As many of you are increasing the number of sales and presentations of networked access control & ID management systems, a common question is arising from IT professionals:

“How will the Lenel OnGuard system affect my network?”

This question is important to many customers. However, it cannot easily be answered nor can broad-based conclusions be drawn based on specific test results. This is because there are many variables that determine the answer to the above question. Each customer will have varying results based on site specific transaction rates, image sizes, number of workstations, etc.

The good news is that B.A.S.I.S. will have a minimal, if not negligible, effect on a customer’s network; even when a customer has a high transaction rate! Let me provide two examples of sample customer systems.

**EXAMPLE #1 - Access Control & Alarm Monitoring System**

Let us assume the following scenario and variables. The record size of an event arriving at the database server from the Intelligent System Controller (ISC) that will be sent to a client workstation for alarm monitoring purposes is 12 bytes plus the size of the header. We will assume the header size, which will vary based on RS-485 or Ethernet communications, is 28 bytes. This is more than adequate. This gives us an event record size of 40 bytes. Let us also assume that we have a sustained transaction rate of 60 events per minute per ISC. Let us assume that we have 8 ISCs. We will double the bits per seconds of the events to consider polling overhead. We will assume that we are using a 10 MB Ethernet Network. Based on these variables, our network bandwidth utilization will be 0.05%. This result is derived from the algorithm below:

$$40 \text{ bytes} = 320 \text{ bits per second (bps)} \times 2 \text{ for polling overhead} = 640 \text{ bps} \times 8 \text{ ports for 8 ISCs} = 5,120 \text{ bps}$$

$$\frac{5,120 \text{ bps}}{10,000,000 \text{ bps network}} = 0.0512\%$$

**EXAMPLE #2 - ID Management System**

Let us assume the following scenario and variables: The cardholder image size is 10 KB that equals approximately 80,000 bits. Signature size is also 10 KB. Our transaction rate is one personnel record added to the system every five minutes per workstation. Let us assume that we have three workstations. With these variables, our baud rate will be approximately 810 bits per second (bps) which amounts to less than 0.02% network bandwidth utilization on a 10 MB Ethernet network. This result is derived from the algorithm below:

$$80,000 \text{ bits} + 80,000 \text{ bits} = 160,000 \text{ bits divided by 300 seconds (five minutes for transaction rate)} = 533.3 \text{ bps times 3 workstations} = 1,600 \text{ bps}; 1,600 \text{ bps divided by 10,000,000 bps network} = 0.016\%$$

As you can see from these examples, B.A.S.I.S. requires negligible amounts of network bandwidth. Again, these are just examples based on the aforementioned variables. These variables will be different for each customer and thus, each customer will have a different outcome. These examples should be used for reference when the issue arises.
A common question posed by our customers is "Why do I need a dedicated computer to run B.A.S.I.S.?" The answer to this question involves the consideration of many issues.

1) B.A.S.I.S. is a security system that should be potentially as stable and secure from outside attacks as possible. Moreover, a security system is intended for 24 hours a day, 7 days a week operation. The simpler the software environment, the better security and stability can be achieved.

2) When maintenance or recovery of a B.A.S.I.S. system is required, a simpler software environment is easier to troubleshoot. Additionally, software upgrades can be better performed without delay when .dll, .ini, and other potential file and hardware conflicts are minimized.

3) Access Control software developers lack the resources that large, general application developers enjoy and cannot test their product against every possible hardware and software configuration. Also, Access Control software assumes control over a wider assortment of computer resources and creates a greater potential for conflicts with other applications. As an example, any application that affects .dll's, .ini's, ODBC, Internet browser, JAVA, Crystal Reports, DirectX, and network functionality has the potential for conflicts with an Access Control application. Since the testing of Access Control software is performed against a narrower platform, performance of untested configurations is difficult to predict.

