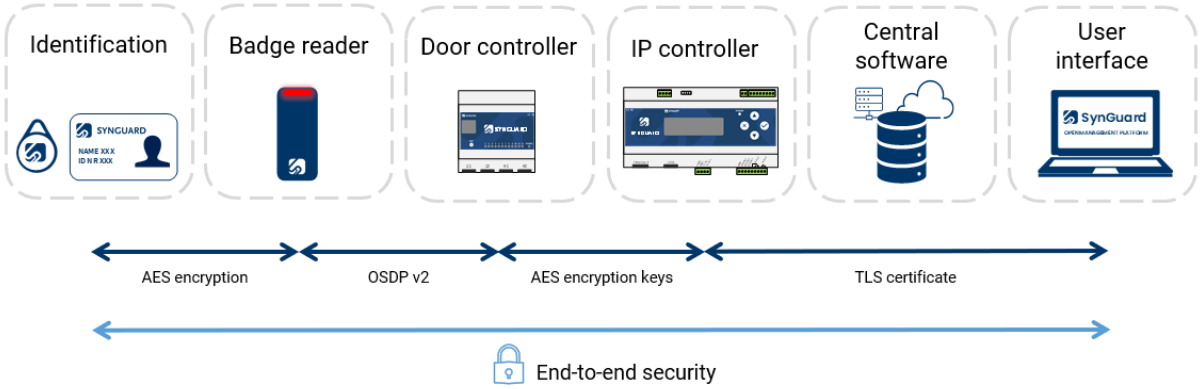
3.2. Uniform user interface

Users and administrators of an access control system want to work in a system as quickly, flexibly and easily as possible. Because our solution is 100% web-based, you log in easily from anywhere using any web browser. So no additional client software is needed. The interface of the embedded software is the same as the server software, on which additional modules can be activated . The different types of users only see the modules and screens to which they have rights, but all work in the same, familiar interface.

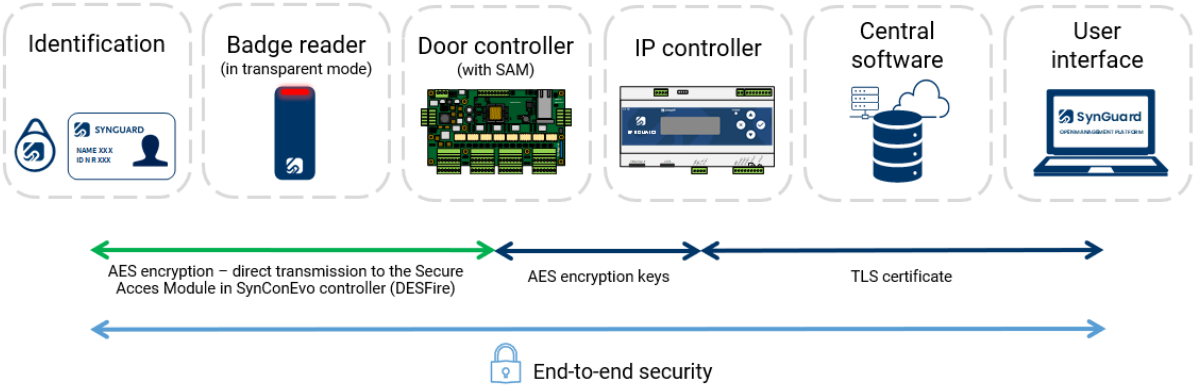
If another solution is integrated, such as wireless locks, digital key boxes, ANPR cameras ... we always work towards 100% unified integration. This way, all use and management can be done within the same user interface.

3.3. Data and cybersecurity

An access control system must be secure from start to finish. That is why our solution is end-to-end secure. End-to-end security means that all communication transfers are secure (encrypted). This happens from the badge to the badge reader, the door controller and the IP controller to the user interface.



Synguard also has a controller with Secure Access Module (SAM) for increased security. This controller supports transparent mode operation of OSDP and SSCP readers as well as key diversification.



4. MULTISITE

Our solution is designed from the basics of software multisite. That is, the software is designed to set up multisite environments and manage/use them in an orderly way. Multisite means having multiple buildings, car parks, sites ... equipped with access control solutions and linking them all to 1 central database. This allows customers with multiple buildings to centralise management. All buildings are then connected to 1 database with employee data. So there is only 1 environment to maintain, without the risk of double entries.

"That one central point enables flexible use, even across different locations"

By using the Multi-Realm module, that single central database can be arranged software-wise to suit your own needs. For example, you can determine what information someone gets to see for each user profile. As an administrator, you can determine that a user:

- only gets to see its own info;
- only get to see info about the establishment/site he manages;
- see info across multiple branches/sites in order to perform central management

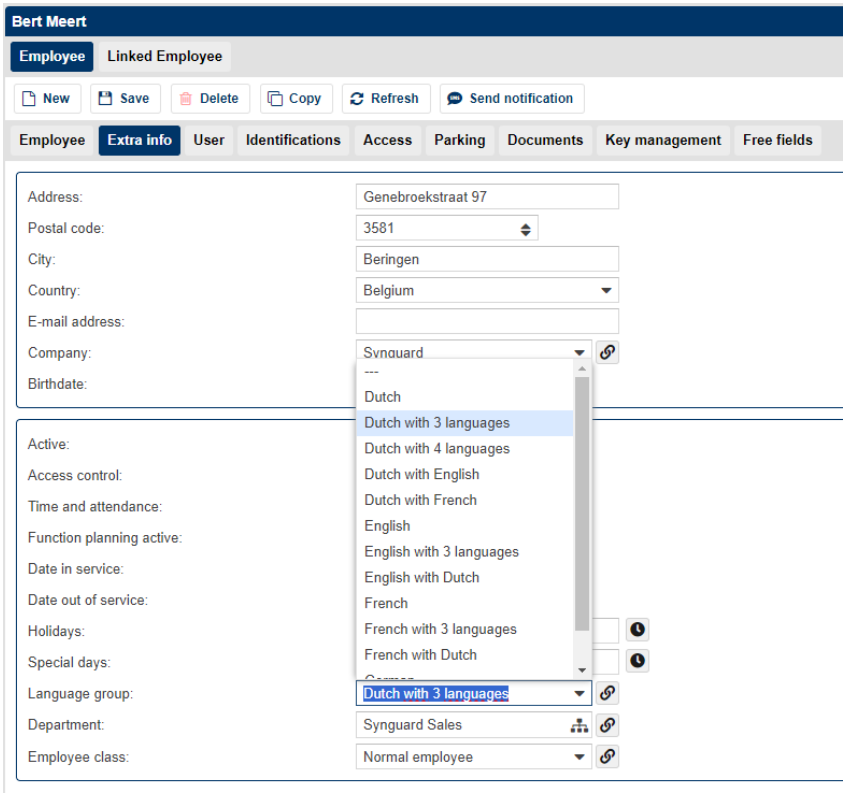
So the user will see only the information related to his/her domain. This maximises usability. Meanwhile, the administrator can manage the overall picture.

5. MULTI-LANGUAGE

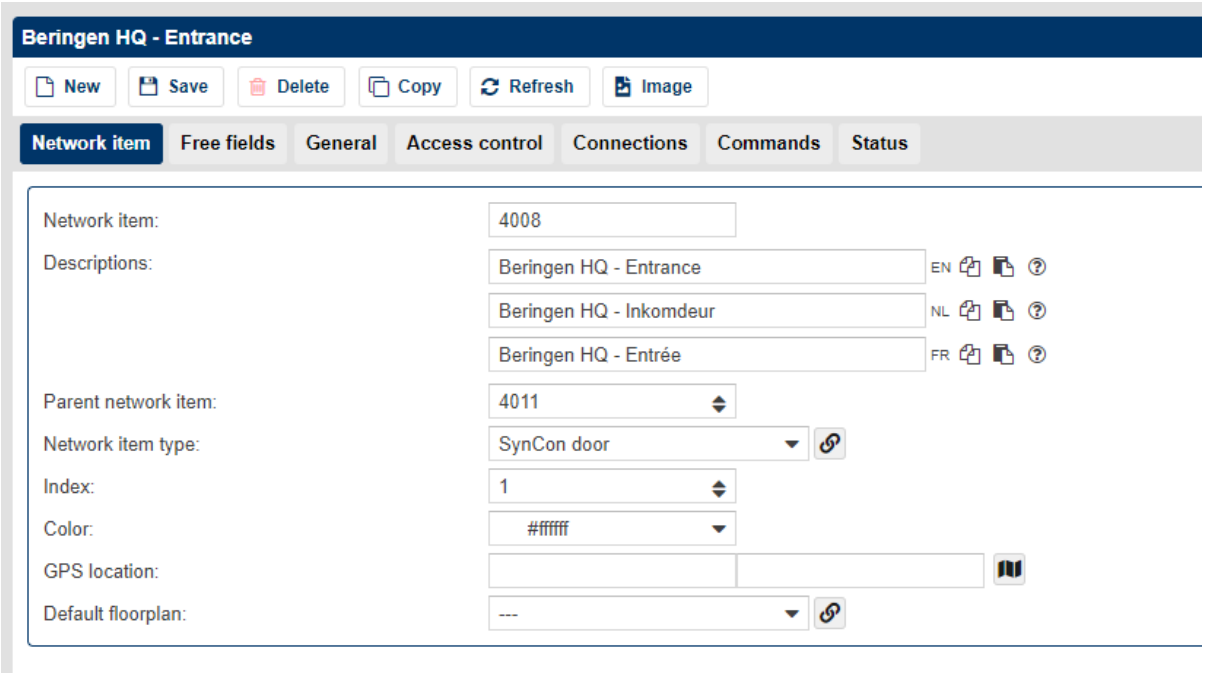
There is also often a need for the availability of the central software in different languages. Just think of multisite environments in different countries/language regions, or when your employees speak different native languages.

