BioAxs 9800IR™
Multi-Modal Biometric Access Panel
Fingerprint & Iris Recognition

Installation & Operations Manual
Version 1.9

BioAxs 9800IR with LG Iris

NextgenID

P/N: NG-DOC-BA9800IR-IOM

THIS PAGE INTENTIONALLY LEFT BLANK

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Notices

Notice: The information in this document is subject to change without notice. Please contact support@NextgenID.com and refer to P/N NG-DOC-BA9800IR-IOM
.
Notice: Any use of this product is subject to the terms and acceptance of the NextgenID Ltd "Software Agreement." You may request a copy of the "Software Agreement" from NextgenID Ltd by contacting support@NextgenID.com. Please review this agreement carefully.

Notice: Windows™, Windows 2000™, Windows NT™, Windows XP™ are trademarks and/or registered trademark of Microsoft Corporation in the United States and/or other countries.

Notice: IrisAccess™ is a registered trademark of LG Electronics Institute of Technology in the United States and/or other countries.

Fire Safety Notice Never connect BioAxs Access Control devices or locks to doors, gates or barriers without first consulting the local fire codes. You must consult with, and get approval of, local fire officials before installing locks or devices on any doors that may be fire exits. Use of request to exit push buttons may not be legal. A single action exit mechanism may be required. Always obtain the proper permits and approvals in writing before installing access control equipment, door locks and associated readers.

Notice: The NextgenID Ltd. Logo, and the NextgenID Ltd products referred to herein are either the trademarks or the registered trademarks of NextgenID Ltd. All other trademarks are property of their respective owners. NextgenID Ltd. assumes no responsibility for errors that may appear in this manual. Information contained herein is subject to change without notice.

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Contacts

Mailing Address
NextgenID, Ltd.
10226 San Pedro
Suite 100
San Antonio, TX 78216 USA

By Phone
Phone (210) 530-9991
Fax: (210) 530-9992

Email
support@nextgenid.com

World Wide Web
Support.NextgenID.com

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Contents

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Introduction

Biometric Access Control

A computerized method used to identify people based on their unique physical characteristics before granting access to secure facilities.

Why biometric access control is better

Today, more than ever before, it's important to know that only authorized people are in your secure areas. NextgenID biometric access control products provide secure, affordable access control for all security needs.

Far superior to pin numbers or card systems, which can be shared or stolen, biometrics utilize a person's unique physical characteristics to identify the user. NextgenID biometric identification and verification systems ensure that only legitimate members can enter your secure area.

NextgenID BioAxs multi-biometric hardware and software platform allows users to choose what biometric technologies they want to deploy at each point to be secured. The BioAxs 9800IR™ is part of the NextgenID BioAxs™ family of multi-biometric, multi-modal access control panels and utilizes both fingerprint and iris biometrics.

Modular / Scalable

The modular, multi-biometric BioAxs solution is designed to treat each biometric component as a verification or identification device within the scalable framework of a particular door's security requirements. NextgenID hardware and algorithm neutrality allow particular algorithms and sensors to be easily integrated to meet customer requirements.

Multi-Modal Authentication Protocol

The BioAxs 9800IR™ provides multi-modal authentication modes meaning the facilities access control administrator can adjust the access protocol necessary to obtain entry to the protected facility. Combining traditional access control methods such as card readers, PIN Entry devices with the latest in biometric authentication technology, the BioAxs 9800IR™ provides a robust access control solution to a variety of threat conditions present in today's environment.

Flexible Authentication Protocols

The BioAxs 9800IR system can be configured as an "and" system that requires both biometrics to be verified for access to be granted. The BioAxs 9800IR™ can also be configured as an "or" system that allows users to authenticate either their iris or their fingerprint.

Threat Level Scalability

Based on the current perceived level of threat to a given facility, the BioAxs 9800IR™ system allows the access control administrator to configure predefined operating configurations for the access panels. As threat conditions increase the level of the security for a facility, the panel behavior may be 'scaled up' to require additional credentials for granting access. Examples of these techniques include: combining a proximity card and biometric, adding a PIN or requiring multiple biometrics before granting access.

Patented Dual Biometric System

The BioAxs 9800IR's patented system combines the power of two biometrics, iris and fingerprint with the optional added security of tailgating detection to provide a formidable access control solution for your secure facility. The system comes standard with the LG IrisAccess™ verification/identification algorithm and NextgenID FingerMatch verification/identification algorithm.

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

FingerMatch™ fingerprint matching technology

FingerMatch™ uses both global (features that are discernible by the naked eye) and local (tiny, unique characteristics of fingerprint ridges) feature analysis to match a fingerprint. Based on these distinct features, fingerprints are given a unique set of numbers, which are sent to a database to find a match. Once a match is made, the user is allowed access.

Our FingerMatch™ technology performs a fast and efficient search of large databases, making our product the perfect solution for high traffic doors.

Stand Alone Capability

The BioAxs 9800IR™ is capable of functioning as a “stand alone” device and will open magnetic locks or strike plates, handle request to exit buttons, and accept fire alarm shunts. The BioAxs 9800IR comes standard with an onboard proprietary door controller board and our powerful Command Center Access Control Software. The Command Center allows for complex granting of access privileges. Users can be granted access to a particular door during defined days and/or hours. User Groups can be created to assign the same door privileges to a large group of users (i.e., Lab A Technicians). All door events are accompanied by pictures and are logged for easy searching, viewing and reporting.

Integrates with existing Access Control Systems

The BioAxs 9800IR™ can act like just another card reader on an existing access control system and will pass card reader output to the access controller in 26-bit Wiegand data format

Weatherproof Design

The BioAxs 9800IR™ is available in a weatherproofed model that can operate in most outdoor conditions. Down pour conditions make fingerprint authentication extremely difficult as a user not carrying an umbrella will be unable to sufficiently wipe his or her finger semi-dry before authenticating. Fingerprint readers cannot read prints through a significant layer of water. For unhindered performance, BioStation™ outdoor mounting or a commercial awning will provide the necessary “dry zone” for users to wipe the moisture from their finger. Obviously, users prefer the amenity of an outdoor authentication spot protected from the elements. It is also available in an XTRM Model that can operate at temperatures from -40°c to +60°c.

Flexible System Architecture

Both the hardware and software architecture of our system is designed to be extremely flexible. If you would like to enhance an existing card swipe or proximity card system with a BioAxs 9800IR™, we are able to accept and deliver the reader’s information in standard card reader format via 26-bit Wiegand input and output.

Flexible Mounting Options

The BioAxs 9800IR™ is available in flush or surface mount designs that utilize wall-mount, low-voltage lighting, (indoor and outdoor available). The BioAxs 9800IR™ is also available in NextgenID’s BioStation™ integrated lighting solution. The BioStation™ lights the user’s face from three positions to provide a uniform, ideally lit image for recognition.

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

BioAxs 9800IR™ ™ Features / General Specifications

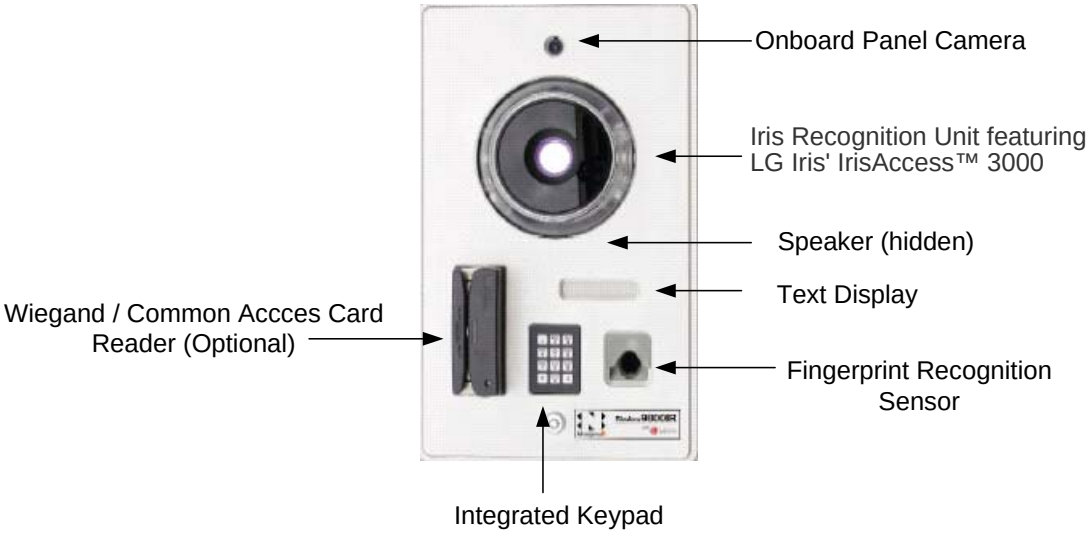


Figure 1 - BioAxs 9800IR™ Biometric Access Panel Front View

Feature	Specification
Fingerprint Identification Algorithm	NextgenID FingerMatch™
IRIS Recognition Identification Algorithm	Algorithm independent Multi Biometric Platform. The BioAxs 9800IR™ comes standard with LG Iris' IrisAccess™ Iris Recognition Engine
Real time network monitoring	Yes
Fingerprint Enrollments per User	10 Templates (All Fingers)
Fingerprint FAR	0.001%
Fingerprint Lookup Modes	Verification & Identification 1-N, 1-1, 1-Few
Fingerprint FRR (After Capture)	0.01%
Iris Equal Error Rate (EER)	1 in 1.2 million
On-The Fly Adjustable Authentication Mode	Standard
Iris Recognition Lookup Modes	Verification 1-1, 1-Few
Identification/ Authentication Modes (some modes listed require optional equipment e.g. card reader)	PIN Only Card Only PIN + Finger Card + Finger PIN + Iris Card + Iris PIN + [Finger or Iris] Card + [Finger or Iris] Card + Iris + Finger PIN + Iris + Finger DoD Common Access Card Configurations also available
Fingerprint Identification Time (After Image Capture)	1 second / 30000 Templates Identification Mode
Fingerprint Verification Time (After Image Capture)	Sub-1 second

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Rotational Tolerance Fingerprint Scan	360°
Iris Verification Time (After Image Capture)	.5–1s Verification Mode
Fingerprint Templates	Unlimited [1]
Iris Templates	Unlimited [1]
Fingerprint Template Cache	10,000 templates (Scalable)[1]
Event Logging	Unlimited[1]
Event Monitoring	Real Time
Networking	TCP/IP (10Base-T, 10 /100Mbps)
Battery Backup	Minimum 2 hours Recommended
Card Reader	Wiegand Output
Lock Control	Wiegand Output (26 bit) and/or Stand Alone Door Control Capable
Tailgating Detection	Yes (optional equipment)
Point of Entry Images captured with Events	Yes
Door Ajar Alarm and Events	Yes
Panel Tamper Alarm	Yes
User Duress Notification via selectable biometric	Per fingerprint enrollment
Multi-Centric User and Panel Management / Department Segmental Management	Yes
Operating Temperature Range	0° C to +60° C Standard -40° C to +60° with Extreme Weather Option
Visitor Enrollment (expiring enrollments)	Yes
Schedule Open Access Periods Per Door	Yes
Schedule Access Periods Per Group or Individual	Yes
Facility Lock Down Mode	Yes
Relative Humidity	0-85% Non-condensing
Access Panel Dimensions	11.25 x 18.25 x 4.75 (285.75 x 463.55 x 120.65 mm)
Fingerprint Reader Sensor Type	Optical
Sensor Size	14.6 mm (nominal width at center) x 18.1 mm (nominal length)
Fingerprint Sensor Resolution	512 DPI
Operating System Support	Microsoft Windows 2000/XP
Power	110 VAC / 220VAC, 24VDC to Access Panel
Notes: [1] Actual capacity may vary depending on user selectable options	

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Chapter 1: Preparing for Installation

Site Survey and Preparation

Locating the BioAxs 9800IR™ Access Panel

The BioAxs 9800IR™ Access Panel should be mounted on a wall or structure to comply with all local and federal laws as they apply to the installation site.

Use the following guidelines when choosing a mounting location for the BioAxs 9800IR™:

- The panel is to be located at least 6 inches from the doorjamb and at least 1’ from any adjacent wall.
- In order to ensure the highest level of performance for facial recognition, the BioAxs 9800IR™ should be mounted such that the bottom of the access panel enclosure is at a height of 50-1/2” inches from the ground.
- Consideration should be given to the overall distance from the BioAxs 9800IR™ to the Entry point. Select a location that will allow a user to enter the secured facility within approximately 2 seconds of being granted access by the access control system.
- Always mount the BioAxs 9800IR™ opposite of the opening door swing direction to prevent interference with individuals exiting the secured area.

