Contents

1 Introduction
   Related documents 1–1
   Getting technical support 1–2
   How to use this guide 1–2
   What you need to get started 1–3

2 Product Overview
   Feature comparison of B.A.S.I.S. G and B.A.S.I.S. V 2–1
   What is Guest Access Control? 2–5
   2–7

2 Installing the B.A.S.I.S. Software
   Overview 2–2
   Confirming computer specifications 2–2
   Checking for and loading missing prerequisites 2–3
   Installing the license key 2–4
   Install the B.A.S.I.S. Software 2–7
Setting up a license file 2–10
Testing the B.A.S.I.S. installation 2–13
Setting up a database 2–14
Logging into B.A.S.I.S. for the first time 2–15

4 Installation of Peripherals
Installing the PDA 4–1
Installing B.A.S.I.S. Transport 4–2
Installing the encoder 4–2

5 Initial Configuration
General system configuration 5–1

5 Hardware Configuration
Hardware Configuration 5–1
B.A.S.I.S. Offline Lock/reader programming is now complete 5–6

6 Standard Access Control
Timezones 6–2
Access Levels 6–4
Adding a Cardholder for Standard Access Control 6–5

6 Guest Access Control
Adding a Cardholder for Guest Access Control 6–1
7 Communicating with the Hardware
   Introducing B.A.S.I.S. Transport 7–1
   Programming locks 7–2
   Retrieving history records 7–9
   Using diagnostics features 7–13

8 Managing Cardholders
   Editing cardholders 8–2
   Searching for cardholders 8–9
   Encoding existing cardholders 8–11

A Glossary of Terms
   Terms A–2
Chapter 1

Introduction

Thank you for choosing B.A.S.I.S.® G and V, the world’s leading combination online and offline access control system.

Use this guide to make sure that you set up your system in the most efficient way and to get the most out of it. The initial setup of the B.A.S.I.S. G and V system is not trivial, but if done thoroughly it will pay many dividends.

Related documents

The following documents are available to help you install, maintain, or operate other related systems. See your Stanley representative for more information.

- Electronic Stand-Alone Lock Service Manual
- Alarm Monitoring User Guide
- BadgeDesigner™ User Guide
- FormsDesigner™ User Guide
- ID CredentialCenter User Guide
Notes

- Basic Import Utility User Guide
- Installation & Setup User Guide
- MapDesigner™ User Guide
- System Administration User Guide
- Universal Interface Server User Guide
- Replicator User Guide
- View/Edit Only Workstation User Guide
- Alternative Wiring Configurations Guide
- Legato® Co-StandbyServer™ User Guide
- Hardware Installation Guide
- Visitor Management User Guide
- Area Access Manager User Guide
- Digital Video User Guide
- Video Archive Server User Guide
- Replication Administration User Guide
- Digital Video Hardware User Guide
- B.A.S.I.S. Interface User Guide

Getting technical support

Stanley Security Solutions/Best Access Systems Representatives provide telephone technical support for all B.A.S.I.S. products. You may locate the representative nearest you by calling 317-849-2250 Monday through Friday, between 7:00 am and 4:00 pm, eastern standard time, or visit us on the web at www.bestaccess.com.

How to use this guide

This manual is intended for use as a training guide and a reference in the installation and initial set-up for B.A.S.I.S. software when using B.A.S.I.S. G and V offline locks.

Chapter 2, Product Overview
Chapter 3, Installing the B.A.S.I.S. Software
Chapter 4, Installation of Peripherals
Chapter 5, Initial Configuration
Chapter 6, Hardware Configuration
Chapter 7, Standard Access Control
Chapter 8, Guest Access Control
Chapter 9, Communicating with the Hardware
Chapter 10, Managing Cardholders
What you need to get started

The following describes the system ‘family’ – all the types of hardware and software that it takes to create an offline B.A.S.I.S. system.

