Digitus Biometrics

2015 PRODUCT CATALOGUE

DIGITUS BIOMETRICS
Access Security Solutions

REQUEST A QUOTE OR DESIGN ASSISTANCE BY EMAILING
SALES@DIGITUS-BIOMETRICS.COM OR CALLING 912.231.8175.

DIGITUS BIOMETRICS
Access Security Solutions

Table of Contents

2 East Bryan Street Suite 502 Savannah, GA USA 31401 | Phone: 912.231.8175 | Email: info@digitus-biometrics.com

DIGITUS BIOMETRICS
Access Security Solutions

Access Control Solutions

SECURITY IS IN OUR DNA

PROTECT YOUR DATA CENTER WITH DIGITUS BIOMETRICS
Data is under constant threat, and physical security is the crucial part of protecting that information. Our patent-pending solutions provide perfect security at access points throughout your enterprise, from the building's entrance to the server cabinet doors in the data center. Compatibility with enterprise systems ensures that your investments are elegantly maximized. And while our customers have never experienced a single security breach through db technology, unauthorized access attempts – including those under duress – trigger alerts for immediate response for the highest level of security. And with an indisputable audit trail, you'll have an ironclad record of all activity to maintain compliance

OUR KNOWLEDGE IS YOUR POWER
db proprietary technology secures any type of server cabinet or access point. From a single platform, you can manage access points around the world and monitor in real time. Digitus delivers superior solutions regardless of budgetary constraints. We have a proven track record of thousands of db installations securing some of the world's largest corporations, military units and intelligence communities.

Digitus Biometrics is the only solution available for 100% physical security at every possible point of vulnerability.

SIMPLE. PERFECT. GUARANTEED.

2 East Bryan Street Suite 502 Savannah, GA USA 31401 | Phone: 912.231.8175 | Email: info@digitus-biometrics.com

DIGITUS BIOMETRICS
Access Security Solutions

db ServerRack Family

CONTROL ACCESS TO SERVER CABINETS & BOOST REGULATORY COMPLIANCE WITH INDISPUTABLE AUDIT TRAILS

Stopping access control at the data center door provides no protection against insider theft. That's why every data privacy rule and regulation – PCI DSS, HIPAA, FISMA and more – considers the protection of physical assets to be as important as protecting the data stored or processed in those assets.