The Synguard solution supports multiple languages by default.
For each employee, it can be set which language or language group the employee is shown.

The choice of the 'primary' language indicates which language the interface will be in when this person will log in and which language will be displayed first for the input fields of variables (e.g. names of doors, readers, profiles, ...).
The 'secondary languages' indicate which other language fields are visible, and can be filled in by this user. The administrator typically adopts a language group with his/her native language and the other languages in use in the system so that the definition of door names and the like can be done in all required languages.



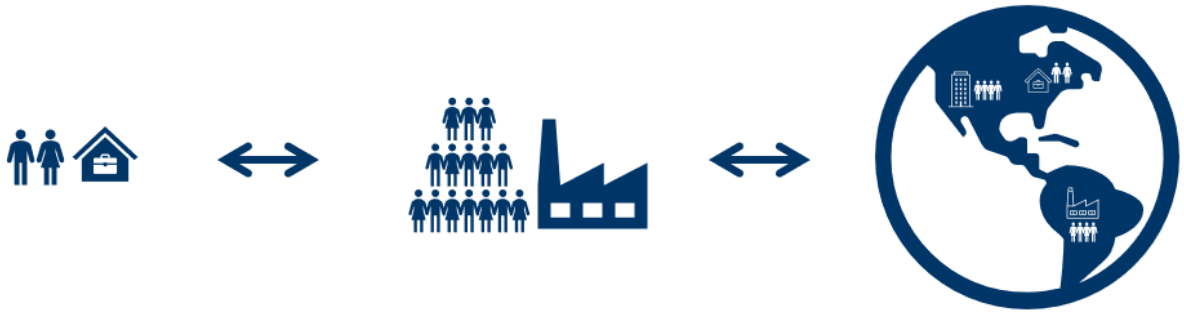
When a person logs in with language group 'Dutch with 3 languages', below is an example of how the fields to be filled in are displayed in multiple languages. The primary language is Dutch, which is how the interface language is displayed.



6. SCALABILITY

The Synguard solution is almost infinitely scalable. The customer can start with a small installation with only a few doors and users. As soon as expansion takes place, the existing IP controller can very quickly be incorporated into a server solution (cloud or on-premise). All existing configuration is then transferred to the new server environment. So no investments are lost. Once a server environment is in place, a new site can be rolled out very quickly and easily. After all, all employee and preference data are already in place. Each local IP controller then communicates directly with the server. An internet connection and power supply are the only needs to add a new installation in the system.

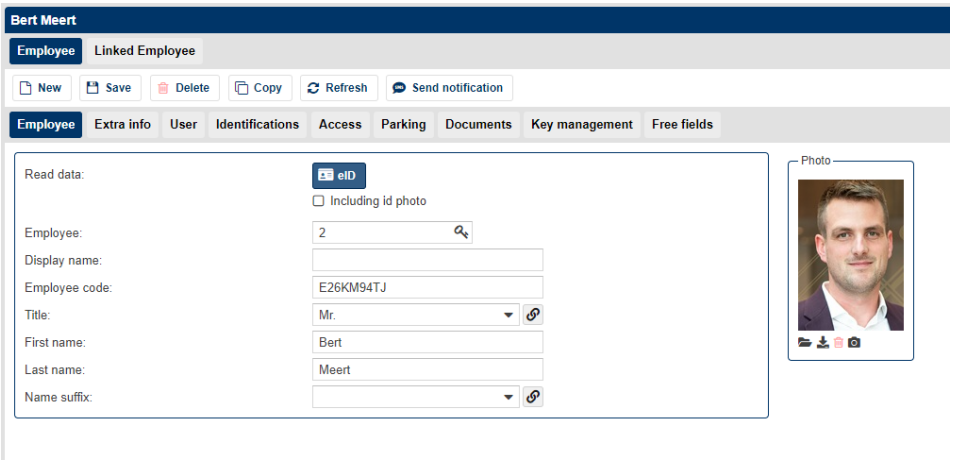
Whether it is 1 door or unlimited doors, 1 employee or unlimited employees, 1 site or multisite, the same environment remains applicable. So no new installation of the software is needed for the system to grow with your business. This also applies to the use of any additional modules (such as parking management). In fact, that activation is done through licence keys.



7. BRIEF OVERVIEW OF SYNGUARD SOFTWARE CAPABILITIES

7.1. Employees

In Synguard, you can enter all the info you want per employee. That simple entry of personnel data is possible via your web browser or via an import (Excel, CSV). A link can also be made with the HR system or the Active Directory (AD) environment to avoid double entries and automate daily operations.



Import and visualise your employees' photos. Importing can be done via your browser or via an eID reader (and SynReg licence). Photos can also be taken via your webcam. Those photos are then usable in the visual module (visual representation of the photos on the floor plans) and are also displayed in certain reports.
When using the SynReg module for badge printing, the employee badge can also be printed with this photo.

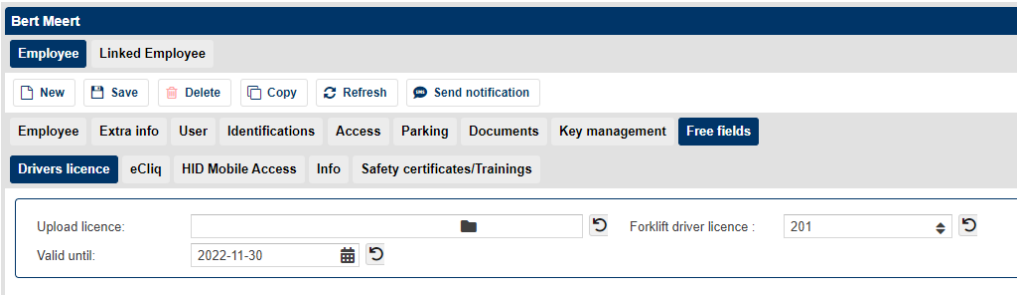
7.2. Freely definable fields

The Synguard database is set up to best fit the customer's environment. By allowing you to create free fields, the Synguard database can be personalised to your company's specific needs.

Free fields can contain different types of data such as:

- Numeric data, e.g. an attestation number
- Documents, e.g. a safety certificate
- A self-defined selection list
- ...

In this way, additional information can be managed that may or may not be security-related. The free fields can be accommodated in clear tabs. They can also be used during certain events as control, test or control fields.



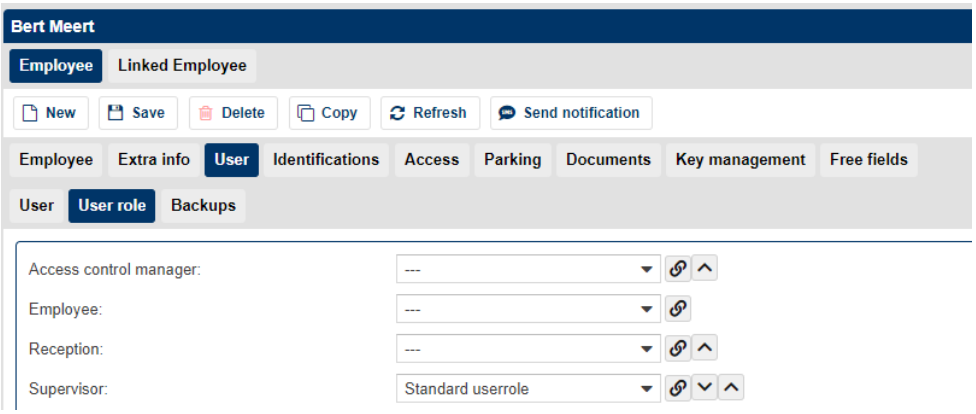
7.3. Type of users:

Within Synguard, each employee can be given a personal login. That login can be tailored to the employee's profile. This way, you determine who has what rights and they do not see info they are not entitled to. For example, a profile can be created for a reception employee. That person can only add a badge and view a floor plan, while the administrator has rights to all actions and screens. This way, you not only comply with GDPR legislation, but also have a positive impact on user-friendliness.

Because this way, the user only gets to see menus he actually uses.

- User role: defines the type of user with its capabilities, e.g. administrator, reception, security etc. This is a combination of an action profile and a data profile.
- Action profile: defines the actions, screens, tabs and reports the user is allowed to use.
- Data profile: determines what data the user is allowed to see and manage.