Components include:

- B.A.S.I.S. software, version 5.8, build 41b or higher
- Dedicated computer, see your Stanley representative for complete details
- B.A.S.I.S. G or V lock, includes *cylindrical, mortise* or exit hardware trim models
- *Personal digital assistant (PDA)*. See www.bestaccess.com for supported models.
- *Encoder*
  - magnetic stripe
- *Cables*
  - computer to PDA
  - PDA to lock (requires PDA proprietary cable and BEST part number BASD-CAB).
Chapter 2

Product Overview

This chapter describes the B.A.S.I.S. G and V Offline product differences and provides an overview of the issue code, look ahead and guest access control features.

Feature comparison of B.A.S.I.S. G and B.A.S.I.S. V

The differences between B.A.S.I.S. G and B.A.S.I.S. V can be confusing since they share many of the same features. Both can support standard and guest access control, but only within the constraints of the hardware specifications and software license. The following table compares the two products side by side.
### Notes

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>B.A.S.I.S.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest access control</td>
<td>Provides the ability to issue pre-created <em>badge ID</em>s to individuals. This supports the assignment of one <em>reader</em> directly to the <em>badge</em>. Other readers may be assigned to the badge through normal <em>access level</em> assignment.</td>
<td>G</td>
</tr>
<tr>
<td>Standard access control</td>
<td>Access control based on time and location (access levels)</td>
<td>G</td>
</tr>
<tr>
<td>Look ahead</td>
<td>Issue code look ahead feature through offset and range fields.</td>
<td>G</td>
</tr>
<tr>
<td>Encoding</td>
<td>Provides the ability to encode both magstripe and smart cards from the cardholder/badge tab.</td>
<td>G</td>
</tr>
<tr>
<td>Passage mode</td>
<td>Allows the <em>cardholder</em> to place the reader into an unlocked mode. This status is cleared only by another passage mode attempt or reader mode change occurrence.</td>
<td>G</td>
</tr>
<tr>
<td>Deadbolt override</td>
<td>Allows the cardholder to retract the deadbolt.</td>
<td>G</td>
</tr>
<tr>
<td>Key override event</td>
<td>An event logged into history whenever the key override feature is used in a mortise lock. Not supported in Cylindrical.</td>
<td>G</td>
</tr>
<tr>
<td>Use activation date</td>
<td>Determines if the lockset will use the activation date field stored in the cardholder record when validating. This option has no impact on building functionality.</td>
<td>G</td>
</tr>
<tr>
<td>Use deactivation date</td>
<td>Determines if the lockset will use the deactivation date field stored in the cardholder record when validating. This option has no impact on building functionality.</td>
<td>G</td>
</tr>
<tr>
<td>Two card control</td>
<td>Requires that two valid users must present their cards in order to unlock the door.</td>
<td>G</td>
</tr>
<tr>
<td>Enforce use limit</td>
<td>Allows for the temporary use of cards. After a certain number of uses the card is disabled. The number of uses is configured through the badge tab.</td>
<td>G</td>
</tr>
<tr>
<td>Denied attempts</td>
<td>Includes attempts count and time out duration. Sometimes referred to as ‘Three strikes your out.’</td>
<td>G</td>
</tr>
<tr>
<td>Logging (grant, denies, status)</td>
<td>Provides the ability to filter the displaying/logging of history events. This feature is implemented at the Management System level.</td>
<td>G</td>
</tr>
</tbody>
</table>