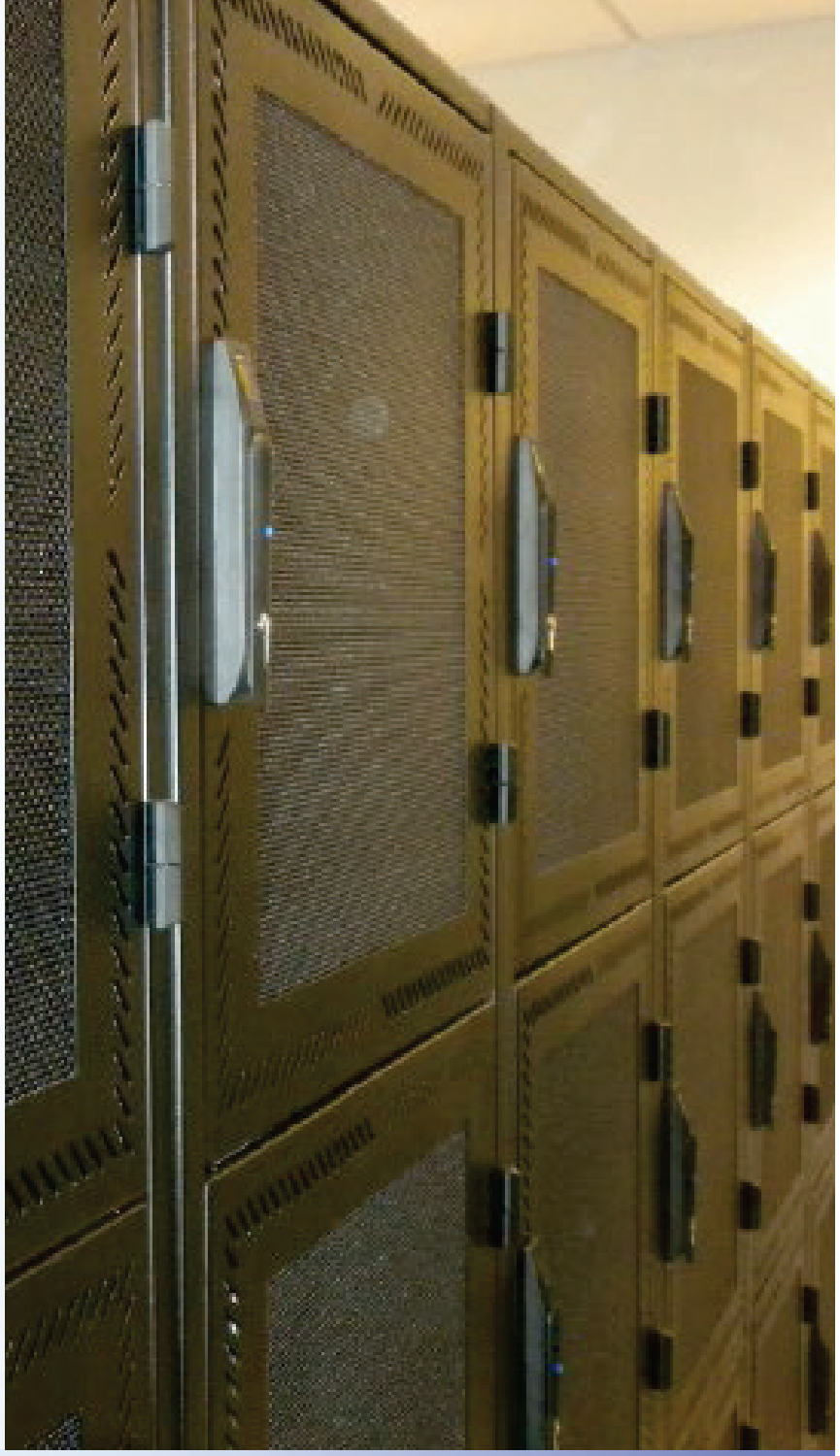
The db ServerRack Family delivers the highest level of compliance with an indisputable audit trail covering all server cabinet access. When paired with db Nexus, that audit trail covers the entire enterprise.

CHOOSE FROM TWO SYSTEM ARCHITECTURES

db Cabinet Sentry, for physical access control to mission critical IT server cabinets. It is suitable for new cabinets or retrofits.

db Bus, a central controller distributes control signals and power to up to 32 cabinets. Choose where the authentication takes place, either at each cabinet or at the end of a row of cabinets. For cabinet level authentication, choose between fingerprint or RFID card. For end of row authentication, the user enters which cabinet door they are attempting to access, then uses any combination of PIN, RFID and fingerprint to authenticate.

- 100% secure access control for server cabinets
- Time-tested technology in a reduced footprint
- Flexibility to choose between fingerprint or RFID card access
- As-needed cabinet access deters data/equipment theft
- Centralized administration of up to thousands of units
- Protection against obsolescence via db Infinity progress.



2 East Bryan Street Suite 502 Savannah, GA USA 31401 | Phone: 912.231.8175 | Email: info@digitus-biometrics.com

DIGITUS BIOMETRICS
Access Security Solutions

db Bus

ADVANCED TECHNOLOGY DELIVERS CABINET SECURITY WITH A WIDE RANGE OF AUTHENTICATION OPTIONS

The db Bus access control system saves cost 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 either at the cabinet or at the end of a row of cabinets.