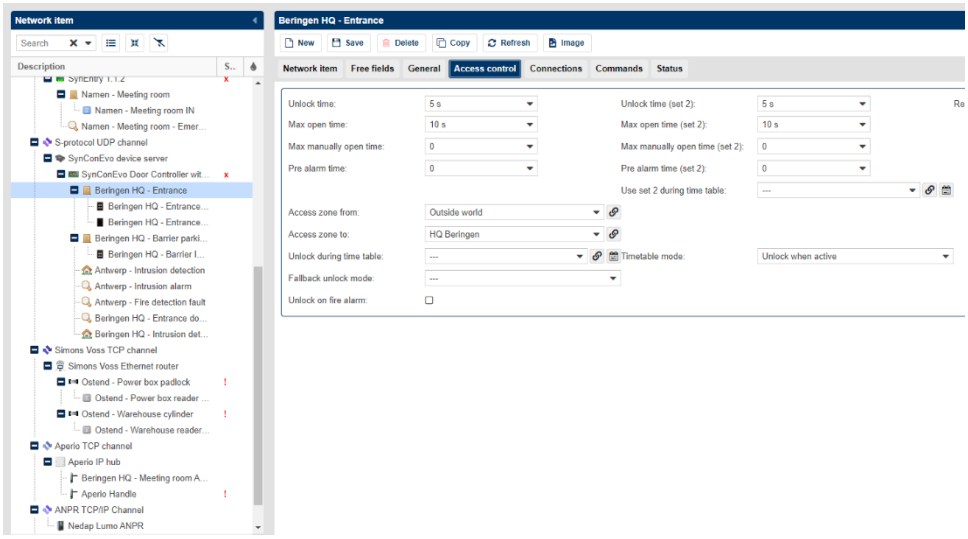
Synguard allows you to choose which user can manage or view which function. If necessary, replacements for people can be designated so that the necessary rights automatically go to the replacement in the event of absence. This can be useful, for example, if the reception employee is on leave and the logistics employee should replace him. As a result, the latter can now easily add badges, whereas otherwise he can only retrieve reports.



7.4. Obstacles

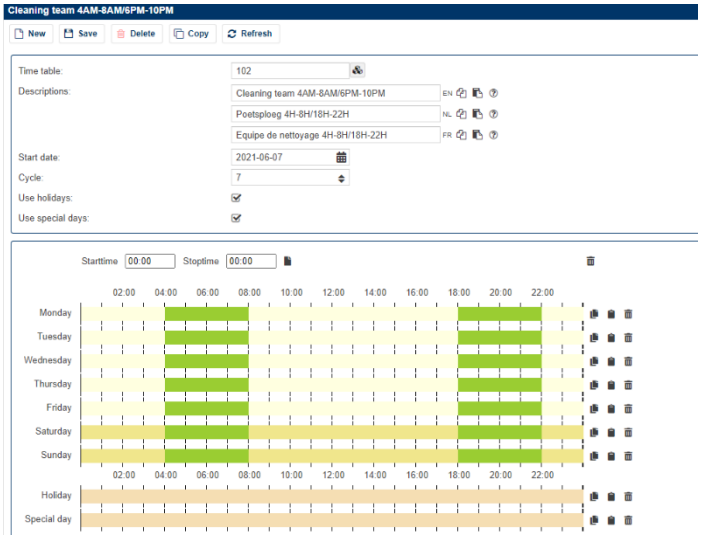
From Synguard, you can manage all possible obstacles with their specific settings. The configuration possibilities are almost unlimited. Thanks to the complete integration of hardware and software, you decide which function is linked to each signal (input, output, reader, timing ...).

Both the control hardware (such as controllers and readers) and the obstacles themselves can be configured using the same unified web interface. The obstacles and other hardware can be scheduled in graphical floor plans to make management and daily use easy.



7.5. Timetables

Easily determine when employees are allowed access through schedules, holidays or self-selected days. These can also be assigned to give obstructions a multi-functional effect, such as opening doors after the first identification until when the schedule is no longer active. Outside the schedule or set working days, valid identification must then happen.



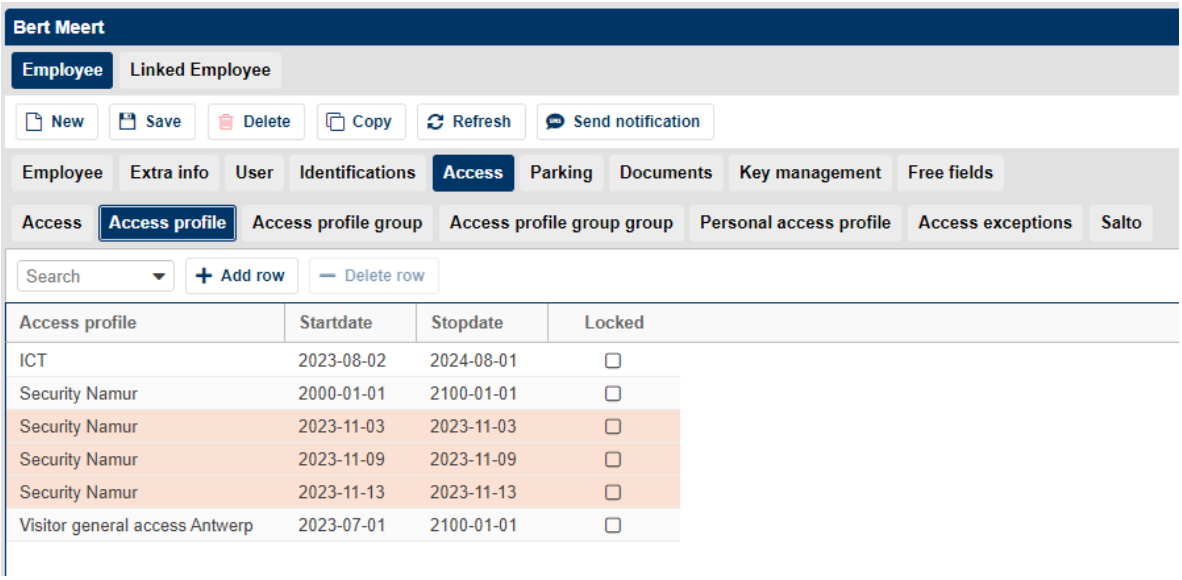
7.5.1. Holidays and special days

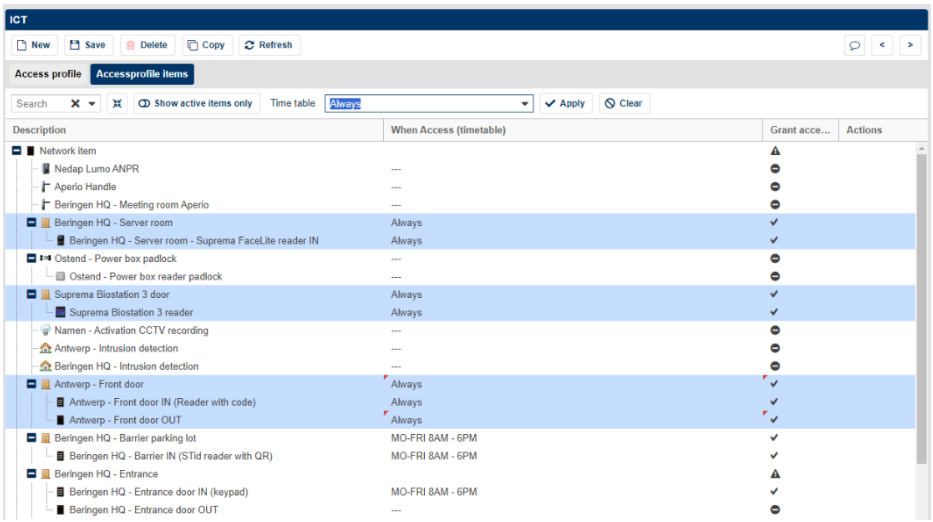
Synguard includes the ability to enter the company's own company holidays and special days. Within those own special days, groups can also be created, e.g. one for workers and another for clerks. Thus, access and operation of barriers can react differently during those special days.

7.6. Access profiles

To keep management clear, where and when are combined into access profiles. One or more access profiles can be assigned to each employee. When the access control system is extended, it is sufficient to include those new accesses in the profiles so that they do not have to be modified for each employee. The following options are available to define access rights:

- Global access profiles: Global access profiles
- Global access profile groups: It is also possible to define access profiles freely in groups. This group or groups can then be assigned to individuals.
- Global access profile group groups: In addition to access profile groups, it is also possible to create and assign access profile group groups to a person. This with the aim of giving regional or national access rights, for example, without creating separate access profiles for this purpose.
- Individual access profile: it is possible to create an additional individual access profile for certain persons. (some doors more/less than the general profile)
- Access exceptions: configure a deviation to the access profile for a specific time. This allows you to easily configure a provisional access change individually without making adjustments to the overall access profile.

