DIGITUS BIOMETRICS
Access Security Solutions

2019 PRODUCT CATALOG

2 East Bryan Street, Suite 502, Savannah, GA USA 31401 Phone: +1.912.231.8175 email: info@digitus-biometrics.com

TABLE OF CONTENTS

2 East Bryan Street, Suite 502, Savannah, GA USA 31401 Phone: +1.912.231.8175 email: info@digitus-biometrics.com

WELCOME TO DIGITUS BIOMETRICS

Because threats to data security are internal to organizations as well as external, securing physical access to server cabinets is essential. That's why corporations, military units, and intelligence communities rely on Digitus Biometrics.

Digitus invented the biometric swing handle lock in 2011, and kept going. Today, we offer the world's most flexible solution set for server-cabinet access control, with options for biometrics, proximity cards, smartcards, and PINs, including single- and dual-factor authentication. In thousands of installations, there have been zero security breaches through any Digitus solution.

Compatibility with third-party systems and cabinets preserves existing investments, and our patented technology delivers an indisputable audit trail. From a single platform, you can manage access points around the world and monitor them all in real-time

Simply put, Digitus Biometrics is the only solution available for 100% physical security of server cabinet access, in any configuration you need.

ZERO SECURITY BREACHES

In thousands of installations, there have been ZERO security breaches involving Digitus solutions.

REAL-TIME EVENT MONITORING

Real-time monitoring and reporting provide an indisputable access audit trail.

REGULATORY COMPLIANCE

Address physical requirements for compliance, including dual-factor authentication.

.

EASY-TO-USE CENTRALIZED ADMINISTRATION

Gain control from a centralized application that fully integrates with existing ACM platforms.

2 East Bryan Street, Suite 502, Savannah, GA USA 31401 Phone: +1.912.231.8175 email: info@digitus-biometrics.com

DIGITUS CABINET ACCESS OVERVIEW

Server Cabinet Access Control Featuring Single and Multi-Factor Authentication

Digitus cabinet locks are available in a range of formats, and providing both single and multi-factor authentication options. Featuring built-in audit trails, these lock systems automatically document every event – including which cabinets have been accessed, when they were accessed and which individual gained access.

KEY BENEFITS:

- Multi-factor authentication capable of combining keycard, biometric, RFID smartcard and PIN inputs
- Seamless enterprise access control integration
- Freedom to manage the system through a central software platform
- Convenience for both system administrators and end-users
- Built-in audit trail to meet regulatory compliance standards for physical access control
- Minimal hardware footprint within server cabinets

AVAILABLE AUTHENTICATION METHODS

Digitus server cabinet locks offer a flexible choice of cabinet authentication methods in a variety of configurations:

Single-factor Handles

- **Biometric**
  - **db BioLock -** fingerprint authentication
- **RFID Card**
  - **db ProxLock –** Prox card authentication
  - **db MultiCardLock-HF** – smartcard
  - **db MultiCardLock-HFLF** – smart/prox card
- **PIN**
  - **db KeypadLock** – PIN

Multi-factor Handles

- **db DualLock** – Fingerprint + smartcard
- **db CodeLock-HF** – PIN + smart/prox card
- **db CodeLock-HFLF** – PIN + smart card

db DualLock

db BioLock

db CodeLock/
db KeypadLock

db ProxLock

db MultiCardLock

db BIOLOCK

Card-free fingerprint biometrics authentication

db BioLock enables cardless access control, storing up to 10 biometric fingerprint templates per user per door

KEY PRODUCT FEATURES

- Works with both db Bus and db Sentry controllers
- Unlimited number of users
- Specify “duress” fingers
- Compatible with server cabinets from most major manufacturers
- Cost-effective & easy to implement
- Anti-counterfeiting features and enhanced encryption capability

TECHNICAL SPECIFICATIONS

DIMENSIONS:
- Height: 199 mm
- Width: 37 mm
- Depth: 24.5 mm

STATUS MONITORING:
- Built-in optical sensor to monitor handle position

OVERRIDE:
- Optional mechanical key (custom key cylinders available)

USE WITH:
- Digitus control equipment
  - db Bus
  - db Sentry

LED:
- Blue and Red

CABINET PANEL PREP
- 25mm x 150mm

db PROXLOCK

125 KHz proximity card authentication

db ProxLock authenticates industry-standard 125 kHz proximity cards for access control. Use the cards that currently authenticate for building/room access, extending their function to server cabinets.

KEY PRODUCT FEATURES

- Works with both db Bus and db Sentry controllers
- Simple integration with any 3rd-party ACM solution
- Unlimited number of users
- For use with low-frequency proximity cards
- Compatible with server cabinets from most major manufacturers
- Cost-effective & easy to implement
- Anti-counterfeiting features and enhanced encryption capability

TECHNICAL SPECIFICATIONS

DIMENSIONS:
- Height: 213 mm
- Width: 37 mm
- Depth: 24.5 mm

COMMUNICATION PROTOCOLS
- Digitus control equipment
  - RS232
- 3rd-party Access Panel
  - Wiegand

STATUS MONITORING:
- Built-in optical sensor to monitor handle position

OVERRIDE:
- Optional mechanical key (custom key cylinders available)

USE WITH:
- Digitus control equipment
  - db Bus
  - db Sentry
- 3rd-party Access Panels (via Wiegand)

CARD FORMATS:
- 26 bit Wiegand (H10301)
- 37 bit (H10302)
- 37 bit (H10304)
- 35 bit Corporate 1000

LED:
- Red and Blue

CABINET PANEL PREP
- 25mm x 150mm

QUICK DISCONNECT:
- Allows door to be easily removed without rerouting cables

db MULTICARDLOCK-HF

High-frequency (13.56 MHz) RFID smartcard authentication

db MultiCardLock authenticates any high-frequency (13.56 MHz) RFID smartcard for access control. Use the cards that currently authenticate for building/room access, extending their function to server cabinets.