PHYSICAL

db Bus Controller
- Dimensions: W7 1/2 x D5 x H1 1/4

db BioLock
- Lock Dimensions: Fits most 25 x 150 mm openings

db CardLock
- Lock Dimensions: Fits most 25 x 150 mm openings

db iCardLock
- Lock Dimensions: Fits most 25 x 150 mm openings

db ELock
- Lock Dimensions: Fits most 25 x 150 mm openings

AUTHENTICATION

At the cabinet
- Independent biometric or card locks on the front and back doors of a cabinet
- Biometric or card lock on the front door, simultaneously unlocks front and back doors

AUTHENTICATION

At the end of a row of cabinets

The db Enline unit allows a user to specify which cabinet they are attempting to access, then provide up to three credentials to authenticate.

db Enline features
- Finger Sensor: capacitive n
- LCD: 2 x 16 character lines
- LED Indication: Tri-Color
- Keypad: 12-Key steel matrix
- HID iClass 13.56 MHz smartcard reader or HID compatible 125 KHz proximity reader

TECHNICAL SPECIFICATION
- 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
- Fingerprint Template Size: 384 bytes
- Log Capacity: 60,000 events
- Finger Sensor Type: capacitive with fake finger detection
- db CardLock Reader Type: 125KHz HID compatible
- iClass Card Reader: 13.56 MHz HID compatible

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

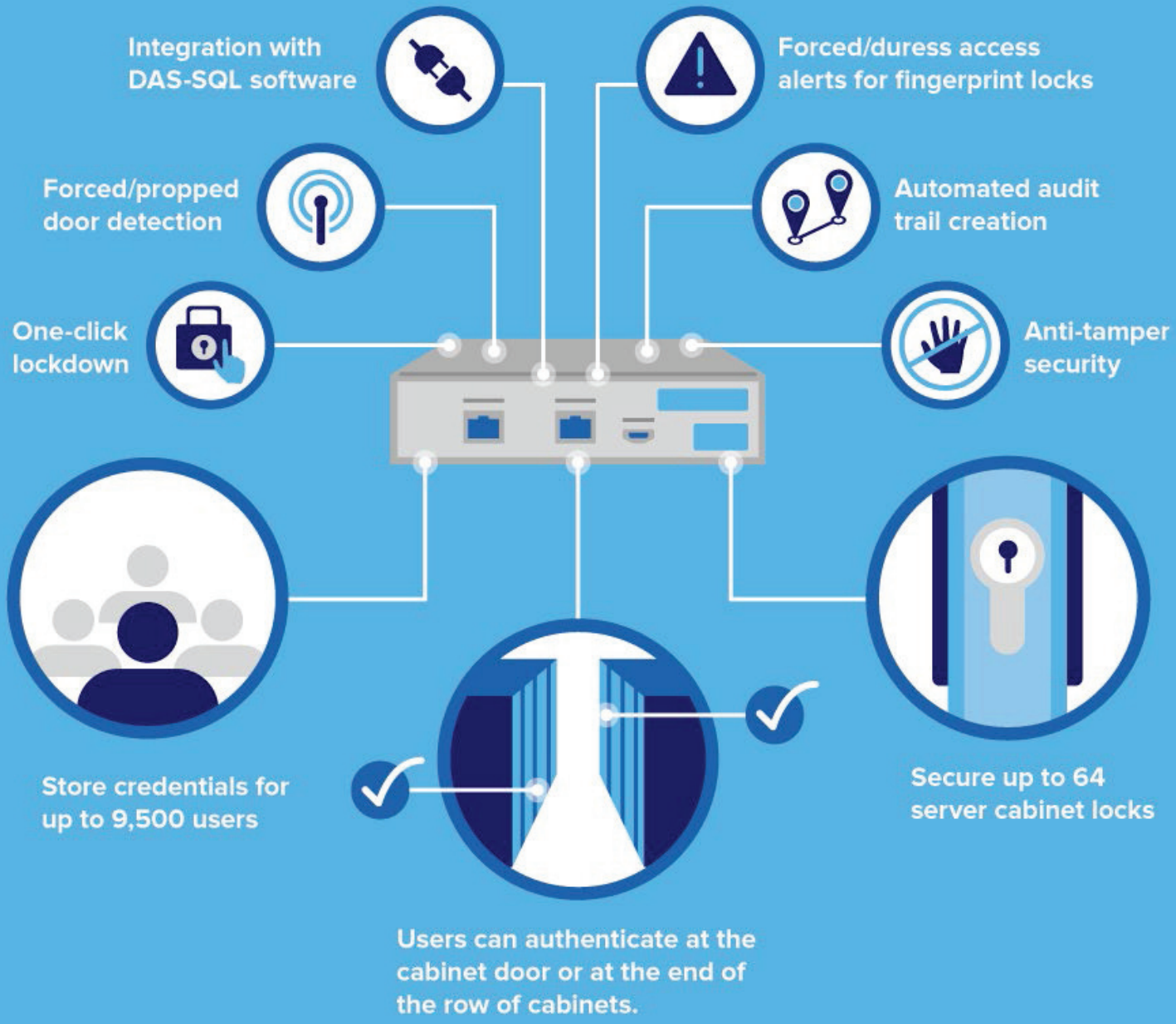
GENERAL FEATURES
- Managed with Digitus' DAS-SQL software
- Indisputable audit trail
- One-click lockdown of system
- Restrict access times
- Duress activated alert (fingerprint door locks only)
- Anti-tamper security
- Forced/propped door detection