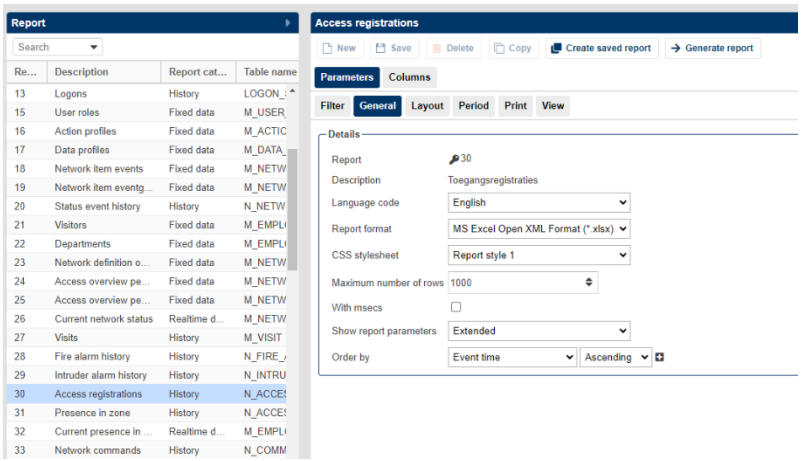




7.7. Reporting

The Synguard solution has very extensive reporting capabilities as standard. There is a choice between a large number of predefined report categories. The reports can be set with the necessary filter and can be generated in various formats, such as HTML (web page), pdf, CSV or Excel format.

When a particular report with certain filters and settings is needed repeatedly, the report with the appropriate filters and settings can be saved. This way, you generate reports later with a single click. They can also be automatically generated and even emailed.

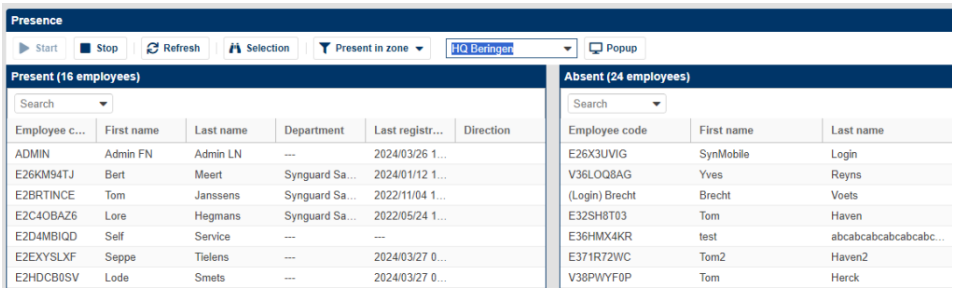


7.8. Monitoring

The Synguard real-time monitor displays all events. These are events from all hardware devices and actions associated with the system. The monitor can operate in single-screen or pop-up mode, so that info from the monitor still remains in the foreground while navigating other screens. The monitor can also be set with filters on certain locations, hardware, type of notifications, etc. For example, the security guard may be interested in who enters certain monitored areas, while the technical department wishes to receive only technical notifications.

7.9. Presence

By creating zones within your environment, you can manage presence within those zones. Synguard indicates who is present or absent in a particular zone of the company. Ideal for reception to find someone quickly or for evacuation purposes. With one click, you can instantly retrieve personal data, so you know how to reach the person. You can also use the zones to configure interactions with the intrusion detection system, for an anti-passback operation or to determine the maximum or minimum number of people that can be present in a zone.

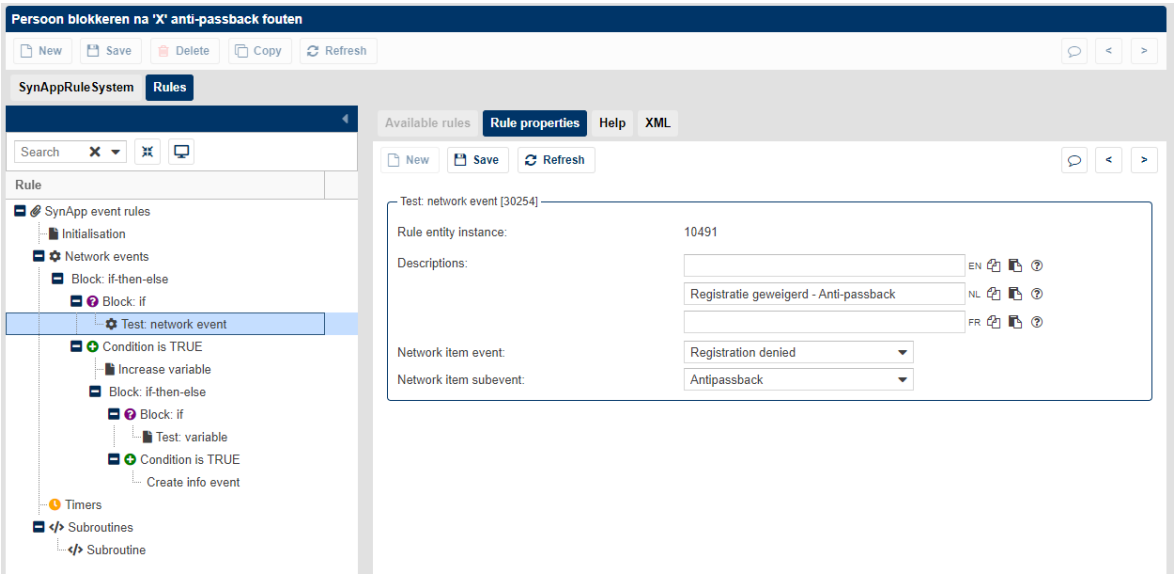


7.10. Automatic open steering on scheduled command

Do you want free access to the entrance door or is there a scheduled event that requires the door to remain loose? Synguard allows certain obstacles to be linked to a schedule and sent open at the chosen time. Or do you want to activate and deactivate the control only when the first authorised person is present? That too can be fully configured.

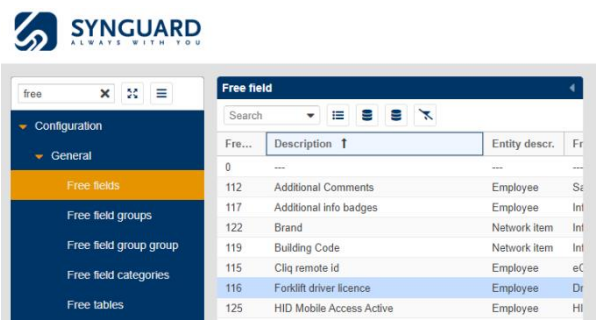
7.11. Event handler

All events are logged in our system. Via the event handler, certain events can be responded to in a simple way. And that through a simple scripting language that you define. For example, an event can trigger certain objects (doors
or other hurdles), send an e-mail/SMS, change regimes, etc.

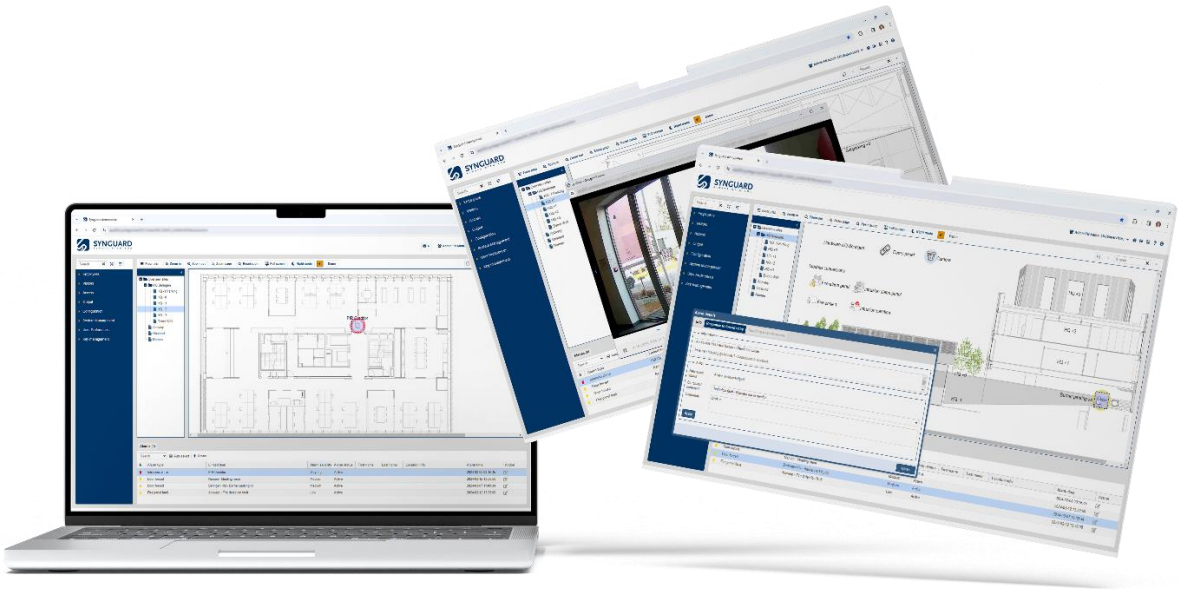


7.12. Search functions and filters

Filter and search capabilities have been built into the Synguard platform to make the solution as user-friendly as possible. For example, searching for a person in a list of thousands of employees is now quick and easy. Not only by using the search functions, but also by setting a filter. For example: only search for employees assigned to department X.