KEY PRODUCT FEATURES

- Simple integration with all 3rd-party access control management (ACM) platforms
- Compatible with server cabinets from most major manufacturers
- Equipped with a tri-color LED, providing visual feedback
- Cost-effective and easy to implement
- Anti-counterfeiting features and enhanced encryption capability
- Capable of reading the following high frequency cards:
  - iClass SE/SR/Legacy
  - Mifare
  - DESFire
  - iClass Seos
  - PIV Card
- Capable of outputting Wiegand data
- Authenticate using custom RFID Keys
- Firmware can be dynamically updated for future feature enhancements

TECHNICAL SPECIFICATIONS

DIMENSIONS:
- Height: 270 mm
- Width: 44 mm
- Depth: 29 mm

STATUS MONITORING:
- Built-in optical sensor to monitor handle position

OVERRIDE:
- Optional mechanical key (custom key cylinders available)

INPUT POWER:
- Available in 12 or 24VDC versions

CURRENT DRAW:
- 40 mA Idle- 240 mA Max

USE WITH:
- Digitus control equipment
  - db Bus
  - db Sentry
- 3rd-party Access Panels (via Wiegand)

CARD FORMATS:
- iClass
- Mifare
- DESFire
- Seos
- PIV Card (75-bit and 200-bit)

LED:
- Green, Amber, Red

CABINET PANEL PREP
- 25mm x 150mm

db MULTICARDLOCK-HFLF

High-frequency RFID smartcard and low-frequency proximity card authentication

db MultiCardLock HFLF is a multi-class card reader that authenticates any high-frequency (13.56 MHz) RFID smartcard and low-frequency (125 KHz) prox card for access control. Ideal for locations that employ a mix of cards, as well as those that currently use prox cards but require a seamless migration to a more secure high-frequency smartcard platform.

KEY PRODUCT FEATURES

- Simple integration with all 3rd-party access control management (ACM) platforms
- Compatible with server cabinets from most major manufacturers
- Equipped with a tri-color LED, providing visual feedback
- Low power consumption
- Cost-effective and easy to implement
- Anti-counterfeiting features and enhanced encryption capability
- Capable of reading the following high frequency cards:
  - iClass SE/SR/Legacy
  - Mifare
  - DESFire
  - iClass Seos
  - PIV Card
  - Prox Cards
- Capable of outputting Wiegand data
- Authenticate using custom RFID Keys
- Firmware can be dynamically updated for future feature enhancements

TECHNICAL SPECIFICATIONS

DIMENSIONS:
- Height: 270 mm
- Width: 44 mm
- Depth: 29 mm

COMMUNICATION PROTOCOLS
- Digitus control equipment
  - RS232
- 3rd-party Access Panel
  - Wiegand

STATUS MONITORING:
- Built-in optical sensor to monitor handle position

OVERRIDE:
- Optional mechanical key (custom key cylinders available)

INPUT POWER:
- Available in 12 or 24VDC versions

CURRENT DRAW:
- 40 mA Idle- 240 mA Max

USE WITH:
- Digitus control equipment
  - db Bus
  - db Sentry
- 3rd-party Access Panels (via Wiegand)

CARD FORMATS:
- iClass
- Mifare
- DESFire
- Seos
- PIV Card (75-bit and 200-bit)
- Prox

LED:
- Green, Amber, Red

CABINET PANEL PREP
- 25mm x 150mm

db DUALLOCK

Dual-factor authentication with biometrics and high-frequency RFID smartcards

db DualLock enables dual-factor authentication at the cabinet door by combining fingerprint biometrics and RFID smartcard technology. By storing the fingerprint template(s) on the RFID card, db DualLock eliminates the requirement to uploading templates to the device, enabling it to integrate with any legacy access control management (ACM) system.

KEY PRODUCT FEATURES

- Simple integration with all 3rd-party Access Control Management (ACM) Platforms
- Unlimited number of users
- Store up to 3 fingerprint templates on the RFID smartcard
- Specify "duress" fingers
- Compatible with server cabinets from most major manufacturers
- Equipped with a tri-color LED, providing visual feedback
- Low power consumption
- Cost-effective & easy to implement
- Anti-counterfeiting features and enhanced encryption capability
- Authenticate using custom RFID keys
- Firmware can be dynamically updated for future feature enhancements

TECHNICAL SPECIFICATIONS

DIMENSIONS:
- Height: 270 mm
- Width: 44 mm
- Depth: 29 mm

COMMUNICATION PROTOCOLS
- Digitus control equipment
  - RS232
- 3rd-party Access Panel
  - Wiegand

STATUS MONITORING:
- Built-in optical sensor to monitor handle position

OVERRIDE:
- Optional mechanical key (custom key cylinders available)

INPUT POWER:
- Available in 12 or 24VDC versions

CURRENT DRAW:
- 60 mA Idle- 250 mA Max

LOCK CONTROL:
- Via 3rd-party ACM panel or Digitus control equipment

CARD FORMATS:
- iClass
- Mifare
- DESFire
- Seos
- PIV Card (75-bit and 200-bit)

LED:
- Green, Amber, Red

CABINET PANEL PREP
- 25mm x 150mm

db CODELOCK-HF

Dual-factor authentication with high-frequency RFID smartcards plus PIN

db CodeLock-HF enables dual-factor authentication at the cabinet door by combining high-frequency (13.56 MHz) RFID smartcard technology and personal identification numbers (PINs).

