BA | Business Area Security Solutions

Electronic Security

# SMI Server

## Version 3.0

## Features & Recommendations

A02005C

Smart Intrusion Solutions

**Electronic Security** Gunnebo
Electronic Security 23 route de
Schwobsheim 67600 Baldenheim
France
**www.gunnebo.com**
**www.smartintrusions.com**

GUNNEBO
For a safer world®

## Copyright

SMI Server V3.0: Features & Recommendations

*A02005C – 100024422 – Ed. 03 - DTD - June 2013*

**Electronic Security**
Gunnebo Electronic Security
23 route de Schwobsheim
67600 Baldenheim
France
**www.gunnebo.com**

*Visiting address:*
7 rue Paul Dautier
78140 Vélizy Villacoublay
France
Phone +33 810 000 800
Fax + 33 1 34 65 41 39

# Contents

# 1 SMI Server - Software specifications

## 1.1 Software environment

SMI Server V3.0 requires the following software environment in order to operate:

- Operating systems:
  - Windows XP SP2
  - Windows 2003 Server SP2
  - Windows Vista SP1
  - Windows 7 (32 & 64 bits) SP1
  - Windows 2008 Server (32 & 64 bits) SP2
  - Windows 2008 Server R2 (64 bits) SP1
- Database engines:
  - SQL Server 2005 SP3
  - SQL Server 2008
  - SQL Server 2008 R2
- Browsers & Web :
  - Internet Explorer 6 and higher

## 1.2 Software architecture

### 1.2.1 SMI Server

SMI Server is divided into several different software modules which can be run on different physical machines.

The following are required for a basic SMI Server installation:

- A database server for storing system data (configuration, logs, user profiles, etc.)

  ***Note:*** A SQL server can be used to manage the databases of several SMI servers.

- A security management service to act as an interface between the physical machines, the database and the MMI
- One or several MMIs are needed to configure and operate the system. Each MMI is connected to the database and to the security management server.

The following modules can be added to the system:

- IIS for creating new users and displaying logs via Internet Explorer
- The Map server for graphic map animations

### 1.2.2 Access Manager

Similarly, Access Manager is divided into the following software modules:

- A database server for storing Access Manager configuration data, as well as user profiles and families that have been set up across the system.
- Replication modules for synchronising the databases with the main workstations and Access Manager.
- IIS for creating new users, displaying logs and showing system status via Internet Explorer.

***Note :*** Access Manager can be installed on one machine which manages an SMI server. Similarly, the SMI server databases and Access Manager can be managed by one single SQL server.

## 1.3 Information exchange - Security

The various modules that make up the SMI server connect directly to the database using standard connection means. This means that SQL Server can be configured to manage encryption and limit access to the database.

The MMIs and the security management server communicate via a proprietary messaging system which, by default, uses encryption support.

Standard communication channels are used to communicate with Internet Explorer. These channels can be encrypted by activating the relevant option in IIS.

## 1.4 Description of ports used

The various ports used by the security management server are all configurable, and can easily be changed.

### 1.4.1 Ports used with Access Manager

| | SQL Server |
|---|---|
| Access Manager<br>(MMI) | SQL Server Ports<br>TCP: 1433<br>UDP: 1434 |
| Replication tool<br>SMI Server / Access Manager | SQL Server Ports<br>TCP: 1433<br>UDP: 1434 |
| IIS Service<br>TCP/IP<br>- Port used by default = 80 | SQL Server Ports<br>TCP: 1433<br>UDP: 1434 |