8. SYNGUARD-VIEW

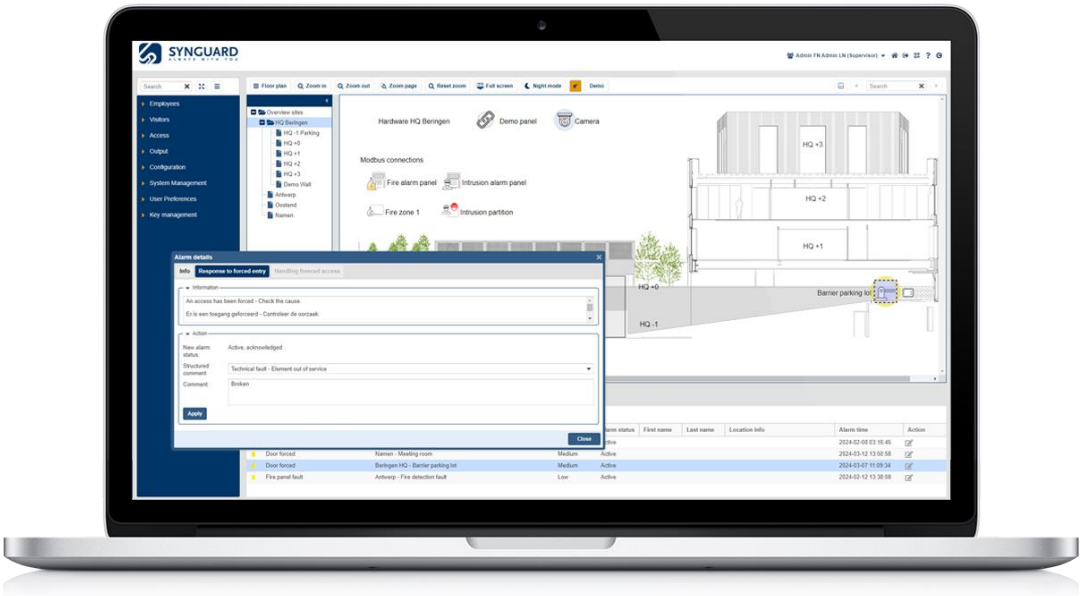


The Synguard-View module features a graphical monitor that allows linked elements to be displayed on floor plans. This allows security to be conveyed visually and enables simple, safe and target-oriented operation (e.g. directing a door or obstacle open, viewing the occupancy in a zone or car park, managing hardware status).

You can import floor plans of your building(s), surroundings and sites into Synguard-View (JPG, PNG, ...) and configure objects on them. Besides floor plans, you could also create pages
that give an overview of certain statuses, or a page with control buttons. Several plans can be linked together, so that a
easy navigation is possible. For example, for a multisite environment, you can start with an overview map of the country, after which you can click through step by step to the different sites, the respective building and the desired floor.

In addition to the graphical monitor, Synguard-View also features alarm handling, allowing you to configure which events should be visualised and handled as alarms. Alarms are configured in different types, allowing a different handling procedure for each alarm type. This allows additional info to be added to the
operator are given, followed by actions to be taken and comments to be completed.

All events and alarms (including those from linked non-Synguard systems) can then be used for specific configurations via calculation rules. A (alarm) sound can also be set for each alarm type, alerting the user to critical alarms.
Besides access control, it is now also possible to include other systems in the graphical monitor. This gives the possibility to include your access management system also
use as a web-based open management platform.

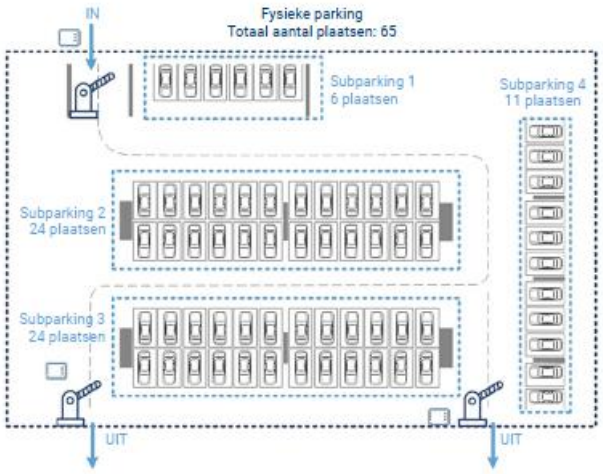


9. SYNGUARD-PARKING

Parking spaces are becoming scarce and can be a source of frustration. Proper management of these spaces can add efficiency and convenience for
employees and visitors. The Synguard parking management module allows the management of parking(s) and/or partial parking areas Multiple physical car parks can be managed via parking management. A physical parking is an area that has at least one entrance/exit. Each entrance/exit is equipped with a gate or barrier, detection loop and/or badge reader.

Each physical car park can be divided into several logical sub-parkings. For each sub-parking, you can indicate how many spaces are available, or you can use

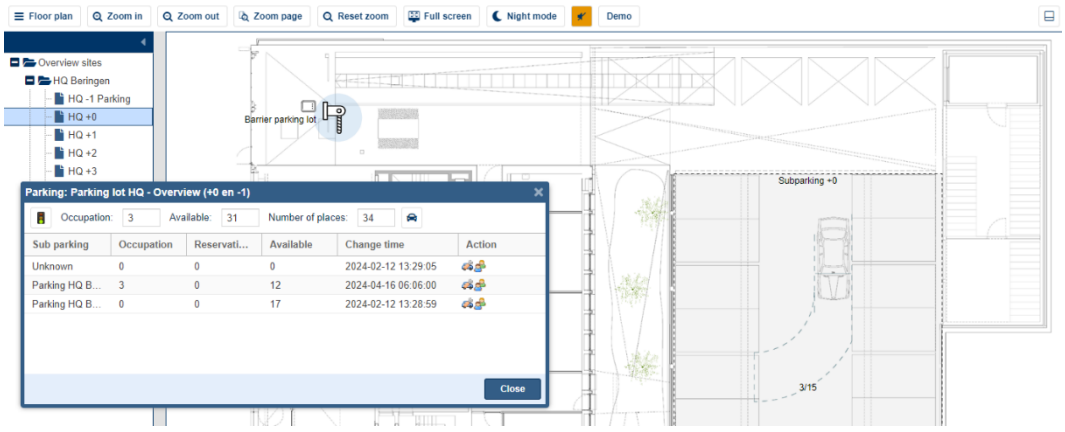
flex spaces can be worked. In this way, the parking spaces can be perfectly managed, entirely as you wish. If there is a need for mobility management (e.g. reservations, co-involvement of charging stations, etc.), we have links with specific parties who can take care of this.



Synguard-Parking is 100% integrated into the access management solution. This allows employees or other people (e.g. local residents) to access certain
(sub)car parks. Access can even be set so that certain people are only allowed within certain times.
As identification can be used:

- Existing employee access control badges
- Long-distance tags in the car
- Automatic number plate recognition using an ANPR camera
- A separate parking ticket machine

The parking spaces and occupancy of all subparkings are fully graphically displayed. This gives you an overview of the occupancy & free spaces at a glance and the necessary corrections can be applied. The same can be done for visitors: they can be given temporary access to a separate, dedicated subparking. Via a list, any costs (e.g. parking rental) can easily be charged to the right companies and/or persons. In this way, parking space is perfectly managed.



10. SYNGUARD-VISITOR

10.1. visitor registration

Synguard-Visitor and Synguard-Visitor Self-Service are two modules in the Synguard access solution to implement visitor management quickly, efficiently and according to the organisation's flows. Visitors are managed and processed in the same database as access control and/or time recording. This has the advantage of allowing flexible configurations. Interactions between employees, obstacles (such as badge readers), mails and welcome screens are extensively configurable through calculation rules such as:

- Who gets to check in which visitor and send an invitation e-mail?
- Do visitors receive a QR code (printed at a kiosk or by mail) upon registration?
- May visitors have access to the car park through the entered number plate?
- ....

The wide range of possibilities makes this module so flexible that it fits into any possible flow for visitor management.

Visitors can be announced by simply entering them in the Synguard-Visitor module. Those actions are done directly in the user-friendly
Synguard user interface. When necessary, visitors can be stored in a specific visitor database, so that a new visit by the same person can be created quickly.

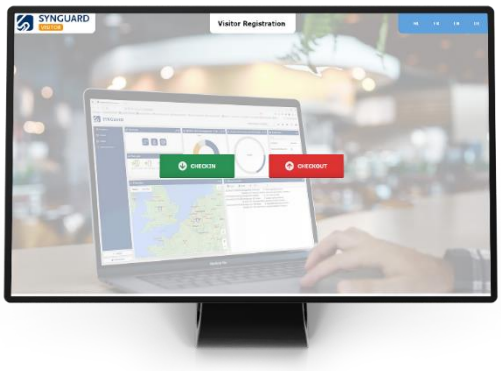
Reception can see on a daily basis who is expected and with whom the appointment was made. Visitors can also check in and out themselves in a convenient way, if required.

The reception, administrator or employee who receives (personal) visitors can register visitors themselves, manage requests and send invitation e-mails to the
visitor(s). As everywhere in Synguard's solutions, the language group can be adapted to both the administrator and the visitor. So each person always gets to see the right info in the right language (e.g. security rules that may need to be signed).

Using strategically placed QR code readers and/or number plate recognition cameras improves efficiency and visitor experience. Visitors receive a valid QR code by e-mail for the duration of their visit. This allows him to drive smoothly into the car park.