KEY PRODUCT FEATURES

- Simple integration with all 3rd-party Access Control Management (ACM) Platforms
- Unlimited number of users
- Compatible with server cabinets from most major manufacturers
- Equipped with a tri-color LED, providing visual feedback
- Low power consumption
- Cost-effective & easy to implement
- Anti-counterfeiting features and enhanced encryption capability
- Authenticate using custom RFID keys
- Firmware can be dynamically updated for future feature enhancements
- Capable of reading the following high frequency cards:
  - iClass SE/SR/Legacy
  - Mifare
  - DESFire
  - iClass Seos
  - PIV Card

TECHNICAL SPECIFICATIONS

DIMENSIONS:
- Height: 270 mm
- Width: 44 mm
- Depth: 29 mm

COMMUNICATION PROTOCOLS
- Digitus control equipment
  - RS232
- 3rd-party Access Panel
  - Wiegand (RFID Card)
  - 8-bit Burst (PIN)

STATUS MONITORING:
- Built-in optical sensor to monitor handle position

OVERRIDE:
- Optional mechanical key (custom key cylinders available)

INPUT POWER:
- Available in 12 or 24VDC versions

CURRENT DRAW:
- 60 mA Idle- 250 mA Max

LOCK CONTROL:
- Via 3rd-party ACM panel or Digitus control equipment

CARD FORMATS:
- iClass
- Mifare
- DESFire
- Seos
- PIV (75 or 200 bit)

KEYPAD:
- 12 keys
- Optional “Enter” key
- Use variable-length PINs

LED:
- Green, Amber, Red

CABINET PANEL PREP
- 25mm x 150mm

db CODELOCK-HFLF

Dual-factor authentication with high-frequency RFID smartcards and low-frequency prox cards plus PIN

db CodeLock-HFLF enables dual-factor authentication at the cabinet door using both cards and personal identification number (PINs). Authenticates high-frequency (13.56 MHz) RFID smartcards and low-frequency (125 KHz) prox cards, ideal for locations that employ a card mix and those that currently use prox cards but require a seamless migration to a more secure high-frequency smartcard platform.

KEY PRODUCT FEATURES

- Simple integration with all 3rd-party Access Control Management (ACM) Platforms
- Unlimited number of users
- Compatible with server cabinets from most major manufacturers
- Equipped with a tri-color LED, providing visual feedback
- Low power consumption
- Cost-effective & easy to implement
- Anti-counterfeiting features and enhanced encryption capability
- Authenticate using custom RFID keys
- Firmware can be dynamically updated for future feature enhancements
- Capable of reading the following high frequency cards:
  - iClass SE/SR/Legacy
  - Mifare
  - DESFire
  - iClass Seos
  - PIV Card
  - Prox

TECHNICAL SPECIFICATIONS

DIMENSIONS:
- Height: 270 mm
- Width: 44 mm
- Depth: 29 mm

COMMUNICATION PROTOCOLS
- Digitus control equipment
  - RS232
- 3rd-party Access Panel
  - Wiegand (RFID Card)
  - 8-bit Burst (PIN)

STATUS MONITORING:
- Built-in optical sensor to monitor handle position

OVERRIDE:
- Optional mechanical key (custom key cylinders available)

INPUT POWER:
- Available in 12 or 24VDC versions

CURRENT DRAW:
- 60 mA Idle- 250 mA Max

LOCK CONTROL:
- Via 3rd-party ACM panel or Digitus control equipment

RFID CARD FORMATS:
- iClass
- Mifare
- DESFire
- Seos
- PIV (75 or 200 bit)
- Prox

KEYPAD:
- 12 keys
- Optional “Enter” key
- Use variable-length PINs

LED:
- Green, Amber, Red

CABINET PANEL PREP
- 25mm x 150mm and 50/50/50

db KEYPADLOCK

Authentication with PIN

db KeypadLock enables single-factor authentication at the cabinet door using personal identification numbers (PINs).

KEY PRODUCT FEATURES

- Simple integration with all 3rd-party Access Control Management (ACM) Platforms
- Unlimited number of users
- Compatible with server cabinets from most major manufacturers
- Equipped with a tri-color LED, providing visual feedback
- Low power consumption
- Cost-effective & easy to implement
- Anti-counterfeiting features and enhanced encryption capability
- Firmware can be dynamically updated for future feature enhancements

TECHNICAL SPECIFICATIONS

DIMENSIONS:
- Height: 270 mm
- Width: 44 mm
- Depth: 29 mm

COMMUNICATION PROTOCOLS
- Digitus control equipment
  - RS232
- 3rd-party Access Panel
  - 8-bit Burst (PIN)

STATUS MONITORING:
- Built-in optical sensor to monitor handle position

OVERRIDE:
- Optional mechanical key (custom key cylinders available)

INPUT POWER:
- Available in 12 or 24VDC versions

CURRENT DRAW:
- 60 mA Idle- 250 mA Max

LOCK CONTROL:
- Via 3rd-party ACM panel or Digitus control equipment

KEYPAD:
- 12 keys
- Optional "Enter" key
- Use variable-length PINs

LED:
- Green, Amber, Red

CABINET PANEL PREP
- 25mm x 150mm and 50/50/50

db ELOCK

Automatically unlock a cabinet's back door upon front-door authentication

db ELock installs on a cabinet back door, working in conjunction with any Digitus front-door lock to simultaneously unlock the back door upon authentication. It is also used to unlock front/rear doors in end-of-row configurations using db Enline.