	db BioLock	db CardLock	db iCardLock	db Enline
Security Layers	Biometric	Card	iClass Cards	PIN, Biometric, RFID (optional 13.56MHZ/125KHz)
User Capacity	9,500	9,500	9,500	9,500
Operation Mode	Ethernet Networked	Ethernet Networked	Ethernet Networked	Ethernet Networked
# of Fingers Enrolled Per User	Up to 10 (with 2 Duress)	N/A	N/A	Up to 10 (with 2 Duress)
Verification/Identification	Identification	N/A	N/A	Both

2 East Bryan Street Suite 502 Savannah, GA USA 31401 | Phone: 912.231.8175 | Email: info@digitus-biometrics.com

DIGITUS BIOMETRICS
Access Security Solutions

db Bus



DIGITUS BIOMETRICS
Access Security Solutions

db Cabinet Sentry

SERVER RACK ACCESS CONTROL

db Cabinet 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 Cabinet Sentry is equally suitable for both new cabinets and as a retrofit for existing cabinets, and a typical installation takes less than an hour.

FEATURES

- 2 x Lock Connections
  - BioLock (fingerprint)
  - iCardLock (HID iClass card)
  - CardLock (prox. or Mifare)
  - ELock (standard electronic lock)
- Power over Ethernet (PoE)
- Auxiliary Power Input

PERFORMANCE

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

TECHNICAL SPECIFICATIONS

- 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)

2 East Bryan Street Suite 502 Savannah, GA USA 31401 | Phone: 912.231.8175 | Email: info@digitus-biometrics.com

db Nexus Solutions - Networked Access Control

CONTROL ACCESS TO UP 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.

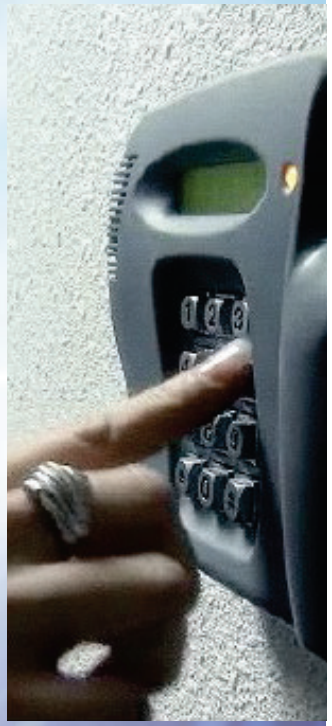
db NEXUS

When granting actual 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 proximity readers, at 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 insures 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.



2 East Bryan Street Suite 502 Savannah, GA USA 31401 | Phone: 912.231.8175 | Email: info@digitus-biometrics.com

DIGITUS BIOMETRICS
Access Security Solutions

db Nexus

"From one office, I can now constantly monitor who has accessed which areas, and when. I can instantly administer privileges for any secure access point."