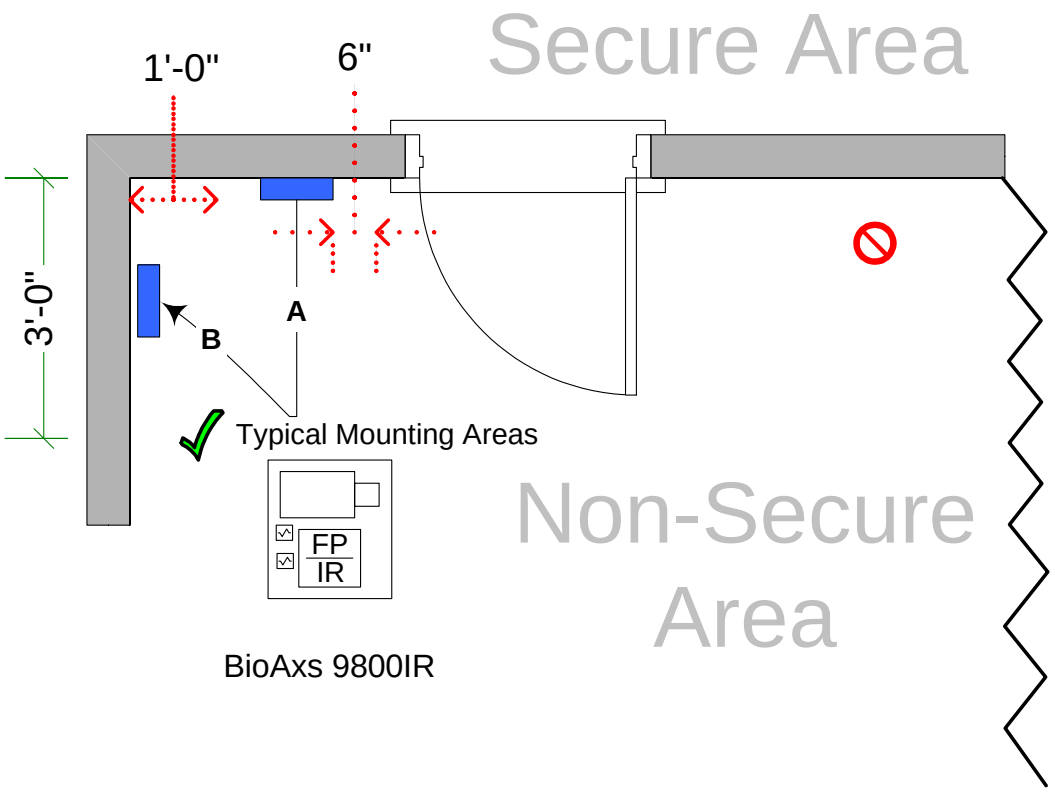


Figure 2 Typical Mounting Locations for the BioAxs 9800

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

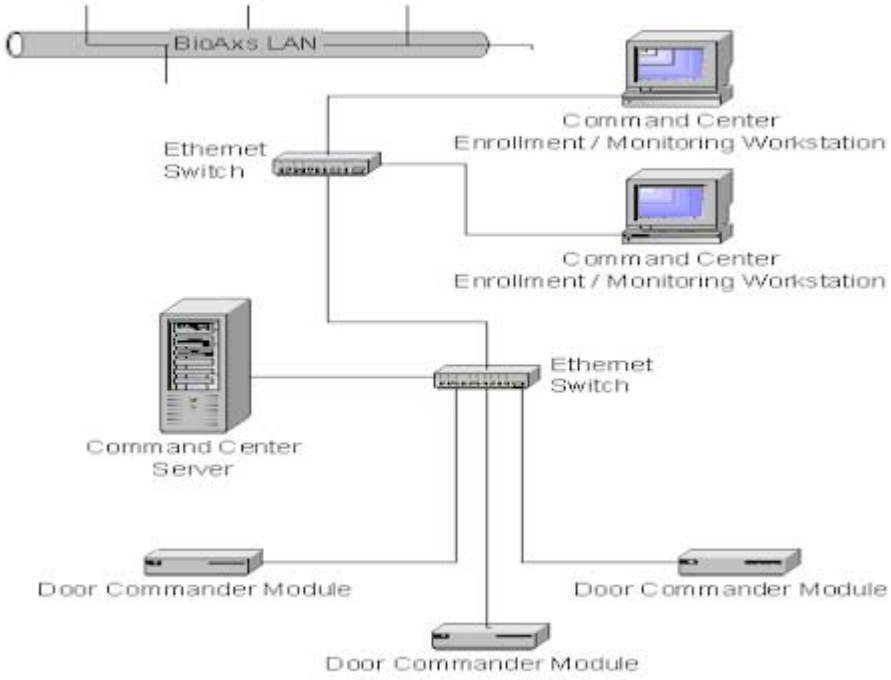
Locating the Door Commander Module (DCM)

The DCM Module is to be located at a cable distance no greater than 100 Meters (328 ft) from the BioAxs 9800IR™ Access Panel. Typical locations for the DCM include building communications closets, electrical rooms, etc.

Generally, the location should provide the necessary connection points for the power and LAN requirements of the system.

Ethernet Connectivity (LAN)

The BioAxs 9800IR™ Door Commander Module (DCM) requires a network connection to the NextgenID *Command Center*™ server across a 10/100 Mb/s Ethernet network. The Command Center Software allows centralized management and user enrollment of all BioAxs family access control panels. For a additional information see the accompanying document, *NextgenID Command Center System Administration and User Guide P*/N BA-DOC-CCSAUG. A standard RJ45 Cat 5 Network Jack is provided on the rear panel of the DCM.



✎ **Note** Always consult with your NextgenID support representative and/or the local site Network Administrator before connecting the BioAxs 9800IR™ system to any existing networks within a facility to ensure the proper network hardware and software security policies have been implemented.

Power Requirements

The BioAxs 9800IR™ access panel operates at 24 VDC requiring approximately 0.33 – 2.0[1] amps. Consideration should be given to common ground requirements when integrating the BioAxs 9800IR™ with existing access control systems. Select a secure location for mounting the power supply and associated cabling. The Door Commander Module (DCM) and the DCM Communications Extender units require 120 VAC.

The power supplies should be:

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

- Isolated from other equipment
- Regulated and filtered
- Protected by means of emergency power and/or battery backup providing at least 2 hours emergency backup power

⚠ Never connect the power supply to any device or component that may put transients on the power supply line or cause the power signal to fluctuate improperly.

See Chapter 3: Hardware Specifications for additional information

1. Amperage requirements may vary based on optional accessory and external device load.

Earth Ground

In order to protect the BioAxs 9800IR™ Access Panel device from electro-static discharge (ESD) The access panel requires a home run connection to Earth Ground[1, 2].

⚠ **Warning:** NextgenID may consider your warranty void if there is an improper earth ground connection to the BioAxs 9800IR™ Access Panel

1. See Chapter 3: Hardware Specifications for specific hardware specifications
2. See Chapter 4: Wiring Specifications for details on specific cabling types

Cabling Runs / Conduit Installation

Consult local building codes and regulations when making cabling runs. The installer should make every effort to minimize the amount of exposed conduit.

Installation Tools Required

- RJ45 Crimper
- Wire Cutters / Strippers
- Coax RCA Crimper
- Mini Screw Driver Set
- Drill and Drill Bits for mounting hardware and accessories to walls
- Carpenters Level
- Tape Measure
- Fish Tape – Pull Wire

Customer / Installer Supplied Hardware and Cabling

Below is a typical list of additional items required to install your BioAxs 9800IR™ Access Control System. Due to the variances in local building codes and regulations, these items are to be supplied by the customer/ installer. Please refer to the appropriate chapters in this document for specific hardware and wiring specifications as well as recommended vendors and item part numbers.

- Magnetic Door Sensor Switch [1]
- Magnetic Door Latch Or Door Strike (Up to 1Amp @ 12V-24V DC Load) [1,3]
- UL-Listed Class II 24V Linear Power Supply rated at 3-4 amps[1.] Battery backup capacity should be sufficient for at least 2 Hours of continuous usage.

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

- Wiring and Cable, for the items listed above [2]
- Wall Anchors - for use when installing wall mounted user access panel enclosure and Door Controller Module wall mount brackets

1. See Chapter 3: Hardware Specifications for specific hardware specifications
2. See Chapter 4: Wiring Specifications for specific details on cabling types
3. Magnetic Door Lock Devices typically require a Request-To-Exit Device. Use of request to exit push buttons may not be legal in your area; a single action exit mechanism may be required. Always consult local codes and regulations when installing such devices

ESD Precautions

The BioAxs 9800IR™ System contains electronics sensitive to electrostatic discharge. Take the necessary anti-static precautions when unpacking, handling and installing all electronic components. Do not remove the BioAxs 9800IR™ access panel from its container until you are ready to install it

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Chapter 2: Unpacking

When you are ready to install the BioAxs 9800IR™ you should unpack, identify and account for all items shipped with your BioAxs 9800IR™ Access Control System.

✎ **Note** Do not remove the BioAxs 9800IR™ from its shipping container until you are ready to install it. Keep the Access Panel in the shipping container until you have determined where you will install it.

⚠ **Caution** When handling the BioAxs 9800IR™ Access Panel without the back box, wear an ESD-preventive strap and use an antistatic mat to avoid possible ESD damage.

Unpacking the BioAxs 9800IR™ Access Control System

To unpack the BioAxs 9800IR™ Access Control System from the shipping container, follow these steps.

Your shipment should contain at least 2 boxes. Carefully remove or cut the tape that seals each shipping container and open the top of the outer shipping containers.

Note: shipping stabilizer material may differ from illustration.

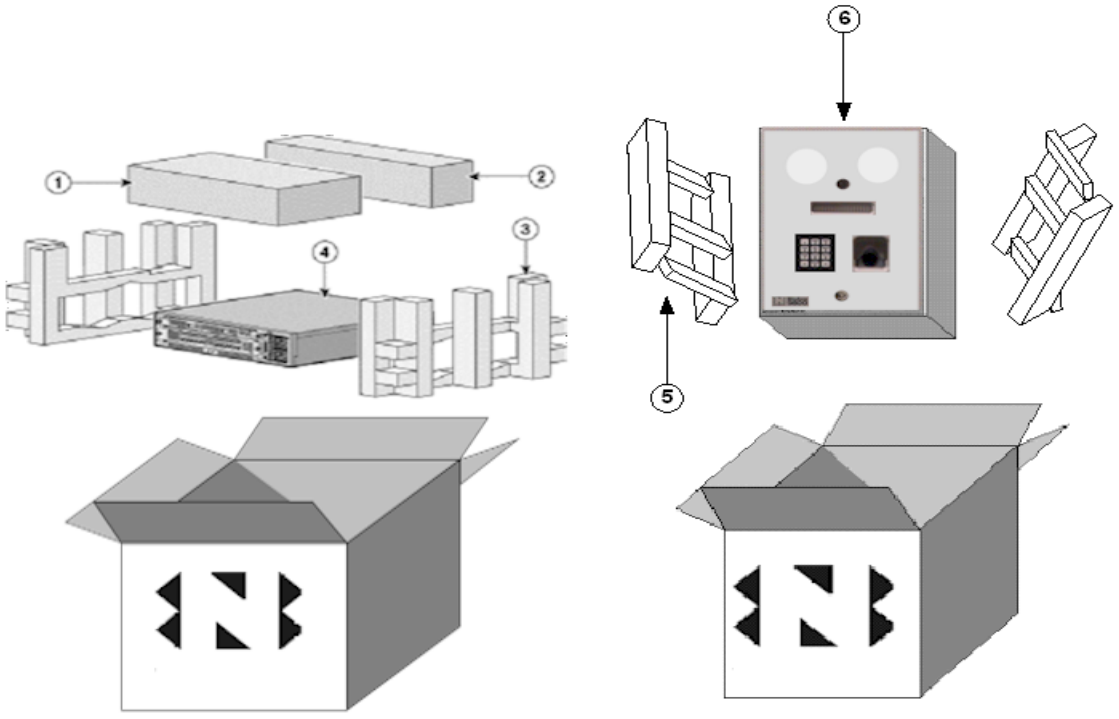


Figure 3 Unpacking

1	Accessory Box 1	**4**	Door Commander Unit (DCM)
2	Accessory Box 2	**5**	Foam brace / Shipping Stabilizer
3	Foam brace / Shipping Stabilizer	**6**	BioAxs 9800IR™ Access Panel and Back Box Assembly

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Verify Shipping Contents

Check the contents of the shipping packaging and verify that the following standard items are included with your shipment:

- BioAxs 9800IR™ Install and Operations Manual P/N: NG-DOC-BA9800IR™-IOM
- BioAxs 9800IR™ Installation and Wiring Diagram P/N: NG-DOC-BA9800IR™-IWDIAG
- Access Panel USB Extender Module P/N: NG-USBLEX-SHLD
- Access Panel DCM Communications Extender AC Adapter P/N: NG-USBLEX-AC
- Access Panel DCM Communications A-to-B USB Cable (3 ft.) P/N: NG-USBLEX-AB3
- FingerMatch HASP License Key (USB) P/N: NG-FM-HASP-USB
- ROU Serial Communications Adapter RS232 to RS 422 DB9 Adapter P/N: NG-BB422-PP9R
- Door Commander Module for IR panels (Pentium 4/ 512MB RAM) P/N: NG-DCM-IR-P4512
- Door Commander Module AC Power Cable (Pentium 4 models) P/N: NG-DCM-ACPWR-P4
- Door Commander Module Mounting Brackets (19" Rack mount) P/N: NG-DCM-BRKT-RM
- Door Commander Module Mounting Brackets (4.5" Wall mount) P/N: NG-DCM-BRKT-WM

- BioAxs 9800IR™ Access Panel (Surface Mount Indoor) P/N: BA-9800IR™-AP-SMI
  OR
  BioAxs 9800IR™ Access Panel (Surface Mount Outdoor) P/N: BA-9800IR™-AP-SMO

- BioAxs 9800IR™ Access Panel Enclosure (Surface Mount Indoor) P/N: BA-9800IR™-ENC-SMI
  OR
  BioAxs 9800IR™ Access Panel Enclosure (Surface Mount Outdoor) P/N: BA-9800IR™-ENC-SMO

Note: The BioAxs 9800IR™ Access Panel usually ships attached to the panel enclosure (back box).

