

Technical data

ENiQ Access Management

Devices supported:

Management of all DOM devices using 13.56 MHz technology:

- ENiQ Pro, ENiQ Pro V2 (BLE)
- ENiQ Guardian / ENiQ Guard / GUARD S
- ENiQ AccessManager / Terminal / ITT - V1 + V2 (BLE)
- ENiQ RF NetManager V1 + V2 (BLE)
- ENiQ Protector
- ENiQ LoQ

- No support for ELS 125 kHz end devices

Transponders supported:

- Mifare locking media
(types supported depend on mode of operation, see below)

System architecture:

- Web application (ASP.NET)
- Platform-independent client access via web browser without client installation
- Web server used: Microsoft IIS

Modes of operation:

“Conventional” offline operation:

Transponder UID is stored on the device:

- Wireless communication with the end devices via radio (868 MHz) or BLE (2.4 GHz) using USB radio stick.
- Use of the software with mobile notebooks or via DOM Service APP as programming devices

“Intelligent” offline operation:

Operation as virtual network (“intelligent transponders”):

- Authorisations are written to closing media using a DOM desktop reader
- In addition, transponder authorisations can be extended by ENiQ® AccessManager Terminal.

“Conventional” online operation:

This concept is intended for properties where authorisations often change or system events have to be represented directly for security reasons.

- Ethernet network (TCP/IP)
- Changes in authorisation are carried out by software and forwarded online to the end devices such as ENiQ AccessManager or ENiQ Guard®. Changes take effect promptly.
- Immediate door opening by ENiQ AccessManagement
- Activation of special functions by ENiQ AccessManagement

“Intelligent” online operation or mixed operation:

In addition, transponder authorisations can be rewritten online and extended through ENiQ® AccessManager ITT.

Technical data **ENiQ Access Management**

Mobile operation:
(e.g. as netbook/notebook)

When the server database is available (individual station installation or available connection to the server):

- Availability of the web application locally
- All data can be changed locally

Without connection to the server database:

- Windows application "ENiQ DeviceManagement" or "DOM Service APP" with simple, reduced-function user interface for offline synchronization of devices with the ENiQ AccessManagement Server database

User interface (GUI):

- Convenient and efficient interface
- User-specific adaptation through defined roles
- Languages: German, English, French, Dutch, Czech, Spanish, Italian

Modules:

Standard module:	Devices	Transponders
• Module S	max. 25	max. 100
• Module M	max. 125	max. 500
• Module L	max. 750	max. 3,000
• Module XL	max. 9,500	max. 32,000
• Module XXL	> 9,500	100,000

Intelligent transponder module:

- (additional) management and programming of intelligent transponders or virtual networks

Online module

- (additional) management and programming of DOM devices via Ethernet and RF NetManager (radio nodes).
- Modules available for the following numbers of devices: 5, 10, 25, 50, 100, >100

Mobile Keys module

- (additional) allowing authorised users to open devices with the smartphone, using the DOM Key app (iOS and Android)
- Available as yearly license, with packages of 5, 10, 25, 50, 75, 100, 250, 500, 750, 1000, 2500, 5000, 7500, 10000 and 20000
- The ENiQ AccessManagement software requires an Internet connection with the following URLs for operation:
 - <https://identitytoolkit.googleapis.com/>
 - <https://securetoken.googleapis.com/>
 - <https://login.tapkey.com/>
 - <https://my.tapkey.com/>

Technical data **ENiQ Access Management**

Database / data management:

Standard database:

- Microsoft SQL Server from 2019 (Express Edition 2022 is included in the scope of supply with the limitation: database size max. 10 GB)

Details: SA password necessary
 Network authorisation requires open ports TCP/IP 1433 +UDP 1434
 With online feature: TCP/IP + UDP Ports 47116-47119 (supports Microsoft SQL servers: 2012-2022)

Event storage:

- Device events are stored
- Selection and filter possibilities
- Time stamp accurate to the second
- Event export in pdf, xls, csv or rtf file format

Data export and import:

- Export of all data as pdf, xls, csv or rtf files
- Import of persons, locking media and devices (via ENiQ DeviceManagement)

Authorisation assignment:

Organisation of the devices in areas:

- Freely definable area hierarchy
- Inheritance of features to sub-areas and devices
- Displayed as tree structure

Organisation of the locking media or users in groups:

- Fast authorisation assignment for groups
- Mapping of organisational structures

Authorisation assignment:

- Allocation of authorisations for individual users, locking media or user groups
- Allocation of device and area authorisations

Storing authorisations in the end device:

- Transponder types supported:
 - Mifare DESFire / DESFire EV1+EV2+EV3 2k, 4k, 8k
 - Mifare Classic 1k, 4k
 - Mifare Plus S/X 2k, 4k
 - Mifare Ultralight / Ultralight C

- Storing of up to 5,000 authorisations in the end device
- Identification of the transponders via their UID