–David Loiacono
Information Management & Office/Network Administrator
Fort Stewart & Hunter Army Airfield

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 (WxHXD) 7.5"X 5.2"X 2.2" (19.1 cm x 12.2 cm x 5.6 cm)
- Weight: 1.2 lbs (549g)

TECHNICAL SPECIFICATION
- 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

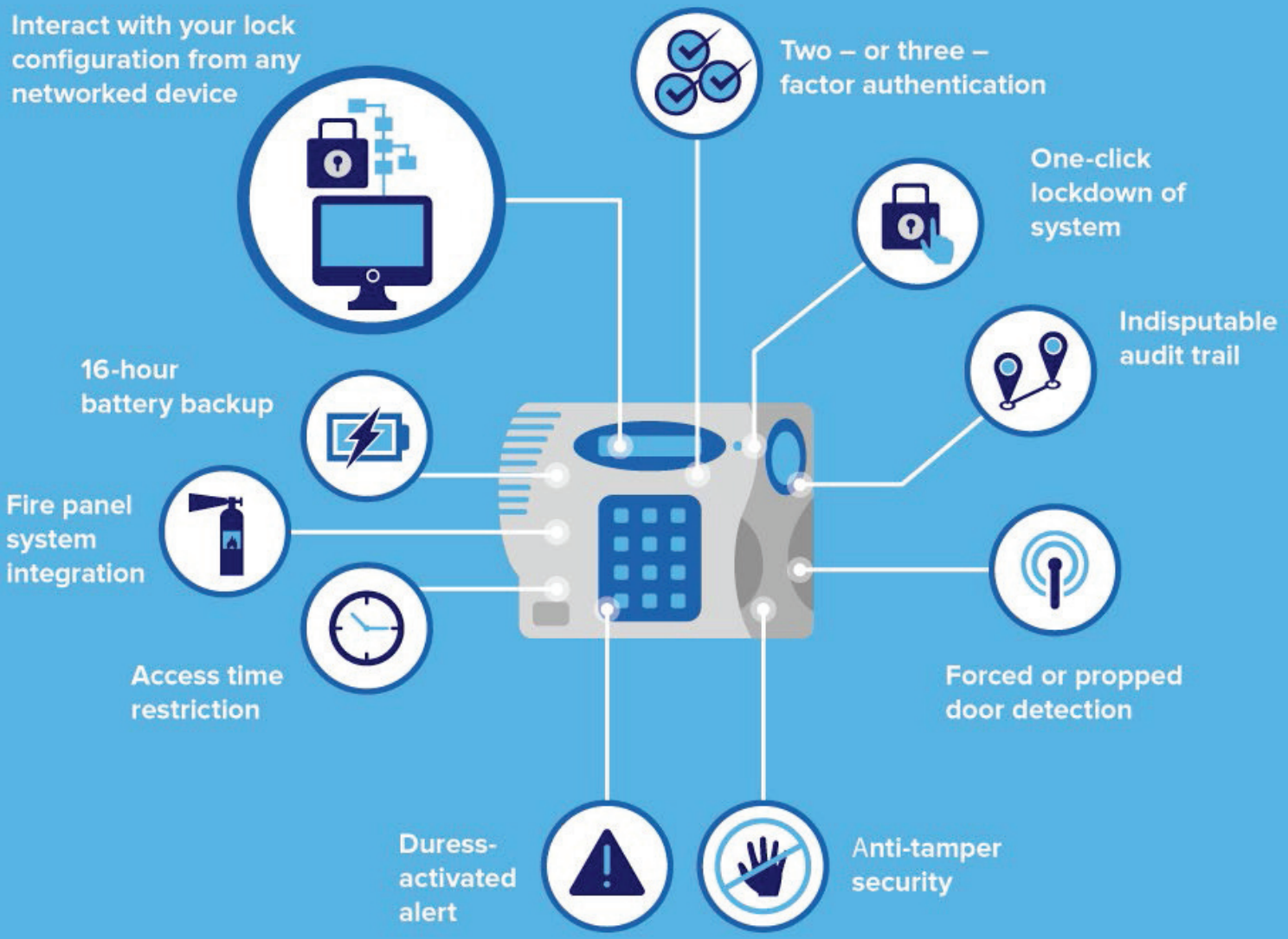
ENROLLMENT AND MONITORING
- Done via Digitus DAS-SQL Software

	dbNEX2C	dbNEX3C
Security Layer	PIN & Biometric	PIN, Biometric & RFID
User Capacity	9,500	9,500
Operation Mode	Ethernet Networked	Ethernet Networked
# of Fingers Enrolled Per User	Up to 10 (with 2 Duress)	Up to 10 (with 2 Duress)
FIPS 201		Compliant
Verification/Identification	Both	Both