KEY PRODUCT FEATURES

- Works with both db Bus and db Sentry controllers
- Used with the end-of-row solution
- Unlimited number of users
- Compatible with server cabinets from most major manufacturers
- Cost-effective & easy to implement

TECHNICAL SPECIFICATIONS

DIMENSIONS:
- Height: 168 mm
- Width: 37 mm
- Depth: 24.5 mm

STATUS MONITORING:
- Built-in optical sensor to monitor handle position

OVERRIDE:
- Optional mechanical key (custom key cylinders available)

INPUT POWER:
- Available in 12 or 24VDC versions

LOCK CONTROL:
- Via Digitus control equipment

LED:
- Red and Blue

CABINET PANEL PREP
- 25mm x 150mm

db BUS

Advanced Technology Delivers Cabinet Security with a Wide Range of Authentication Options

The db Bus access control system saves costs by eliminating the need for a controller, network point and power supply at each cabinet. A sophisticated bus architecture distributes fail-safe signals and electrical power from a single controller to up to 64 cabinet door locks. The db Bus offers multiple options for authentication: choose where the authentication takes place, either at each cabinet door or at the end of a row of cabinets. For cabinet level authentication, choose any of the Digitus intelligent handles. For end of row authentication, the user enters which cabinet door they are attempting to access, then inputs any combination of PIN, RFID and fingerprint to authenticate.

KEY PRODUCT FEATURES

Bus architecture principles allow the db Bus access control platform to provide power and an Ethernet connection for as many as 64 locks on cabinet doors.

- 100% secure access control for server cabinets
- Time-tested technology in a reduced footprint
- Flexibility to work with all of the Digitus handles
- As-needed cabinet access deters data/equipment theft
- Centralized administration of up to thousands of units

TECHNICAL SPECIFICATIONS

AUTHENTICATION OPTIONS:

- At the cabinet
  - Independent intelligent handles on the front and back doors of a cabinet
  - Intelligent handle on the front door simultaneously unlocks front and back doors
- At the end of a row of cabinets, the db Enline unit allows a user to specify which cabinet they are attempting to access before providing up to three credentials to authenticate.

db ENLINE FEATURES

- Finger Sensor: Capacitive
- LCD 2 x 16 Character Lines
- LED Indication: Tri-Color
- Keypad: 12-Key Steel Matrix
- iClass, Mifare, DESFire, Seos, PIV (75 or 200 bit) and Prox Cards

POWER AND DRAW:

- Input Power: 48V DC, 4.6A
- Current Draw (with no Bus devices): 20 mA @ 48V DC
- Bus Power: 48V, Maximum Current 4.167A
- Operative Temperature: 32° F-158° F (0° C-70)

ENROLLMENT:

- Enrollment Time: < 5 Seconds
- Identification Time (1-1): < 1 second
- Identification Time (1-N): < 1 second/1,000 users • EER Rate: <0.1%
- Security Levels: 3

MEMORY STORAGE:

- User Capacity: 9,500
- Log Capacity: 60,000 Events

db BUS (CONTINUED)

Advanced Technology Delivers Cabinet Security with a Wide Range of Authentication Options

TECHNICAL SPECIFICATIONS

ARCHITECTURE:

- Single Ethernet Connection to Bus Controller
- Single 48V Power Supply to Bus Controller
- Bus Controller Provides Power and Data Signals to All Devices
- Control 64 Doors from a Single Bus Controller

GENERAL FEATURES:

- Managed with Digitus' DAS' SQL Software
- Indisputable Audit Trail
- One-Click Lock-Down of System
- Restrict Access Times
- Duress Activated Alert (Fingerprint Door Locks Only)
- Anti-Tamper Security
- Forced/Propped Door Detection

DIMENSIONS:

db Bus Controller

- Height: 191 mm
- Width: 127 mm
- Depth: 32 mm

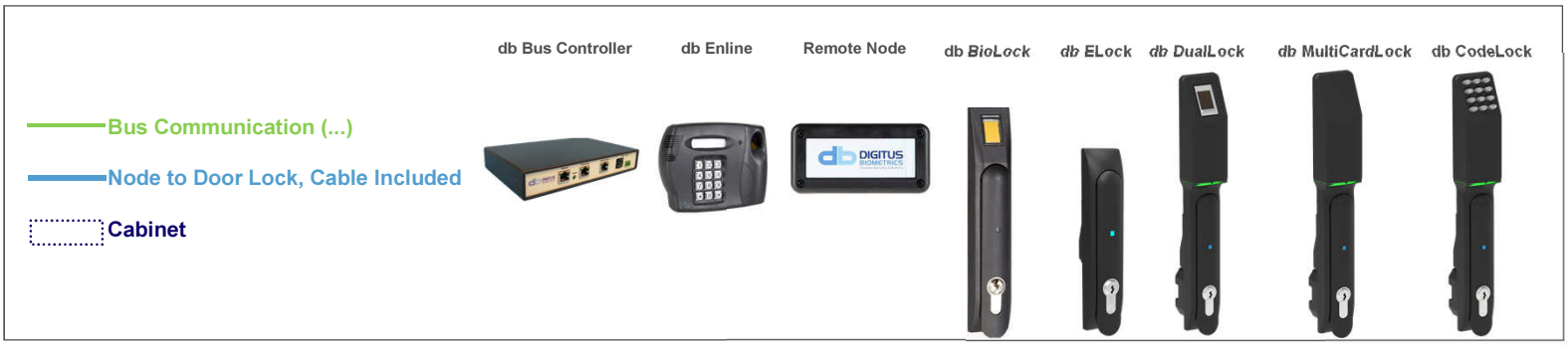
db ENLINE END-OF-ROW AUTHENTICATION OPTION