Note: The Panel Keys are attached to the BioAxs 9800IR™ Front Faceplate.

If you did not receive everything you ordered, contact a NextgenID customer service representative for assistance.

Optional Equipment and Accessories

In addition to the standard items included with the BioAxs 9800IR™, your system may be configured with optional accessories. Verify you have received all optional equipment. If you did not receive everything you ordered, contact a customer service representative for assistance.

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Chapter 3: Hardware Specifications

Power Requirements

Access Panel Power Supply
The BioAxs 9800IR™ access control panel requires a 24VDC linear (4 amp continuous). NextgenID suggested manufactures and P/Ns:

Electronic Security Devices	SPS-20EL
Altronix LPS5C24X Linear Power Supply/Charger	LPS5C24X
Or Equivalents	

Door Commander Module (DCM)
120V AC Power

DCM Communications Extender
Input 120V AC
Output DC capacity 15V DC @ 1A

Battery Backup

Access Panel Power Supply
At least 24 VDC (4amp / hr.) battery backup should be supplied or integrated with the Access Panel 24VDC Power Supply providing 2-4 hours of full operational backup.

✎ **Note:** Actual backup time is dependent on the load and age of the battery. To maintain the maximum backup time, it is recommended that you replace the DC power supply battery every two to four years. Test regularly according to manufacturers instructions.

DCM Uninterruptible Power Supply (UPS)
An uninterruptible power supply device providing backup power to the DCM, Communications Extender and Optional Network Hub should be rated for at least 750VA / 800W, (Input 120V Output 120V) providing at least 2-4 hours of full operational backup.

✎ **Note:** To maintain the maximum backup time, test regularly and replace the UPS batteries every two to four years.

✎ **Note:** To maximize continuous operation, It is suggested that all 120 VAC connections be tied in to the Building Emergency Power when available.

Output Power

505X/506X Door Controller Board (DCB)
12 VDC (10 to 14 volts) 500 mA for readers and accessories requiring 12 VDC
5 VDC, 500 mA output is available for readers and accessories requiring 5 VDC

Earth Ground

Access Panel Earth Ground Connection
Proper Earth Ground Requires <4 ohms resistance when measured against a known local earth ground.

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

⚠ **Warning:** NextgenID may consider your warranty void if there is an improper earth ground connection to the BioAxs 9800IR™ Access Panel

Relay Output Points

- 1 double pole, double throw (DPDT) relay contact with both normally open and normally closed sides. Rated for 5 / 12 / 24 VDC 2 amp inductive loads.

Alarm Input Points

- Enclosure tamper switch
- Door Sensor
- Alarm Shunt
- Request To Exit

Operating Temperatures

BioAxs 9800IR™ Access Panel
-0°C to +40°C

Door Commander Module
+0°C to +50°C

DCM Communications Extender
+4°C to +40°C

Operating Relative Humidity

BioAxs 9800IR™ Access Panel
0% to 85% non-condensing

Door Commander Module
0% to 85% non-condensing

Dimensions

BioAxs 9800IR™ Access Panel
11.25” x 18.25” x 4.75” (285.75mm x 463.55mm x 120.65mm)

Door Commander Module
260 mm x 240 mm x 62mm

DCM Communications Extender
100mm x 80mm

Weight

BioAxs 9800IR™ Access Panel
11 pounds, 2oz

Door Commander Module
3.0 Kg.

DCM Communications Extender
0.11 lb (50g)

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Chapter 4: Wiring Specifications

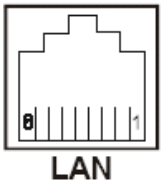
Networking

UTP Category 5 Ethernet Cable (Plenum / PVC / Riser per Application)

Suggested P/N:

- Belden 1585A Plenum UTP Cat 5e
- Belden 1583A PVC UTP Cat 5e
- Belden 1583R Riser UTP Cat 5e
- Or Equivalent

LAN Connector Pin Assignments



Straight Through Network Cable Pinouts

PIN	Assignment	Wire Color
1	TX+	Orange / White
2	TX -	Orange
3	RX+	Green / White
4	ISOLATED GND	Blue
5	ISOLATED GND	Blue / White
6	RX-	Green
7	ISOLATED GND	Brown / White
8	ISOLATED GND	Brown

Distance guidelines apply to wired networks:

Type	Maximum Distance
Hub-to-Hub (100BaseTX)	5 Meters (16.4 Feet)
Hub-to-Hub (10BaseT)	100 Meters (328 Feet)
Hub-to-Switch	100 Meters (328 Feet)
Workstation to Hub or Switch	100 Meters (328 Feet)
Node-to-Node with Multi-mode Fiber Optic Cabling in Full Duplex Mode	2000 Meters (6560 Feet)

DCM Communications Extender (Access Panel to DCM Extender Unit)

UTP Category 5 Shielded Ethernet Cable (Plenum / PVC / Riser per Application)

Note: Shielded cable requires the use of shielded RJ45 Connectors Ends**.**

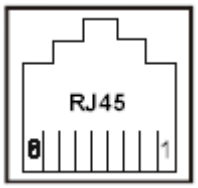
Suggested P/N:

- Belden 1624P Plenum shielded 4-pr. Cat 5
- Belden 1624R Riser shielded 4-pr. Cat 5
- Or Equivalent

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Maximum DCM Extender Cable Distance: 100M (328ft)

DCM Communications Extender Pin Assignments

PIN	Wire Color
	
1	Orange / White
2	Orange
3	Green / White
4	Blue
5	Blue / White
6	Green
7	Brown / White
8	Brown

Access Panel Video Cable

Suggested P/N:

- RG-59U, 23 AWG, solid, braid shield, PVC jacket
- RG-6U, 18 AWG, solid, foil/braid shield, PVC jacket
- Or Equivalent

✎ **Note** 1 RCA Video Connector End suitable for the chosen cable type is necessary for connection to the Composite Video Input of the Door Commander Unit

Iris Recognition Video Cable

Suggested P/N:

- RG-59U, 23 AWG, solid, braid shield, PVC jacket
- RG-6U, 18 AWG, solid, foil/braid shield, PVC jacket
- Or Equivalent

✎ **Note** 2 BNC Female Video Connector Ends suitable for the chosen cable type is necessary for connection to the BNC Iris Video Inputs of the Door Commander Unit and BioAxs 9800IR

Iris Recognition Serial Communications RS422 Cable

UTP Category 5 Ethernet Cable (Plenum / PVC / Riser per Application)

Suggested P/N:

- Belden 1585A Plenum UTP Cat 5e
- Belden 1583A PVC UTP Cat 5e
- Belden 1583R Riser UTP Cat 5e
- Or Equivalent

Door Commander Unit Connector for IrisAccess™ 3000 Serial communications (DB9M)
The DB9 Male pin configuration of the Iris Recognition Unit serial communication cable for connection to Door Commander Unit is shown in the following table

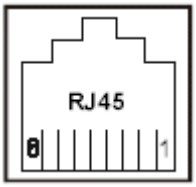
Copyright ©2004 NextgenID, Ltd. All Rights Reserved

IrisAccess 3000 ROU Serial Connection (DB9 Male)

Pin	Wire Color 	Function
1	Not Used	NC
2	Orange	RxD-
3	Brown	TxD+
4	Green / White	GND
5	Not Used	NC
6	Green	GND
7	Orange / White	RxD+
8	Brown / White	TxD-
9	Not Used	NC

Access Panel Connector for IrisAccess™ 3000 Serial communications (RJ45)
The pin configuration of the serial communication cable for connection to ROU 3000 Iris Recognition Unit is shown in the following table

IrisAccess 3000 ROU Serial Connection (RJ45)

PIN	Wire Color 	Function
1	Orange / White	RxD+
2	Orange	RxD-
3	Green / White	GND
4	Blue	NC
5	Blue / White	NC
6	Green	GND
7	Brown / White	TxD-
8	Brown	TxD+

24V Power Cable

- 14 AWG 2 Conductor Cable

Alarm Input points

- 18 – 22 AWG shielded twisted pair.

Relay outputs

- 18 – 22 AWG shielded twisted pair.

Wiegand Signaling

- 18 AWG 6-conductor shielded twisted pair.

Earth Ground

Access Panel Earth Ground Connection

- 14 AWG Solid - 10 AWG Stranded

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

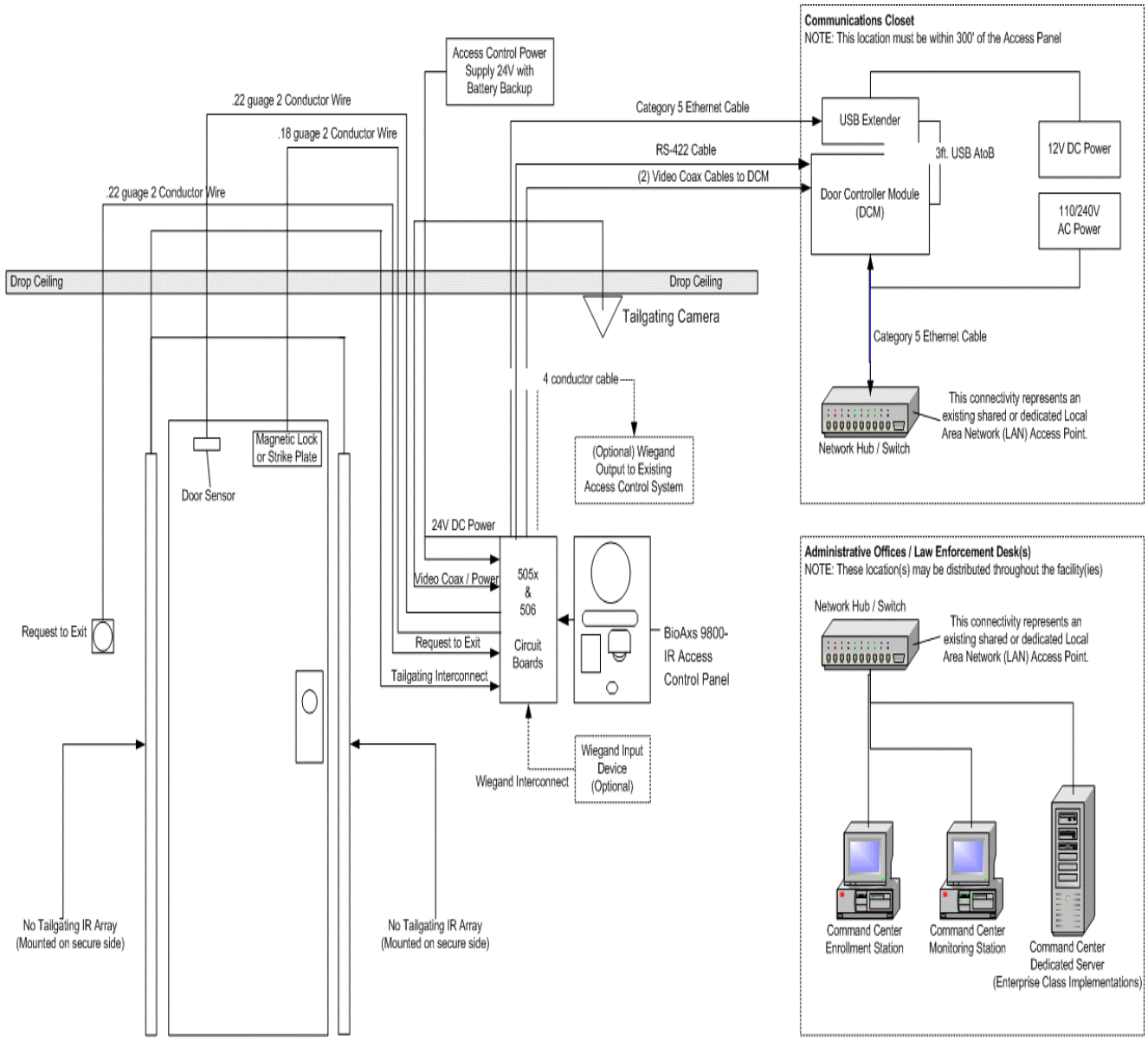
Chapter 5: Wiring Overview

This chapter provides a conceptual overview of the general wiring layout for the installation of a BioAxs 9800IR™ Access Control System.

Note: A detailed large-scale connection and wiring diagram is available on request. P/N NG-DOC-BA9800IR-IWDIAG. To obtain a copy of the detailed connection diagram, Please contact your NextgenID support representative.

The following diagram insert depicts a typical wiring installation for a single BioAxs 9800IR Access Panel.

