# White Paper: Deploying Bosch Access Management System (AMS) on Intel NUC-Class Hardware

## Constraints and Limitations of a Small Form Factor Platform with Reduced Resources

Contents

## 1 Introduction

Bosch Access Management System (AMS) is designed and specified for server-grade hardware that fulfills or exceeds the requirements defined in the official AMS 6.1 datasheet. In some small or distributed installations, compact platforms such as Intel NUC-class PCs are requested to save space, power and cost.

This white paper outlines the main limitations and constraints when AMS is deployed on a NUC-class PC whose performance is lower than the recommended specification. It is based on internal validation activities using an AMS Lite-scale configuration and is intended to guide system designers, sales and product managers in correctly positioning such solutions.

## 2 Scope and Scenario

The scenario considered in this white paper is characterized by the following:

- AMS server and AMC communication components installed on a single Intel NUC-class PC.
- CPU performance below the level recommended in the official AMS server hardware specification.
- A small site (“AMS Lite”) configuration with a limited number of doors, cardholders and AMCs.

High-traffic, multi-site, or real-time critical security applications are not covered and should use fully compliant server hardware as described in the AMS installation manual.

The internal validation used a NUC-class device with these characteristics:

CPU: Intel N150, base frequency 800 MHz

Memory: 32 GB RAM

Operating System: Windows 11

AMS version: AMS 6.1

Because the CPU is significantly less powerful than typical server-class processors, CPU headroom becomes a central limiting factor when AMS, AMC communication and operator tools run on the same machine.

## 3 NUC-class PCs under 24/7 operation

Intel NUC-class mini PCs are generally suitable for continuous 24/7 operation, provided that certain technical and operational conditions are met. Intel explicitly defines continuous use (e.g., over multiple years at moderate average utilization) and requires that the original thermal design (cooling and fan configuration) remains unmodified.

### 3.1 Model Selection

Business, Pro, and especially embedded/industrial variants are recommended for continuous operation, as they are designed for sustained workloads and typically undergo more rigorous validation. Consumer models can also be used in 24/7 scenarios, but usually lack the same level of industrial robustness.

### 3.2 Key Factors for Reliable Operation

- Cooling & Power Management: Stable thermal conditions are critical. Adjusted power limits (PL1/PL2) and optimized fan curves help reduce temperature and component wear.
- Thermal Design (Active vs. Passive): Fan-based systems are prone to dust accumulation and mechanical wear, while fanless designs reduce maintenance but require stricter thermal constraints.
- Storage Selection: SSDs with high endurance (TBW) or enterprise-grade drives are recommended for continuous workloads.
- Operating Environment: Compliance with specifications (ambient temperature, airflow, power quality, ESD protection) is essential for reliability and warranty compliance.
- Maintenance & Monitoring: Regular cleaning, temperature monitoring, and SMART-based storage monitoring improve operational stability.

## 4 Recommended Configuration

For functional and performance testing, an AMS Lite- configuration is requested:

- 32 doors with mixed reader setup
- 1 MAC controller
- 16 AMCs
- 1,024 permissions
- 1000 cardholders
- 50 guard tours
- SDK connectivity enabled
- No Intrusion panels
- No Deister key cabinets
- No SSO offline Locks
- No Pegasys offline locks
- No SmartIntego Online locks

This configuration reflects a compact access control installation typical for small sites that are candidates for NUC-based deployments.

## 5 Conceptual Limitations of AMS on NUC

When AMS is deployed on a NUC-class PC with reduced performance, the following general limitations apply.

### 5.1 Restricted System Size

The platform is suitable only for small configurations, as described under 4. , and not for large or complex enterprise installations. System growth should be planned with a clear migration path to server-class hardware.

### 5.2 Narrow Performance Margin

CPU utilization can increase rapidly when access events, operator activity and background processes overlap. There is significantly less headroom for unexpected peaks than on server-class hardware, which increases the risk of temporary slowdowns.

### 5.3 Sensitivity to Configuration Choices

Enabling certain AMS features and tools on the same NUC, such as graphical map clients and extensive logging, has a strong influence on responsiveness and perceived system performance. Misconfiguration can lead to noticeable delays in the user interface and event presentation.

### 5.4 Unsuitability for Real-Time Intrusion Use Cases

While access control functions can operate correctly, real-time intrusion scenarios with strict response time expectations are not recommended on this platform. Frequent high-rate alarms and messages may no longer be presented in near real time when the system is heavily loaded.

## 6 Recommended Restrictions

### 6.1 Operator Tools and Graphical Clients

Running MapView on the NUC introduces a permanent CPU load even when the system is idle. When MapView additionally displays access alarms and dynamic symbols, the NUC's limited CPU capacity can become a bottleneck.

For installations that require many simultaneous viewers, MapView should be moved to a separate workstation with sufficient resources, and the NUC should be reserved for AMS server and AMC communication roles.

### 6.2 Logging and Antivirus Impact

Debug logging in AMS is resource-intensive and should be restricted to troubleshooting situations. Keeping debug logging permanently enabled on a low-performance NUC increases CPU usage and disk I/O load.

Real-time virus scanners that monitor AMS log and trace directories can further increase CPU and storage activity. If allowed by the customer's IT policy, these paths should be excluded from continuous scanning and limited to scheduled scans outside core operating times.

### 6.3 Access Event Load and Traffic Patterns

The NUC platform is intended for moderate access traffic typical of small sites. Strongly burst-like high event rates should be avoided, as they can overload the limited CPU resources.

Operational concepts should be designed to avoid artificial peaks, for example by planning shift start times so that not all cardholders pass doors within very short time windows.

### 6.4 Combined Operator and System Load

Heavy analytical or administrative tasks should be moved to a better equipped workstation or scheduled for times with low access traffic.