### 1.4.2 Ports used with SMI Server

| | SQL Server | SMI Server<br>(field server) |
|---|---|---|
| SMI Server<br>(field server) | SQL Server Ports<br>TCP: 1433<br>UDP: 1434 | --- |
| SMI Server<br>(MMI) | SQL Server Ports<br>TCP: 1433<br>UDP: 1434 | TCP / IP:<br>- Default port = 10001<br>- Corresponding service on the server: "Gunnebo SMI Server" |
| Replication tool<br>SMI Server / Access Manager | SQL Server Ports<br>TCP: 1433<br>UDP: 1434 | TCP / IP:<br>- Default port = 10001<br>- Corresponding service on the server: "Gunnebo SMI Server" |
| IIS Service<br>TCP/IP<br>- Port used by default = 80 | SQL Server Ports<br>TCP: 1433<br>UDP: 1434 | TCP / IP:<br>- Default port = 10001<br>- Corresponding service on the server: "Gunnebo SMI Server" |
| SM400, SM200, SM220<br>UDP:<br>- IP set by the automaton<br>- Default port = 6000 | --- | UDP:<br>- Fixed IP address<br>-Default port = 6001<br>- Corresponding service on the server: "Gunnebo SMI Server" |
| SMIT<br>UDP:<br>- IP set by the central unit<br>- Default port = 20000 | --- | UDP:<br>- Fixed IP address<br>-Default port = 20001<br>- Corresponding service on the server: "Gunnebo SMI Server" |
| PCI3 | --- | TCP / IP:<br>- Default port = 2999<br>- Associated application: "PCI3_NET.exe" |
| SI1/SI2 | SQL Server Ports<br>TCP: 1433<br>UDP: 1434 | --- |
| Event channel | --- | TCP / IP:<br>- Default port = 1511<br>- Corresponding service on the server: "Gunnebo SMI Server" |
| IDLock server<br>TCP/IP:<br>- Default port = 7000 | --- | TCP / IP:<br>-Default port = 7001<br>- Corresponding service on the server: "Gunnebo SMI Server" |

| | SQL Server | SMI Server<br>(field server) |
|---|---|---|
| Map management | SQL Server ports<br>TCP: 1433<br>UDP: 1434 | TCP / IP:<br>- Default port = 8045<br>- Corresponding service on the server:<br>" Map editor" |
| | | TCP / IP:<br>- Default port = 8045<br>- Corresponding service on the server:<br>" Gunnebo Map Server " |
| | | TCP / IP:<br>- Default port = 943<br>- Corresponding service on the server:<br>" Gunnebo Socket Policy Server " |
| | | HTTP:<br>- Default port = 8732<br>- Corresponding service on the server:<br>" Map editor & Gunnebo Map Server " |
| Software connector | | TCP / IP:<br>- Default port = 8050<br>- Corresponding service on the server:<br>" Gunnebo SMI Server " |
| Morpho server | SQL Server ports<br>TCP: 1433<br>UDP: 1434 | TCP / IP:<br>- Default port = 11010<br>- Corresponding service on the server:<br>" Gunnebo SMI Server " |

## 1.5 Volumetric analysis

### 1.5.1 Database

The database contains:

- System configuration data
- Access rights for users
- Maps and configuration files for devices
- Logs

Restoring the database makes it possible to reboot the system after a crash.

The following take up a lot of space in the database:

- User profiles, especially ones with a photo associated with them (profiles with photos take up 30kb)
- Logs (200 MB are needed to log 1 million events)

These volumes vary: the figures given here are based on real-life cases. Volumetric analysis can change a lot, depending on the type of data stored in the database (Quality of photos, event type, etc.).

### 1.5.2 Network

For the SM400, communication is via the UDP protocol. Common messages are of the following sizes:

- Polling: 120 octets. The polling time between each device can be configured on a per-device basis via the MMI
- Upload: the configuration is uploaded via a compressed file (zip). It is less than 500 kB for 50,000 users
- Communication recovery: Status exchange and command replication is carried out via a compressed file (zip). It is less than 20 kB in size
- All logs are processed via an exchange of messages of less than 150 octets

The sizes given are for data that was captured by a network sniffer (Etherreal) while the action in question was being executed. The overhead for IP and the management of the messages is therefore included in the values given.

A system that manages 256 SM400 units, each one of which sends out an access log every two seconds (i.e. 128 logs sent out per second) uses less than 15 kB of bandwidth on IP.

# 2 SMI Server – Architectures

As indicated in the previous paragraphs, SMI Server is made up of several software components:

- The database server
- The field server
- The Web Server (IIS)
- The operating interface

These different components can be installed on one or several machines, depending on the application load and target performance.

