FOUR-DOOR ACCESS CONTROLLER — ETHERNET

IDE-DC300

The IDE-DC300 manages four doors and four readers from a single Ethernet-connected controller. Its field wiring uses pluggable screw terminals. For installations with doors cabled to a common point, it is available either as an enclosed controller or in a sheet-metal cabinet with an integrated power supply.

4
DOORS

4
READERS

40,000
CREDENTIALS

200,000
OFFLINE RECORDS

TWO ENCLOSURES, ONE CONTROLLER



150 × 130 × 27 mm

IDE-DC300

Four-door access controller, plastic enclosure; power supply not included

ENCLOSURE ABS, UL94-HB	DIMENSIONS 150 × 130 × 27 mm
POWER SUPPLY Not included	MAINS INPUT —
MOUNTING Surface-mounted, indoors	OPERATING TEMPERATURE 0 to +50 °C
HUMIDITY 10–90% RH, non-condensing	



300 × 320 × 75 mm

IDE-DC300-S

Four-door access controller, metal cabinet; integrated 60 W power supply

ENCLOSURE Sheet metal cabinet	DIMENSIONS 300 × 320 × 75 mm
POWER SUPPLY Included, 12 V / 5 A / 60 W	MAINS INPUT 100–260 VAC, 50/60 Hz
MOUNTING Wall-mounted, indoors	OPERATING TEMPERATURE 0 to +40 °C
HUMIDITY 20–90% RH, non-condensing	

Both variants contain the same controller electronics and report the same device type to the management software. The suffix identifies the cabinet and power supply. Photos are shown at approximately the same scale.

KEY FEATURES

Four doors on one controller
Four Form C relays, four independent Wiegand reader channels and six isolated inputs serve four doors. Each door has a reader LED and buzzer output. A single controller reduces the number of network connections and devices to configure and maintain.

Interlock decisions made locally
Door interlock is evaluated on the controller as part of the access decision. A door can be denied while another door in its interlock group is open or being granted access, without relying on a server round trip.

Access control continues during network outages
Credentials, permissions and schedules are stored on the controller. All four doors continue to make local access decisions while offline. The controller buffers up to 200,000 access events and sends them when connectivity returns.

Controller-wide emergency release
A configured input can hold all four doors in the released state for egress until the input condition clears.

Automatic card-format recognition

The controller recognises supported 26-, 34-, 35- and 37-bit formats, including HID H10306, H10304, Corp 1000, Honeywell/Northern and iCLASS. Raw-value fallbacks are available for HID Prox, Mifare CSN and iCLASS UID. Each reader can use a different supported card format.

Direct system integration

The controller provides both an HTTP server and an HTTP client. It can post live access events and buffered events to an external system, or an external server can retrieve them using a fetch-and-acknowledge exchange. The published protocol includes exact sample messages and a runnable reference receiver.

Remote firmware updates with automatic recovery

The management software can deploy firmware across a fleet. Updates can be applied automatically, with a configurable check interval and time of day, so that they are installed outside working hours. If the updated firmware fails to start, the controller automatically reverts to the previous working version.

Alarm functions are built into the controller

A motion sensor connects to a controller input and a siren is driven from a controller output. Alarm partitions are armed and disarmed by presenting a card at the door reader. There is no separate alarm panel to buy and no integration between two systems to build.

“Why did the door not open?” is answered in the log

When a request is refused, the reason is recorded with it: was the card unrecognised, does the user lack permission, was the attempt outside the permitted hours? Complaints and incidents are investigated directly from these records.

Every site is managed from one place

The controller opens the secure connection to the management server itself. No fixed public IP, port forwarding or VPN setup is required; controllers in different buildings and cities are managed from the same screen.

Pluggable field terminals

Field connections use 3.5 mm pluggable screw terminals. Each relay has NC, COM and NO connections, and each reader has a dedicated six-position terminal block. A terminal block can be unplugged when replacing the controller, without disconnecting its individual wires.

SPECIFICATIONS

CAPACITY

Credentials (cards, PINs and mobile)	40,000
Permission rules	5,000
Schedules	5,000
Usage-limited credentials	60,000
Offline access-event capacity	200,000

A card, PIN and mobile credential registered to one person count as three credentials. They share one identity, permission set and anti-passback position.

