FUNCTIONAL OUTLINE

MICRO-SESAME

SECURITY SYSTEMS

www.til-technologies.fr

TiL TECHNOLOGIES

TABLE OF CONTENTS

OVERVIEW

MICRO-SESAME integrates **Centralised Security Management** (access control, intrusion, video) and a **Building Management System**.

MICRO-SESAME ensures global monitoring of electronic data.

Features are controlled by a common graphical interface that simplifies their use and improves efficiency.

Interaction between systems can be completely automated (event-based actions), ensuring quick processing.

The system contains software elements and centrals over IP connecting to different hardware items.

This architecture is supported by durable standards ensuring cost-effective evolutions.

By integrating SDK or protocols such as MODBUS, **MICRO-SESAME** can monitor information coming from external systems (such as fire security systems) or from digital video systems.

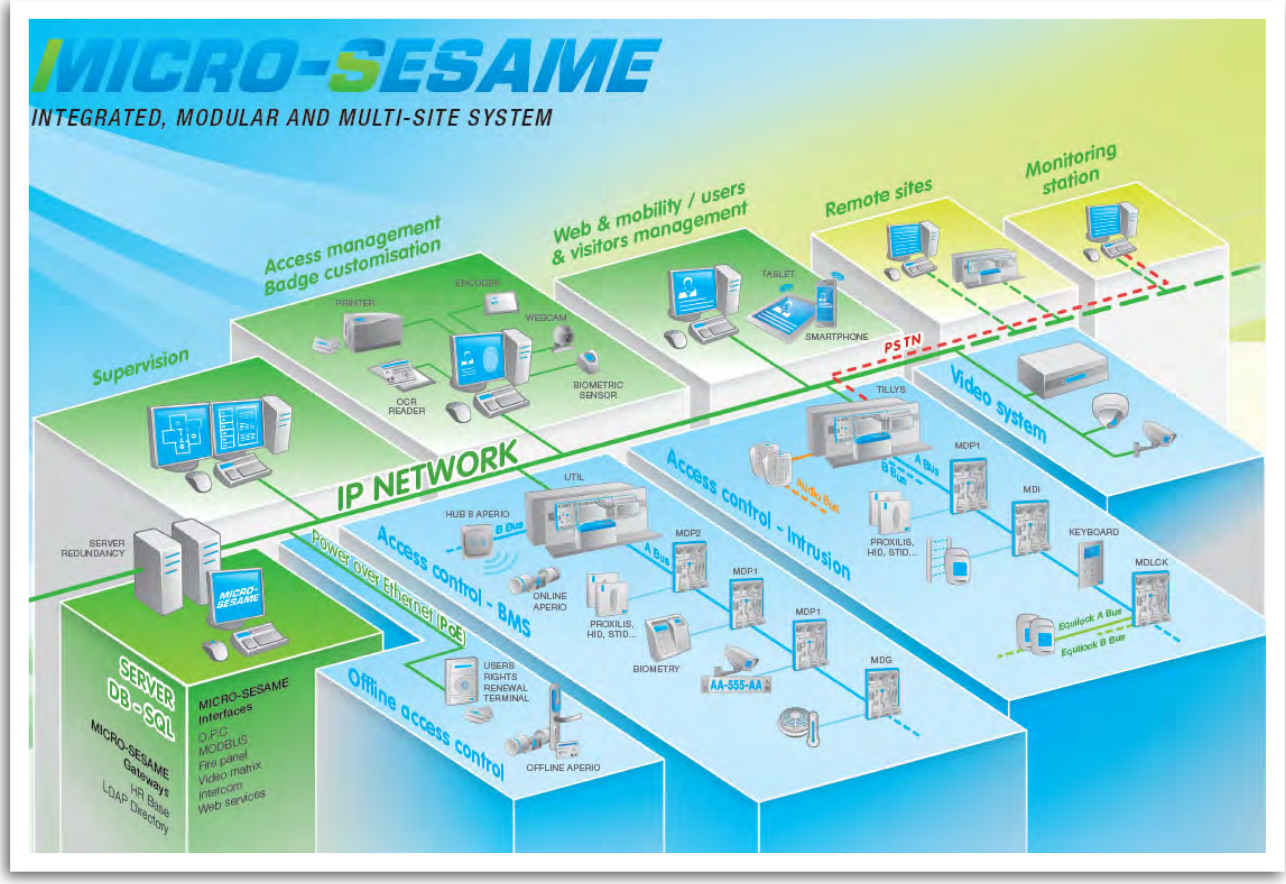
MICRO-SESAME communicates with programmable logic controllers (PLC) as well as with other safety and security equipment using gateways (OPC, text…)

FUNCTIONAL ARCHITECTURE

The **MICRO-SESAME** architecture contains the following hardware elements:

- An easy to implement and user-friendly server, acting both as configuration workstation and as operation workstation under a standard Windows graphical environment.
- TCP/IP over Ethernet network connecting Local Processing Units (UTL), modules and automated systems.

  Additional operation workstations (client workstations) can be deployed. The Wi-Fi connection ensures web-based operation through mobile or tablet devices.
- Local Processing Units connected to the TCP/IP over Ethernet network: **UTIL** for access control and BMS, **TILLYS** for intrusion, access control and BMS, and **PULSE** for PoE (power over Ethernet) access control.
- Specific modules offset onto secondary LPU buses: door modules, intrusion modules, BMS modules, video modules...
- Readers supporting different technologies are connected to these modules or directly to the UTiL, TILLYS and PULSE.
- Keypads, displays, sensors, detectors, measuring or counting devices connected to modules or LPU.



SECURITY FEATURES

MICRO-SESAME is an open system that offers a wide choice of features. Its configuration can be adapted to fit the exact needs of the end-user:

Online & Offline access control

- Supporting up to 4096 “online” badge readers that are monitored in real time, and an almost unlimited badge number.
- Individual access management by clearance or profile.
- Identifiers organized by site or entity.
- Badge customization (graphics, encoding, biometric scanning).
- Supporting different badge technologies and all access control reader types:
  - Proximity badge readers (125 kHz and 13,56 MHz. MIFARE, DESFIRE, ICLASS, …)
  - Long distance readers
  - Car plate readers
  - Online & offline mechatronic door locks
  - Biometry readers
- Commands to control different elements (barrier, strike plate, electric lock, video camera, etc.)

Intrusion

- Supervision using site plan graphical representation
- 40960 analogical or logical points on one or several sites
- Supporting all detection technologies (radars, contacts, infrared barriers…)
- Alarm acknowledgement and notification by operator category
- Automatism and interaction with other systems (video, access control)

Video

- Supervision of digital video recorders. Supporting main market providers (MILESTONE, GENETEC, GEUTEBRUCK, CASD...)
- Display and control performed on the same supervision device.

Specialized features

- Visitor management.
- Management of parking spaces, lifts, single passage detection systems.
- Area monitoring, emergency plan and crisis mode.

Many interfacing possibilities for third party hardware or software

- Key panels
- Fire centrals
- Matrix & video multiplexers
- Staff or directory management systems
- SMTP messaging …

BMS FEATURES

MICRO-SESAME is a system equipped with numerous **Building Management System (BMS)** features. **MICRO-SESAME** uses its own modules and LPU, but it can also monitor PLC and interface with numerous subsystems (air conditioning, heating, fire protection, etc.) over MODBUS, OPC and BACnet protocols. For further information, contact us.

Alarm processing

- Supervision with graphical animation for plans and synoptic diagrams
- Fire alarm processing
- Technical alarm processing: lift/air conditioning faults ...
- Acknowledgment of alarms assigned by operator category
- Set up of associated instructions

Energy management

- Consumption follow up
- Power (partial or total) consumption monitoring
- Exemption of zones, depending on the priority level and the contracted power
- Annual programming for the different monitored areas (up to 3 annual programs)

Lightning management

- Start/Stop command, hourly programming
- Configurable timer (for premises with irregular occupancy)

Management of heating, ventilation & cooling systems

- Start/Stop command, hourly programming
- Defining temperature parameters and operating regimes: frost protection, reduced, economy, comfort...
- Temperature report

Management of hot water for sanitary use

- Start/stop command, hourly programming
- Programming of operating modes: Automated, manual or programmed triggering

SYSTEM CAPACITY

Hardware settings	
Simultaneously connected client workstations	400
Drivers (lines) supported by polling	128
Polling-related processes (monitoring, automated systems)	32
Programmable modules (UTIL, TILLYS, PULSE)	1 024
UTiL or TILLYS on a single "UTiL over IP" line	255
Badge readers	4 096
Video recorders	256

Access Control Settings	
Users	Unlimited
Identifiers	Unlimited
Sites	128
Entities	128
Reader groups	Unlimited
Readers per group	1 024
Group/reader combination limit	20 480
Access areas	128
Clearance	256
Access visual control points	256
Patrolling itineraries	64

Supervision settings	
Variables (total)	40 960
Variables (per line)	8 192
Variables (categories)	64
Totalizers	2 048
Variables in a formatting chain	16

Operation settings	
Operators (centralised system)	Unlimited
TILLYS users (standalone system)	150

Access Control (user/ID records)	
Reader technology to associate to a badge record	4
ID per reader technology	99
Badge code length (LPU driver harmonization required)	32 char.
Site code length (LPU driver harmonization required)	32 char.
Customizable fields (size, case, length, assisted/required input, open text, etc.)	16
Downloadable fields (must not exceed 20 characters)	First and last name, first 6 f.