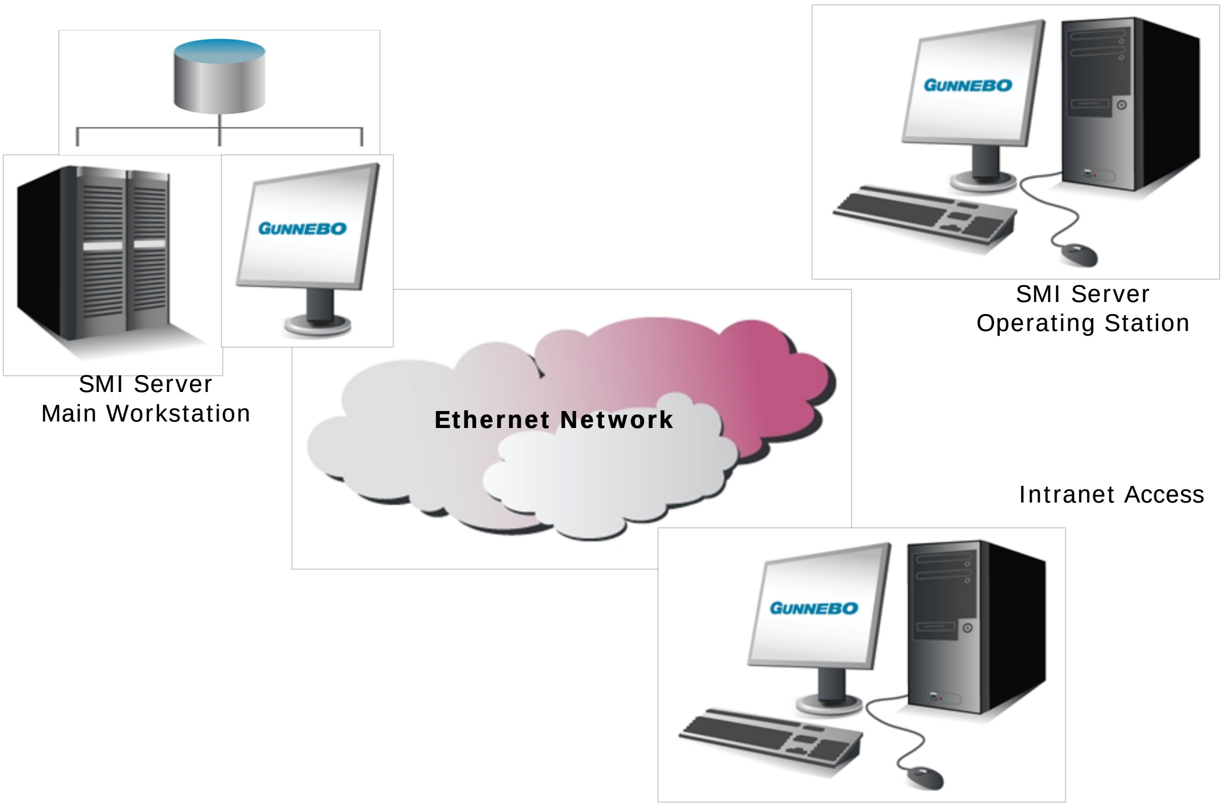
The different possible architectures are described in the following paragraphs.

## 2.1 "Simple" Mono SMI Server Architecture

The main workstation contains the following core applications:

- The database server
- The field server
- The Web Server (IIS)
- An operating interface

Additional operating stations can be added.

