SINGLE-DOOR ACCESS CONTROLLER — POE AND CONFIGURABLE WI-FI

IDE-DC150

The IDE-DC150 combines Ethernet and IEEE 802.3af PoE in a single-door controller. It can also use an auxiliary 12 V DC supply for power continuity. Ethernet is the default network interface; Wi-Fi can be selected in the management software for sites that require a wireless connection.

1	1	40,000	200,000
DOORS	READERS	CREDENTIALS	OFFLINE RECORDS



IDE-DC150 ABS · 120 × 80 × 23 mm

KEY FEATURES

PoE for power and network connectivity
IEEE 802.3af PoE supplies the controller over the Ethernet cable. Where the installation permits it, this removes the need for a separate local controller power supply.

Two power inputs with automatic switchover
PoE and the auxiliary DC input can be connected simultaneously. A priority multiplexer selects the preferred source and switches to the other if it fails, without restarting the controller. Continuity of readers and locks also depends on how they are powered.

Ethernet with a configurable Wi-Fi alternative
Ethernet is the default network interface. The management software can select Wi-Fi as an alternative; one interface is active per boot. Network selection is configured in software and is distinct from the automatic power-source switchover.

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

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. Present a card to a reader on the site to enrol it through the software.

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.

Mobile credentials and local recovery
Bluetooth Low Energy (BLE) supports phone-based access alongside the card reader. It also provides a local route to correct network settings on site.

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.

Protected connection interfaces

The three inputs provide 5 kVrms optical isolation; the PoE front end provides 1,500 Vrms transformer isolation. Transient suppression is fitted to the power input, RS-485 lines and field connections.

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	1
Card readers	1 × Wiegand
Relay outputs	1 × Form C (NC / COM / NO), dry (voltage-free) contact
Max. switching voltage	30 V DC
Max. switching current	5 A
Inputs	3 × optically isolated (5 kVrms), for dry contacts; configurable debounce
Reader outputs	3 outputs for reader LED and buzzer control
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.

Multi-credential authorisation	Credentials from 2–8 different authorised people are required within a configurable 1-second to 1-hour window. 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.
Door interlock (mantrap)	Not available on this single-door model. See IDE-DC300.
Fire and emergency release	A configured input holds the door 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

Settings include 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; 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, shielded
Wi-Fi	2.4 GHz, on-module PCB antenna
Interface selection	One active interface per boot; Ethernet default; selectable in software
Bluetooth	Bluetooth 5 (LE) — mobile credential open, local recovery
Data at rest	Encrypted on the controller

POWER

PoE	IEEE 802.3af powered device, transformer-isolated at 1,500 Vrms
Auxiliary input	12 V DC
Protection	Reverse-polarity, overvoltage and surge protection
Source selection	Priority multiplexer, seamless switchover, no restart
Controller consumption	1.0 W typical, 2.2 W maximum — approximately 80 mA and 180 mA at 12 V
Reader supply	12 V DC, 1 A maximum
Recommended auxiliary supply	12 V; 180 mA for the controller plus the reader's consumption (up to 1 A)
Backup battery	CR1220 coin cell; backs up the real-time clock (RTC) only; does not power the controller.
PoE class	Class 3 (IEEE 802.3af Type 1), 12.95 W at the powered device

Class 3 reserves 12.95 W at the powered device. The controller uses up to 2.2 W of it (180 mA at 12 V); the rest is available to the reader.

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.

CONNECTION INTERFACES

Pre-fitted cable leads eliminate the need to assemble connectors on site. Ethernet and PoE connect through a shielded RJ45 socket.

LOOM	PITCH	CONDUCTORS
Reader and bus	1.25 mm	Wiegand D0, D1 · RS-485 A, B · IN+, IN−
Inputs and outputs	1.25 mm	OUT1, OUT2, OUT3 · IN1, IN2, IN3
Relay	2.5 mm	NC, COM, NO
Auxiliary DC input	1.25 mm	IN+, IN−

READER AND BUS 1.25 MM

1	Black	GND
2	Red	12–24 V IN
3	White	WIEGAND D1
4	Dark green	WIEGAND D0
5	Orange-white	RS-485 B
6	Orange	RS-485 A

INPUTS AND OUTPUTS 1.25 MM

1	Light green	OUTPUT 3
2	Green-white	OUTPUT 2
3	Blue	OUTPUT 1
4	Blue-white	INPUT 1
5	Brown	INPUT 2
6	Brown-white	INPUT 3

RELAY 2.5 MM

1	Brown	RELAY NO
2	Blue	RELAY NC
3	Gray	RELAY COM

AUXILIARY DC INPUT 1.25 MM

1	Red	IN+
2	Black	IN−

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. If the run exceeds the fitted lead length, select the extension cable gauge using the table above.

MECHANICAL AND ENVIRONMENTAL SPECIFICATIONS

Enclosure	ABS
Dimensions	120 × 80 × 23 mm
Mounting	Surface-mounted, indoors
Operating temperature	0 to +50 °C
Humidity	10–90% RH, non-condensing
Ingress protection	Indoor use

ORDERING

IDE-DC150	Single-door PoE access controller with configurable Wi-Fi

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

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