The controller’s behaviour when the log is full can be selected. Preserving the existing records means the oldest entries are never overwritten and new requests are refused; keeping access available means new events overwrite the oldest records. The first option gives priority to the existing audit history, the second to entries continuing and current events being recorded.

The maximum number of **permissions per person** is configurable. Higher limits reduce credential capacity as shown below:

Permissions per person	16	32	48	64	128	255
Credentials	40,000	40,000	29,000	23,000	12,500	6,500

DOORS, READERS AND I/O

Doors	4
Card readers	4 × Wiegand, independent channels
Relay outputs	4 × Form C (NC / COM / NO), dry (voltage-free) contacts
Max. switching voltage	30 V DC
Max. switching current	5 A
Inputs	6 × optically isolated, for dry contacts; configurable debounce
Reader outputs	8 outputs: 4 LED and 4 buzzer controls
On-board buzzer	Yes
Status indication	2 × addressable RGB LEDs
RTC	Battery-backed during power loss; synchronised by NTP

The relay contacts include transient suppression and are intended for low-voltage lock loads. Mains switching is not supported.

ACCESS CONTROL FUNCTIONS

Access decisions are made on the controller without a server round trip.

Door interlock (mantrap)	Any subset of the four doors can form an interlock group. Access at one door is denied while another group member is open or in an active grant cycle. The rule applies in both directions.

Multi-credential authorisation	Credentials from 2–8 different authorised people are required within a configurable 1-second to 1-hour window. Reader groups can be configured so entry uses two readers while exit uses one. Re-presenting the same credential does not count.
Anti-passback	Zone status is replicated directly between controllers without a server connection, allowing site-wide global anti-passback. Configurable per door. Hard and soft anti-passback are both supported.
Fire and emergency release	A configured input holds all four doors released for egress until the condition clears.
Alarm partitions	Scenarios are grouped into partitions. A partition is armed or disarmed with an authorised credential; motion in a disarmed partition produces no action.
Exit button	Any input can be configured as a direct exit-button input.
Door contact	Accepts a turnstile-rotation signal, and detects forced opening and doors held open, with a configurable timeout. If no door contact is fitted, its input remains available for another function.
Time schedules	Schedules, holidays and date ranges are evaluated on the controller.
Usage-limited credentials	A credential is valid for a fixed number of entries, counted per door.
Scenario engine	Rules stored on the controller, triggered at set times or by input state, door events and access events. A triggered scenario can run a relay for a set period, sound the buzzer, drive a relay on another controller, or arm and disarm another scenario.
Detailed access records	When access is refused the reason is recorded: unrecognised card, missing permission, use outside the schedule, exhausted usage allowance, anti-passback rule, inactive or expired record, facility-code mismatch, offline state, door interlock and authentication failure. Forced opening, doors held open and the return to normal are also recorded.
Facility-code check	An accepted facility code can be set per reader. A card whose code does not match is refused, and the reason is recorded as a facility-code mismatch.
Reader feedback	Separate LED and buzzer patterns can be defined per reader for accepted and refused attempts.
Card number format	The facility code and card number can be read as separate fields, or as the long number printed on the card.
Before clock synchronisation	Configurable behaviour before the clock is synchronised.
Offline behaviour	Configurable behaviour when the server is unreachable.

PER-DOOR SETTINGS

Each door can be configured independently for unlock pulse duration; relay mode (pulse, toggle or latch); default and power-restore states; early relock on door opening; an option to count access only when the door opens; door-open timeout; anti-passback mode and zone; interlock group; and usage counting.

INTEGRATION AND INTERFACES

On-board HTTP server	Accepts direct HTTP commands to release a door, read status, and read or change settings.
HTTP client — push	Posts live and buffered access events to an external server, along with heartbeats and input telemetry.
HTTP server — pull	Allows an external server to retrieve and acknowledge events in separate steps.
Management protocol	MQTT over TLS. The controller opens the connection; no open port, port forwarding or VPN is required.
Serial bus	RS-485, half-duplex; up to 500 kbps and 256 nodes; ±18 kV IEC ESD.
Also available	TCP and UDP
Discovery	mDNS / DNS-SD
Device health	Uptime, restart reason, processor temperature and memory status are reported.
Network rollback	If an incorrect static IP is applied the controller does not become unreachable; it reverts to DHCP.
Documentation	Published protocol specification, exact message samples and a runnable reference receiver.