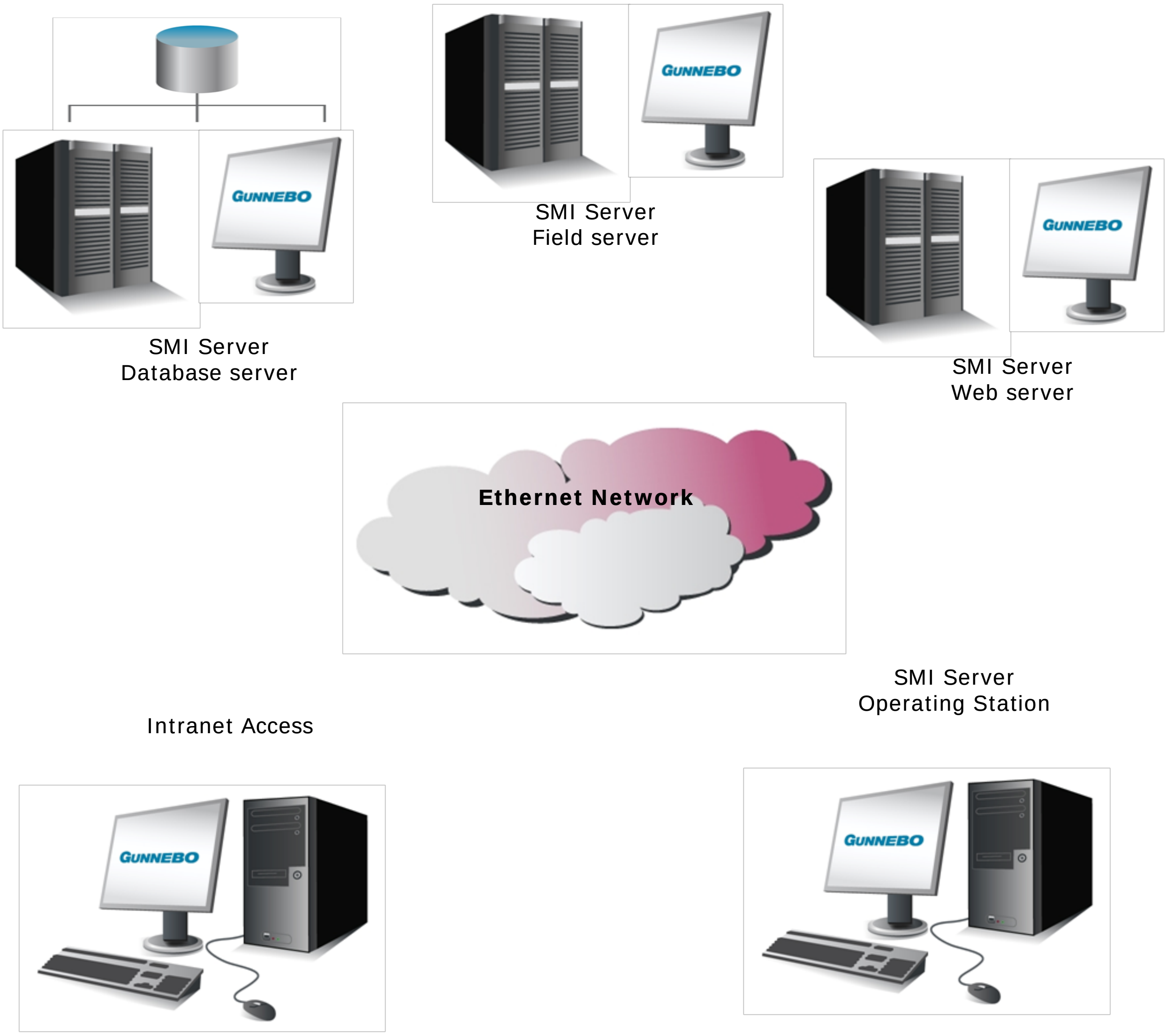


## 2.2 “Distributed” Mono SMI Server Architecture

With this kind of architecture, each machine serves only one function:

- The database server
- The field server
- The Web Server (IIS)
- The Operating Station

This architecture can be used to distribute the load across the system, thus improving performance.