Figure 4 typical wiring installations BioAxs 9800IR™



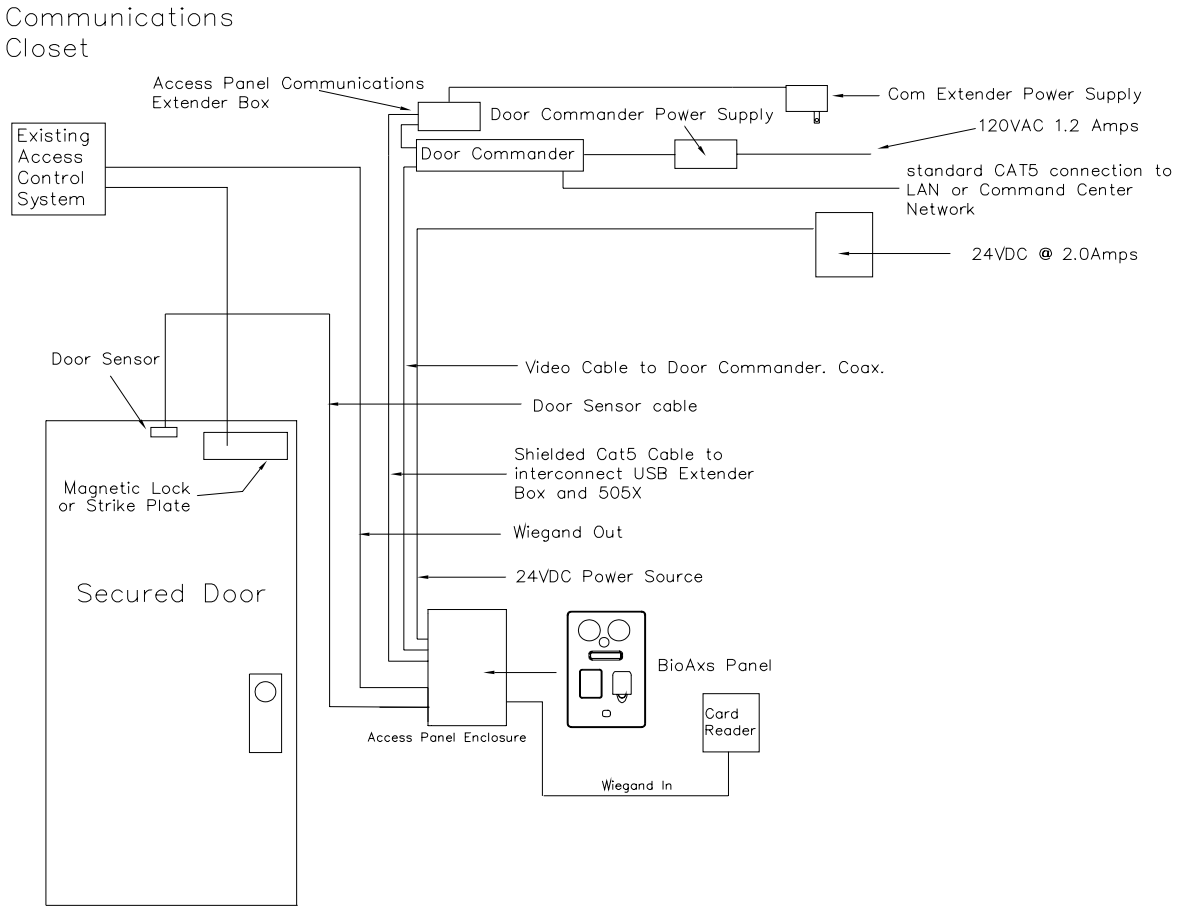
NextgenID BioAxs 9800IR with Tailgating Countermeasure Wiring Installation Diagram

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Wiring for an Integrated Installation

An Integrated Installation refers to the installation scenario where the BioAxs Access Control System works in conjunction with an existing access control system to control access to a facility. In this case, the BioAxs Access Control System typically handles the tasks of user Identification and access rights verification. The existing access control system handles lock control and is informed of access granted events via the 26-bit Wiegand output functionality of the BioAxs system. Figure 6 illustrates the typical cable routing and wiring connections for an integrated installation.

Figure 5 typical wiring installations: Integrated with Existing Access Control System



Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Chapter 6: Installation

Door Commander Module Installation

The Door Commander Module (DCM) is an industrial small form factor computer that is included with each BioAxs 9800IR™ system. The DCM and BioAxs 9800IR™ must be located within 100 meters of one another. Operating temperature range for the DCM is 32° F to 140° F (0° - 60C).

Located with the DCM is the DCM Communications Extender, this device is responsible for relaying communications between the BioAxs 9800IR™ Access Panel and the DCM. The Communications Extender plugs directly into an available USB port on the DCM.

The DCM and the DCM Communications Extender should be powered thru an Uninterruptible Power Supply (UPS) (Battery Backup device rated at least 750 VA.

The following sections layout the typical installation procedures for the DCM unit and associated devices.

Mount the Door Commander Module (DCM) Unit

Upon choosing the location for the DCM (see Chapter 1: Locating the Door Commander Module), Mount the DCM in the appropriate configuration (Rack or Wall mount) using the supplied mounting brackets.

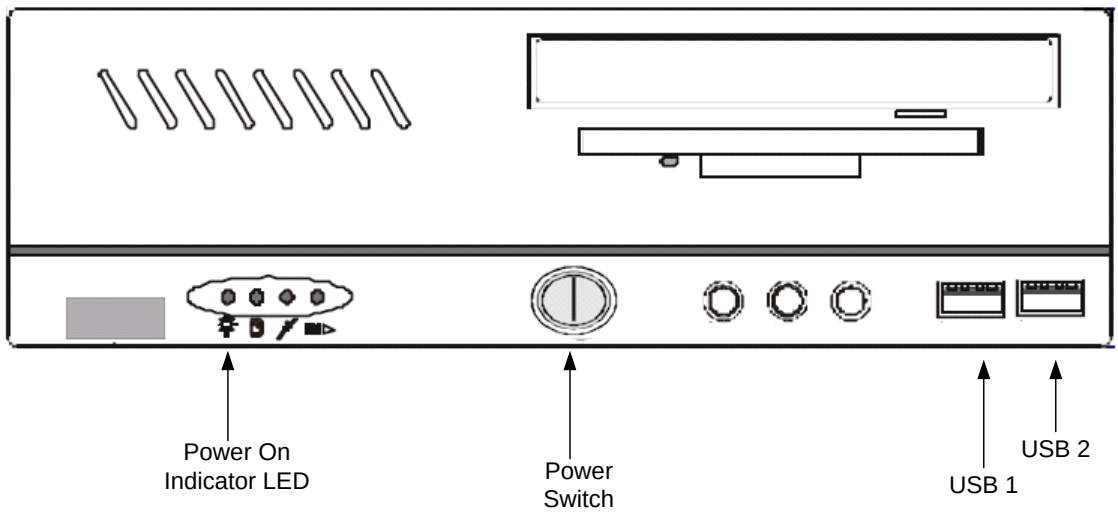


Figure 7 DCM Front View

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

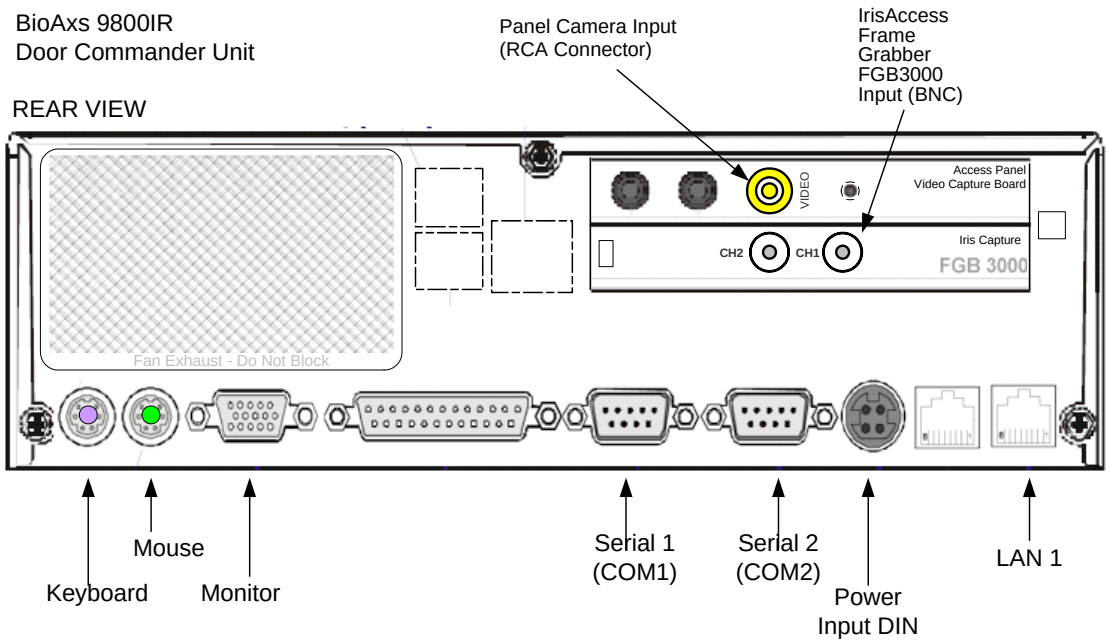
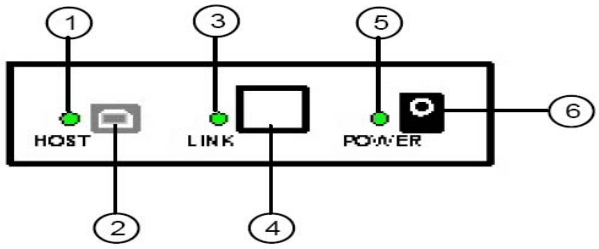


Figure 8 Door Commander Module Rear Panel View

Mount the DCM Communications Extender Unit

Locate and mount the DCM Communications Extender near the DCM
The distance from the Communications Extender to an available USB port on the DCM should not exceed 6 feet.

Once mounted, connect the DCM Communications Extender to an available USB port located on the front panel of the DCM using the supplied USB cable.



1 Host LED
2 Host Port (USB Type B)
3 Link LED
4 Link Port (RJ45)
5 Power LED
6 Power connector

Figure 9 DCM Communications Extender Connections

Install the FingerMatch™ Hardware Licensing Device

Attach the licensing device to the DCM by plugging it into the USB 2 port on the front panel of the DCM

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Figure 10: FingerMatch™ Hardware Licensing Device (USB)

Install the Uninterruptible Power Supply (UPS)

Locate the UPS at a distance sufficient to attach the supplied DCM power cable and the supplied DCM Communications Extender AC Adapter. Connect the UPS to an available 120V AC outlet. Leave the UPS Un-Powered at this time.

Note: To ensure optimum performance, most UPS battery systems require at least a 24-hour connection to wall current before use. Always Read and observe manufacturer instructions before use. Be sure to attach the DCM and DCM Communications Extender power cables to UPS outlets with Battery backup protection.

DCM & DCM Communications Extender Power Connections

Attach the Supplied DCM power cable to the AC Power Jack located on the rear panel of the DCM (figure 8). Plug the cable into a UPS outlet supplying battery backup.

Attach the DCM Communications Extender AC Adapter to the Rear of the Extender Unit. Plug the Adapter into a UPS outlet supplying battery backup

Install the 24VDC Access Panel Power Supply

Locate the 24VDC power supply according to the guidelines in Chapter 1:Power Requirements. Always follow the Manufacturers instructions when mounting and installing this unit. When installing the BioAxs 9800IR™ Access Control system in integration mode, observe common grounding requirements. Refer to the Section *Wire Installation* later in this chapter for attaching the 2-conductor power cable to the BioAxs 9800IR™ Access Panel.

BioAxs 9800IR™ Panel Enclosure Installation

The following sections layout the typical installation procedures for the BioAxs 9800IR™ unit

Mounting the BioAxs 9800IR™ Access Panel Enclosure

Select a location for the 9800IR™ Access Panel (see Chapter 1 - Locating the BioAxs 9800 Access Panel). Remove the BioAxs 9800IR™ access panel from its packing. Detach the BioAxs 9800IR™ Access Panel Face Plate from the Access Panel Enclosure (Back Box) by using the attached keys. Set the faceplate aside at this time.

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

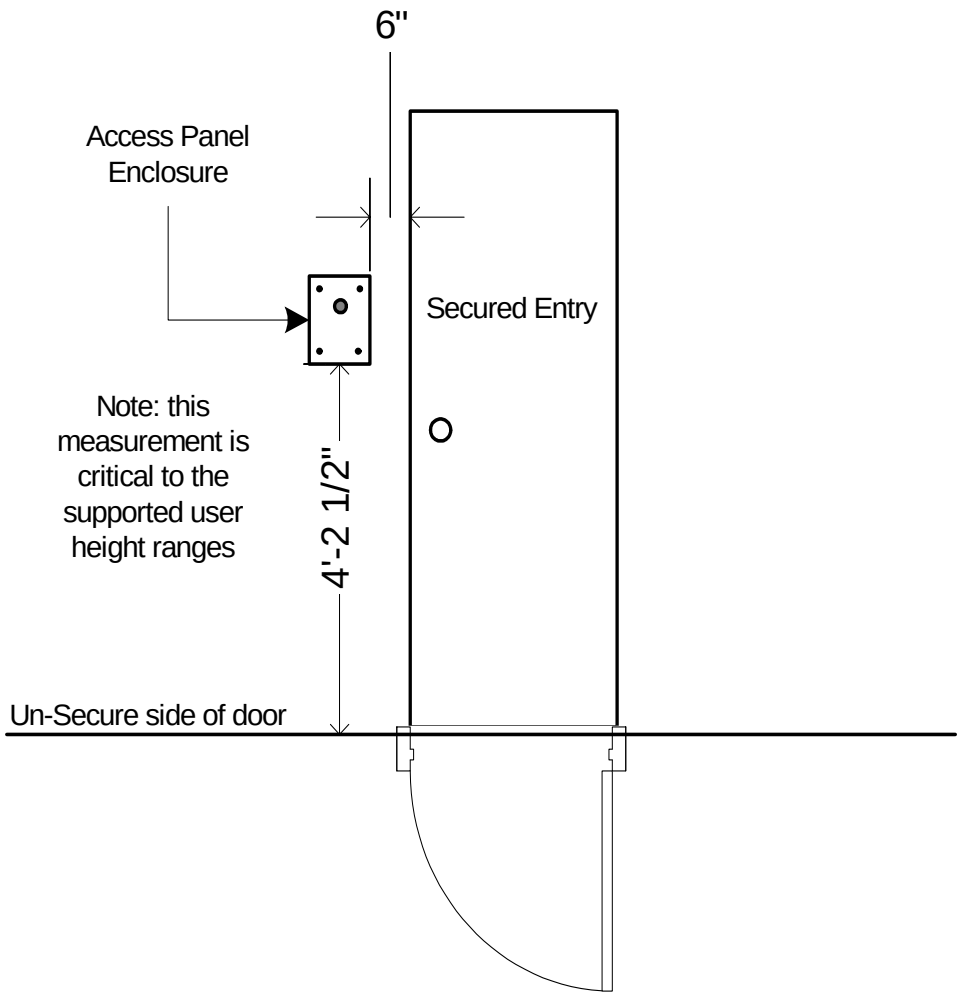


Figure 11: BioAxs 9800IR™series Enclosure mounting height

Figure 11 above shows the proper mounting height for the BioAxs 9800IR Access Panel Enclosure. The bottom of the enclosure should measure 50-1/2" from the floor.