Schedules and holidays	
Schedules per site	128
Days per schedule	9 (week + holiday + exceptional day)
Time slots per day	4
Min. time slots	1 min.
Exceptional days	32

History	
History events	Unlimited (subject to DB features)
Max. event number per history request	Unlimited
Retention period	Default value : 30 days (Adjustable)

UTIL & TILLYS capacity	
Downloadable badges (subject to firmware)	5 000, 19 000, 40 000, 100 000
Readers per module (subject to firmware)	2, 8, 16

MODBUS equipment capacity	
Tables per line	512
Bit elements per table	128
Word elements per table	64

OPERATOR MANAGEMENT

Accurate management of MICRO-SESAME user rights

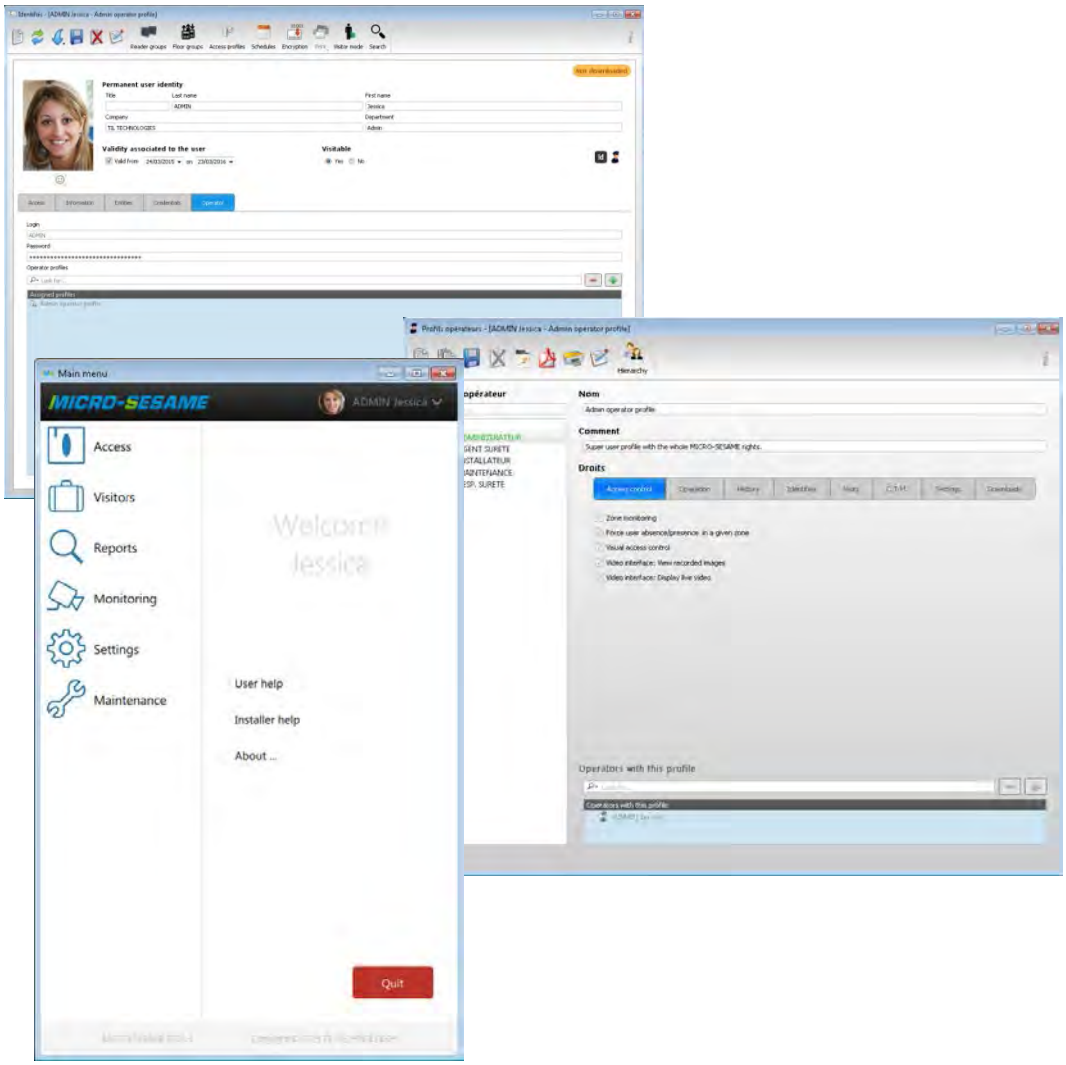
An operator is a physical person, authorized to use the **MICRO-SESAME** supervision interface. Depending on his role, his hierarchy or his geographical situation, an operator can access all or some of the **MICRO-SESAME** features (access control, set up…).

To assign only the necessary rights to each operator, **MICRO-SESAME** integrates the "operator profile" concept.

Profiles features are assigned by selecting different checkboxes, corresponding to the 5 main features:

- Access control (access control alarms, black list, video interface, area supervision)
- Operation (monitoring/polling, history, operator management, intrusion…)
- BMS (synoptic graphs, BMS alarms, tele commands…)
- Settings (operator management, access management, schedules, badge records, zones, authorizations, database exports...)
- Downloads (data that can be downloaded to the centrals)

Each declared operator needs to have one or several profiles assigned. Right management is made easier.



MULTI-SITE / MULTI-CLIENT MANAGEMENT

Physical or company-based operation

MICRO-SESAME manages up to 128 different sites under one single system. This feature can be helpful for any of the three situations below:

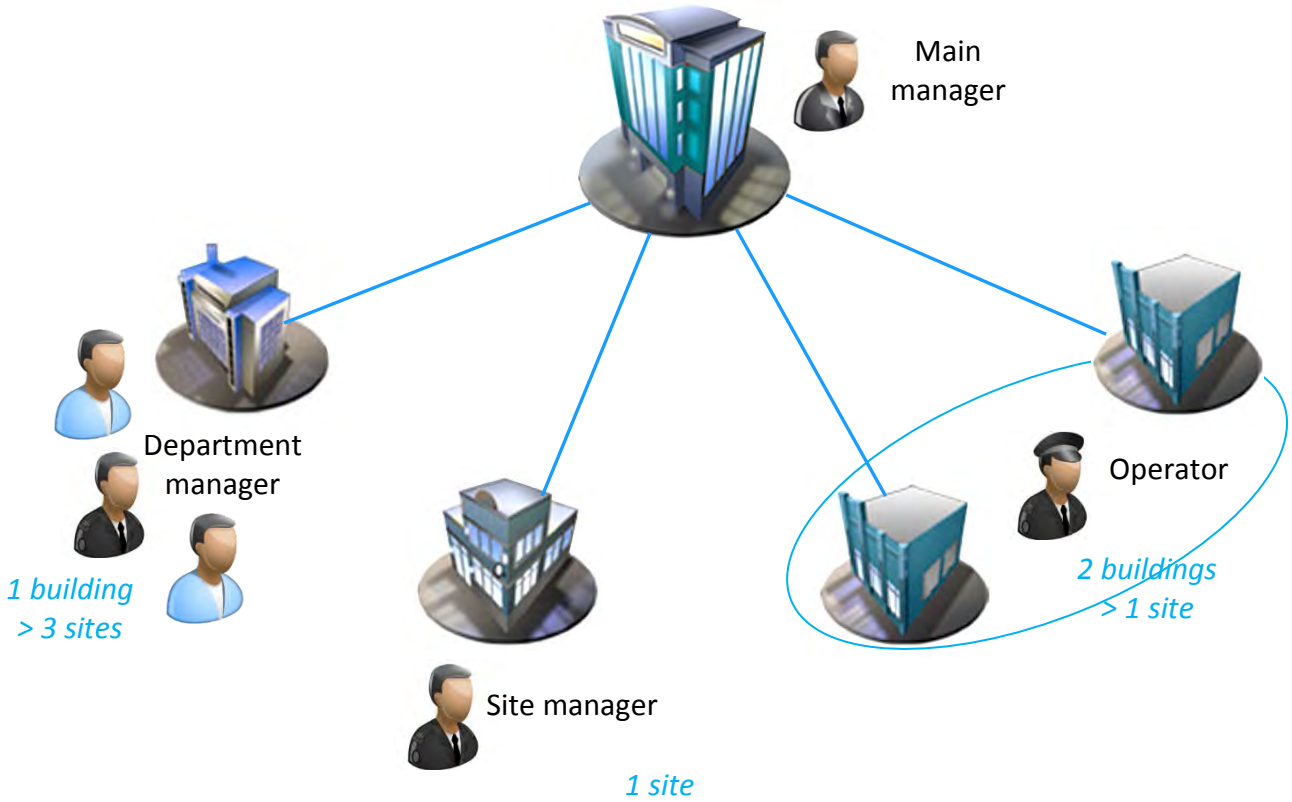
- Building management systems for sites that are geographically spread out: agencies from the same network, local communities, production sites...
- The need to keep right management at a department level in a site.
- A building hosting several companies: common and company-specific access must be kept apart.