10.2. Synguard-Visitor Self-Service

Synguard-Visitor Self-Service is designed to let visitors sign in themselves. So no physical reception is needed. Registration is done in an HTML page that forms a front-end over our Synguard-Visitor database in the Synguard server.



This HTML page is configurable and can be set up according to the customer's house style. The content of the registration is also flexibly customisable. For example, you determine which fields are mandatory to enter.

Since sign-up is web-based, the possibilities for visitors with the Synguard-Visitor Self-Service module are virtually unlimited:

- He can sign in at the reception desk on a touchscreen or tablet.
- He can sign in at the reception desk at a kiosk, for example, when using printed QR codes.
- He can log in on his own PC or smartphone by opening the page on the internet.
- ...

The flow of the self-service notification can be set according to customer demand:

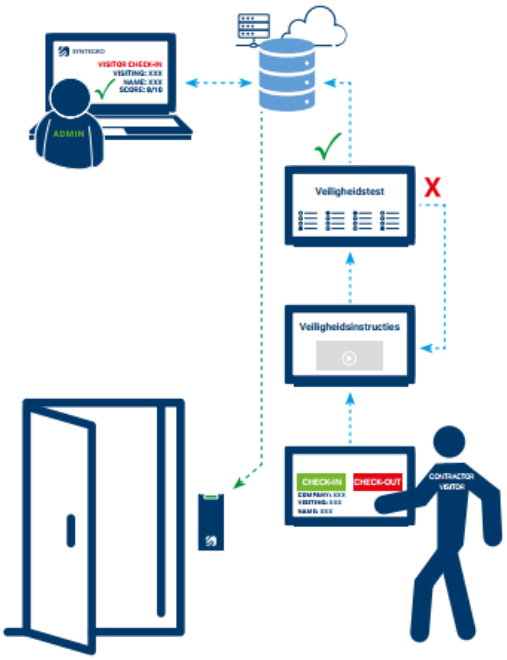
- Which fields are mandatory?
- Which fields are visible?
- Do general terms and conditions or safety rules need to be approved?
- Should an introduction or safety film be played?

Free fields can also be created for use in self-service. Examples of free fields are:

- Entering (mandatory) the contractor's (framework agreement) number
- Uploading a work order

The visitor registration module with self-service front-end is made for visitor management, but it is also excellent for managing the wide variety of contractors and their registrations.
Access management of own employees and contractors is then in one database with one user interface. It is also possible to give visitors and/or contractors a
test based on multiple choice questions.

This may be necessary in high-risk places.
Only after achieving a certain score will the application be processed and given access to (one or more) locations. Creating and modifying that test can be done by the administrator.



11. SYNGUARD OPEN MANAGEMENT PLATFORM AN IMPROVEMENT FOR YOU?

The Synguard open management platform, that is the central place where you see the movements of employees and visitors while managing the various access control and security solutions from A to Z. A platform that fits your needs seamlessly thanks to the best-of-breed principle and the many integration options that characterise Synguard.

Smart interactions between systems is an advantage for you. Because the 'best-of-breed' principle ensures that you, the customer, choose which hardware and software you want to work with. The ultimate way to create your own personalised access management. Moreover, you manage everything easily from the Synguard open management platform.

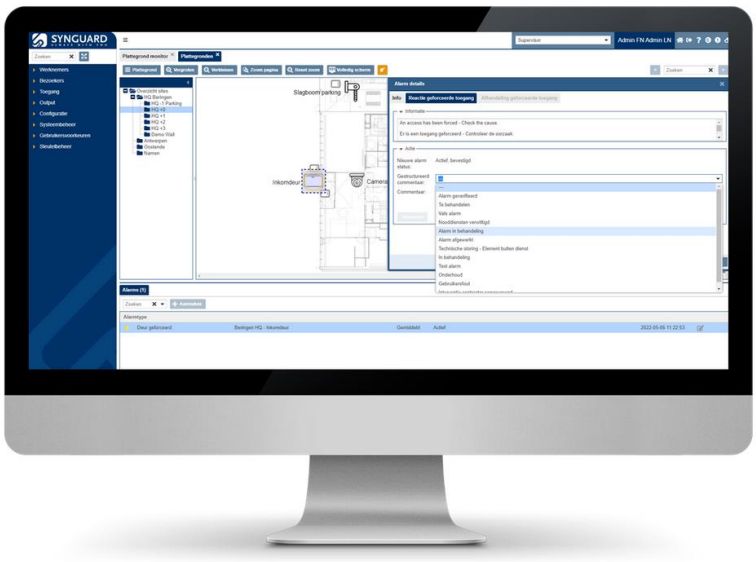
Thanks to smart interactions, information is exchanged between the systems and you always have the information you need. Linking your other security solutions such as intrusion detection, fire detection and camera surveillance to your access management has never been easier. Central management, secure and efficient.

The Synguard open management platform can do even more for you. Thanks to the wide range of modules and linking possibilities, the central calculation rule engine and the extensive configurability, you can automate and digitise your building(s) and access flows with Synguard as a total solution. Naturally in a state-of-the-art cloud solution, robust and secure.

Some examples of how Synguard open management platform makes your life easier and can mean a quick ROI (Return On Investment)?

- Full automation of visitor registration, accesses and communication
- Employees who forget or lose their badge can get a (temporary) new one without intervention, while their old one is deactivated
- Daily, weekly or monthly emails listing everyone who has entered a particular location

- ...



12. SYNGUARD HARDWARE

At Synguard, we offer controllers of sublime quality, ranging from IP controllers to door controllers. We develop them all in-house to ensure that the hardware works superbly with our software. In short, your access control solution is in safe hands at Synguard, where software and hardware go hand in hand.

Synguard thus develops proprietary Intelligent controllers for flexible configurations and complex migrations (centralised or decentralised, ...) that support a free choice of identification readers used based on market standards and open protocols without restrictions.

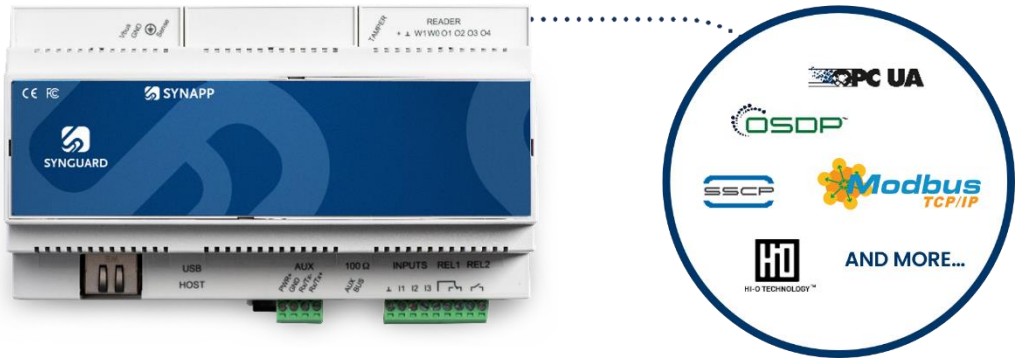
Synguard chooses to develop the intelligent controllers itself instead of integrating existing OEM controllers. This choice has several reasons:

- Freedom in development
  Many developments and (product) integrations happen in access management mainly at controller level. Because product integrations must continue to work even if the network with the server fails (fallback mode). For example, integration of a number plate camera happens at the level of the IP controller. Also integrations of open standards and protocols such as OSDP, OPC, Modbus TCP/IP, HI-O, and more take place at the controller level. By developing the controllers ourselves, we avoid unnecessary loss of time between controller and software development. Moreover, there are no restrictions on future development.
- Harmonious Cooperation
  If the intelligent controller is developed by the same software manufacturer, you are assured of harmonious operation between the controller and the software. This maximises the functionalities of both components.
- Flexibility in New Technologies

With emerging technologies, trends or new cabling models, you have the freedom to develop new controllers that work perfectly with the existing ones. You are not dependent on unknown or external parties.

- Independence and security
  You have full control over the end-to-end secure solution, without depending on third parties. We offer proprietary vulnerability management, even for hardware and embedded software.
- Life cycle management
  Our controllers have been backward compatible for 16 years. This means you don't have to worry about different firmware versions, as is often the case with third-party controllers.
- Quality control
  We maintain control over the quality, design, development process and updates of the product. As a result, we guarantee a high-quality access control solution.
- Reliable supply chain
  Our entire supply chain is in-house, so deliveries always run smoothly. You are not dependent on long delivery times or unavailability
- Smart design and easy to install
  Our range of controllers up to 8 doors and 16 readers caters for different cabling models and needs. Customers can choose between centralised and decentralised set-ups controllers, or a combination of both.
- Our powerful controllers offer 100% fallback including embedded software, embedded event handler and much more.

Some of our controllers below.
For more info, request our detailed catalogue.