4) To recap, a dedicated computer for the B.A.S.I.S. Access Control applications provides a better environment for:
   - Security
   - Stability
   - Reliability
   - Maintenance
   - Troubleshooting
   - Upgrading

Although a dedicated machine is not required, it is highly desirable for the reasons mentioned, and computer professionals could probably come up with other reasons based on the points in this discussion. If circumstances require that it is not possible to have a dedicated computer, it should be realized that the security system would not be in optimal condition. It is further recommended that at least the server be dedicated. The workstations or clients could be integrated with other applications to some degree as the potential for hardware/software conflicts is lessened due to their functionality in an Access Control system.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5 123</td>
<td>Yes-Service Pk 2 or higher</td>
<td>Yes-Second Edition</td>
<td>No</td>
<td>Yes-Service Pk 3 or 5</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5.5e 178</td>
<td>Yes-Service Pk 2 or higher</td>
<td>Yes-Second Edition</td>
<td>No</td>
<td>Yes-Service Pk 3 or 5</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5.5e 214</td>
<td>Yes-Service Pk 2 or higher</td>
<td>Yes-Second Edition</td>
<td>No</td>
<td>Yes-Service Pk 5</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5.7 240</td>
<td>No</td>
<td>Yes-Second Edition</td>
<td>No</td>
<td>Yes-Service Pack 6a</td>
<td>Yes-With No Service Pack</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5.7 244</td>
<td>No</td>
<td>Yes-Second Edition</td>
<td>No</td>
<td>Yes-Service Pack 6a</td>
<td>Yes-Service Pack 1</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5.8 041b</td>
<td>No</td>
<td>Yes-Second Edition</td>
<td>No</td>
<td>Yes-Service Pack 6a</td>
<td>Yes-Service Pack 2</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5.8 310 OnGuard Only</td>
<td>No</td>
<td>Yes-Second Edition</td>
<td>No</td>
<td>Yes-Service Pack 6a</td>
<td>Yes-Service Pack 2</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5.8 311 BASIS Only</td>
<td>No</td>
<td>Yes-Second Edition</td>
<td>No</td>
<td>Yes-Service Pack 6a</td>
<td>Yes-Service Pack 2</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5.8 501 OnGuard Only</td>
<td>No</td>
<td>Yes-Second Edition</td>
<td>No</td>
<td>Yes-Service Pack 6a</td>
<td>Yes-Service Pack 2</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5.9 124 OnGuard Only</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes-Service Pack 2</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5.9 131</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes-Service Pack 2</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5.9 132 OnGuard Only</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes-Service Pack 2</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5.10 210</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes-Service Pack 2</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5.10 215</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes-Service Pk 2, 3, 4</td>
<td>Yes-Service Pack 1</td>
<td>No</td>
</tr>
<tr>
<td>5.10 423</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes-Service Pk 2,3,4</td>
<td>Yes-Service Pack 1</td>
<td>Yes</td>
</tr>
<tr>
<td>5.11.105</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes-Service Pack 4</td>
<td>Yes-Service Pack 1a</td>
<td>Yes-All Critical Patches</td>
</tr>
<tr>
<td>5.11.216</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes-Service Pack 4</td>
<td>Yes-Service Pack 2</td>
<td>Yes-Service Pack 1</td>
</tr>
<tr>
<td>5.12.012</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes-Service Pack 4</td>
<td>Yes-Service Pack 2</td>
<td>Yes-Service Pack 1</td>
</tr>
<tr>
<td>5.12.110</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes-Service Pack 4</td>
<td>Yes-Service Pack 2</td>
<td>Yes-Service Pack 1</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------</td>
<td>------</td>
<td>----------------</td>
<td>-----------------</td>
<td>------------------</td>
<td>-----------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>5.8.405</td>
<td>YES</td>
<td>NO</td>
<td>SP1, SP2, S3</td>
<td>SP1, SP3a</td>
<td>NO</td>
<td>NO</td>
<td>8.0.5, 8.0.6, 8.1.6(8i)</td>
</tr>
<tr>
<td>5.8 501 OnGuard Only</td>
<td>NO</td>
<td>NO</td>
<td>SP1, SP2, S3</td>
<td>SP1, SP3a</td>
<td>NO</td>
<td>NO</td>
<td>8.0.5, 8.0.6, 8.1.6(8i)</td>
</tr>
<tr>
<td>5.9 124 OnGuard Only</td>
<td>NO</td>
<td>SP3a w/ Security Patch</td>
<td>NO</td>
<td>SP1, SP2, SP3a</td>
<td>NO</td>
<td>NO</td>
<td>8.1.7(8i), 9.0(9i)</td>
</tr>
<tr>
<td>5.9 132 OnGuard Only</td>
<td>NO</td>
<td>SP3a w/ Security Patch</td>
<td>NO</td>
<td>SP2, SP3a</td>
<td>NO</td>
<td>NO</td>
<td>8.1.7(8i), 9.0(9i)</td>
</tr>
<tr>
<td>5.10 210</td>
<td>NO</td>
<td>SP3a w/ Security Patch</td>
<td>NO</td>
<td>SP2, SP3a</td>
<td>NO</td>
<td>NO</td>
<td>8.1.7(8i), 9.2(9i)</td>
</tr>
<tr>
<td>5.10 215</td>
<td>NO</td>
<td>SP3a w/ Security Patch</td>
<td>NO</td>
<td>SP3a</td>
<td>NO</td>
<td>NO</td>
<td>8.1.7(8i), 9.2(9i)</td>
</tr>
<tr>
<td>5.10 309</td>
<td>NO</td>
<td>SP3a w/ Security Patch</td>
<td>NO</td>
<td>SP3a</td>
<td>NO</td>
<td>NO</td>
<td>8.1.7(8i), 9.2(9i)</td>
</tr>
<tr>
<td>5.10 423</td>
<td>NO</td>
<td>SP3a w/ Security Patch</td>
<td>NO</td>
<td>SP3a</td>
<td>NO</td>
<td>NO</td>
<td>9.2(9i)</td>
</tr>
<tr>
<td>5.11.105</td>
<td>NO</td>
<td>SP3a w/ Security Patch SP4</td>
<td>NO</td>
<td>SP3a, SP4</td>
<td>NO</td>
<td>NO</td>
<td>9.2.0.5(9i), 9.2.0.7(9i)</td>
</tr>
<tr>
<td>5.11.216</td>
<td>NO</td>
<td>SP4</td>
<td>NO</td>
<td>YES,SP4</td>
<td>NO</td>
<td>NO</td>
<td>9.2.0.7(9i)</td>
</tr>
<tr>
<td>5.12.012</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>YES,SP4</td>
<td>YES</td>
<td>SP1</td>
<td>9.2.0.7(9i), 10.2.0.2(10g)</td>
</tr>
<tr>
<td>5.12.110</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>YES,SP4</td>
<td>YES, SP1</td>
<td>YES, SP1</td>
<td>9.2.0.7(9i), 10.2.0.2(10g)</td>
</tr>
</tbody>
</table>
Hardware Options