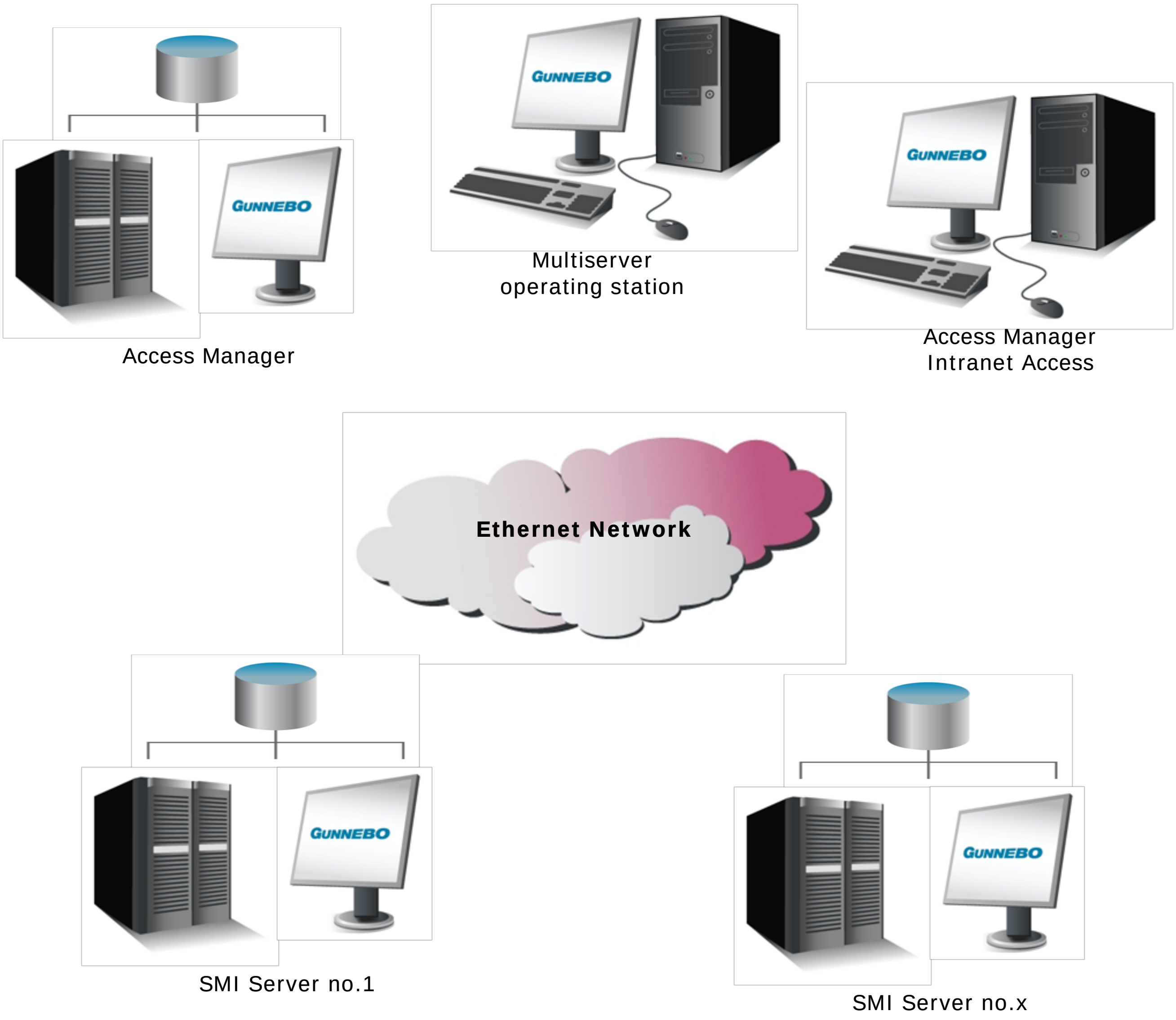
**Note :** In order to avoid having three servers (for cost-related reasons, for example), the Web Server can be installed on the same machine as the field Server.

## 2.3 Access Manager Multi SMI Server Architecture

This architecture is used for very large configurations, and/or multisite management needs.