Each entity can use up to 128 independent time schedules, used for access control or building management (alarms, automated irrigation...)

A multi-site configuration needs a main manager for the user database. This database is where IDs are created, deleted or changed.

The entity managers (services, sites or companies) manage access rights only for the IDs assigned to their own staff on their own sites, or for readers in common areas (if any), such as the entrance hall, parking spaces, lifts,...).

They can also check the access history records for their own staff. They will not be able to check readers, badges or history records for any other sites.



ACCES MANAGEMENT

Readers, schedules, profiles, clearance, areas...

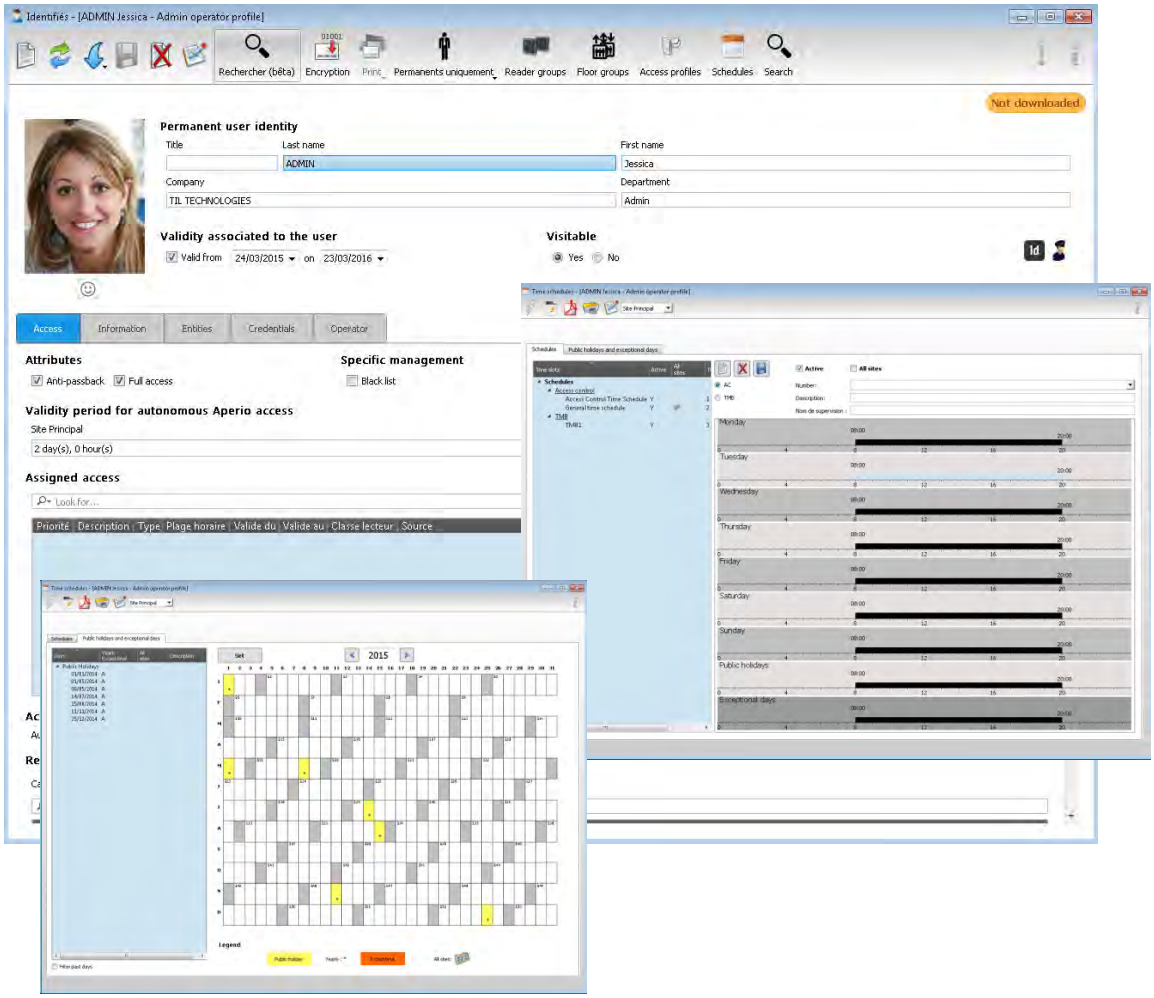
Individual access management

Access rights authorize the user to go through a reader or a reader group, depending on the defined schedules (128 different time schedules available).

Each user is associated to a validity period. The validity period makes possible to quickly activate (or deactivate) an ID, without the need to delete its actual granted rights.

The user/ID record contains and defines the following:

- Customizable user information: validity date, company, department, contact details as well as 16 additional customizable labels..
- User IDs: IDs can be set up using 4 different technologies (For instance, 13,56 MHz badges, 125kHz badges, keypad codes, car plate detection...). Each technology can store up to 99 different number or codes.
- Specific features such as master-key badges, anti-passback badges, blacklist (used for specific monitoring of stolen badges), clearance (crisis mode), visitor hosting…



Profile-based access management

Access profiles define access for a specific category of users. Access may apply to one or several sites.

Access profiles are composed by a list of readers/reader groups. Each reader/reader group can be associated to a different time slot.

Each user can be associated to one or several access profiles. Access profiles are not prioritized over individual access. That means that exceptions for individuals may be created by using reader-based access.

A "general" profile can be associated for common access. A "service" profile can be used for accessing particular areas or dealing with individual particularities (due role or hierarchical levels, for instance).

Area-based management

MICRO-SESAME contains a feature for managing geographical areas:

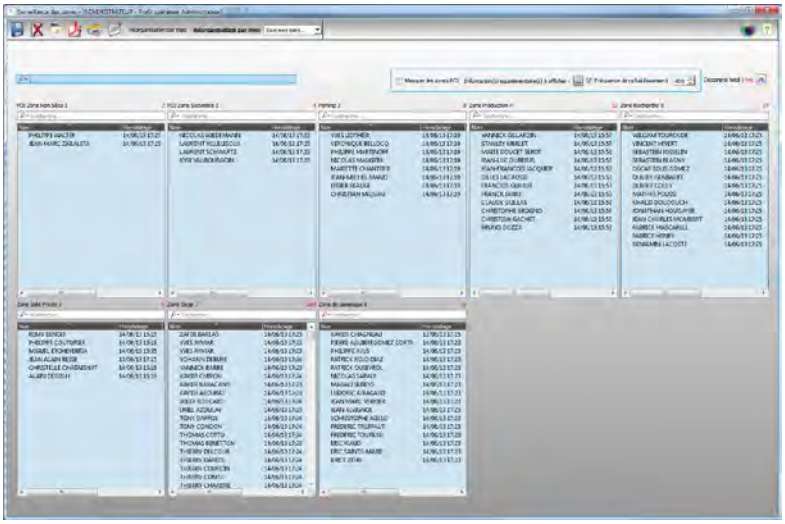
A reader list allows entrance to a particular area, and another reader list allows exiting the concerned area.

It is also possible to know the exact number of individuals present in each area. A list in alphabetical or chronological order can be created.

Widely used in SEVESO sites, area-based management is essential for integrating features such as the Emergency Plan.

Area-based management also ensures an exact passage control:

"Mandatory passage" areas can be set up, obtaining an exact passage control.



Clearance management

Access to specific zones or readers can be subject to obtaining a security clearance:

- electrical clearance ,
- EXAT,
- vehicle driving licence,
- temporary contracts...

This validity condition can be assigned and renewed by different people

(For instance, the HR department staff).

Up to 256 security clearance elements are available.

Each user can have several clearance elements assigned, each of them having its own validity period.

Each reader can also be associated to different clearance elements.

Reinforced security features

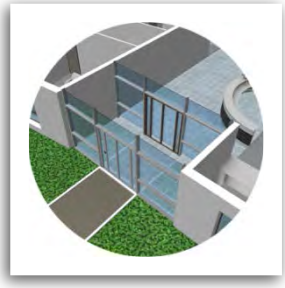
Anti-passback :

Sites using the area-based management feature and having entrance/exit readers can easily deploy an anti-passback mechanism.

This mechanism prevents people from entering a zone several times in a row without having left it before.

Single passage detection:

The single passage detection feature sets up inter-dependent doors. The system can be used to connect several zones. This feature can combine multiple technologies: contact mat, unicity mat, video recorder, biometric readers…



Reinforced control:

MICRO-SESAME offers the possibility use double security checks on certain readers. When reinforced control is used, authorized badges must be presented on readers, but also secret codes must be entered on keypads.

The codes used can be identical for all identiers, or customized for each user.

Duress code :

MICRO-SESAME immediately generates a silent alarm on the operator workstation after a duress code is entered.

"Blacklist" monitoring:

An alarm is triggered when a "blacklisted" badge is detected by any reader in the site.

Detecting a fraudulent attempt to use a lost or stolen badge may require a site intervention .

Crisis management:

MICRO-SESAME manages different crisis thresholds. Based on site specific criteria, 7 different crisis levels can be set as threshold values. Such thresholds can be applied to users (based on hierarchy, clearance…) or to readers (based on areas, alarm types…).