Personal Computer Minimum Shipping Configurations
for all B.A.S.I.S. Turnkey Systems

Windows XP Workstation

SERVER PC:
Dell Precision 380 Workstation - Pentium 4 Processor 3.0 GHz, 120/220V 200 Watts, 512 MB ECC SDRAM, 2 MB cache, 16X DVD+/-RW 48X CDRW, 80GB SATA 7200 rpm hard drive, 10/100/1000 WuOL Ethernet communication, 17" Flat LCD Monitor (must support 1024 x 768), 64 MB Dual Monitor Video Card, (1) serial ports, (1) parallel port, (8) USB 2.0 ports, audio with speakers, USB keyboard, USB optical mouse with surge suppression strip, 3 year limited warranty.

CLIENT PC:
Dell GX520SFF - Pentium 4 Processor 2.8 GHz, 120/220V 200 Watts, 512 MB ECC RDRAM, 1 MB cache, 24X CD ROM, 40GB SATA 7200 rpm hard drive, 10/100/1000 WuOL Ethernet communication, (1) serial ports, (1) parallel port, (8) USB 2.0 ports, 17" Flat LCD Monitor, 64MB Video, audio with speakers, USB keyboard, USB optical mouse with surge suppression strip, 3 year limited warranty.

Windows 2003 Server (w/5 clients) with SQL 2000 (w/5 clients)

NETWORKED DEDICATED SERVER PC:
Dell Poweredge 2800 – Pentium 4 Processor 3.2 GHz Xeon, 120/220V 330 Watts, 1 GB SDRAM, 512 KB cache, 24X CD-RW/DVD ROM, 36GB 10K RPM SCSI hard drive, 10/100/1000 Ethernet communication, 17" Flat CRT Monitor, 16 MB Video Card, 36/72 GB DAT72 SCSI tape backup, (1) serial ports, (1) parallel port, (4) USB 2.0 ports, PS/2 keyboard, PS/2 mouse with surge suppression strip.