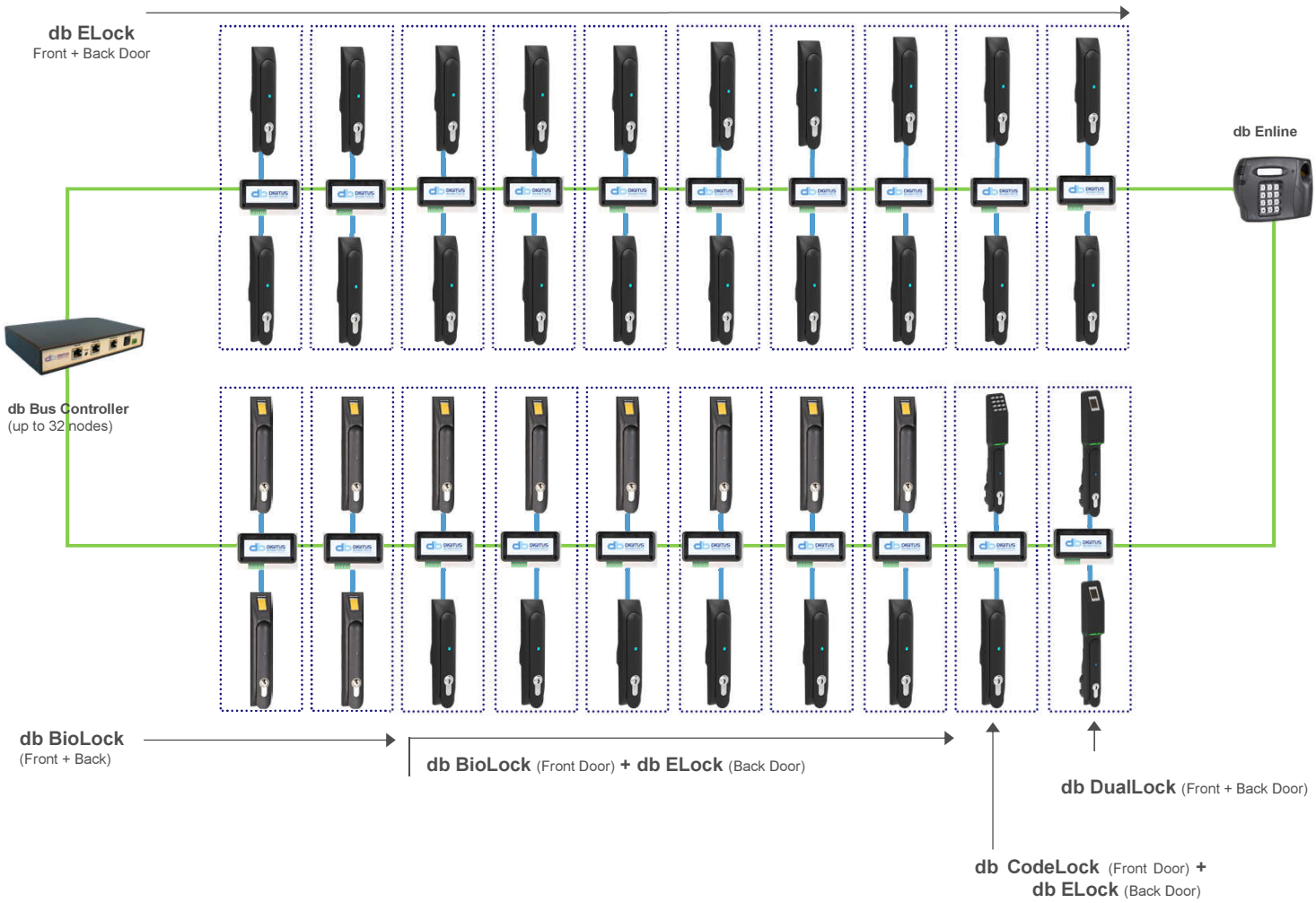
The db Bus system allows authentication to take place at either each cabinet or at the end of a row of cabinets. If end of row authentication is preferred, at least one db Enline reader is required. The db Enline reader allows a user to specify which cabinet they are attempting to access by identifying the cabinet by row/ cabinet/ door number. Once a valid cabinet has been entered, the user must then authenticate be presenting the required credentials, PIN/RFID card/fingerprint. If the credentials authenticate and the user has access to the specified cabinet, the cabinet door will unlock. The utilization of db Enline units on any db Bus system is very flexible. It's possible to have a reader installed at both ends of a single row of cabinets, or to have a single db Enline reader control multiple rows. The end of row authentication method can be used in conjunction with the db Elock or will work with existing electromechanical cabinet locks.

PART NUMBER:	DETAILS:
dbENLINE-2	db Bus End-of-row reader with fingerprint and PIN
dbENLINE-HF	db Bus End-of-row reader with fingerprint, PIN, and 13.56 MHz SmartCard Reader
dbENLINE-LF	db Bus End-of-row reader with fingerprint, PIN, and HID compatible 125 KHz Proximity Card Reader
dbENLINE-HFLF	db Bus End-of-row reader with fingerprint, PIN, and 13.56 MHz SmartCard/HID compatible 125 KHz Proximity Card Reader

db BUS ARCHITECTURE

db Bus Components





db SENTRY

Server Rack Access Control

db Sentry access control solutions deliver physical access control to mission critical IT server cabinets. The product is used within data centers, colocation facilities, military, government, educational, healthcare and industrial environments. db Sentry is equally suitable for both new cabinets and as a retrofit for existing cabinets, and a typical installation takes less than an hour.

KEY PRODUCT FEATURES

Intelligent cabinet control unit. db Sentry has everything you need.