2 East Bryan Street Suite 502 Savannah, GA USA 31401 | Phone: 912.231.8175 | Email: info@digitus-biometrics.com

DIGITUS BIOMETRICS
Access Security Solutions

db Nexus



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 crititical 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

- 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)

PHYSICAL

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)

TECHNICAL SPECIFICATION

- 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 AND MONITORING

- Done via Digitus DAS-SQL Software

INPUTS

- 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

	dbNEXDUO3C
Security Layer	PIN & Biometric & RFID
User Capacity	9,500
Operation Mode	Ethernet Networked
# of Fingers Enrolled Per User	Up to 10 (with 2 Duress)
Verification/ Identification	Both

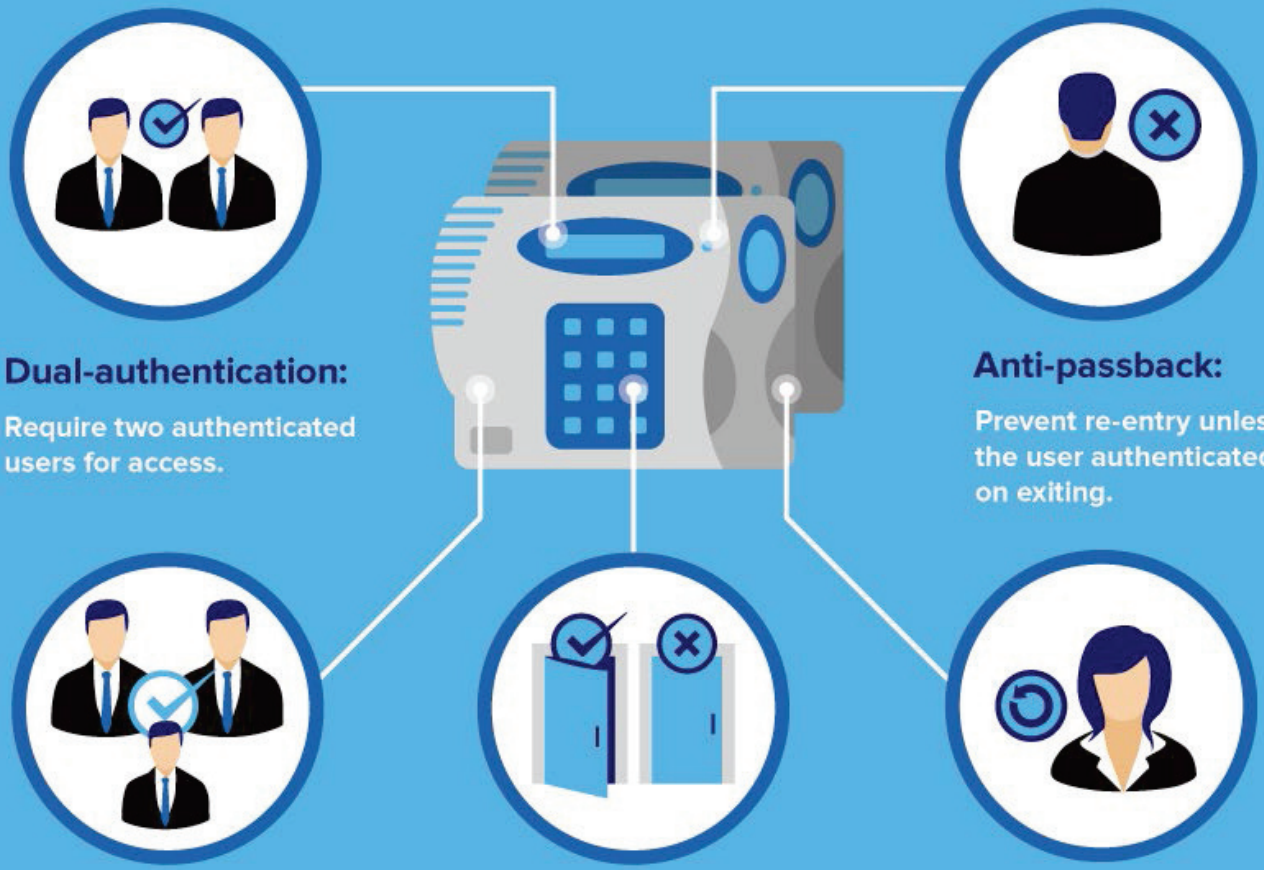
	dbNEXDUO2C
Security Layer	PIN & Biometric
User Capacity	9,500
Operation Mode	Ethernet Networked
# of Fingers Enrolled Per User	Up to 10 (with 2 Duress)
Verification/ Identification	Both