When an authorized operator triggers the crisis mode (which is generally integrated on a synoptic graph), each LPU in the system receives threshold update orders and matches user accreditations and reader security levels.

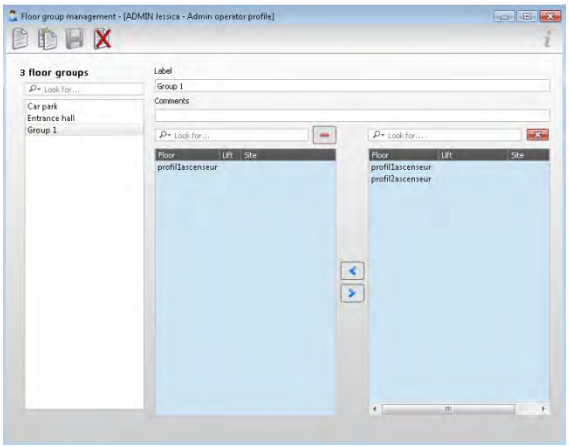
Lift management

In multi-site facilities, limiting access to particular floors can be obtained by installing badge readers inside the lifts in the building, by setting specific individual rights and/or by setting staff/entity profiles.

MICRO-SESAME natively manages the lift management feature. It is available from the user right interface.

Individual floors/groups of floors are considered as any badge reader in the building, and can therefore be part of any reader group or access profile.

On a multi-site facility, the main manager controls the common areas (entrance hall/ lower ground, parking spaces, cafeteria…). The main manager will administer the schedules concerning these common areas.



Companies hosted in the building will only be able to view information for their assigned floors. They will only be able to grant access to their assigned floors or to the common areas.

A dedicated central is required to benefit from the lift management feature.

Vehicle access and parking lot management

MICRO-SESAME can supervise specific readers, such as long-distance remote-controlled readers or license plate readers.

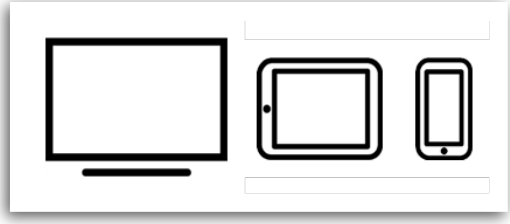
User comfort and vehicle flow -especially during rush hour- are made easier.

The integration to the **MICRO-SESAME** system is transparent: After detection, a number is sent to MICRO-SESAME, like any badge would do. Car plate numbers are directly managed on the User/ID record (An unlimited number can be associated per user).

As a result, the system is capable of providing data such as:

- the total vehicle number
- the total occupancy rate by staff type, department or company, if a common parking lot is shared
- the duration and occupancy rates for imputation or invoicing…

User management via the web interface



For a simplified access control, and in addition to the thick client and server interfaces, "light" web interfaces are available for managing visitors and users.

Any PC or mobile device equipped with an internet browser and a connection is able to display the new **WEB-SESAME** interface:

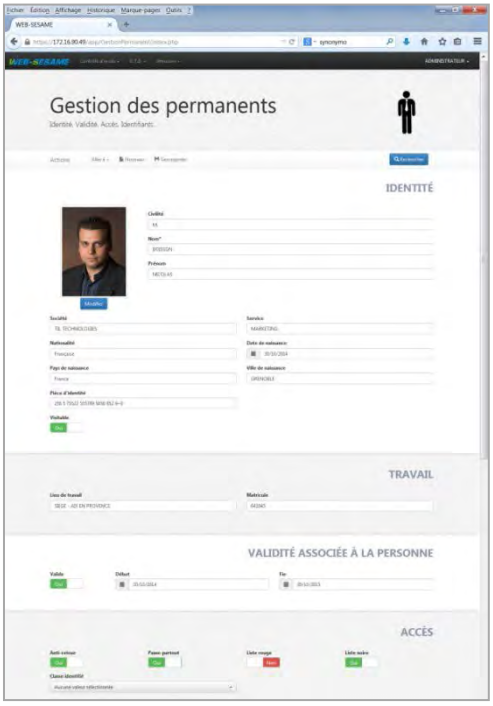
- Searching and displaying «User» records according to different criteria.
- Creating or changing records, adding a picture (via smartphone).
- Assigning pre-set access profiles.
- User import/export.

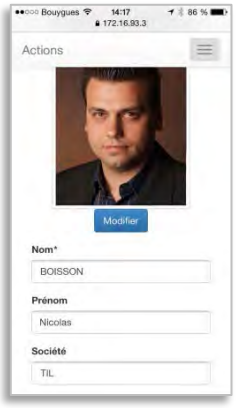
These features are also available for managing external visitor records.

A third interface displays meetings for external visitors.

Ergonomics in **WEB-SESAME** are optimized for tablets and smartphones:

- Auto-adaptive screens (resolution & layout).
- Field auto-completion and photo display.
- Checkboxes.





« OFFLINE » ACCESS CONTROL

Standalone mechatronic door locks

MICRO-SESAME natively manages the « offline » access rights diffusion logic. It applies to standalone mechatronic locks that are not connected to the system in real time. Access rights are directly encrypted using **MICRO-SESAME**. Validity periods must be defined.

Rights must be periodically loaded by presenting the badges on specific terminals that are connected to **MICRO-SESAME** (PoE IP connection).

The operator assigns rights for non-connected access in the same way as they would be assigned for online readers from the "user/ID" interface. No need to manage two different interfaces or databases.

Standalone access benefits, as any other site reader would, from the **MICRO-SESAME** features for multi-site management and access profile attributions.

Data escalations are performed as well.

Every time a user uses one of the right loading terminals, the following information is escalated to **MICRO-SESAME**:

- Badge history
- Low battery alarms.

The features of the offline terminal include:

Initial badge encoding does not need a dedicated workstation. It can be done just by presenting the badge to one of the right-loading terminals.

If connection is lost between the terminal and the **MICRO-SESAME** server, the standalone mode is activated (up to 40 000 users).

BADGE ENCRYPTION

Electrical customisation

The electrical customization (MS-ENCODBADGE) is a **MICRO-SESAME** software option allowing to write data to the chips and/or magnetic fields in proximity badges.

This software supports most encryption formats: MIFARE, DESFIRE EV1, ISOII, … by defining the ID format (decimal, hexadecimal, alphanumerical…) and the location (for ex., the MIFARE sector). IDs can be generated using MICRO-SESAME or be provided by a third party application.

Physical encoding can be individually or batch processed, using a table encoder or a badge printer (in case of simultaneous graphical customization).

Biometry management

With MORPHOACCESS biometry readers, biometry features are fully integrated to the **MICRO-SESAME** system:

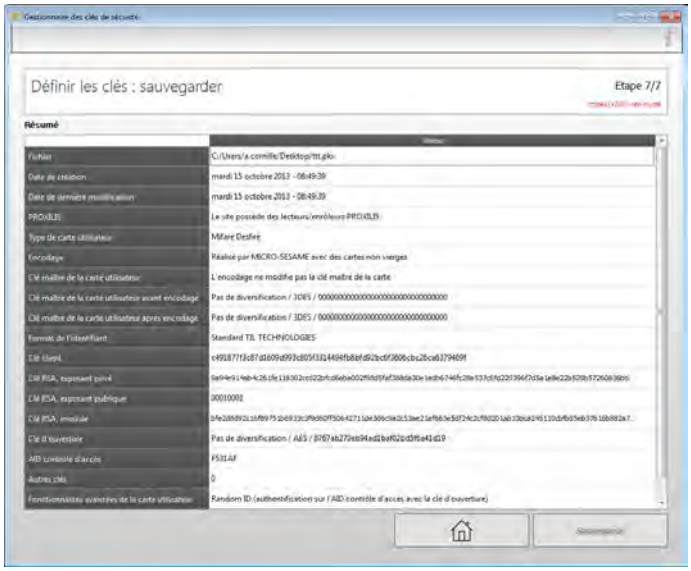
- Enrolment directly for the user record
- Immediate badge encryption

KSM secure encryption

The **KEY SECURE MANAGER** software is a key manager and a badge mapper. Secure customized encryption is provided to the final user:

- Defining sectors/memory inside the badge.
- Key configuration (depending on the format and the type of keys in use).
- Key generation.
- Creation of documents related to key management.

To perform physical badge encryption, this software must be associated to the MS-ENCODBADGE licence.



BADGE CUSTOMIZATION

Graphical printing

Badge customization (MS-PERSOGRAPH) is a software option in **MICRO-SESAME** allowing graphical creation (customized text, logo, photos, pictograms…) and thermal printing.

This option captures a photo from an existing file, a scanner, a video source or a webcam from the same network.

A graphical editor makes possible the customization of badge backgrounds and the setup of different labels (name, clearance…). Labels are compatible now with Arabic characters.

Pictograms representing specific authorizations for the badge holder can be added (electrical clearance, hazardous atmosphere, licences...)

MONITORING & SUPERVISION

Real time data, synoptic graphs…

Alarm, status and event management

Alarm and event processing can be fully setup in **MICRO-SESAME** and it can be adapted depending on:

- the type of information: access control, intrusion, fire, system...
- the concerned person: displayed in the interface of the concerned users.
- the associated directives: display, automatism, acknowledgement (auto video launch, specific text…).
- alarm schedules: Alarm escalated to the fire brigade during the day, and escalated to the Security responsible during the night.