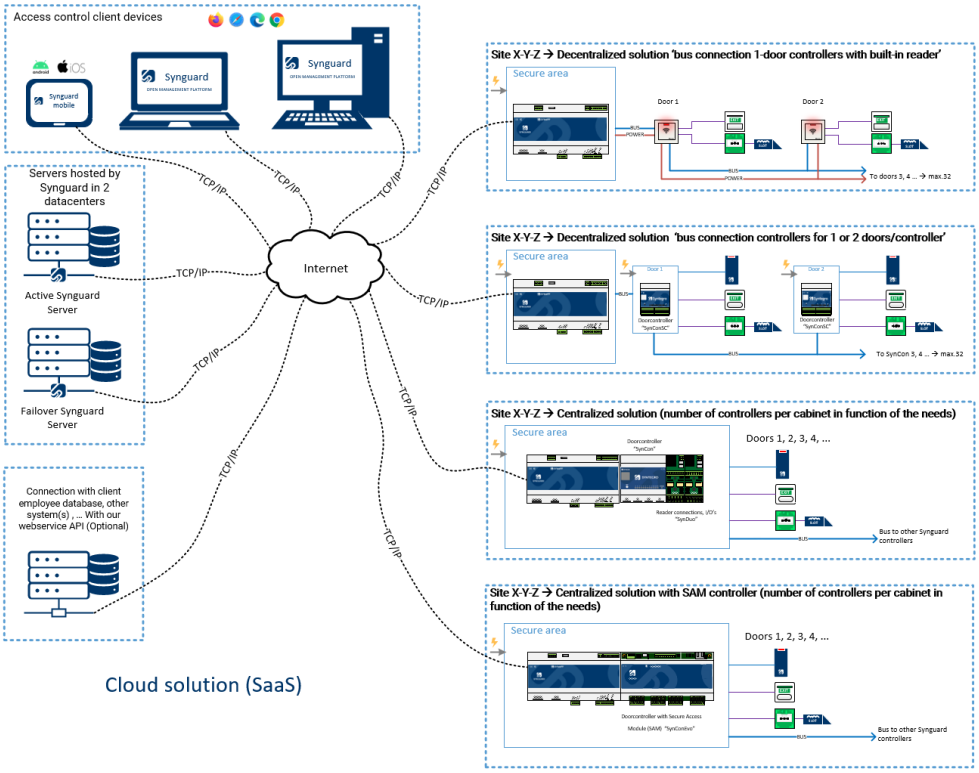


13. DIFFERENT SYNGUARD SOLUTIONS

	Embedded	On-premise	Cloud
Small and medium projects	✓	✓	✓
Major projects		✓	✓
	• Up to 128 readers/doors • (mix between wireless and wired) • Up to 32 Synguard door controllers • Access control only	• Unlimited scalability (management of multiple IP controllers) • All Synguard modules available • All integrations available • Easy roll-out of multi-site projects • Open management platform	
			• Guaranteed availability and connectivity • Automatic upgrades • Automatic backups • Redundant setup

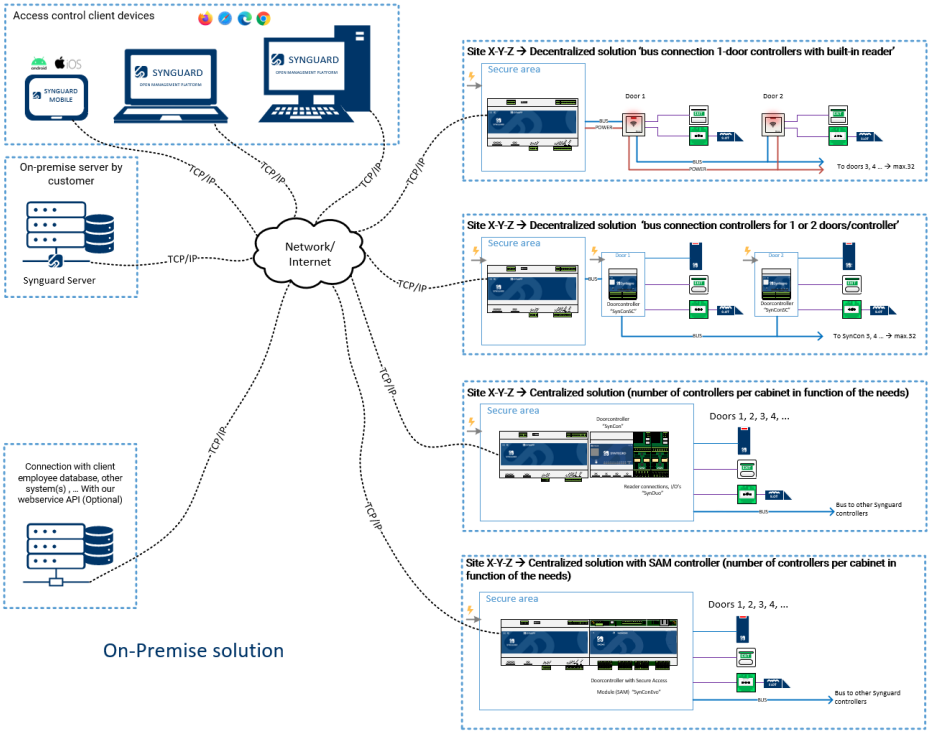
13.1. Architecture: various possibilities

13.1.1. SaaS solution:



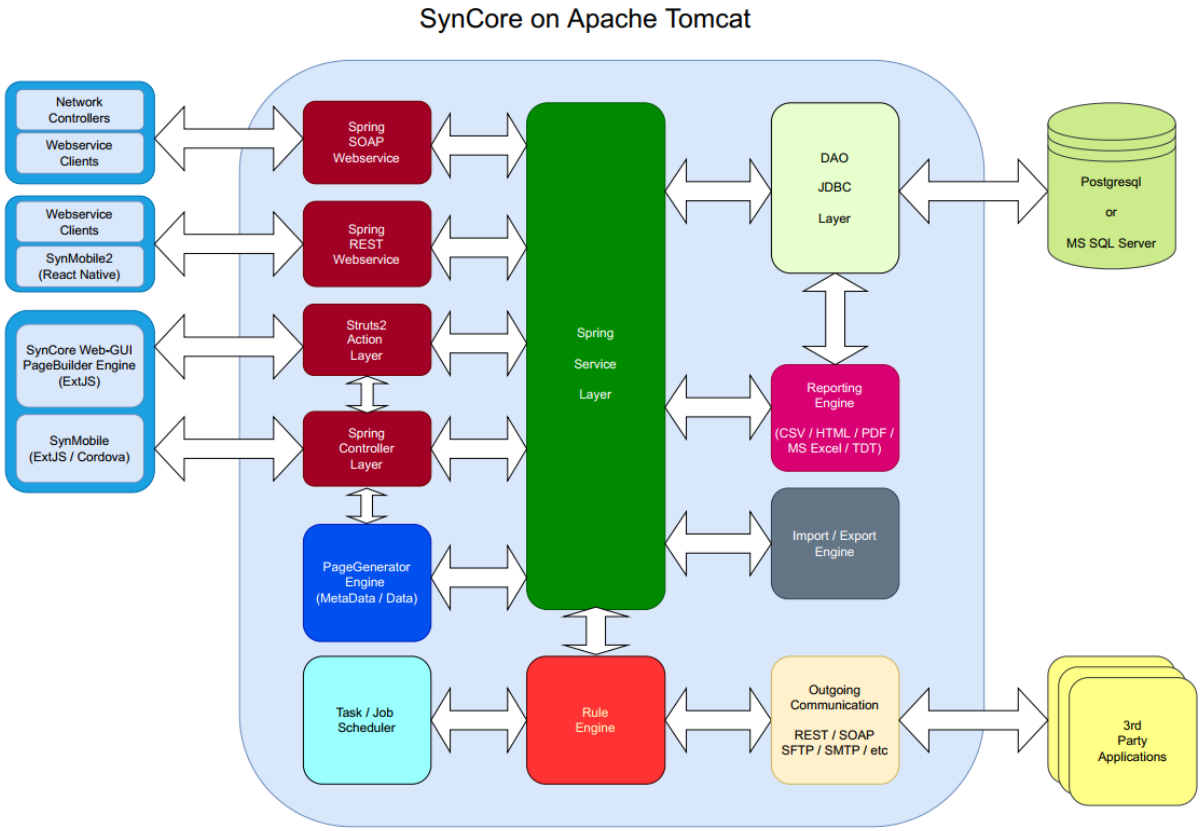
Cloud solution (SaaS)