**Note :** With this type of configuration, the ‘SMI Server’ systems can be designed as described above:
- *‘’Simple’ Architecture*
- *‘’Distributed’ Architecture*

**Note :** With this configuration, all the databases can be grouped together on one ‘"Database Server" machine



# 3 Various recommended hardware configurations

## 3.1 Server Configuration

- Intel Core i7
- 8 GB of RAM minimum
- 80 GB of disk space, 15,000 RPM, for the operating system and SMI Server
- Additional disk space for storing the database (to be provided)
- Screen resolution 1280x1024 – DirectX 10 compatible graphic board
- 100/1000 Mbps network card
- CD/DVD ROM drive

## 3.2 Configurations required for:
## - The workstations (creating cards & settings)
## - The MultiServer stations
## - The Access Manager station

- Intel Core i5
- 4 GB of RAM
- 80 GB of disk space, 7200 RPM, for the operating system and SMI Server
- Screen resolution 1280x1024 – DirectX 10 compatible graphic board
- 100/1000 Mbps network card
- CD/DVD ROM drive

## 3.3 Configurations required for workstations dedicated to Supervision

- Intel Core i7
- 8 GB of RAM minimum
- 80 GB of disk space, 7200 RPM, for the operating system and SMI Server
- Screen resolution 1280x1024 – DirectX 10 compatible graphic board
- 100/1000 Mbps network card
- CD/DVD ROM drive

## 3.4 Selecting machines and architectures

The specifications of the architectures/machines will depend on the flow of information managed by the system.

This section defines the following, depending on needs:

- The architecture type to implement
- The types of machine to use

The machines to use and the architecture to implement will be determined by a number of different factors. The most important are the following:

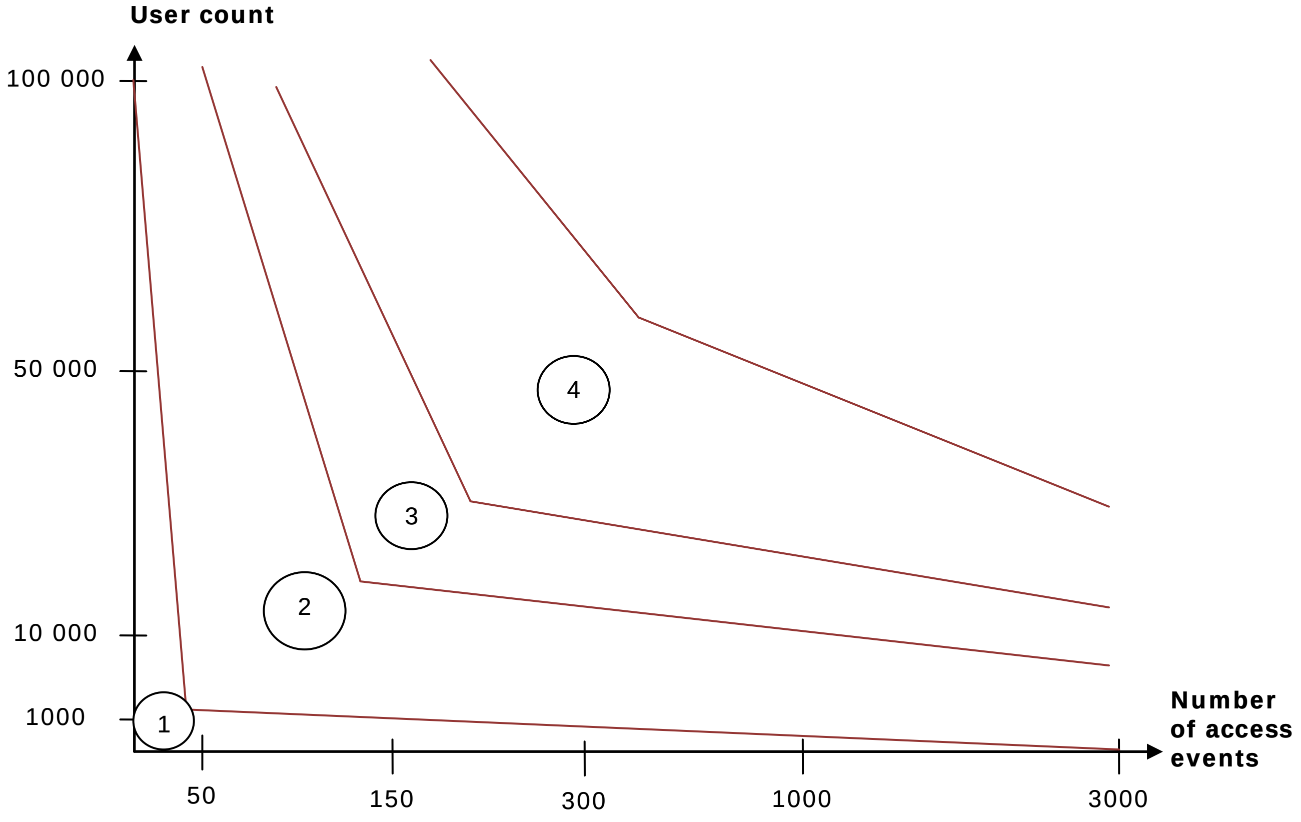
- Number of card swipes / minute
- Number of alarms / minute
- Number of visitor access events (number of visitors, and the number of access points at which they must present their cards)
- Number of operating & MultiServer stations