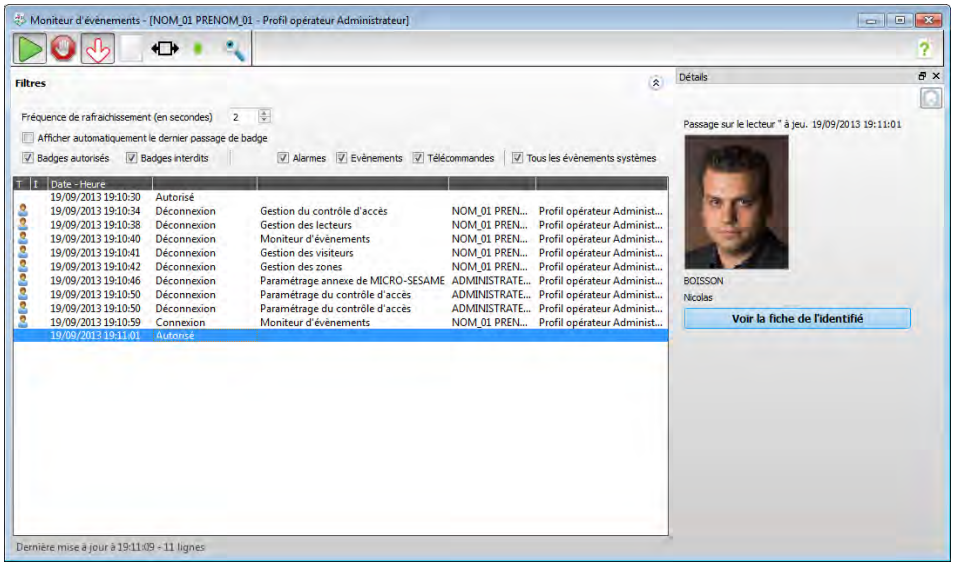
In any case, alarm information displayed, acknowledged and deleted are subject to a timestamp and archived to the database for future checks.

Interactive monitoring

Interactive monitoring displays events in real-time, using a colour code to signal the different type of events.

These events are clickable to signal an action (for ex: quitting a zone) or to perform a verification checks (for ex: photo checked when presenting a badge).

Real-time information display can be "frozen" to provide the necessary amount of time to check the events. This allows the responsible for event verification to view events happening before or after the checked event.



Synoptic graphs

The Synoptic graph option in **MICRO-SESAME** makes possible the creation of graphical views of a site.

All monitoring features can be easily integrated: alarms, logical status, numerical values, commands...

This representation can be composed of several screens, conceived as site arborescence (for instance, a floor-specific view of a building or a global view allowing to click onto each zone for details, etc.)

Each screen contains elements that can be:

- animated, depending on the status changes for the monitored equipment,
- actioned, using the mouse.

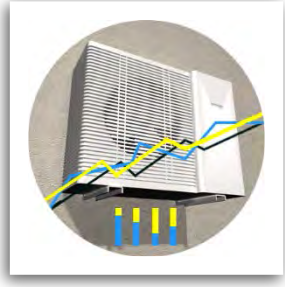
A synoptic graph editor adds page backgrounds and graphical objects and defines the link between the supervisor and the objects.

Curve management

Variable evolution is graphically displayed in **MICRO-SESAME** (up to 5 graphs can be displayed) during a defined period of time and using superimposed or juxtaposed curves.

The application can be launched from different **MICRO-SESAME** menus:

- History
- BMS monitoring
- Synoptic graphs



Values can be adjusted:

- Colours, background, lines, axis, thresholds.
- Scale (min., max., origin, graduations).
- Graph titles.
- Label for "Y".

VIDEO MONITORING

VISIO-SESAME

The **VISIO-SESAME** software option allows the dialogue with many digital video recorders. Using this interface, most of the current operations in video monitoring can be executed from any **MICRO-SESAME** workstation.

The available features include:

- Ability to select and display images from a camera by clicking on an operational synoptic diagram. The image is transmitted over the IP network.
- Viewing real time images, launching video recordings, controlling dome and video display matrix.
- Video actions subject to events/variables. For instance, positioning domes when unauthorized badges are detected.
- Checking and accessing images from the History feature in **MICRO-SESAME**. Information is synchronized (creating a single history file for access control, intrusion and video), making it easier to search for video sequences associated to a system alarm.
- Management of operational alarms (detection of activity by video) and functional alarms (loss of video signal or other issues) coming from the recorders.

Packaged video solutions proposed by TIL TECHNOLOGIES make easy to deploy pre-integrated video surveillance systems, including server and cameras.

Access video monitoring

When an access is equipped with a badge reader and a video camera, the MS-CVA option ensures the simultaneous display of the ID holder and the access video images.

An icon indicates the ID status (for instance, a badge is authorized, unauthorized, unknown).

Door opening can be manual or automated.

Other actions can be set up: turning on the lights, displaying a message, deactivating the intrusion detection on the zone…

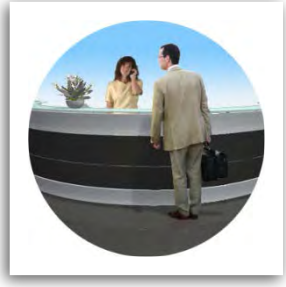
Interfaced solutions

The list of solutions, supported versions and accessible features is constantly evolving.

Before installing, compatibility must be confirmed by TIL TECHNOLOGIES.

VISITOR MANAGEMENT

Appointment planning and visitor hosting



The Visitor management feature is a software option in **MICRO-SESAME** to plan and manage the flow of external visitors in a site.

Composed of client workstations and web applications, it can be adapted to any type of organization:

The client version boosts **visitor hosting** procedures, allowing quick processing and visitor flow.

A web application can be used to **plan appointments.** It can be accessed from the company intranet, for instance..

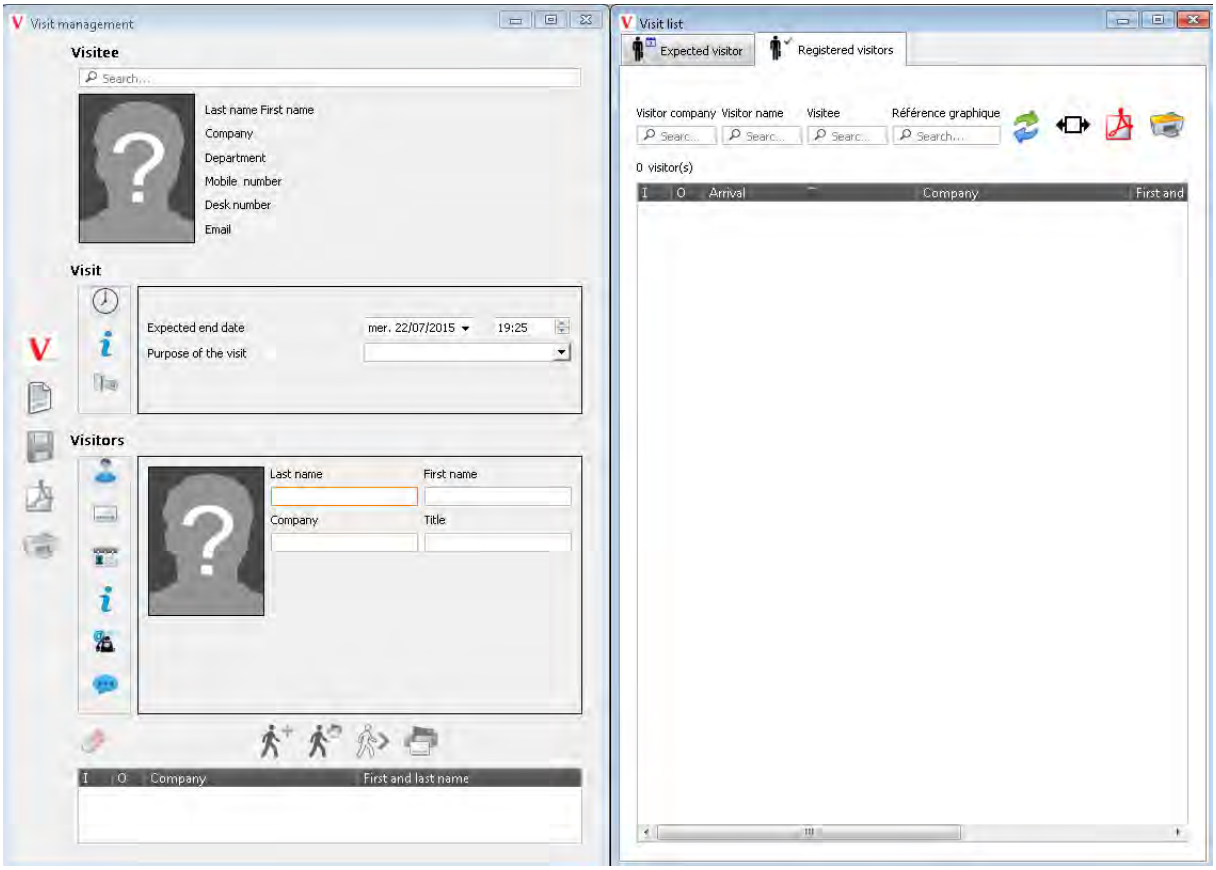
Both application versions can be operated from non-dedicated workstations.