2 East Bryan Street Suite 502 Savannah, GA USA 31401 | Phone: 912.231.8175 | Email: info@digitus-biometrics.com

DIGITUS BIOMETRICS
Access Security Solutions

db Nexus Duo

Deploy advanced security features beyond the db Nexus, including:



Dual-authentication:

Require two authenticated users for access.

Anti-passback:

Prevent re-entry unless the user authenticated on exiting.

Dual-authentication override:

Bypass dual-authentication when two users are already in an area.

Mantrap access:

Prevent access to a door when another door is already open.

Anti-passback override:

Reset anti-passback for individual users.

DIGITUS BIOMETRICS
Access Security Solutions

Digitus Access Software (DAS-SQL)

ANCHORING THE MOST SECURE ACCESS CONTROL TECHNOLOGY IN THE WORLD

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.

2 East Bryan Street Suite 502 Savannah, GA USA 31401 | Phone: 912.231.8175 | Email: info@digitus-biometrics.com

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

2 East Bryan Street Suite 502 Savannah, GA USA 31401 | Phone: 912.231.8175 | Email: info@digitus-biometrics.com

DIGITUS BIOMETRICS
Access Security Solutions

db Infinity Maintenance Program

FUTURE-PROOF YOUR INVESTMENT IN TOTAL SECURITY.

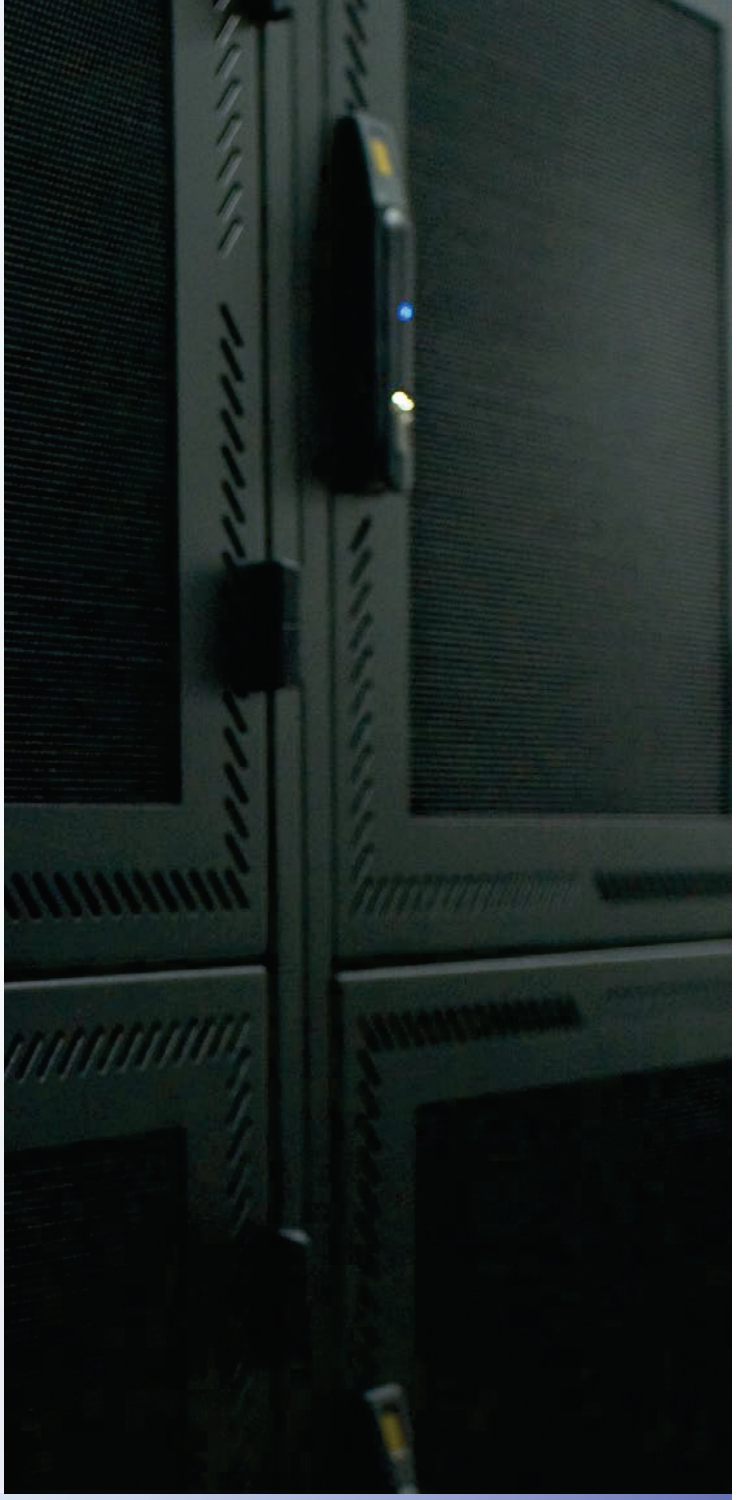
The db Infinity Maintenance Program – available for a low annual fee – ensures comprehensive end-to-end protection of your db biometric access control system.