Using the enclosed *9800IR series enclosure as a template*, mark the wall locations for the Access Panel enclosure anchor points and cabling exit hole. The cable exit hole should be at least 1" in diameter to accommodate standard wiring installations.

In a typical installation, the required cabling will run hidden through wall and enter into the Access Panel Enclosure through the cable exit hole. If your requirements differ, please consult with a NextgenID Installation Specialist.

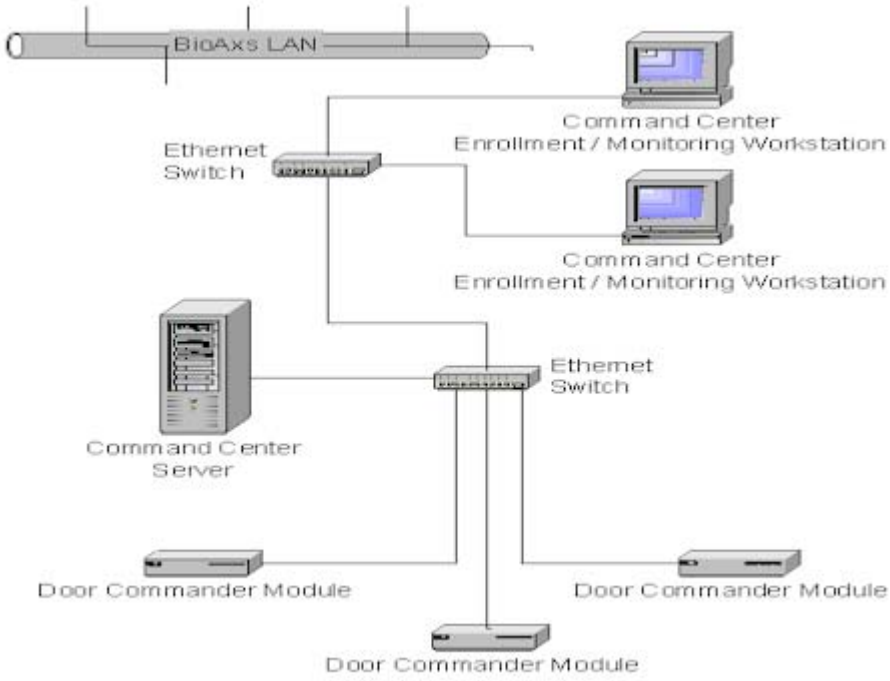
✎ Select wall anchors recommended for the type of wall material and security needs at the installation site.

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Wiring Installation

Door Commander Module (DCM) Connections

DCM Ethernet Connection (LAN)
The BioAxs 9800IR™ Door Commander Module (DCM) requires a network connection to the NextgenID *Command Center*™ server across a 10/100 Mb/s Ethernet network. A standard RJ45 Cat 5 Network Jack is provided on the rear panel of the DCM (figure 8).



Note Always consult with your NextgenID support representative and/or the local site Network Administrator before connecting the BioAxs 9800IR™ system to any existing networks within a facility to ensure the proper network hardware and software security policies have been implemented.

DCM Communications Extender
Using the supplied USB host cable, connect the DCM Communications Extender (figure 9) to the USB 1 connection on the front panel of the DCM (figure 7)

Access Panel Video
Access Panel video is carried over coaxial cable from the J12 connector on the BioAxs 9800IR™ Access Panel to the composite video in input located on the rear panel of DCM. Terminate the coaxial cable with a male RCA video connector. Plug the terminated cable into the *composite video in (access panel video)* input on the rear panel of the DCM (figure 8)

Iris Recognition Video Frame Grabber Connection (FGB3000)
Iris recognition Video is carried over coaxial cable from the BNC Video connector on the BioAxs 9800IR™ Access Panel to the FGB3000 BNC video CH1 input located on the rear panel of DCM. Terminate the coaxial video cable with a female BNC video connector. Plug the terminated cable into the *Channel 1 (CH1)* input on the rear panel of the DCM (figure 8)

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Iris Recognition Serial Communications Connector
The DCM Communicates with the IrisAccess™ 3000 unit via RS422 Serial communications..
Plug the DB9M D-Sub connector into the RS422 Side of the provided RS232 to RS422 converter.
Plug the Converter into the *Serial 1 (COM1)* input on the rear panel of the DCM (see figure 8)

BioAxs 9800IR™ Door Controller Board (DCB) Layout
The figure below shows the rear panel of the BioAxs 9800IR™ Access Control Panel. The Door Controller Boards (DCBs) are positioned on the rear of the access panel faceplate in a two-level design.