Multi-site operation is possible by providing certain operators with granting access rights, based on management profiles.

The « Thick client » version needs a network connection to the **MICRO-SESAME** server. The web application needs an internet connection and a browser.

Visitor hosting (client workstation)

- Assigning visitor badges:
  - With our without prior reservation.
  - Access granted using visitor profiles (visitor parking,...).
  - Validity definition.
- Badge edition:
  - Badge customization (graphic chart, name, colour codes, other...).
  - Printing customized access record containing information such as the subject of the visit, signatures of visit validators, etc.
- Gateway with third party applications appointment planning, prevention plans, etc...
- An OCR reader can be connected to scan standard identity documents (ID cards, passports). And feed data directly to the software interface.
- The visitor hosting application is fed by the web-based appointment planning application.
- Visitors waiting and waiting times can be displayed.
- Temporary exit with temporary access deactivation (contractors, etc…).
- Viewing and finding on site visitors.
- Possibility to blacklist lost or not returned badges.
- Visit history, sorting, searching, editing or exporting to spreadsheets.



Web-based appointment and visitor management

The WEB-SESAME interface, accessible from any browser in site network workstations, does not require specific software. Two tabs are available, displaying two different interfaces:

- The **visitor** management interface, which is designed to register external visitor data. Access control features are simplified (compared to a MICRO-SESAME thick client), but adapted to the needs and the staff in charge of hosting visitors.
- The **appointment** management interface, which is designed to manage access granted to visitors and visitor hosting features.

INTERCOM

Intercom operation through MICRO-SESAME

The **MICRO-SESAME** generic text driver ensures communication with many different equipment types.

For instance, settings for COMMEND centrals perform most of the **standard communication operations** from any **MICRO-SESAME** workstation:

- Display of intercom calls on the master workstation.
- Two levels of data processing: urgent or regular communication.
- Call processing, interruption or cancelling.
- Total virtualization of the main workstation (microphone & speakers directly connected to the operating workstation).
- Communication between 2 workstations (button in the graphical supervision interface or keypad of the virtual main workstation).
- Remote listening.
- Main workstation calls transferred to other workstation (for instance, during the day/night shifts).

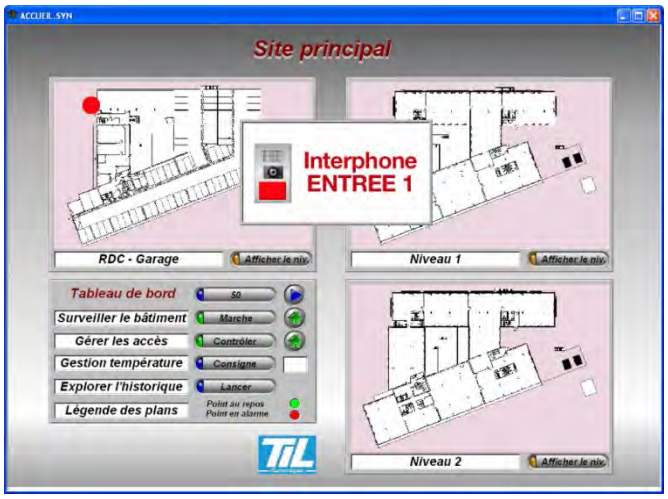
Interacting elements

By integrating intercom features in **MICRO-SESAME**, the communication features are controlled from the same graphical interface as the other building security systems (access control, video, BMS, etc).

Event-related actions can be completely automated. Operation becomes easier for users and efficiency is guaranteed.

For instance, intercom calls provide real time visual checks or are able to control lightning.

All calls and status changes are also traced in the **MICRO-SESAME** History feature.



EMERGENCY PLAN

Emergency and assistance interventions

The emergency plan defines the organizational measures, methods of intervention and the necessary resources for the operator to deploy in order to protect staff, citizenry and environment.

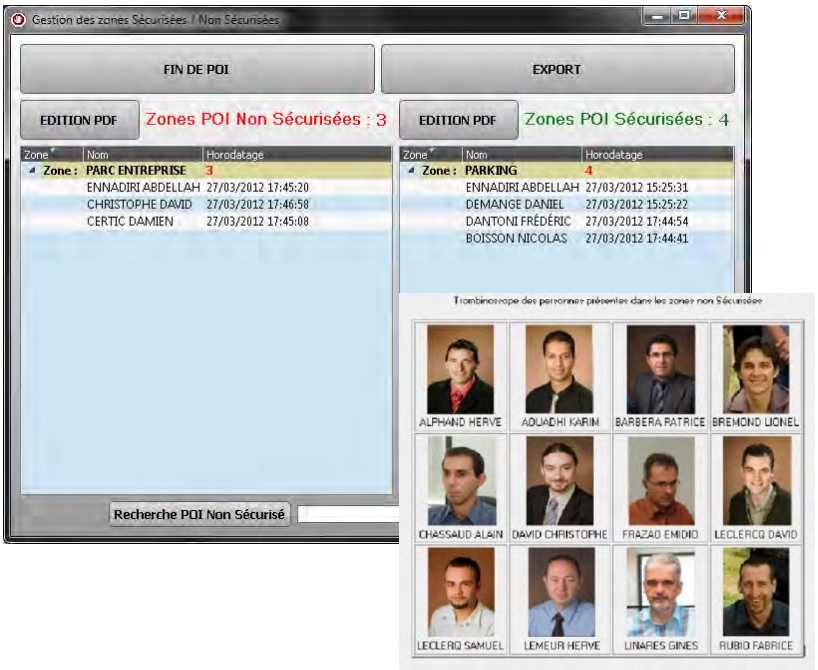
This feature is required for facilities presenting a high risk for humans and the environment, particularly for those facilities subject to a specific response plan.

MICRO-SESAME integration

The Emergency Plan feature in **MICRO-SESAME** helps protect site staff by deploying the following features:

- Providing a list of individuals present on site in real time.
- Real-time monitoring of staff moving from work areas to secure areas (meeting points) after triggering an emergency plan.
- Search for individuals to know their locations (check presence in a secure zone).
- Providing a list of individuals (and their photo) present in the selected areas.

This interface is displayed in priority during the whole evacuation process. The display of “Secure/Non-secure” areas is launched from a synoptic graph.



The MOBILIS mobile reader simplifies the headcount in gathering zones (secure zones). No need to install wired readers. Badges are now read by the evacuation wardens.

RESTING TIME MANAGEMENT

Ensuring compliance with local employment legislation

Employee resting times may be defined by local employment legislation or by company specific policies.

The resting time management feature in MICRO-SESAME ensures the employment legislation is respected by controlling the employee access to the workplace.

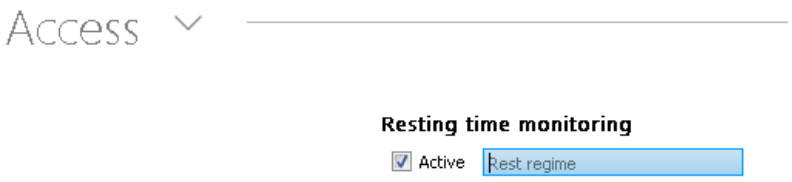
Badge data are automatically processed to calculate resting times and check if these were respected by employees.

Automated analysis ensures the following:

- Site access is temporarily blocked for those employees not following the defined site entrance and exit times.
- A notification is send to site operators. Data is displayed on the concerned user records.
- Reports are generated, anomalies are easily detected.

To setup this feature, entrance and exit readers must be declared. Week days and times must also be entered in order to be able to perform weekly and daily calculations.

Different resting regimes may be setup to fit to every site user needs. Resting regimes can be assigned using a gateway or using the MICRO-SESAME interface.



Once this feature is active, unauthorized access will be signaled as “out of schedule” access attempts. Such notifications will be displayed in the event monitoring and history features in MICRO-SESAME.

The temporary access ban is displayed on the user record. The date and time for the next authorized access is also indicated on the user record.

The temporary access ban may be manually removed by authorized operators.
In case of exceptional events occurring in the site, this feature can also be deactivated for the whole set of employees.

HR and security staff can perform global employee follow ups by using the report generator tool in MICRO-SESAME :

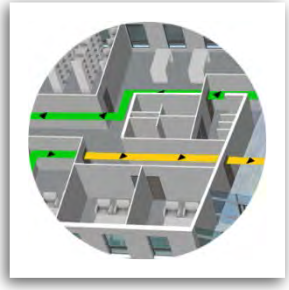
This tool generates reports based on weekly analyses.

A file containing « out of schedule » access attempts will be included in the report.

For further detail, check the History feature, the Report feature and the Report generator feature in MICRO-SESAME.

PATROLLING

On-site patrolling assistance



The patrolling management feature (MS-PCR) is a software option in **MICRO-SESAME** to track staff performing on-site patrolling on tertiary or industrial sites.

This option allows you to check the progress of the patrol (one or several staff members) performing on-site patrolling using the readers defined in the patrolling itinerary (64 different patrolling itineraries).