Some of these factors are difficult to get information for. For example, the ‘door position'-type and 'radar'-type sensors do not behave in the same way, and so do not have the same effect on the system. Let us try and provide an estimate nonetheless, in accordance with the following main criteria:

- Number of access events
- Users count
- Number of alarm points

***Note :*** “PC servers 1 & 2” can be:
- Either office-type PCs
- Or industry-standard PCs, designed to function as servers, and much more noisy as a consequence (but, they have room for 2 quad-core processors, 8 memory modules, 2 to 7 15,000 RPM hard drives, a Raid controller can be added, etc.).
Depending on the type of machines selected, it might be necessary to install the machines in dedicated IT rooms.

## 3.5 Users & Access



This illustration shows the type of configuration recommended depending on the number of access events and users:

- ***Conf. 1***: Architecture: "Simple" / Main workstation: "Server 1"
- ***Conf. 2***: Architecture: "Simple" / Main workstation: "Server 2"
- ***Conf. 3***: Architecture: "Distributed" / Servers: "Server 1"
- ***Conf. 4***: Architecture: "Distributed" / Servers: "Server 2"

An "Access Manager" multisite configuration is recommended for higher numbers of access incidents and users.

## 3.6 Influence of the number of alarm points

Using the "Users & Access" illustration, a rule can be established which expands the configuration depending on the number of alarm points.

| No. alar.<br>Basic Conf. | 1 000 | 2 000 | 5 000 |
|---|---|---|---|
| Conf. 1 | Conf. 2 | Conf. 3 | Conf. 4 |
| Conf. 2 | Conf. 3 | Conf. 4 | |
| Conf. 3 | Conf. 4 | | |
| Conf. 4 | | | |

## 3.7 Other influences

Other factors can affect the choice of system to be implemented:

- The number of web workstations is not a determining factor (they only involve connections to the database and not to the field Server).
- However, the number of operating workstations and MultiServer workstations, as well as the network load, are all factors which affect how the system is sized.
- Criteria based on the operating mode should also be taken into account: Monitoring mode (switching between graphics and/or corresponding video, regular alarm acknowledgement, etc.) or User Administration mode / cards / profile & access time. *For info*: It seems that a daily frequency modification > users | cards / hours of a large-scale operation activity, for which a type 2 server or distributed architecture should be recommended.
- If the system has to manage a high number of visitors (and these visitors all have to swipe their cards), additional resources will need to be added, as this will put a strain on the network.
- Factors associated with connecting the SMI Server system to external systems (via SI1, SI2 and/or an event channel). Depending on the type of these exchanges, the system's overall performance might be affected.

It is not possible to precisely quantify all of these factors in this document. A more detailed study has to be carried out on a case-by-case basis in order to determine all the parameters which might influence performance and recommend a suitable architecture.