ENTERPRISE MASTER SERVER PC:
Dell Poweredge 2800 – Pentium 4 Processor 3.2 GHz Xeon (dual processor), dual power supplies 120/220V 320 Watts each, 2GB SDRAM, 512 KB cache, RAID5 configuration with PERC4 128MB controller card SCSI, 3.5" floppy drive, 24X CD-RW/DVD ROM, (qty. 3) 36 GB 10K RPM SCSI hard drives, 36/72 GB DAT72 SCSI tape backup drive, 10/100/1000 Ethernet communication, 17" Flat CRT Monitor, 16 MB Video Card, (1) serial ports, (1) parallel port, (4) USB 2.0 ports, PS/2 keyboard, PS/2 mouse and surge suppression strip.

Windows XP Laptop Computer

MOBILE COMPUTER CONFIGURATION:
Dell Latitude D610 – Pentium M Processor 2.13 GHz Laptop, 100 to 250 VAC and 164 to 264 VAC AC adapter, 14.1" XGA active matrix color display, 512 MB RAM, 512 KB cache, 24X CD ROM, 30 GB Hard drive, 16 bit stereo sound, Touchpad type mouse, PCI Bus with 128-bit graphics accelerator, (4) USB 2.0 ports, (1) parallel port, (1) communications port, infrared, modem, 10/100/1000 Ethernet and carrying case.

Note: All PC minimum requirements are subject to change based on equipment availability and industry standards.
System Requirements

☐ Computer that meets current specifications
   a) See current B.A.S.I.S. computer specifications

☐ B.A.S.I.S. Software
   a) See B.A.S.I.S. OS matrix for supported operating system
   b) See B.A.S.I.S. OS matrix for supported operating system service packs
   c) See B.A.S.I.S. DB matrix for supported databases and service packs

☐ Network requirements for ISC
   a) Static IP address: __________________
   b) Default gateway: __________________
   c) Sub-net mask: __________________

☐ Network requirements for Server PC
   a) Static IP address: __________________
   b) Default gateway: __________________
   c) Sub-net mask: __________________

☐ Network requirements for Client PC (each client)
   a) Static IP address: __________________
   b) Default gateway: __________________
   c) Sub-net mask: __________________

☐ System power requirements
   a) ISC location – 110vac 15amp circuit by others
   b) Remote panel locations – 110vac 15amp circuits by others

☐ Remote diagnostics (optional)
   a) Internet access at server machine only
   b) Standard telephone line terminated at server machine only
Customer Considerations

Information meeting between Sales Agent, Customer IT Administrator, Customer System Administrator
- Discuss system requirements
- Discuss network considerations
- Determine IP timelines
- Discuss power requirements
- Determine termination locations
- Discuss initial programming parameters for access system
- Determine end user training schedule and location

Database considerations (medium to large systems)
- HR data may be used to pre-populate Cardholder database
- Student data records may be used to pre-populate Cardholder database
- Custom scripts may be required between databases
- Deliver sample import file to appropriate customer contact prior to installation

Pre-Installation Considerations

Pre-installation meeting with Sales Agent, PM, Customer
- Complete scope of work
- Complete materials list
- Installation drawings

Confirm assignment of IP address

Confirm power requirements

Initial programming considerations
- Number of system users
- Number of cardholders
- Timezones
- Access levels
- Data import file

Training considerations
- Confirm customer training schedule
- Confirm location for customer training
Cables dressed neatly
   a) Wire ties wrapped and organized
   b) Wires routed around perimeter of enclosure and boards

Wires labeled and marked
   a) Marked with permanent markers
   b) Marked with printed labels or stickers
   c) Marked with wire tags

Cable numbers listed
   a) Wire numbers list left in panel
   b) Number list attached to panel door

Lantronix device secured
   a) 2 mounting stand-offs installed in panel
   b) Power cable routed and secured neatly
   c) Network cable routed and secured neatly
   d) IP information noted on wire numbers list

Panel tamper switches
   a) Plunger type tamper switch
   b) Magnetic tamper switch
   c) Connected to board tamper input

Unused inputs normalized
   a) Unused tampers – jumpers installed
   b) Unused inputs – jumpers installed
   c) Unused power supervision – jumpers installed

Stand-by batteries
   a) Installation date marked on batteries
   b) Batteries installed in appropriate enclosures

Power supplies
   a) Test for AC fail and switch over
   b) System runs correctly for five minutes on standby – batteries
   c) DC output voltage measured and noted on wire numbers list
   d) DC output current measured and noted on wire numbers list
   e) Battery charging voltage measured and noted on wire numbers list
System Installation – Software Considerations

☐ Software loaded on server and clients
  a) All machines loaded with Adobe Acrobat Reader
  b) All machines loaded with B.A.S.I.S. documentation

☐ Panels and boards
  a) All panels show normalized tampers
  b) All panels show normalized inputs
  c) Tampers masked only at Customer’s request
  d) Inputs masked only at Customer’s request
Confirm Current Version and Build of B.A.S.I.S.