COMMUNICATIONS

Ethernet	10/100, RJ45 with integrated magnetics, shielded
Wi-Fi / Bluetooth	Not fitted — wired installation
Data at rest	Encrypted on the controller

POWER

Input	12–24 V DC
Protection	Reverse-polarity, overvoltage and surge protection
Controller consumption	1.0 W typical, 3.1 W maximum — approximately 80 mA and 260 mA at 12 V
Reader supply	Same voltage as the controller input (12–24 V); 250 mA maximum per reader
Recommended supply	12 V / 2 A or 24 V / 2 A minimum
Backup battery	CR1220 coin cell; backs up the real-time clock (RTC) only; does not power the controller.

With four readers at 250 mA the controller draws about 1.26 A at 12 V, which is why 2 A is the recommended minimum.

The relay contacts are volt-free. The lock is powered from its own supply and the contact only switches it, so lock current is not part of these figures and must be provided separately.

The **IDE-DC300-S** variant includes a sheet-metal cabinet and an integrated 12 V / 5 A / 60 W supply (100–260 V AC, 50/60 Hz, 85% efficiency, EN 62368-1).

CONNECTION INTERFACES — 3.5 MM PLUGGABLE SCREW TERMINALS

TERMINAL	WAYS	SIGNALS
Power input	2	IN+, IN−
Relay 1–4	3 each	NC, COM, NO
Reader 1–4	6 each	D0, D1, LED, buzzer, IN+, IN−
Inputs	2 each	IN1–IN2, IN3–IN4, IN5–IN6
RS-485	2	A, B
Ethernet	RJ45	10/100, shielded

CABLE AND DISTANCE

CONNECTION	CABLE	MAXIMUM RUN
Wiegand data	Shielded AWG22 twisted pair	150 m
RS-485	Shielded AWG24 or heavier twisted pair; 120 Ω termination at both ends	1,200 m at the default 9,600 baud; approximately 200 m at 500 kbps
Ethernet	Cat-5e	100 m
Reader power	Distance depends on supply voltage drop; see below	—

Reader power. The reader draws from the controller supply. The maximum cable length is limited by conductor resistance. For a 12 V supply and a maximum 2 V voltage drop:

READER CURRENT	AWG22	AWG20	AWG18
100 mA	190 m	300 m	475 m
150 mA	125 m	200 m	315 m
250 mA	75 m	120 m	190 m

For long cable runs, check both the data limit and the reader power limit. Use the shorter distance. The terminals accept conductors up to AWG16, so a suitable cable can run directly to the controller.

MECHANICAL AND ENVIRONMENTAL SPECIFICATIONS

FEATURE	IDE-DC300	IDE-DC300-S
Enclosure	ABS, UL94-HB	Sheet metal cabinet
Dimensions	150 × 130 × 27 mm	300 × 320 × 75 mm
Power supply	Not included	Included, 12 V / 5 A / 60 W
Mains input	—	100–260 VAC, 50/60 Hz
Mounting	Surface-mounted, indoors	Wall-mounted, indoors
Operating temperature	0 to +50 °C	0 to +40 °C
Humidity	10–90% RH, non-condensing	20–90% RH, non-condensing
Ingress protection	Indoor use	Indoor use

The integrated power supply determines the narrower environmental range of the IDE-DC300-S variant.

ORDERING

IDE-DC300	**Four-door access controller, plastic enclosure; power supply not included**
IDE-DC300-S	**Four-door access controller, metal cabinet; integrated 60 W power supply**

Both variants contain the same controller electronics and report the same device type to the management software. The suffix identifies the cabinet and power supply.

WARRANTY

The product is warranted against defects in materials and workmanship for two years from the date of delivery.

The following are excluded from this warranty:

- The RTC backup battery
- Damage caused by surges, lightning, overvoltage or a supply outside the specified input range
- For IDE-DC300-S, the integrated power supply, which has a separate manufacturer's warranty

IDE Smart Teknoloji A.Ş

Bilişim Vadisi Muallimköy Mah. Deniz Cad. No: 143-8 C1 Blok Gebze, Kocaeli, Türkiye · info@idesmart.com · +90 (216) 909 0195