INFINITE BENEFITS

- 24-hour SLA to replace any failed unit
- Unlimited DAS-SQL software updates
- Unlimited firmware updates
- Unlimited telephone and remote connection support

THE db COMPLIANCE GUARANTEE

Digitus guarantees compliance with all government or industry regulations pertaining to physical security. Should you fail a physical security audit, db will either refund 100% of the system price or provide all additional features required to ensure compliance.



2 East Bryan Street Suite 502 Savannah, GA USA 31401 | Phone: 912.231.8175 | Email: info@digitus-biometrics.com

DIGITUS BIOMETRICS
Access Security Solutions

Leading Biometric Access Control Technology

SIMPLY THE BEST PROTECTION FOR YOUR PHYSICAL ASSETS

VALUE PROPOSITION

Proven performance with 1,000's of installed units worldwide.

Zero false positives, and zero security breaches, across all customer installations.

A single technology platform secures everything from the front door to the server cabinet door.

Centralized control of units anywhere in the world, with real-time monitoring and alerts, detailed log reports, and indisputable audit trails.

Technology that won't obsolete itself, with the excellent long-term protection via the db Infinity program.

Flexible/adaptable to new access control applications.

Easy-to-install and easy-to-use.

FINGERPRINT TECHNOLOGY

Enrollment stores no actual fingerprint - at no time is the actual fingerprint stored in the system.

Easy-to-use Fingerprint Identity - proprietary biometric fingerprint template identification used for 100% accuracy.

Finger Fraud Protection - system will not generate false postives for fake fingers or fingers of deceased.

Emergency/Breach Detection - "duress finger" programming to alert security personnel to forced entry or other trouble.

TECHNOLOGY VALIDATION

In its January 2010 edition, Secure Computing Magazine reviewed the Digitus technology and gave it the following ratings:

Features	★★★★★
Support	★★★★★
Ease of use	★★★★★
Value for money	★★★★★
Performance	★★★★★
Documentation	★★★★★
Overall Rating	★★★★★

2 East Bryan Street Suite 502 Savannah, GA USA 31401 | Phone: 912.231.8175 | Email: info@digitus-biometrics.com

DIGITUS BIOMETRICS
Access Security Solutions

FOR MORE INFORMATION

2 EAST BRYAN STREET
SUITE 502
SAVANNAH, GA USA 31401
PHONE: 912.231.8175
EMAIL: INFO@DIGITUS-BIOMETRICS.COM