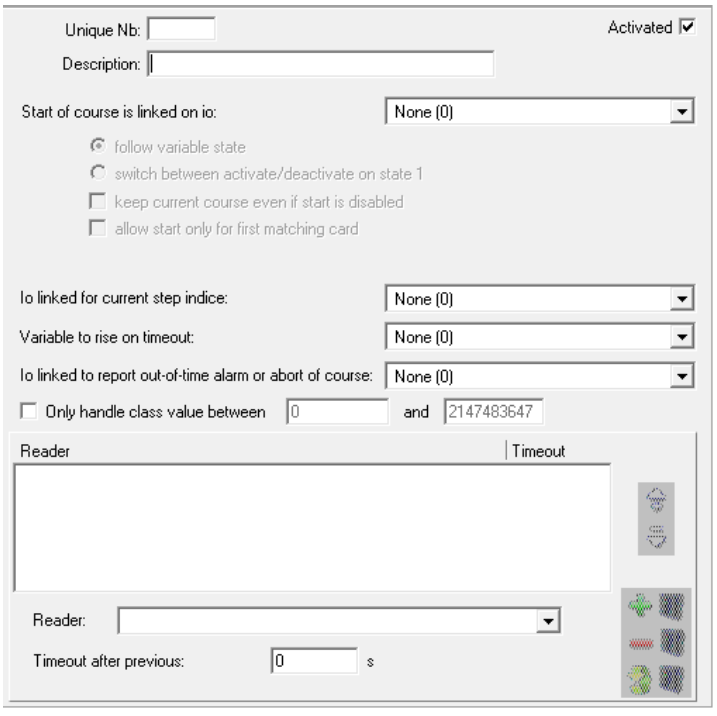
When the time required to go from one reader to another in the patrolling itinerary is exceeded and a badge was not presented on the next reader of the itinerary, an alarm is triggered flagging the concerned person and patrolling itinerary.

The presentation of the badge over the itinerary reader can be deferred, or the course can be halted.

All events are archived and the itinerary history can be checked (individuals, status, alarms...).

This feature can use any access control reader already available on-site.

No dedicated hardware is required.



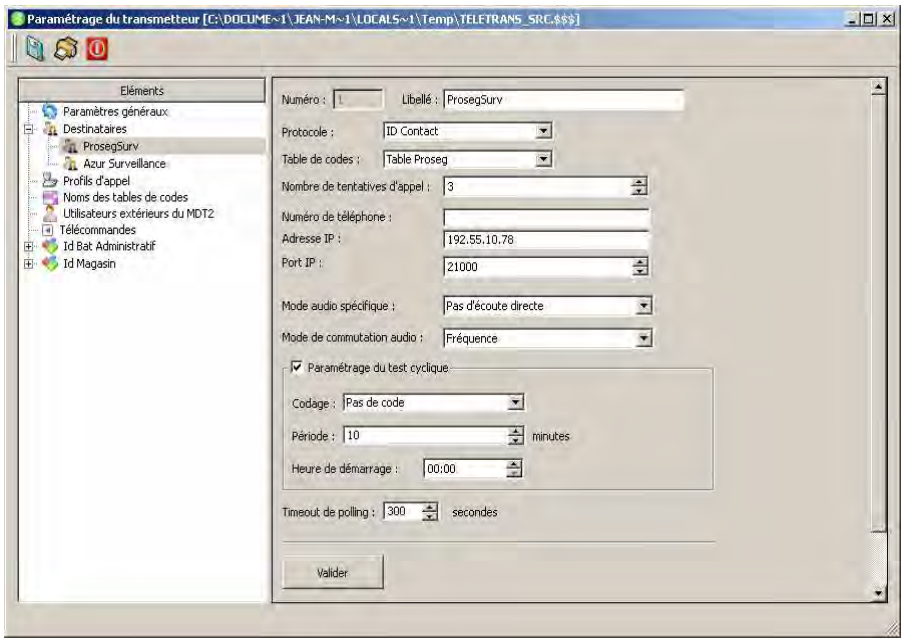
ALARM TELETRANSMISSION

The TELETRANS driver transmits alarms from **MICRO-SESAME** towards one or more remote monitors.

This software option merges the transmission of alarms from different systems using the IP or STN network.

TELETRANS transmits many more alarm points than any other intrusion unit in the market.

The system can manage thousands of transmission codes in ID-Contact or CESA 200 format.



The system can manage different alarm codes for the same alarm (**MICRO-SESAME** variable) **depending on the defined alarm recipients.**

This group of codes can be merged under various client identifiers for the remote surveillance device (for instance, a client code per site or geographical area).

Every alarm transmission can also be conditioned by the state of another MICRO-SESAME variable. For instance, transmitting alarms only at night or during monitoring periods.

TELETRANS works in a similar way as a TILLYS alarm central:

- 4 potential recipients for receiving alarms.
- 12 alarm transmission profiles.

HISTORY AND REPORTS

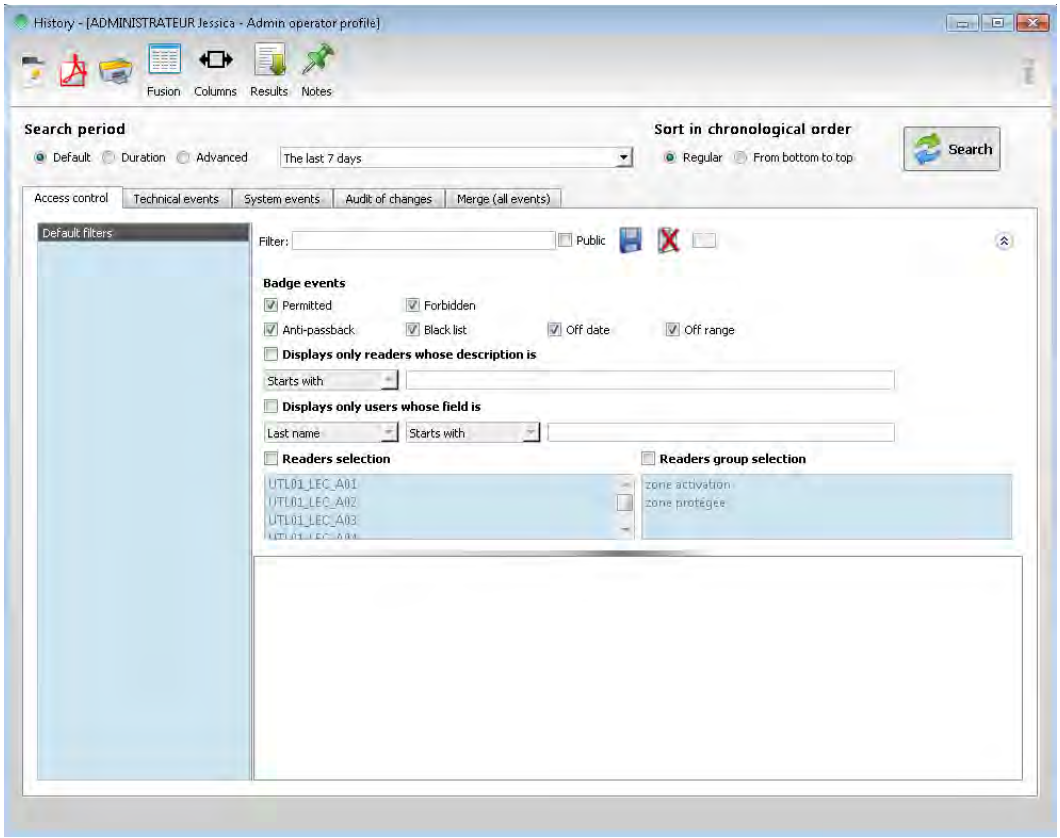
The History interface

The History interface displays any event in the database. It keeps track of site operations (badges read, technical alarms…), system operations and operator actions.

The storing capacity is unlimited. By default, event retention is set to 30 days, but this value may be adjusted.

Events are displayed using 4 different tabs matching different event classifications. A global view can also be displayed:

- Access control
- Technical events
- System events
- Audit of changes (operator actions).
- Fusion (all events)



For specific searches, detailed fields allow accurate event filtering. These fields are specific to each tab. The default search period contains the current date and time and includes the last 7 days.