Confirm Database Type
a) SQL 2005 Express (bundled with software)
b) SQL
c) Oracle

Check and Confirm Computer Specifications

Optimize Operating System
a) Virtual Memory
b) Event Viewer
c) Monitor and Power Settings

Confirm Network Connectivity
a) Static IP Addresses
b) Gateways
c) Subnet Masks
d) Domains

Install 3rd Party Devices and Software
a) Third Party Database
b) Printer Drivers
c) Video Capture
d) Other Peripherals

Install B.A.S.I.S. Software
a) Load Required Programs
   • Service Packs
   • Direct X
   • Acrobat Reader
b) Choose Computer Type
   • Server
   • Client
c) License File Location

Install License File
a) License Administrator

Setup the Database
a) Database Setup from the Program Group
System Configuration
a) Cardholders

Card Formats

Access Panels
a) Direct
b) LAN/WAN
   • Static IP Addresses
   • Gateways
   • Subnet Masks
c) Dialup
   • Host TX
   • Device TX
d) Download Firmware (Alarm Monitoring)

Readers
a) Reader Type
b) Online/Offline Modes
c) Card Formats

Alarm Panels
a) Inputs
b) Outputs

Time Zones
a) Holidays
b) Time Zones
c) Reader Modes

Access Levels

Cardholders
a) Cardholder
b) Badge
c) Access Levels

Global I/O

Alarm Configuration

Users

Monitor Zones
Confirm Capture Device
- a) Install Video Card
  - See current specifications
  - Test Video Card
- b) Install Digital Camera
  - Test Camera
- c) File Import
- d) Install Scanner
  - Test Scanner

Install Printer
- a) SCSI or Parallel
- b) Printer Driver
- c) Test printer

Load B.A.S.I.S. Software

Design Badges
- a) Obtain Graphics From Customer
- b) Front Layout
- c) Back Layout

System Configuration
- a) Cardholders

Card Formats

Badge Types
- a) Select Encoding Format
- b) Select Front and Back Layout
- c) Select Printer
- d) Default Access Group

Cardholders
- a) Badge Type
- b) Badge ID
- c) Crop Photo
- d) Effects Gallery
- e) Print Card
System Components

- Lockset
  - a) Mortise
  - b) Cylindrical

- B.A.S.I.S. Software

- Computer that meets current specifications
  - a) See current B.A.S.I.S. computer specification

- Personal Digital Assistant (PDA)
  - a) See BEST Website for recommended brands and models

- Encoder
  - a) Magstripe
  - b) Smartcard

- Cables
  - a) Computer to PDA
  - b) PDA to Lockset

Setting up the System

- Install the B.A.S.I.S. software

- Install and set up the Encoder
  - a) Workstation setup
  - b) Test the encoder

- Establish PDA Connection
  - a) ActiveSync

- Install B.A.S.I.S. Transport
  - a) From B.A.S.I.S. CD
Configuring the System

☐ Define Card Formats
  a) Guest
  b) Offline

☐ Define Badge Types
  a) Standard
  b) Guest
  - Badge ID allocation table
  - Guest defaults
  - Printing/Encoding Form

☐ Access Panels

☐ Readers
  a) Reader Type
  - Offline
  - Guest
  - Offline/Guest
  b) Reader Mode
  - Automatic
  - Card and Pin
  - Pin or Card

☐ Time zones
  a) Holidays
  b) Time zones
  c) Time zone/Reader modes

☐ Access Levels

☐ Cardholders
  d) Encode

☐ Programming the Locks
  a) Lock Configuration
  b) History
  c) Diagnostics
Alarm Monitoring - An application that displays information about events as they occur in the system, and provides alarm acknowledgement with instructions, cardholder tracking, live video display of an area in alarm, and live video verification of a cardholder's identity. Additionally, the application provides real time status and real time control of field hardware.

Area Manager - A network-based application that enables users to be given independent control over their assigned/defined areas, without the need to request permissions and/or the removal of permissions from a single security administrator. An Area Manager is limited to adding or removing pre-defined access levels to pre-defined cardholders.

Badge Designer - A unique graphic design program that is used to create badge layouts for use with the ID CredentialCenter application.