Storing authorisations on the transponders:

- Transponder types supported:
 - Mifare DESFire EV1+EV2+EV3 2k, 4k, 8k
 - Mifare Classic 1k

- Possible storage configuration Mifare Classic:

	Description	available from	Devices	Areas	Blacklist entries	Memory occupied (Bytes)
	A1	1k	112	240	6	896
	A2		32	512	0	896
	A3		192	0	6	896
	A4		176	48	6	896
	A5		160	64	6	896

Technical data **ENIQ Access Management**

A6	96	256	6	896
A67	80	240	6	768

- Possible storage configuration Mifare DESFire:

Description	available from	Devices	Areas	Blacklist entries	Memory occupied (Bytes)
B3	2k	64	64	8	1056
B4		240	240	8	1792
B5		256	256	8	1824
B6		48	48	8	1024
C2	4k	832	256	8	3616
C3		256	2048	8	4160
C4		512	512	8	2848
D1	8k	1408	2048	16	7200
D2		2048	256	8	7040
D3		1024	1024	16	5024

- Further data on the transponder:
 - "Blacklist" with blocked transponders
 - Authorisation period, week plan on the end device

Week and day plans:

- Storage of max. 252 freely definable week/day plans

- Every week plan references any 10 day plans (7 days of the week and 3 special days for public holidays/holidays):

1	2	3	4	5	6	7	8	9	10
Mon	Tue	Wed	Thu	Fri	Sat	Sun	Pub. holiday / holidays		
TP1	TP2	TP3	TP4	TP5	TP6	TP7	TP8	TP9	TP10

- Each day plan is made up of 96 time windows à 15 minutes, each of which must be defined as authorised or non-authorised:

0 ⁰⁰	1 ⁰⁰	2 ⁰⁰	3 ⁰⁰	...	20 ⁰⁰	21 ⁰⁰	22 ⁰⁰	23 ⁰⁰
■	■	■	■	...	■	■	■	■

- Access rights to day/week plans:
 - Plan 0: No access (not authorised)
 - Plan 1: Access unlimited in terms of time, active special functions restrict access
 - Plans 2-254: Freely definable
 - Plan 255: Access unlimited in terms of time, active special functions are ignored

Special functions

- Permanently open and permanently closed week plans
- Temporary authorisation (Office function)

Pub. holidays / holidays:

- Max. 256 public holidays or holiday intervals can be stored per device
- Definition of 3 different public holiday/holiday types
- Begin / end as from / to date

Technical data

ENiQ Access Management

Recommendations:

- Client/Server: No more than 20 permanently activated desktop readers should be used in the system.
- ENiQ AccessManager ITT: No more than 20 permanently activated ACM ITTs should be used in the system.

Installation note:

- Local administrator rights are required
- The automatic installation can be influenced by external software that has already been installed. If you have any problems, please call our service telephone to find a solution.

Operating systems supported / system prerequisites:

- MS Windows 10/11 Pro, 64-Bit only (Premium, Professional, Enterprise, Ultimate, not Home) or MS Windows Server 2014-2025 (Essential / Small Business)
- Not compatible with Citrix servers
- Note: at least Net Framework 4.5.2 (Windows update)
- Current standard web browser e.g. MS Edge, Mozilla Firefox, Chrome-Browser
- An internet connection is required for installation (to download Windows updates) and for using additional services like Mobile Keys
- Minimum screen resolution: 1024x768px (XGA)
Optimum: $\geq 1280 \times 768$ px WXGA
- Network speed for client/server: ≥ 100 Mbit
- The ENiQ AccessManagement software is incompatible with the following extensions: EXCHANGE-Server, WSUS-Server, Domain Controller

Recommended Server configurations:

Config – Minimal	Processor: i3 or compatible Windows 10/11 Pro 8 GB main memory 2 processor cores 50 GB HD (better SSD) MS SQL Server EXPRESS 2019
Config – Optimal	Processor: $\geq i7$ or compatible, XEON Windows 10/11 Pro, Windows Server Version ≥ 16 GB main memory ≥ 4 processor cores ≥ 100 GB SSD MS SQL Server STANDARD 2019 Virtual server, data center Backup System

Requirement-based server configuration:

Facility type	Config Minimal	Config Optimal
Offline conventional	X	
Online conventional <10 Online devices	X	
Online conventional <100 Online devices		X
Online conventional >100 Online devices		X
Offline intelligent < 100 Devices	X	
Online intelligent < 10 ACM, 0 RFNM	X	
Online intelligent < 4 ITTs, 0 RFNM	X	
Online intelligent < 10 RFNM + End devices	X	
Online intelligent > 200 RFNM + End devices		X
Online intelligent > 25 Desk reader		X
Online intelligent > 3 ITTs		X



*All specifications correspond to the current development status.
We reserve the right to make technical changes at any time.*