- Single cabinet control unit
- PoE and/or auxiliary power
- Support 2 Digitus Handles
- Monitor door and handle positions
- Monitor cabinet side-panels
- At-the-cabinet authentication capability
- Up to 9,500 users
- Stores 60,000 event logs locally
- Encrypted network connection

TECHNICAL SPECIFICATIONS

HARDWARE:

- 2 x Lock Connections
  - db BioLock (Fingerprint)
  - db MultiCardLock (13.56 MHz Smartcard and 125 KHz Prox)
  - db DualLock (RFID card + fingerprint)
  - db CodeLock (RFID card + PIN)
  - db KeypadLock (PIN)
  - db ProLock (125 KHz Prox Card)
  - db ELock (Standard Electronic Lock)

- Auxiliary Power Input

PERFORMANCE:

- Biometric
  - Enrollment Time: <5 seconds Identification Time: (1-N)
  - < 1 second/1,000 templates EER: < 0.1%
  - Security Levels: 3

- RFID Card
  - Card Programming Time: < 5 seconds
  - Card Authentication Time: < 1 second
  - User selected Encryption Keys

COMMUNICATION:

- Protocol
  - Encrypted TCP/IP over Ethernet (supports PoE)
- Inputs
  - 2 x Lock Sensors
  - 2 x Door Sensors 2 x Tamper Inputs
- Outputs
  - 2 x Door Locks
  - 2 x Wiegand

STORAGE CAPACITY:

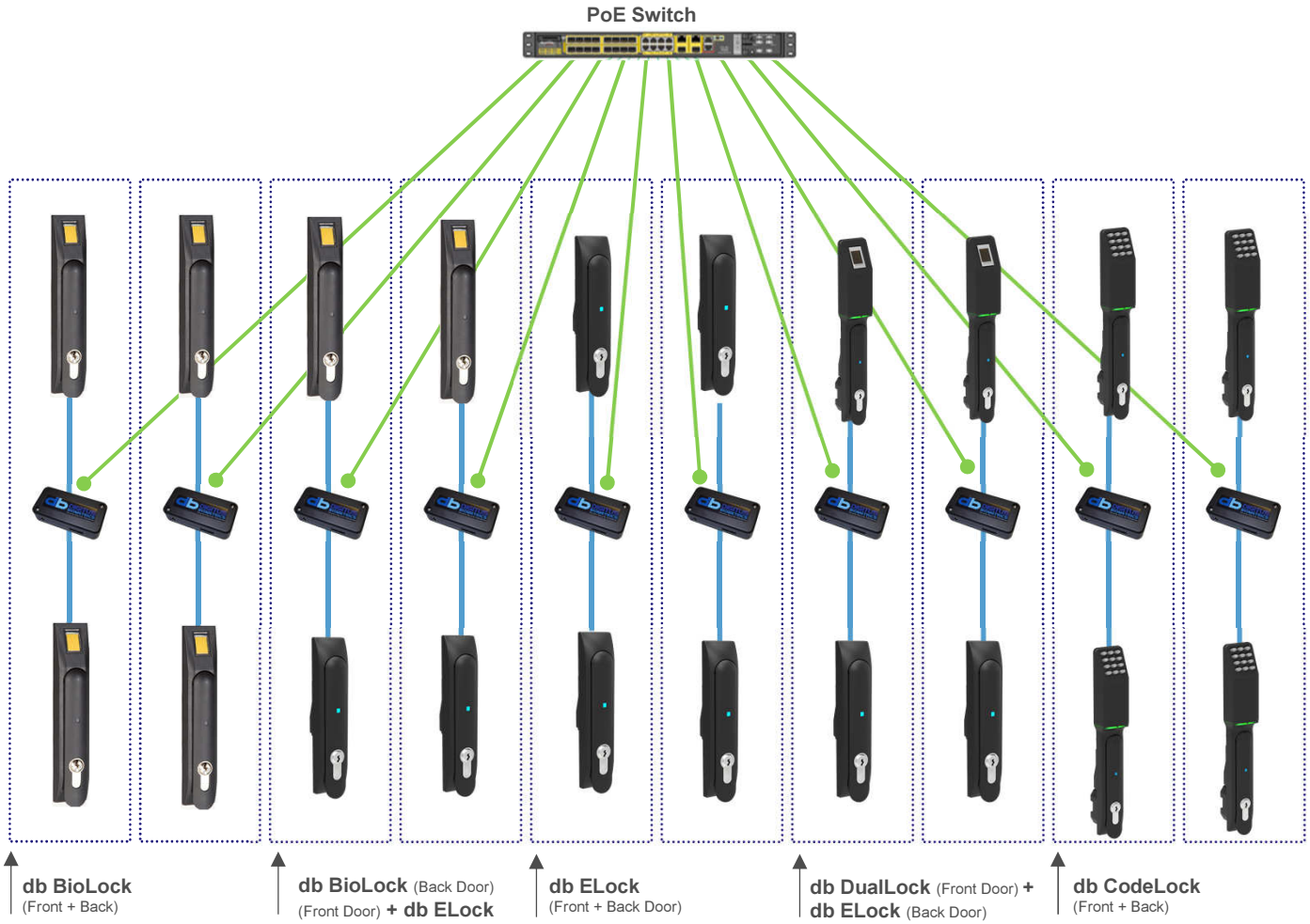
- User Capacity: 9,500 Users
- Biometric Template: 384 Bytes
- Log Capacity: 60,000 Events

DIMENSIONS AND ADDITIONAL DETAIL:

- Control Unit Dimensions: (W)102mm x (D)52mm x (H)29mm
- Lock Dimensions: Fits all 25 x 150mm and 50/50/50mm openings
- Power Input: PoE or Auxiliary Power Supply
- Voltage: 18-48V DC
- Current Draw: Idle-30 mA at 48V (without locks)
- Operative Temperature: 32-158° F (0-70° C)

db SENTRY ARCHITECTURE

db Cabinet Sentry Components



DIGITUS BUILDING/ROOM ACCESS PRODUCTS

Control Access to Thousands of Doors From a Single Location

db Nexus controls access to buildings and rooms with fingerprint and/or RFID identification. The platform is offered in two versions, the db Nexus and db Nexus Duo. Both versions are available with PIN and fingerprint or with PIN, fingerprint and RFID reader. Like all Digitus products, the db Nexus solutions are managed via the DAS-SQL software platform.

db Nexus:

When granting access, db Nexus units operate independently. No network communication is required for ID verification, and secure access control continues normally in the event of network failure.