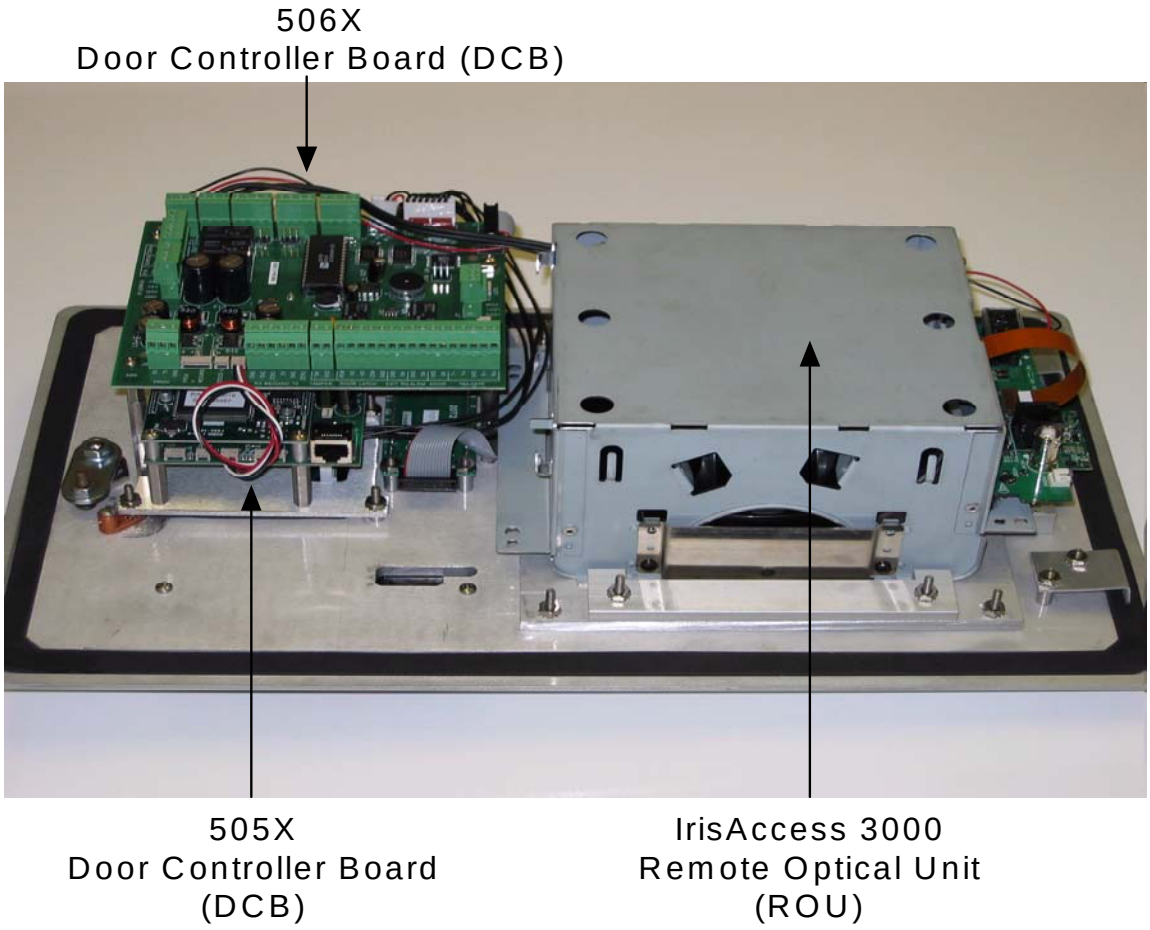


Figure 12: Rear View BioAxs 9800IR™ Access Panel

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

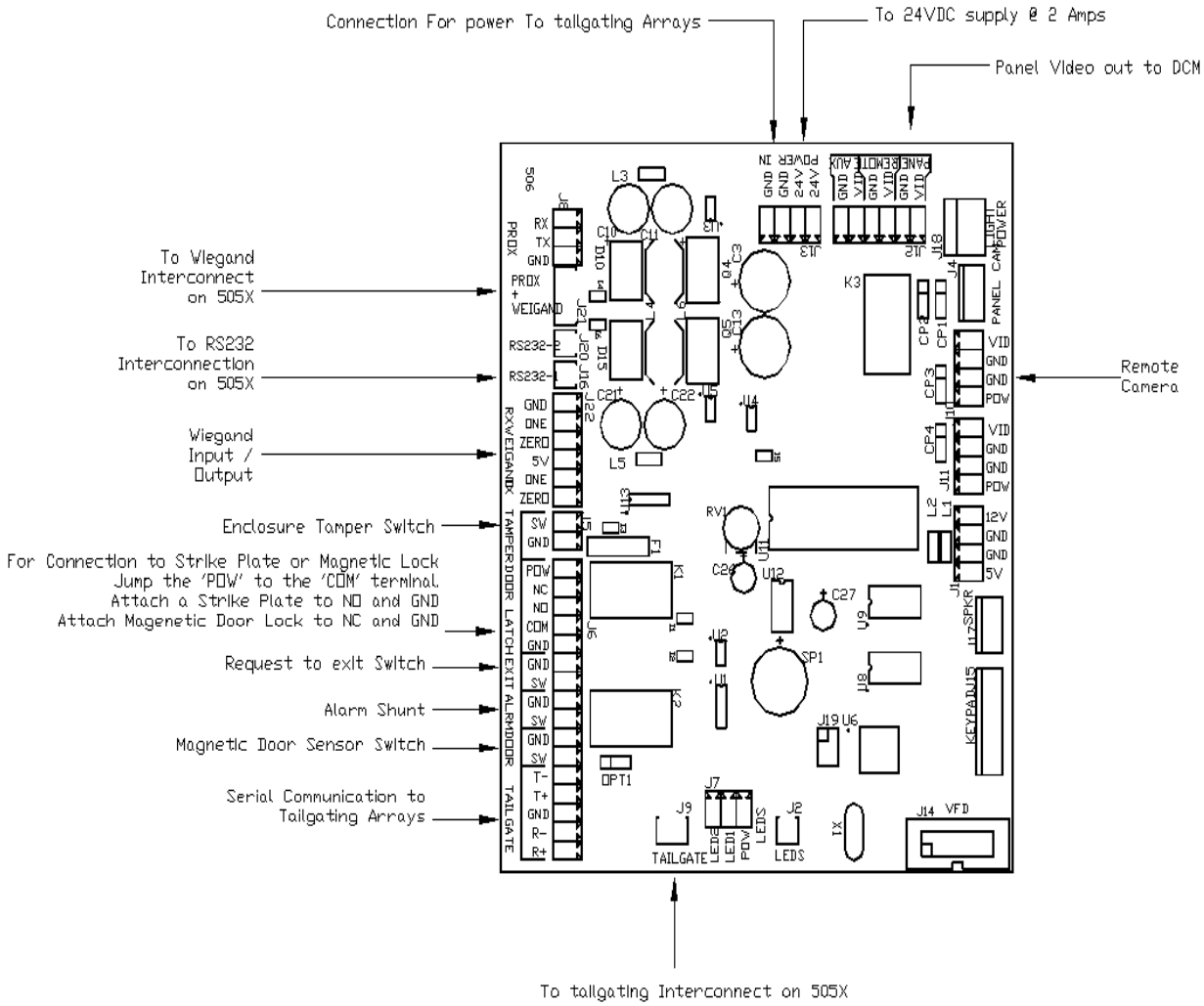


Figure 13: 506X DCB Connection Overview

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

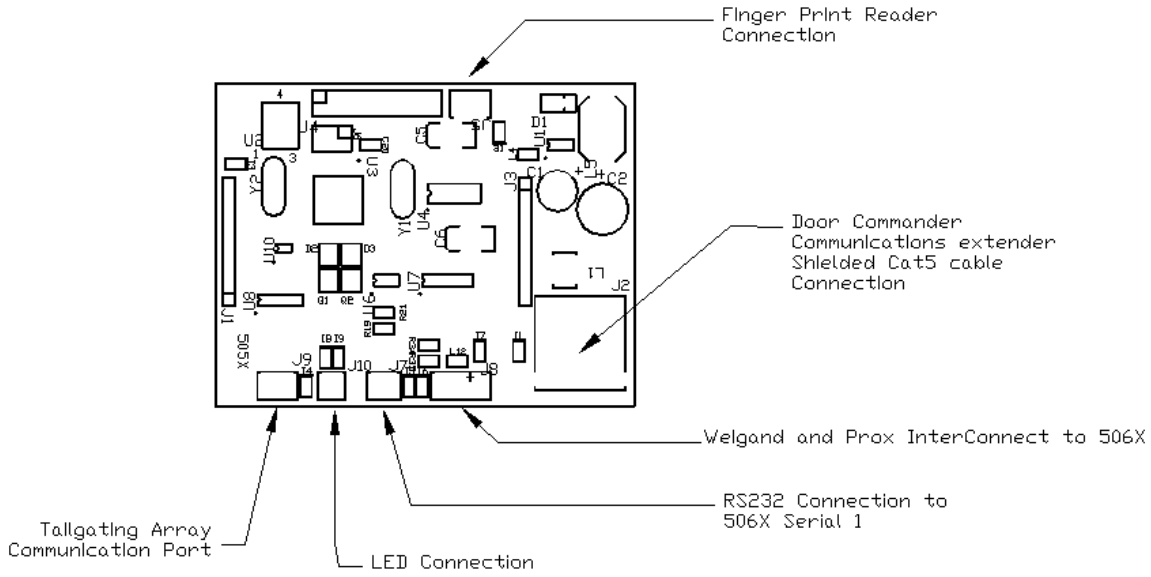


Figure 14: 505X DCB Connection Overview

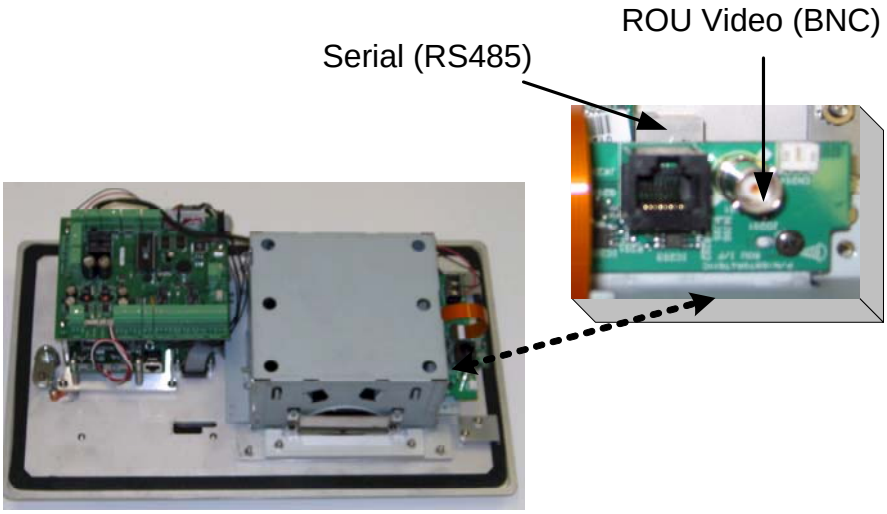


Figure 15 IrisAccess 3000 Remote Optical Unit Connection Overview

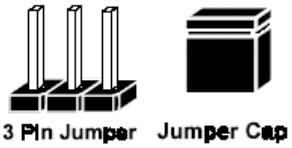
BioAxs 9800IR™ Access Panel DCB Wiring Connections

The following section details the connections necessary to complete the wiring installation of your BioAxs 9800IR™ Access Control Panel.

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Jumpers

The various jumper configuration options that are referred to in the following sections utilize 3 pin jumper terminals requiring the use of 2 pin Jumper caps



LG Iris IrisAccess™ 3000 Connections

Iris Recognition Video

Connect the Iris Recognition BNC Video Cable to the Male BNC Connector on the ROU 3000 located on the rear of the access panel (top). See figure 15

Iris Access™ 3000 Remote Optical Unit (ROU) Serial Communications

Connect the Iris Recognition Serial Communications RJ45 Connector Cable to the female RJ45 connector on the ROU 3000 located on the rear of the access panel (top). See figure 15

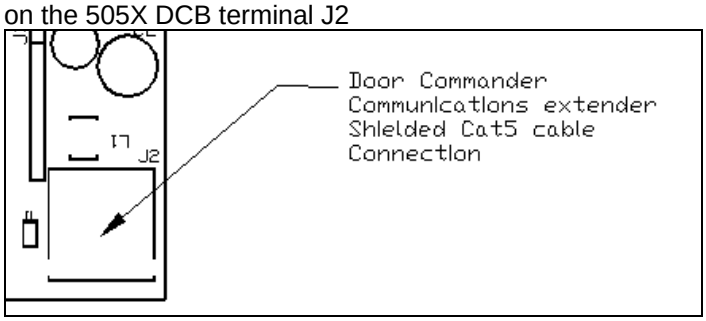
505X DCB Standard Connections

505X DCB to 506X DCB Interconnects

The 505X to 506X DCB Interconnections are factory installed. DCB Board interconnects points are illustrated in figures 13 and 14 above. For additional information, contact a NextgenID Support Representative.

DCM Communications Extender (J2)

Connect the Shielded Cat5 DCM Communications Extender Cable to the RJ45 connector on the 505X DCB terminal J2



DCM Communications extender RJ45 connector (J2)

506X DCB Standard Connections

505X DCB to 506X DCB Interconnects

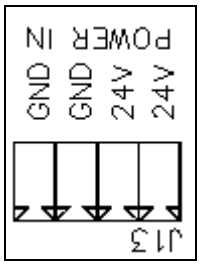
The 505X to 506X DCB Interconnections are factory installed. DCB Board interconnects points are illustrated in figures 13 and 14 above. For additional information, contact a NextgenID Support Representative.

Power (J13)

Connect the ground and power leads from the 24VDC Linear Power Supply to the [GND, 24V] terminals on J13 terminal.

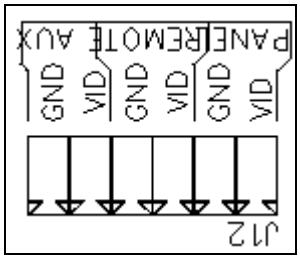
Copyright ©2004 NextgenID, Ltd. All Rights Reserved

✎ **Note** It is only necessary to use a single set [GND and 24V] of terminals for this connection. The remaining [GND, 24V] terminals serve as an auxiliary 24VDC output source for external devices.



Power (J13)

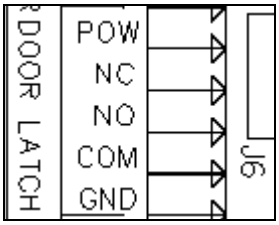
Panel Video (J12)
The output for all connected video sources is provided by the connections on the J12 Terminal. Connect the coaxial video cable run from the DCM to the J12 terminals labeled PANEL (VID +, GND -)



Panel Video Out (J12)

Relay Output Points

Door Latch (J6 & OPT1)
The door latch mechanism (Magnetic Lock / Electric Door Strike) connections are made on terminal J6. (POW, NC, NO, COM, GND).



Door Latch (J6)

Door Latch Power
Depending on the type and manufacturer of your door latch hardware, your latch mechanism may require either 12VDC or 24VDC. Configure the DCB to deliver power to the latch mechanism as follows:

12V Door Latch Mechanism

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Using a small section of cable, jumper from the J6 **POW** terminal to the J6 COM terminal.

24V Door Latch Mechanism
Using a small section of cable, jumper from the J13 **24V** terminal to the J6 **COM** (Common) terminal.

Door Latch Ground
Attach the ground connection from your door latch mechanism to the **GND** terminal in the DOOR LATCH section of Terminal Block J6.

Door Latch Operation Mode (OPT1)
Your latch mechanism may operate in either NORMALLY OPEN (NO) or NORMALLY CLOSED *(*NC) mode. Attach the power lead from your door latch mechanism to either the NO or NC terminal in the DOOR LATCH section of Terminal Block J6.

Configure the 506x **OPT1 Jumper** to operate in either NO or NC mode as follows

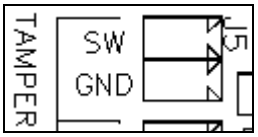
Door Latch Mode Configuration Options (OPT1 Jumper Settings)

Normally Closed (NC) – Typical for Magnetic Lock

Normally Open (NC) – Typically for Door Strike

Alarm Input Points

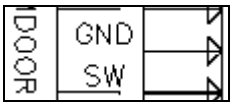
Enclosure Tamper Alarm (J5)
The access panel enclosure comes with a tamper switch and leads pre-installed at the factory. Connect the tamper switch leads to the TAMPER section of terminal **J5** at the SW and GND connection points (polarity neutral)



Enclosure Tamper Switch (J5)

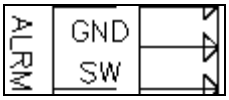
Door Sensor Switch (J6)
Connect the door sensor switch leads to the DOOR section of terminal **J6** at the SW and GND connection points (polarity neutral)

Copyright ©2004 NextgenID, Ltd. All Rights Reserved



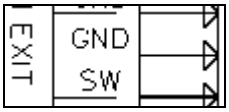
Door Sensor Switch (J6)

Alarm Shunt (J6)
Connect the alarm override release leads to the ALRM section of terminal **J6** at the SW and GND connection points (polarity neutral)



Alarm Shunt (J6)

Request To Exit Switch (J6)
Connect the Request To Exit switch leads to the EXIT RQ section of terminal **J6** at the SW and GND connection points (polarity neutral)



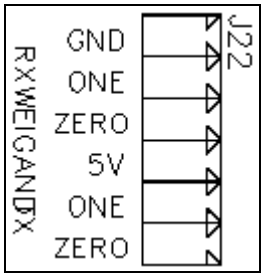
Request To Exit (J6)

Optional Connections

Wiegand Input and Output Connections (J22)

External Wiegand Reader Input
Connect the external Wiegand reader leads to the [GND, ONE, ZERO, 5V] terminals on the RX (receive) side of terminal **J22**. For 12V readers connect Ground and Power leads to terminal J1

Card Reader Output (Wiegand Out)
Connect the external Wiegand out leads to the [ONE, ZERO] terminals on the TX (transmit) side of terminal **J22**. Observe common ground requirements.



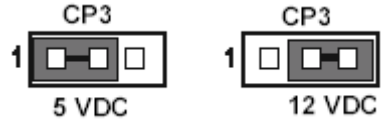
Wiegand Transmit and Receive J22

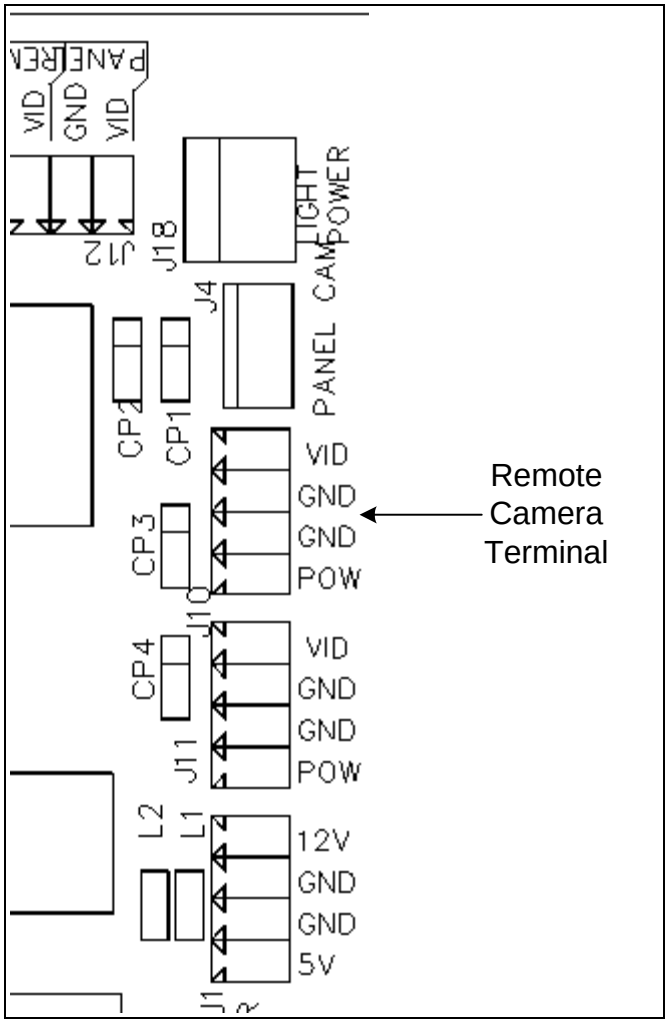
Note The [ZERO, ONE] labels on J22 correspond to typical Wiegand data0 and data1 signals respectively. For integrated installations, if ground fault conditions exist between the 506 DCB and the external access control system, it may be necessary to provide opto-isolation for the Wiegand output signal. Contact a NextgenID support representative for additional information.