13.1.2. On-premise solution:

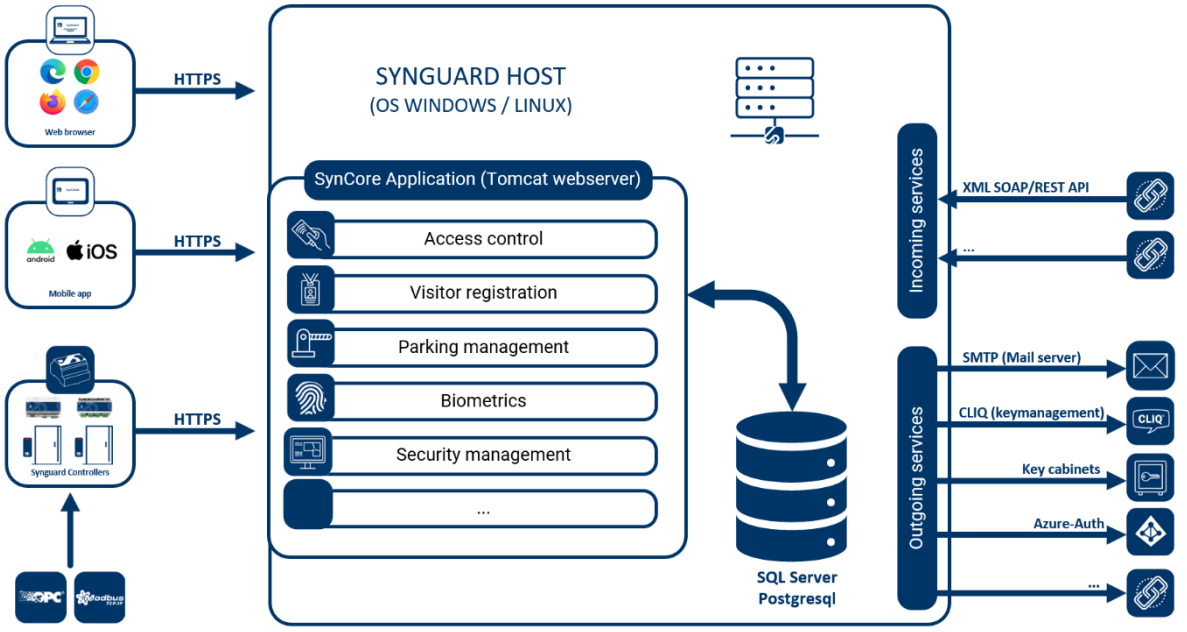


On-Premise solution

13.1.3. Synguard server software overview



13.1.4. Synguard on-premise solution



13.1.5. Hardware requirements:

The requirements listed below are minimum requirements. They may be higher, depending on the system size.

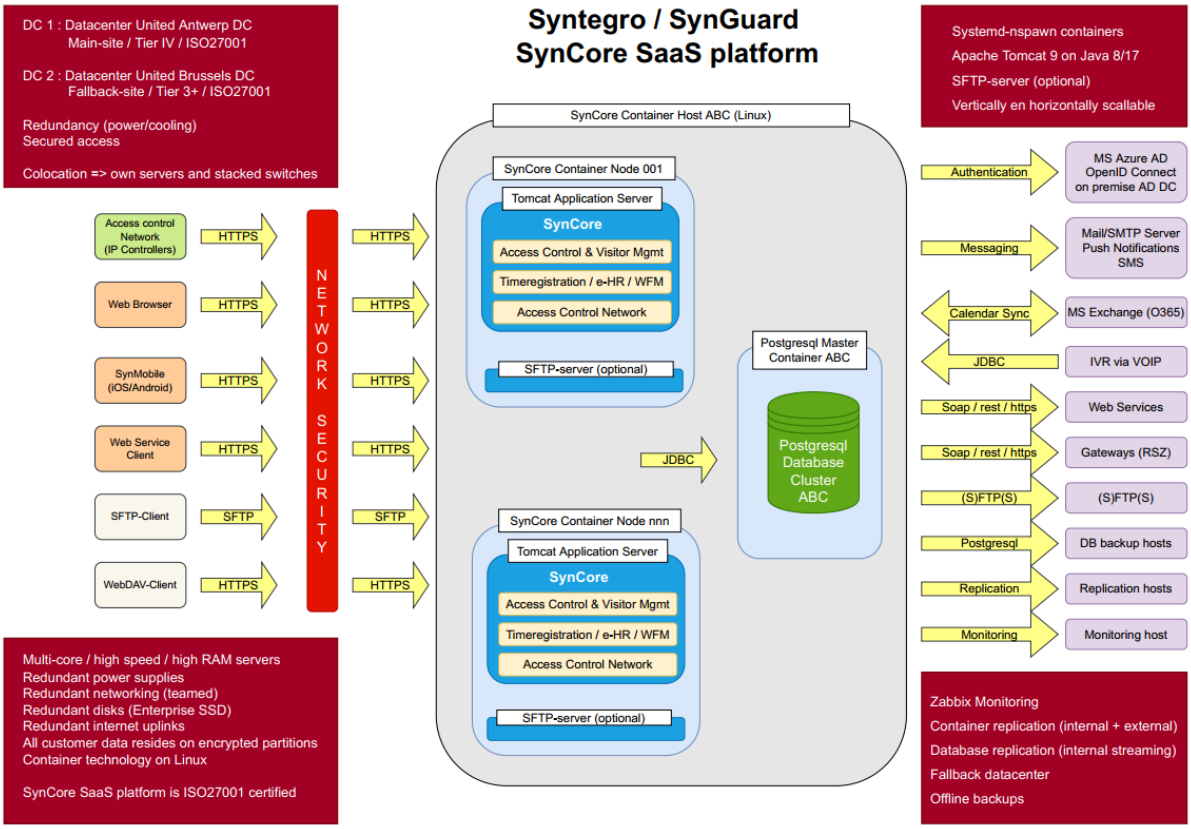
- System with min. 4 GB RAM
- Minimum 2 core CPU
- The CPU should be performant, desktop/server class, no low power / low
- performance CPU
- System with min. 40 GB free disk space

When installing on virtualisation platform:

The operating system within which Synguard will be installed can be either on physical hardware as well as running on a virtualised environment.
Among others, the following virtualisation platforms are supported:

- VMware ESXi
- Microsoft Hyper-V
- Linux KVM

13.1.6. Synguard cloud (SaaS) solution:



Benefits of cloud/SaaS?

- ✓ Better support accessibility
- ✓ Automatic backups
- ✓ Automatic upgrades
- ✓ Unburdening your own server security
- ✓ No need for in-house IT equipment (and power consumption)
- ✓ Easier links with other systems
- ✓ Fully redundant in 2 ISO 27 001 data centres
- ✓ Grows with the size of the environment

Guarantees

- ✓ +99.9% uptime
- ✓ Redundantly deployed
- ✓ Tier 4 data centre: highest level of security and business continuity
- ✓ Software upgrades included
- ✓ Daily backups
- ✓ Links to other cloud systems/smartphones without local IT impact
- ✓ Scalability without IT constraints
- ✓ 100% GDPR proof - ISO27001

13.1.7. Comparison, On-premise vs. SaaS

		
	On premise	**SaaS**
Operational security	Depending on own environment, hardware and services	Guaranteed (Redundant arrangement)
Software upgrades - compatibility	Not included	Included
Own local IT infrastructure	Own environment and services needed	Restricted
Power consumption	Own cost	Included
Proprietary IT hardware and services	High own cost	Restricted
IT maintenance cost	High own cost	Included
Right environment for IT infrastructure	Own responsibility and cost	Included - ISO 27001-certified data centre
Data Security	Own responsibility and cost	Included
Ease of use	Depending on own IT settings (DNS, port forward)	Included
Budget	Variable and unreliable (IT hardware failures)	Fixed and known
Investment cost	High	Bearing
Software / Licences	One-off purchase	Rental agreement

14. SUMMARY

	Embedded version	On-Premis	Cloud (SaaS)
Application	100% web-based (no installation of client software required)		
Software licences & extensions	Simple entry of a licence key		
Updates	Manually in SynApp	Manually in server	Automatic
User interface	Edge, Chrome, Firefox & Safari		
Security	TLS 1.3 encryption over TCP/IP		
Maximum number of users	1000	Unlimited	
Maximum concurrent users	Max. 5	Quasi unlimited (i.f. server specification)	
Maximum number of access control persons	1000	Unlimited	
Maximum number of access profiles	Unlimited*	Unlimited	
Maximum number of time schedules	Unlimited*	Unlimited	
Maximum number of holidays and special days	Unlimited*	Unlimited	
Maximum number of free fields	20	Unlimited	
Maximum number of graphical floor plans	-	Unlimited	
Maximum number of obstacles	256 (1 SynApp)	Unlimited (with multiple SynApps)	
Controlling lifts (food dishes)	Available as standard		
Configurable obstacles and zones	Available as standard		
Anti-passback	Logical and/or pseudo anti passback control adjustable		
Mastermode	Available as standard		
Multiple identifiers under 1 person (badges, codes, QR, mobile, ...)	Available as standard		
Visitor registration module	Not possible	Optional (SynVisitor)	
Parking management module	Not possible	Optional (Synguard parking)	
Graphical management system with alarm processing module	Not possible	Optional (Synguard-View)	

*Depending on the size of the entire configuration within this embedded controller

	Embedded	Server
Operating system	Embedded Linux	The operating systems listed below are all 64-bit: • MS Windows 2012 server R2 or later • MS Windows 10 (for smaller installations) • Linux RedHat 7.x / CentOS 7.x • Linux RedHat 8.x / CentOS 8.x
Database	SQLite	• Postgresql 12.x (our standard delivery) • MS SQL Server 2012 or later • MS SQL Server Express 2012 or later (for smaller installations)

VERSION HISTORY

Version	Date	Responsible	Adaptation
3.01	16/04/2024	MEEBE	New style and adaptations
3.02	10/05/2024	MEEBE	Addition hardware + architecture examples
3.03	15/05/2024	HAVRO	Customise layout
3.04	20/12/2024	HAVTO	Customise screenshots & titles
3.05	21/12/2024	HAVTO	Adjusting tables