Communication Server - A communication "gateway" for information flow between the B.A.S.I.S. software and the access control field hardware.

Database Backup - A utility used to backup the B.A.S.I.S. database.

Database Setup - A utility used to prepare a supported database for use with B.A.S.I.S. applications

Forms Designer Lite – Forms Designer Lite is a scaled-down version of Forms Designer, allowing you to make cosmetic changes to the user interface that do not impact the database.

Forms Designer – OnGuard Forms Designer enables you to customize the cardholder database and data entry screens to meet the needs of your environment.

Global Output Server (GOS) - GOS supports on-demand messaging from the Alarm Monitoring module. Functionally, an Alarm Monitoring user (such as a security guard) can send an electronic mail or pager message pertaining to a specific alarm displayed on his/her workstation.

Behind the scenes, the GOS client (i.e. the Alarm Monitoring module) sends the message to GOSServer (which runs as a Windows NT service). GOSServer then directs the message to the appropriate Global Output Device.

ID CredentialCenter – Use the OnGuard ID Management application to add cardholder records to the OnGuard database and manage cardholder information, including capturing photos/signatures, creating and printing ID badges, and defining access levels.
**Import Module** – A basic import utility. In contrast to the Universal Interface Server, this is typically used for a one time-only record import (i.e., you can only add records) from an existing cardholder database.

**License Administration** - A program used to manage license files on the system.

**License Server** - A program used to connect the B.A.S.I.S. application to the license file.

**Linkage Server** - The Linkage Server directs automatic email/paging messages in response to specific alarms. The Linkage Server is responsible for:
- Global I/O
- Digital Video
- Automatic E-mail and Paging
- Time reporting in Guard Tour
- Expected Events for Receivers
- Scheduler
- OpenIT Service for OpenIT API

**Login Driver** – A service that is used to change the B.A.S.I.S. database password (NOT the user passwords). The service is run on the computer on which the database resides.

**Map Designer** – A straightforward way to create facility maps with icons representing B.A.S.I.S. hardware components at the locations shown. The maps are used by the B.A.S.I.S. Alarm Monitoring application.

**System Administration** – An application is used to configure access control and alarm monitoring environments, including all access control hardware devices, non-hardware system features, and user permissions.

**Universal Interface Server** – A global import/export utility that enables advanced users to import data and images into the B.A.S.I.S. database or to export data and images from the database.

**Video Archive Server** – A system service that is responsible for archiving video data from multiple video servers onto one or more designated storage devices.

**Visitor Manager** – A networked-based application that enables a user to schedule and track visitors throughout an organization.
Troubleshooting Cardholder Issues
(Shaded entries represent those issues most occurring in day-to-day operations)

- **Invalid Card Format**
  - a) Wrong card used in system
  - b) Card presented improperly
  - c) Incorrectly configured Card Format
  - d) Incorrect Card Format chosen for reader
  - e) Incorrect Reader Type chosen for reader
  - f) Incorrect setting at reader for communication
  - g) Incorrectly terminated data wires (Green/White) at reader
  - h) Insufficient power to reader
  - i) MOV or Diode not installed

- **Invalid Facility Code**
  - a) Wrong card used in system
  - b) Incorrectly configured card format
  - c) Incorrect Card Format chosen for reader

- **Invalid Badge** (without Name/Cardholder Record is not in panel)
  - a) No Cardholder record for the badge

- **Invalid Badge** (with Name)
  - a) No Access Level assigned to Cardholder
  - b) Incorrect memory setting for Access Panel
  - c) Incorrect Cardholder capacity chosen for Access Panel

- **Invalid Issue Code**
  - a) Incorrect Issue Code for Cardholder record

- **Invalid Access Level**
  - a) Reader not listed in the assigned Access Level
  - b) Token presented at reader outside of the time zone

- **Granted Access No Entry**
  - a) Door not opened after presentation of token at reader
  - b) Malfunctioning or missing Door Position Switch
  - c) Assume Door Used not checked in the Settings tab when Door Position Switch is not installed