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Remote Camera (J10)
Connect the Video Signal (+) lead to the [VID] connector of terminal **J10**. Connect the Video Signal ground lead to the GND connector adjacent to the VID terminal. 12V DC power is provided on connectors [GND and POW]

Remote Camera Voltage (CP3)
Depending on the camera voltage (5V or 12V) set option on Jumper **CP3** as follows





Remote Camera Video Signal and Power (J10)

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

NoTailgatingIR (J6)
Connect the Transmit (-) lead from the NoTailgatingIR array to the [T-] connector in the TAILGATE section of terminal J6

Connect the Transmit (+) lead from the NoTailgatingIR array to the [T+] connector in the TAILGATE section of terminal J6

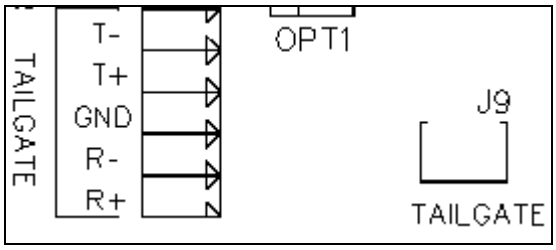
Connect the Ground lead from the NoTailgatingIR array to the [GND] connector in the TAILGATE section of terminal J6

Connect the Receive (-) lead from the NoTailgatingIR array to the [R-] connector in the TAILGATE section of terminal J6

Connect the Receive (+) lead from the NoTailgatingIR array to the [R+] connector in the TAILGATE section of terminal J6

The factory installed 505x interconnection cable is required on J9.

Detailed information for installation of the NoTailgatingIR can be found in the NoTailgatingIR Installation Manual



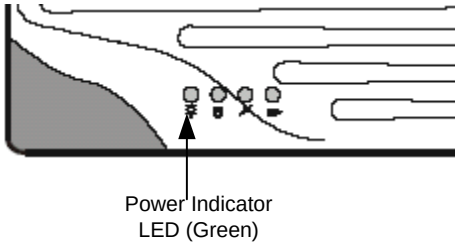
NoTailgaitingIR (J6), 506x to 505x Tailgating Interconnect (J9)

Powering the System

When all DCB connections have been completed, power may be applied to the system.

1. Power on the UPS supplying power to the DCM and DCM Communications Extender. The DCM indicates power on with a Green Led on the Front Panel. If the DCM power indicator is not lit, press the power button to turn it on.

DCM Front Panel



2. Apply Power to the 506X DCB by activating the 24V Power Supply.

Verify your connections and secure the faceplate to the enclosure and lock.

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Chapter 7: System Activation

NextgenID Command Center Server and Client Software

Activating the BioAxs 9800IR™

Once the installation of the access panel hardware and its supporting components has been completed, the next step in the implementation process is DCM and BioAxs Panel Activation.

The BioAxs 9800IR™ Access Panel is always implemented in a one-to-one relationship with a Door Commander Module (DCM). The details of the cabling between these two components are covered in previous chapters of this guide.

To prepare the system for activation, complete the following steps:

Power the access panel 506 Door Controller Board (DCB) with 24 Volt DC Power
Power the USB Extender and DCM units with 110V AC Power
Ensure that a network cable (Category 5 Ethernet) is connecting the DCM to a local area or private network that provides connectivity between the DCM and the Command Center server.
DHCP Client – The default configuration of the DCM unit is to come online as a DHCP Client (i.e. on startup/boot up it will search the network for a DHCP Server to receive a valid TCP/IP Address). If no such server exists, connectivity establishment between the DCM and the Command Center server will fail (in this case use fixed IP Address as explained in option ii.)
Fixed IP Address – To use a fixed TCP/IP Address on the DCM, connect a keyboard, mouse and monitor to the system prior to booting up. Modify the TCP/IP settings to use a fixed IP Address instead of acting as a DHCP client.

For logging onto the DCM system use:
Username: `administrator`
Password: `NextgenID`

Ensure that all Windows Services required for the Command Center application are ‘started’. These required services are:
DoorCommanderRestartService
NGIDDoorCommander
Message Queuing
MSSQL Server

Each of these services will be configured to start automatically by default when the DCM is installed and configured at the factory. To confirm that each of the above services are ‘started’ log on to the DCM computer and use the ‘Services’ console in the Administrative Tools folder of the computer’s Control Panel.

Once each of the above steps has been completed or confirmed, the DCM and Access Panel are ready to be activated by your Command Center system. For specific instructions on performing this task, refer to the Administration section of the *Command Center System Administration and User Guide*.

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Chapter 8: Using the Panel

This chapter will review the typical activation and usage scenarios associated with the BioAxs 9800IR™ access panel.

Pre-Requisites for Panel Use

Before using your BioAxs 9800IR™ Access Panel, the following items must be completed:

Hardware Installation

The physical installation of the Access Panel hardware has been completed and tested (see detailed installation instructions in Chapter 6 of this manual).

Access Panel Activation

An authorized administrator of the Command Center Access Control Software™ has activated the BioAxs 9800IR™ Access Panel (detailed instructions may be found in the Administration section of the *Command Center System Administration and User Guide*).

Member Enrollment and Privilege Assignment

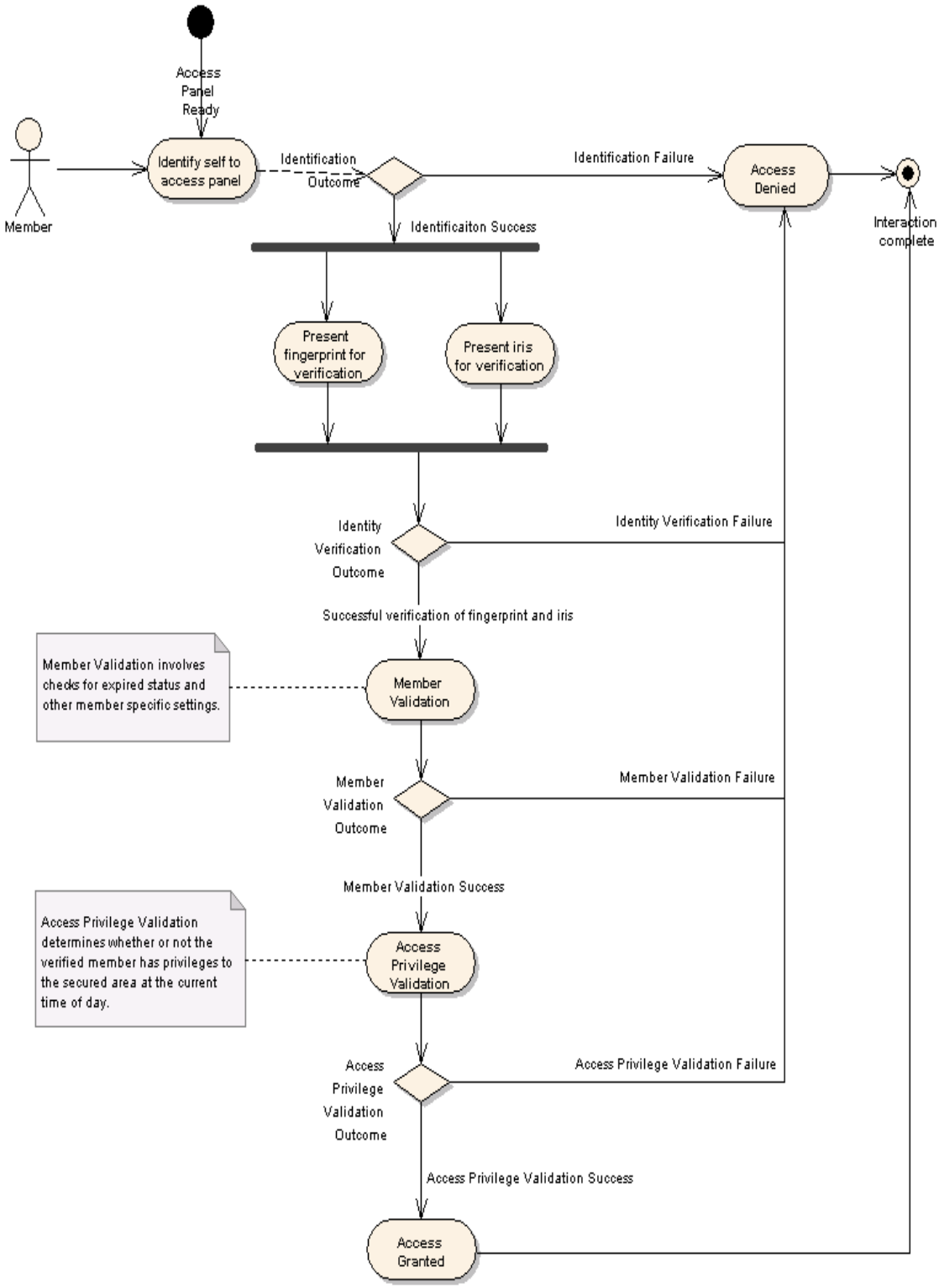
Members have been enrolled and privileges assigned to grant access to the facilities being controlled by the BioAxs 9800IR™ Access Panel (detailed instructions in the Enrollments section of the *Command Center System Administration and User Guide*).

Introduction

The BioAxs 9800IR™ access panel is designed to achieve maximum flexibility for integrating into the most diverse range of access control environments. To function properly, fingerprint and/ or facial templates must be enrolled in the system using the NextgenID Command Center™ Client software. Use of the BioAxs 9800IR™ Access Panel is simple and straightforward. The diagram below illustrates the typical user interface flow for the BioAxs 9800IR™.

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Authentication Protocol Overview for the BioAxs 9800IR™



Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Step 1: Member Identification

This first step in gaining access to a controlled facility is for an individual to identify themselves to the access panel. There are numerous identification technologies supported by the BioAxs 9800IR™ platform, the most common are:

- Personal Identification Number (PIN)
- Wiegand Identification Device (Proximity Card, Magnetic Stripe, etc.)
- Identification Badge with Barcode (DoD's Common Access Card)

Using Personal Identification Numbers (PIN)

If PIN is the chosen identification token, a user will enter their designated PIN using the onboard keypad in the following manner. Assuming that a user's PIN is '1234', to properly present this to the panel the user would enter '*1234#'. PINs are always prefixed by the '*' key. The panel will not begin a PIN lookup for identification until it is given the '#' key.

Panel Feedback

The access panel will provide two types of feedback (audio and visual) through an onboard speaker and text display. On success, the text display will read: 'Please touch the fingerprint sensor'. On failure, the text display and speaker will read: 'Access Denied'.

Step 2: Member Verification

The BioAxs 9800IR™ Access Panel verification components operate in an 'OR' capacity. Member verification will be successful following a positive facial recognition OR fingerprint verification whichever comes first.

Upon successful member identification, the panel will actively begin the process of attempting to authenticate the member's facial biometric. The face recognition process is immediately initiated once a member has been identified; the fingerprint verification process is only initiated in response to the member touching the onboard fingerprint sensor.

If neither face nor fingerprint has been successfully verified within the allotted time period (default of 10 seconds), the Member Identity Verification process will experience a timeout resulting in a denial of access outcome for the member attempting access.

It is generally recommended that a member touch the fingerprint sensor within 1-3 seconds if the face recognition process has not successfully verified their identity.

Panel Feedback

The access panel will only provide feedback (audio and visual) if the member identity verification process fails to authenticate the member. The text display and speaker will read: 'Access Denied' in this event.

Step 3: Member Validation

Upon successful member verification, the panel will automatically begin the process of validating the verified member examining the following criteria:

Member Profile Expiration

The Command Center Access Control System provides an expiration date for all member enrollments. This feature is commonly used when granting temporary access to visitors or contract personnel. Another use for member profile expiration is to use it as an alternative to member deletion.

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

When the panel performs this check, if the member expiration date is prior to the current date and time, the member will be denied access.

Access Panel 'Lockdown' State

The Command Center Access Control System provides security administrators the ability to place any BioAxs access panel (including the BioAxs 9800IR™) in a 'lockdown' state. This temporary condition will deny any verified member access to the entrance unless the verified member has the lockdown override privilege.

Both the Member Profile Expiration Date and Lockdown Override settings are available on the Member Information tab of the Command Center Access Control System software.

Panel Feedback

The access panel will only provide feedback (audio and visual) if the member identity verification process fails to authenticate the member. The text display and speaker will read: 'Access Denied' in this event.