- Secure access control for buildings, rooms, gates, turnstiles and cages
- More accurate than RFID readers and at a lower cost
- Nearly a decade of installations
- Centralized administration of up to thousands of units
- Indisputable audit trail across the enterprise
- Protection against obsolescence via db Infinity program

db Nexus Duo:

- **One or two reader units per control unit** – The ability to attach two reader units to a single control unit. This is useful for datacenter cage applications where authentication is needed to both enter and exit an area.
- **Dual-custody Authentication** – The ability to require two people to authenticate in order to gain access to secured areas. When a device is in dual-custody authentication mode, the second user must authenticate with 10 seconds of the first user.
- **Dual-custody Authentication Override** – The system detects how many people are in a secure area. If two or more people have already entered the secure area, the third person will be granted access without dual-custody.
- **Anti-passback** – This ensures that a person who enters a secure area must authenticate to exit that same area prior to re-entry.
- **Anti-passback Override** – The system provides the capability of issuing a passback reset at the individual user level.
- **Auxiliary Output Relays** – This allows the system to turn on devices, like cameras, when a user defined event occurs.
- **Two or Three credential mode** – Like the db Nexus, the db Nexus Duo can be configured with a card reader in addition to the biometric fingerprint reader and pin pad.
- **Mantrap application** – A person entering and leaving an area, must wait for the first door to close prior to gaining access to the second door.

db NEXUS

Networked Access Control for Managing, Monitoring and Reporting

db Nexus is the networked version of the Digitus access control product line. In conjunction with Digitus' DAS-SQL software, db Nexus units can be controlled and managed from a single location, allowing units to be anywhere in the world . db Nexus is available in either a two or three credential format. The db Nexus II uses a fingerprint and PIN. The db Nexus III uses a fingerprint, RFID Card and PIN.

PHYSICAL:

- Dimensions (191mm x 122mm x 56mm)
- Weight: 1.2 lbs (549g)

TECHNICAL SPECIFICATIONS:

- Voltage: 18-22v DC
- Current Draw: Idle-520 mA; Max 650 mA (without lock)
- Operative Temperature: 32° F-158° F (0° C-70° C)

USER INTERFACE:

- Finger Sensor: Capacitive
- LCD: 2 x 16 Character Lines
- LED Indication: Tri-Color
- Keypad: 12-Key Steel Matrix
- HID iClass 12.56 MHZ Contactless Reader (db Nexus III only)

ENROLLMENT:

- Enrollment Time: < 5 seconds
- Verification Time (1-1): < 1 second
- Identification Time (1-N): < 1 second/1,000 users EER Rate: <0.1%
- Security Levels: 3

MEMORY STORAGE:

- User Capacity: 9,500
- Template Size: 384 bytes
- Log Capacity: 60,000 events
- Sensor Type: Capacitive with Fake Finger Detection

COMMUNICATION:

- Network Protocol: TCP/IP over Ethernet Inputs: Fire Panel, Door Sensor, Request to Exit Switch
- Outputs: Door Lock Relay, Alarm Condition Relay, 26Bit Wiegand output

FEATURES:

- Indisputable Audit Trail One-Click Lockdown of System Restrict Access Times
- Duress Activated Alert Anti-Tamper Security Forced/Propped Door Detection Fire Panel Integration
- 16-Hour Battery Backup

ENROLLMENT AND MONITORING:

- Done via Digitus' DAS-SQL Software

db NEXUS DUO

Networked Biometric Access Control with Enhanced Security Features

db Nexus Duo is the newest version of the Digitus access control product. The db Nexus Duo product offers a host of enhanced security features, making it ideal for securing access to your mission critical facility. With features such as dual-authentication, anti-passback and mantrap access, the db Nexus Duo is in a class all by itself, when it comes to physical security.

ENHANCED SECURITY FEATURES:

- Dual Authentication Option requires 2 users to gain access
- Dual Authentication Override allows single user authentication after 2 people are already in an area
- Anti-PassBack prevents re-entry, unless user authenticated on exit
- Anti-Passback Override reset anti-passback for individual users
- Man-Trap prevents access to a door when another door is open

FEATURES:

- Dual Authentication Option requires 2 users to gain access
- Includes 2 readers. Use to secure two separate doors or secure in/out access through a single door
- Indisputable audit trail
- One-click lockdown of system
- Restrict access times
- Duress activated alert
- Anti-tamper security
- Forced/propped door detection
- Fire Panel Integration
- Up to 16-Hour Battery Backup
- Works with any 12V locks (power provided)
- Works with any 24V locks (external 24V power-supply required)

NEXUS READER UNIT:

- Dimensions: (W x H x D) 7.5” x 5.2” x 2.2” (19.1cm x 12.2cm x 5.6cm)
- Weight: 1.2lbs (549g)

NEXUS CONTROLLER UNIT:

- Dimensions: (W x H x D) 10” x 10” x 4” (25.4cm x 25.4cm x 10.2cm)
- Weight: 10.8lbs (4.9KG)

COMMUNICATION:

- Network Protocol: TCP/IP over Ethernet

USER INTERFACE:

- Fingerprint Sensor Type: Capacitive with fake finger detection
- LCD: 2 x 16 Character Lines
- LED: Tri-color
- Keypad: 12-Key steel matrix
- HID iClass 13.56 MHz contactless reader (dbNExDuo3C only)

db NEXUS DUO

Networked Biometric Access Control with Enhanced Security Features

TECHNICAL SPECIFICATIONS:

- Fingerprint Sensor Type: Capacitive with fake finger detection
- Voltage: 18-40V DC
- Current Draw (without locks):
  - w/one Reader: Idle 310 mA, Max 430 mA @ 18.5V DC
  - w/Two Readers: Idle 450 mA, Max 600 mA @ 18.5V DC
- Operative Temperature: 32˚ F-158˚ F (0˚ C-70˚ C)

MEMORY STORAGE:

- User Capacity: 9,500
- Fingerprint Template Size: 384 bytes
- Log Capacity: 60,000 events

ENROLLMENT:

- Enrollment Time: < 5 seconds
- Verification Time (1-1): < 1 second
- Identification Time (1-N): < 1 second up to 1,000 users
- Fingerprint EER Rate: <0.1%

ENROLLMENT & MONITORING:

- Done via Digitus DAS-SQL Software

INPUTS:

- Fingerprint Sensor Type: Capacitive with fake finger detection
- 2 x Reader units
- 2 x Door sensor
- 2 x Auxiliary sensor
- 2 x Request to exit switch
- Fire Panel (auto-unlock doors when fire-alarm activates)

OUTPUTS:

- 2 x Door lock relay
- 1 x Auxiliary relay
- 1 x Alarm relay
- 26-bit Wiegand

DIGITUS ACCESS SOFTWARE (DAS-SQL)

Management Software

DAS-SQL is a full-featured client-server application that manages Digitus Biometrics' networked access-control solutions. DAS-SQL uses Microsoft SQL Server as its server database platform and runs as a system service, providing true multithread communication to each Digitus device. For large installation, multi-scale architecture enables DAS-SQL to run up to five slave servers. There is no limit to the number of workstations that can run the DAS-SQL client software.

REPORTING

DAS-SQL provides detailed audit (log) reports, with the industry's only indisputable audit trail and tremendous flexibility for defining report criteria. DAS-SQL can generate reports by user, unit, user group or department, and allows users to define custom sorts and specify date ranges for reports. These reports can be customized and automated along with a list of standard reports. The ultra secure nature of the alert management features and SYSLOG capability puts the DAS-SQL platform in a security field all by itself. Some of the alert management and automated report capabilities include the following:

- The system will log who acknowledges an alarm
- The system facilitates text fields to describe cause and resolution of alarm
- Time and date stamps of the acknowledgment
- Facility and location of person acknowledging the alarm

SCALABILITY

DAS-SQL can scale to operate with thousands of access control units. The database resides on a centrally accessible server that enables administration of all units from a single desktop. The database can also be partitioned to enable multiple parties to manage, monitor, alert, and report on specific access points or groups of access points, as in allowing colocation clients to remotely monitor their own assets.

PARTITIONS

Partitions are used to create "virtual systems" within DAS-SQL. When partitions are not defined, every object (user, unit, zone, and user group) created in DAS-SQL is accessible to every other object. Partitions segment objects within DAS-SQL so that they are accessible only by other objects within that partition. For example, a colocation facility may want to segment its customers' cabinets to create a distinct partition for each customer. Doing so allows each customer to remotely manage, monitor, and report on all of their own access points, without any visibility into objects outside their partition. The "system partition" still has access to all partitions, allowing colocation administrators to manage the entire system.

SYSTEM OPTIONS

The System Setup tabs provides a single management point for all system- wide settings:

- Configure server settings, peripheral devices, email server settings, slave servers and Wiegand parameters
- Create and manage DAS-SQL partitions, default settings for any new device added to DAS-SQL and user-defined fields for user records

DIGITUS ACCESS SOFTWARE (DAS-SQL)

USER MANAGEMENT

Central enrollment through Digitus Access Software - SQL (DAS-SQL) allows for the easy addition of users, followed by unique features for assigning individual or group permissions. Each user can register up to ten fingers, with any two fingers being designated “duress fingers.” Managing who has access on what days/times was never easier. This full function, user friendly software platform anchors an access control platform that has been rated by industry experts as being “the most secure in the world.” Features like dual custody, require two users to authenticate to gain access to a given area or cabinet. The anti-passback feature ensures that a person who enters a secure area must authenticate to exit that same area prior to re-entry. In mantrap applications, a person must wait for the first door to close prior to gaining access to the second door.

UNIT MANAGEMENT

DAS-SQL manages all Digitus devices, from auto discovery through configuration, enrollment, monitoring, and reporting. This single platform can manage any mixture of db Nexus room access controllers and db ServerRack cabinet access controllers. Managing the access control units (hardware) themselves is also made easy through DAS-SQL. This robust software platform works with every product in the Digitus product line. The software intelligently adds new local units to the system by sending a broadcast to the network, and remote units by specifying the unit’s IP address. DAS-SQL allows the manager to manage settings on each unit to determine which features are enabled and which are disabled.

REAL-TIME MONITORING

DAS-SQL provides a wide range of monitoring and control capabilities. The system status window displays access events as they occur for real-time monitoring of all devices. The software will monitor the status of doors, including open/ closed status as well as propped door or forced entry. DAS- SQL tracks individual users as they pass through access points around the enterprise, around the world.

REAL-TIME ALERTING

DAS-SQL provides real time alerts via the central monitoring station. The software presents a list of potential “alerting” events a manger can choose from. These alerts can also be delivered via email to handheld devices, providing those who need to know up to the minute information about their security system. The software also allows the database to be partitioned to segment various customers, as might exist in a public data center environment. These customers can be granted access to the DAS-SQL platform via “client licenses” and take advantage of the many features, as they relate to their access points on their server cabinets.

DIGITUS BIOMETRICS
Access Security Solutions

2 East Bryan Street, Suite 502
Savannah, GA USA 31401
Phone: +1.912.231.8175
email: info@digitus-biometrics.com