- **Granted Access**
Line Errors Reported for B.A.S.I.S. Panel Devices

UL requires that 4 conditions be reported for supervised circuits:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>shorting of the line</td>
<td>Reported by B.A.S.I.S. as a “Shorted Line Alarm Active” for both B.A.S.I.S. and Apollo Hardware.</td>
</tr>
<tr>
<td>breaking the line (open line)</td>
<td>Reported by B.A.S.I.S. as an “Open Line Alarm Active” for both B.A.S.I.S. and Apollo Hardware.</td>
</tr>
<tr>
<td>grounding either side</td>
<td>Reported by B.A.S.I.S. as a “Grounded Loop Alarm Active” for both B.A.S.I.S. and Apollo Hardware.</td>
</tr>
<tr>
<td>introducing a foreign voltage or resistance</td>
<td>Reported by B.A.S.I.S. as a “Line Error Active” for B.A.S.I.S. Hardware only.</td>
</tr>
</tbody>
</table>

Additional B.A.S.I.S. Reporting

B.A.S.I.S. Hardware also recognizes a 5th condition. This condition of a non-settling voltage is also reported as a “Line Error Active” by B.A.S.I.S.

A non-settling voltage occurs when a switch or relay that is connected to the monitoring input changes state more than once within a 200-millisecond period. The usual cause of this condition is a non-functioning, out of alignment, or oxidized contact.

The "Shorted Line Alarm Active," "Open Line Alarm Active," and "Grounded Loop Alarm Active" are reported only when the "Supervised" checkbox is checked on the "Settings" tab of the reader configuration screen.
Note: When using the File Import option, the first record of the import file must be the exact header record below. The file should be an ASCII, comma delimited file.

Header with two sample records:

ssno,first,middle,last,addr1,city,state,zip,homephone,title,bdate,dept,div,loc,phone,building,floor,ext,email,PhotoFile,badgeid,type,embossed,activate,deactivate,status,issuecode,pinnumber,acc_lvl1,acc_lvl2,acc_lvl3,acc_lvl4,acc_lvl5,acc_lvl6

017645613,Justin,A,Moretta,114 Malasis Street,Fairpoort,NY,14450,377-8374,Senior Engineer,2/5/67,Engineering,Research & Development,Headquarters,248-9720,Headquarters,2nd,109,tech@bestacces.com,,1000,Engineer,2392,3/3/95,10/1/96,Active,0,65,Staff,,,,

124586612,Maria,L,Arquette,84 Lincoln Ave.,Rochester,NY,14445,425-6532,Sales Representative,7/29/70,Marketing,,,248-9729,Headquarters,2nd,110,improvements@bestacces.com,C:\DATA\32\SAMPLE.BMP,1500,Engineer,1192,10/10/95,10/10/05,Active,0,65,1,1,
Access Control Data – Information that is encoded on a credential, which authenticates the credential for use in an access control system. Usually this data is comprised of a facility code, badge ID, and sometimes an issue code.

Access Group – An organization method that can be used to combine access levels into one assignment action for a credential holder. The number of access levels that can be combined into an access group cannot exceed the system configuration limits on the number of access levels that can be assigned to a credential holder.

Access Level – An access control relationship made between a reader or readers and a timezone or timezones. An access level is assigned to a badge ID for the purpose of granting access through a reader or readers during a specified time.

Access Panel (Intelligent System Controller/ISC) – A circuit board with onboard memory that is responsible for making most of the decisions in an access control system.

Activation Date – The date that the access authority for a credential is set to begin.

Antipassback – A configuration limiting the ability of consecutive uses for a credential at a reader. Usually, configured with readers installed on both the secure and non-secure side of an opening. Once a credential has been used in a reader to gain access on one side of the opening, the credential cannot be used in the same reader until the credential is used to gain access in a reader from the opposite side of the opening.

APB Exempt – Antipassback exempt. The cardholder with this privilege is exempt from antipassback rules.

Badge – The credential or token that carries a cardholder’s data.

Badge ID – Part of the access control information that is encoded to a credential. This information, usually numerical, is unique to a particular credential holder.

Badge Type – Used in B.A.S.I.S. to determine a number of parameters for a particular badge ID. These parameters include the activation and deactivation dates, default access groups, the applied badge design, the printer used to print the badge, the required data fields for cardholder entry, and a range of badge ID’s to be used for a specific group of badges.

Card Format – The way the data is arranged and ordered on the card.

Card Reader – A device that, upon presentation of a credential, interprets the access control data on the credential and sends it on to the access control system for a decision.
Cardholder (Credential Holder) – An individual who is issued a particular credential.

Client/Workstation – A computer that contains the access control application. All installed access control applications would point to and access a single database location (usually the/a server). Many times all access control applications, services and the database reside on one computer. This single computer would be classified as both a server and workstation.