Step 4: Access Validation

Upon successful member validation, the panel will automatically begin the process of validating access for the verified member examining the following criteria:

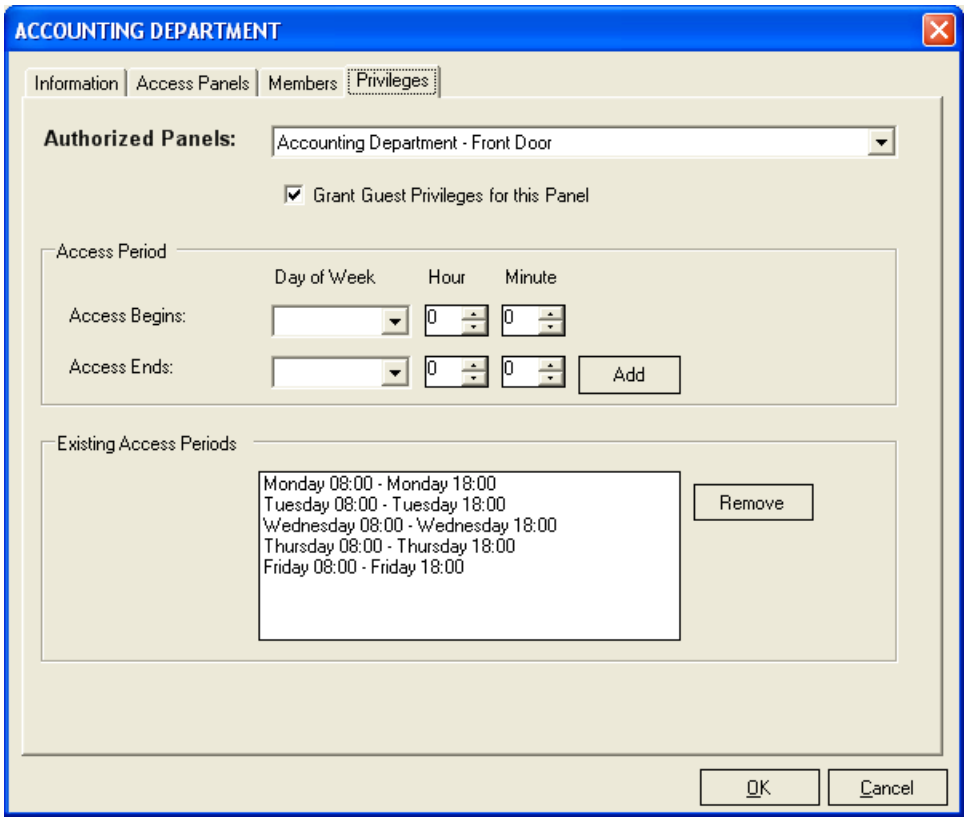
Member Access Privileges

The Command Center Access Control System provides two options for granting a member access to a secured entrance. By default, a member enrolled in the system will have NO access to any of the panels on the system. Access is provided by enrolling the member in a Group Security Privilege or individual granting the member specific periods of access.

Group Security Privileges:	Access panels and members may be grouped together to establish access times for multiple members for a single security privilege entry. There is no limit to the number of groups an access panel or member may belong to.
Individual Privileges:	Any member may be individually granted additional privileges to one or more panels thus augmenting any settings applied from a Group Security Privilege.

The screen shot below depicts a group security privilege for an access panel granting access on Monday – Friday from 8:00 a.m. to 6:00 p.m.

Copyright ©2004 NextgenID, Ltd. All Rights Reserved



Guest Privileges

The BioAxs 9800IR™ Access Panel may be deployed with NextgenID Tailgating Countermeasure detection arrays. In this scenario, each access privilege examined (group security and individual) will also determine if the verified member has the authority to escort individuals into the secured facility. Referring to the screen shot above for the Account Department group security privilege, notice the check-box setting directly below the panel name 'Accounting Department – Front Door'. The 'Grant Guest Privileges for this Panel' with a 'true' setting when combined with a valid access period will add the optional step discussed in more detail below.

Step 5: Guest Prompts (Conditional)

As briefly mentioned in Step 4: Access Validation, the BioAxs 9800IR™ when combined with a Tailgating Countermeasure device will conditionally prompt the verified member for guest input. If the Tailgating Countermeasure device is not present or guest privileges are not applicable to the verified member, this step will be automatically skipped.

Panel Feedback

The access panel will provide feedback (audio and visual) in this situation. The text display and speaker will read: *With guests press #, alone any other key*.

If the verified member presses any key other than the '#' key or does nothing within the time allotted, the panel will assume that no guests are being escorted into the facility and proceed to

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

unlock the door or communicate the verification state to a third party access controller (if applicable).

If the verified member pressed the '#' key when instructed, the text display will update to read: 'Enter the number of guests followed by #'.

Once the number of guests has been entered using the keypad device on the panel, the panel will proceed to unlock the door or communicate the verification state to a third party access controller (if applicable). The tailgating countermeasure input will be examined for this access control event and be communicated to the Command Center system.

Access Panel Modes of Operation

One of the features of the BioAxs 9800IR™ Access Panel is an ability to dynamically alter its operating behavior or configuration based on settings applied from the Command Center Access Control System software.

When you received your BioAxs 9800IR™, it was preconfigured for one of the following behaviors:

Code	Description
IH	PIN plus Iris OR Fingerprint Verification
II	PIN plus Iris OR Fingerprint Verification with Tailgating
JE	Wiegand plus Iris OR Fingerprint Verification
JF	Wiegand plus Iris OR Fingerprint Verification with Tailgating
KE	CAC plus Iris OR Fingerprint Verification
KF	CAC plus Iris OR Fingerprint Verification with Tailgating

Each of the above entries is commonly referred to as the 'base' or 'default' configuration for the access panel. They are individually responsible for the various operating configurations that will be available for your access panel.

IH: PIN plus Iris or Fingerprint

The default behavior of this configuration will be to identify the member using a unique Personal Identification Number (PIN) and then verify that member's identity using an iris or fingerprint biometric. This panel may be 'scaled down' to operate in any of the following modes:

Code	Description
IC	PIN plus Iris Verification
IE	PIN plus Iris AND Fingerprint Recognition

II: PIN plus Iris or Fingerprint with Tailgating Countermeasure

The default behavior of this configuration will be to identify the member using a unique Personal Identification Number (PIN) and then verify that member's identity using an iris or fingerprint biometric. The tailgating countermeasure device will record its input for all appropriate events generated during the use of this panel. This panel may be 'scaled down' to operate in any of the following modes:

Code	Description
ID	PIN plus Iris Verification with Tailgating
IG	PIN plus Iris AND Fingerprint Recognition with Tailgating

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

JE: Wiegand (Proximity Card / Magnetic Swipe) plus Iris or Fingerprint

The default behavior of this configuration will be to identify the member using a proximity or magnetic swipe card and then verify that member's identity using an iris or fingerprint biometric. This panel may be 'scaled down' to operate in any of the following modes:

Code	Description
JA	Wiegand plus Iris Verification
JC	Wiegand plus Iris AND Fingerprint Verification

JF: Wiegand (Proximity Card / Magnetic Swipe) plus Iris or Fingerprint with Tailgating Countermeasure

The default behavior of this configuration will be to identify the member using a proximity or magnetic swipe card and then verify that member's identity using an Iris or fingerprint biometric. The tailgating countermeasure device will record its input for all appropriate events generated during the use of this panel. This panel may be 'scaled down' to operate in any of the following modes:

Code	Description
JB	Wiegand plus Iris Verification with Tailgating
JD	Wiegand plus Iris AND Fingerprint Verification with Tailgating

KE: Common Access Card (CAC) plus Iris or Fingerprint

The default behavior of this configuration will be to identify the member using a Department of Defense (DoD) issued Common Access Card (CAC) and then verify that member's identity using an iris or fingerprint biometric. This panel may be 'scaled down' to operate in any of the following modes:

Code	Description
KC	CAC plus Iris Verification
KE	CAC plus Iris AND Fingerprint Verification

KF: Common Access Card (CAC) plus Iris or Fingerprint with Tailgating Countermeasure

The default behavior of this configuration will be to identify the member using a Department of Defense (DoD) issued Common Access Card (CAC) and then verify that member's identity using an iris or fingerprint biometric. The tailgating countermeasure device will record its input for all appropriate events generated during the use of this panel. This panel may be 'scaled down' to operate in any of the following modes:

Code	Description
KB	CAC plus Iris Verification with Tailgating
KD	CAC plus Iris AND Fingerprint Verification with Tailgating

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Miscellaneous Configurations

The following authentication protocols are also available for the BioAxs 9800IR™.
Some configuration options shown require additional hardware to be installed. Contact your NextgenID support representative for any questions regarding the capabilities of your BioAxs 9800IR™ system.

Code	Description
AA	Fingerprint Only
AB	Wiegand plus Fingerprint
CB	PIN plus Fingerprint or Fingerprint Only
CC	PIN plus Fingerprint or Fingerprint Only with Tailgating
CD	Wiegand plus Fingerprint or Fingerprint Only
CE	Wiegand plus Fingerprint or Fingerprint Only with Tailgating
CF	PIN only
CG	PIN only with Tailgating
EA	Wiegand only
EB	Wiegand only with Tailgating
DA	CAC only
DB	CAC only with Tailgating
DC	CAC plus Fingerprint Verification
DD	CAC plus Fingerprint Verification with Tailgating

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

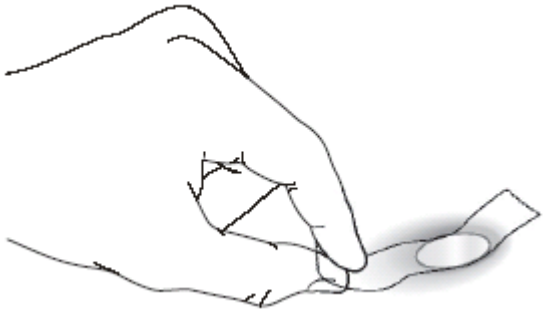
Appendix A: General Maintenance Tasks

Fingerprint Sensor Hardware Maintenance

Each enrollment kit contains a *Digital Persona* fingerprint-imaging device. Periodic maintenance of the fingerprint sensor is necessary to maintain quality enrollment templates and sensor life.

Cleaning the Sensor

Depending on the amount of use, the sensor window may need to be cleaned periodically.
To clean it, apply the sticky side of a piece of adhesive cellophane tape on the window and peel it away.



Under heavy usage, the window coating on some sensors may turn cloudy from the salt in perspiration. In this case, gently wipe the window with a cloth (not paper) dampened with a mild ammonia-based glass cleaner.

Sensor Maintenance Warnings

⚠ **There are several things you should never do when cleaning or using the sensor**

- Do not pour the glass cleaner directly on the sensor window.
- Do not use alcohol-based cleaners.
- Never submerge the sensor in liquid.
- Never rub the window with an abrasive material, including paper.
- Do not poke the window coating with your fingernail or any item, such as a pen.

Copyright © 2002 Digital Persona Incorporated. All Rights Reserved.

Fingerprint Sensor Frequently Asked Questions

We have included a collection of frequently asked questions related to the proper care and maintenance of the fingerprint sensors provided with your NextgenID system.

Do I need to clean my sensor to keep it working well?

Depending on the amount of use, the sensor window will need to be cleaned from time to time. It will pick up dirt and salts from fingers. Refer to the “Cleaning the Sensor” section above.

If a scratch or smear on the glass lens occurs, does this reduce performance? What is the repair procedure if a failure occurs?

Scratches, pokes or other physical damage to the window coating can compromise the system’s ability to recognize fingerprints. Such damage cannot be repaired. Contact a NextgenID support representative.

Will a buildup of dust on the sensor window reduce performance?

A small amount of dust on the sensor window will not cause problems. A large amount of dust may make it more difficult for readings. Applying the sticky side of a piece of adhesive cellophane tape on the window and peeling it away can easily remove dust.

My sensor window looks a little cloudy. What causes this and will it affect the sensor’s performance?

Under heavy usage, the window coating on some sensors may turn cloudy. This happens when salt from perspiration builds up. The sensor window can be cleaned with a cloth dampened with a mild ammonia-based glass cleaner. Do not pour the glass cleaner directly on the sensor window and do not use alcohol-based cleaners.

What do I do if the coating comes off the sensor window?

The film on the sensor window is an integral part of the sensor. It is formed from a liquid silicone with a special formula. If it comes off, the sensor sensitivity may decrease, resulting in reduced performance. Rubbing the sensor or cleaning it incorrectly can cause the coating to come off. Follow the cleaning instructions in the accompanying user guide to avoid this.
In the event that this does occur, please contact your NextgenID support team for additional guidance.

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Appendix B: Biometric Recognition Performance

Below is a list of the most common issues adversely affecting the performance of the biometric recognition systems configured in your BioAxs 9800IR™ access panel.

Fingerprint Recognition Performance Issues

- The sensor is having difficulty acquiring an image of your finger; the sensor window may need cleaning, as described in “Cleaning the Sensor” (above).

- You may not be touching the sensor correctly. In order for the sensor to acquire a good image of your finger, you must place the pad of your finger—not the tip—in the center of the oval window, and apply gentle, even pressure. Do not “roll” your finger. Pressing too hard will distort your fingerprint.

- Pressing too lightly will not expose a large enough area of your finger. Also, make sure to hold your finger on the sensor until you see the sensor light blink; this may take longer for dry fingers. Then, lift your finger. Although you may use any finger with the sensor, your index finger of either hand works best.

- If the sensor is capturing your finger image (as indicated by the sensor blink) and you have tried all the above suggestions, you may need to reregister your finger or try registering a different finger.

Iris Recognition Performance Issues

- Significant glare on eyeglasses that obstructs the eyes. Adjusting the lighting that causes the glare can typically solve this. Sunglasses should also be removed during recognition and enrollment cycles to ensure optimal facial feature analysis.

- Ensure there is not long hair obscuring the central part of the face.

- Poor lighting that would cause the face to be overexposed or underexposed (low contrast)

- Ensure both Panel Lights are in proper working order. Contact NextgenID Support if one or both of the panel lights are not functioning.

- (Optional Equipment) The NextgenID BioStation Panel lights may need replacement. The BioStation is designed to optimize lighting conditions for outdoor panel locations, replace any burned out lamps.

- There are no enrolled facial recognition candidates or, the system administrator has not approved facial recognition candidate enrollments for the given member.

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Notes

Copyright ©2004 NextgenID, Ltd. All Rights Reserved

Notes

Copyright ©2004 NextgenID, Ltd. All Rights Reserved