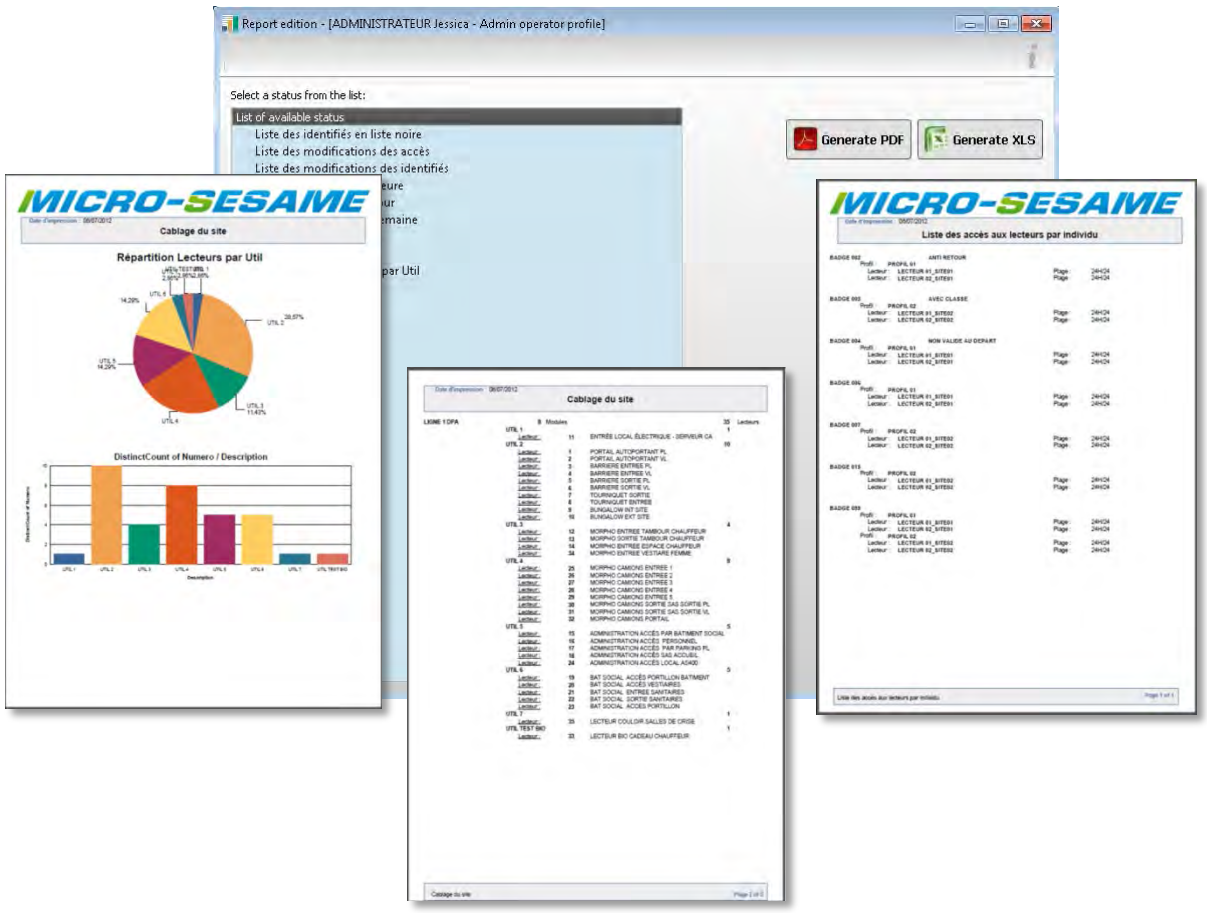
It is possible for users to save and name the different queries. Users will no longer need to enter the same criteria over and over.

Report generator

When using an SQL Database, default reports can be easily generated by using the Crystal Reports application.

These reports can be printed in PDF format (including graphs) or exported to a XLS file spreadsheet. .

Additional customized reports can also be generated. They can be generated with a Crystal Reports (Developer edition) license, or you can request them to TIL TECHNOLOGIES.



GATEWAYS & INTERFACES

Supervisors, BMS, fire, intrusion, display…

MICRO-SESAME includes different gateways for supervision of BMS, security or safety equipment and for communicating with other applications.

Standard IT protocols

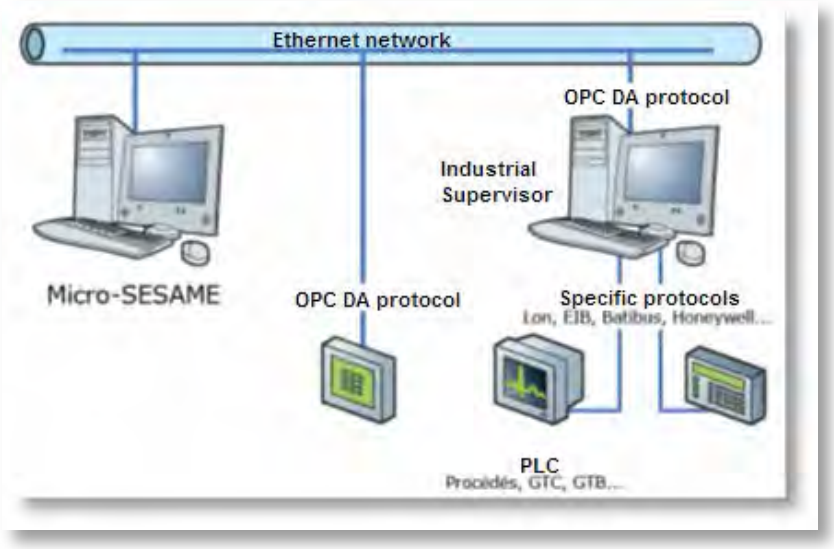
CTM systems or programmable logic controllers can be interfaced using the **MODBUS** mode:

- DIRIS (SOCOMEC)
- PCD-2 (SAIA BURGESS)
- CERBERUS fire centrals

MICRO-SESAME also supports **OPC**, the standard protocol used in automated systems to connect to CTM or BMS systems.

The following can also be interfaced:

- Supervisors
  - Panorama E2
  - Wonderware
  - Wizcon V 9.3
  - PCVUE 8.1r
- Programmable Logic Controllers
  - Schneider Twido OPC Factory Server 3.3
  - Schneider OPC RSLYNX
- Fire centrals
  - DEF Mezzo, Forte, Altaïr
  - Antares 4



MICRO-SESAME can also interface with PLC over the **BACnet** protocol. Contact us for further information.

Other technical interfacing systems

Third parties and hardware can be interfaced to **MICRO-SESAME** with the help of the MS-SYNC synchronization gateway or the text generic driver.

Contact your TIL TECHNOLOGIES representative for detailed information.

- AASTRA autocoms
- SCHINDLER elevators
- PROXSAFE key panels
- GORGY display panels
- MEMOGUARD on-call management
- Lone Worker Protection systems
- …

Honeywell
GALAXY

AASTRA

Schindler

SORHEA

deister electronic

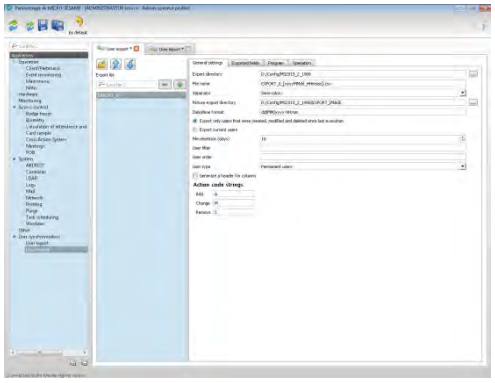
proxSafe®

H.R, management applications…

Data exchange between MICRO-SESAME and other existing databases may be necessary to align badge databases and staff databases.

Employees, providers or visitors are managed using a dedicated software for appointment or human resources management (Permanent or temporary contracts, retirement, etc.).

Automating the synchronisation of both the database and the access control system is particularly important when dealing with a large number of badges:



- Preventing duplicates, less time consuming processing
- Access (by role, department, etc.) is automatically assigned to individuals
- Staff changes are immediately updated

Automatic data recovery can be set up at specific times or after a source file is modified with the help of the different available gateways. Manual synchronisation is also possible.

MICRO-SESAME supports multi-source synchronisation (optional). Each of the sources can have specific synchronisation settings. In this case, the multi-source gateway option is strongly recommended.

LDAP directory

The **MICRO-SESAME** integrates an LDAP authentication feature. This feature ensures one single login for all applications accessed by a company user. Each user needs to be entered to the directory. A new field will then define the user rights.

Easy to maintain: When access rights are deleted or modified in the LDAP directory, access rights in MICRO-SESAME are automatically updated.

Messaging

MICRO-SESAME integrates a messaging feature sending alarm notifications via the SMTP gateway. Messages (intrusion, access control, technical alarms) can be dispatched via email or SMS.

SMS dispatch is not directly managed via MICRO-SESAME. An external service must be implemented.

Inter-system gateways

Data exchange over an IP network is available to exchange data between different **MICRO-SESAME** independent systems (UDP protocol). Data exchange is based on the variable name.

IT ENVIRONNEMENT

Depending on your system size, hardware and software recommendations are proposed. OS and DB supported versions are reviewed on a regular basis, as these may change depending on the MICRO-SESAME version.

Prior to any installation or migration, two specific documents must be checked. These contain the latest changes and are available from your TIL technologies representative.

- Latest OS and DB:
  - Windows 8 (64 bits) & Windows Server 2012 (64 bits)
  - SQL Server 2012 DB (64 bits)

- Adapted to« thin client » infrastructures
  - Supported by TSE & Citrix
  - No **MICRO-SESAME** installation required
  - Connection from any network workstation
  - Floating license / simultaneous connections

CITRIX®

Windows **TSE**

- VMWARE server virtualization
  - Recovery solutions
  - Server mutualisation
  - Energy saving
  - Software key

vmware

- Hardware redundancy
  - Supported by the SAFEKIT solution
  - **MICRO-SESAME** pre-set interface
  - **MICRO-SESAME** operating in continuous service

EVIDIAN
A Bull Group Company