Common Door – A configuration setting that allows for the allocation of duplicate badge ID ranges in separate offline locksets.

Credential – A physical token, usually a card or fob, encoded with access control information.

Credential Holder (Cardholder) – An individual who is issued a particular credential.

Deactivation Date – The date that the access authority for a credential is set to expire.

Deadbolt Override – The ability for an authorized credential to retract both the spring latch and the deadbolt when the deadbolt is engaged.

Dongle/Hardware Key – A physical device that connects to a computer’s parallel or USB port that authenticates a valid license file. The identification number of the dongle and license file must match before a successful launch of an access control application can be accomplished.

Extended Unlock/Held Open – The extra period of time the lock will unlock or the door can be held open without generating an alarm when an authorized credential with extended unlock privileges is presented.

Facility Code – Part of the access control information that can be encoded to a credential. This information, usually numerical, is unique to a group of credentials. Usually this feature is used to authenticate a credential to a particular organizational unit.

First Card Unlocked – The ability of an authorized credential, upon presentation to a card reader, to place a lock into the unlocked mode. Usually, used to ensure someone is on location before a reader will change to an unlocked mode during a timezone controlled reader mode configuration.

Input – A hardware connection point used for status reporting of a particular sensor.
Interval – A specific range of time, which corresponds to a particular day or days of the week. A timezone can be comprised of several, individual intervals up to a maximum of six.

Issue Code – Part of the access control information contained on a credential that allows reuse of the badge ID when a credential is lost, damaged, or stolen. Usually one or two digits in length, this code increments forward when creating a new credential. Access is granted only when the badge ID and the issue code match the current database information.

Issue Code Lookahead – An offline feature where a higher issue code for a particular badge ID knocks out the same badge ID with a lower issue code from an offline lock when the badge ID with higher issue code is presented to the lock.

License File – The file that becomes part of the license server once installed and controls access to various software options within the access control application. The entire access control application suite can be installed, but the license file limits navigation to the options listed in the license file.

Offline Reader Mode – The desired mode for reader operation when the Reader Interface Module has lost communication with the Intelligent System Controller. In this case, the reader has lost contact with the database that resides in the Intelligent System Controller. The supported offline reader modes are Locked, Unlocked, and Facility Code Only.

Online Reader Mode - The desired mode for reader operation when the Reader Interface is communicating with the Intelligent System Controller. In this case, the reader has contact with the database, and all available reader modes are supported.

Output – An onboard relay or switch that is configurable to follow the status of an input, system condition, or a timezone.

Passage Mode – The ability to double present an authorized credential within the strike time to unlock an opening. The lock is returned to its original status by a second, double presentation of an authorized credential.

Reader Interface Module (RIM) – A circuit board that acts as the integration point for access activity at a particular opening. The RIM integrates Card Reader, Door Position, Request-to-Exit, and Lock Control activity with the ISC. The RIM communicates this access control activity to the ISC so that the ISC can make the access control decision.
Reader Type – In the case of an online system, the reader type determines what the Reader Interface Module is expecting from the card reader in the way of access control data and communication format. In an offline system, the reader type is matched with the feature and functionality set of a purchased offline product. A reader type selection of Guest refers to the B.A.S.I.S. G product while a selection of Offline Guest refers to the B.A.S.I.S. V product.

Request-to-Exit (RQE or REX) – A sensor usually installed on the non-secure side of the door that will mask the door position switch upon activation. A secondary function of the RQE is to unlock the locking device for the strike time.

Server – The computer that manages the access control environment, including communications with the field hardware. Technically, a server is responsible for running one or many of the services that are responsible for various functions in an access control system. These services include the Communication Server, Linkage Server, Global Output Server, and License Server and can be run on the same computer or distributed across several computers. All computers in this case would be classified as a server. Many times, the database would also reside on a server.

Strike Time – The period of time the lock will energize or de-energize upon presentation of an authorized credential.

Timezone – A defined range of time for assignment to various access control activities. A timezone may be applied to a reader or readers when creating an access level, to a reader to change the mode of operation, to a relay to activate and deactivate, to an input to mask and unmask, and a host of other operations.

Two Card Control – The requirement for the presentation of two separate, authorized credentials in order to gain entry through an access controlled opening.

Unlock Duration (Strike time) – The time that the lock monetarily unlocks.

Use Limit – A configuration limiting a credential to a defined number of uses.