**Configurability:**
- **G:** Global
- **V:** Visible
- **always logged:** Always logged
### Table: Feature Summary

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>B.A.S.I.S.</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daylight saving time</td>
<td>Support for all OS world timezones.</td>
<td>G V</td>
<td></td>
</tr>
<tr>
<td>128K RAM</td>
<td>5000 Users/History</td>
<td>G V</td>
<td></td>
</tr>
<tr>
<td>Card formats (8)</td>
<td>Support for up to eight card data formats per reader. Facility codes are assigned through card formats.</td>
<td>G V</td>
<td></td>
</tr>
<tr>
<td>Magnetic</td>
<td>5 bit ABA data only</td>
<td>track 3 tracks 1 &amp; 2</td>
<td></td>
</tr>
<tr>
<td>Wiegand</td>
<td>Any valid Wiegand format</td>
<td>G V</td>
<td></td>
</tr>
<tr>
<td>Online mode</td>
<td>Automatic (timezone control of reader mode), Facility Code, Card Only, Unlocked, Locked, Card and Pin, and Card or Pin.</td>
<td>G V</td>
<td></td>
</tr>
<tr>
<td>Reader modes (automatic unlock/relock)</td>
<td>This feature provides the ability to change operational modes at specified periods through timezone control. The current modes would be Facility Code, Card Only, Unlocked, Locked, Card and Pin, Card or Pin, and First Card Unlock.</td>
<td>2 32</td>
<td></td>
</tr>
<tr>
<td>Unlock duration</td>
<td>The amount of time that the lockset will remain unlocked for a valid access grant.</td>
<td>G V</td>
<td></td>
</tr>
<tr>
<td>Extended unlock</td>
<td>This feature provides the ability to extend the unlock duration for certain cardholders.</td>
<td>G V</td>
<td></td>
</tr>
<tr>
<td>Chassis type</td>
<td>Cylindrical &amp; Mortise with support for a user defined type ‘Custom’.</td>
<td>G V</td>
<td></td>
</tr>
<tr>
<td>Holidays</td>
<td>Special days of the year can be categorized as one of eight types.</td>
<td>8 32</td>
<td></td>
</tr>
<tr>
<td>Timezones</td>
<td>Timezones are necessary for the use of Access Levels. A timezone can be comprised of up to six intervals.</td>
<td>4 32</td>
<td></td>
</tr>
<tr>
<td>Access levels</td>
<td>Access Level assignment to readers (standard access control).</td>
<td>G V</td>
<td></td>
</tr>
<tr>
<td>Battery warn/alarm</td>
<td>Reported through the activation of LED’s and the lock internal sounder.</td>
<td>G V</td>
<td></td>
</tr>
<tr>
<td>Panel password</td>
<td>Communication password is configured at the Access Panel level.</td>
<td>G V</td>
<td></td>
</tr>
<tr>
<td>Diagnostics (PDA)</td>
<td>The PDA will support the capability of performing diagnostics on the lockset.</td>
<td>G V</td>
<td></td>
</tr>
<tr>
<td>Cycle count/reset</td>
<td>The lockset will maintain a current count of access grants. The count can be reset by the user.</td>
<td>G V</td>
<td></td>
</tr>
<tr>
<td>Diagnostics code</td>
<td>This code provides some feedback of the lockset’s status.</td>
<td>G V</td>
<td></td>
</tr>
</tbody>
</table>
### Notes

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>B.A.S.I.S.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup battery level</td>
<td>Displays the current level of the backup battery.</td>
<td>□ □</td>
</tr>
<tr>
<td>Electronics level</td>
<td>Displays the current level of the main electronics battery.</td>
<td>□ □</td>
</tr>
<tr>
<td>Unlock once</td>
<td>This feature allows for the unlocking of the door for the unlock duration.</td>
<td>□ □</td>
</tr>
<tr>
<td>Reader mode</td>
<td>This feature allows for the setting of the current operating mode directly to the reader through the PDA. This action would override the online mode set at the management system level. All online reader modes are supported.</td>
<td>□ □</td>
</tr>
<tr>
<td>Reader support</td>
<td>Dual Validation</td>
<td>□ □</td>
</tr>
<tr>
<td>Magstripe</td>
<td>track 3 tracks 1 &amp; 2</td>
<td></td>
</tr>
<tr>
<td>HID Proximity</td>
<td></td>
<td>□</td>
</tr>
<tr>
<td>Motorola Proximity</td>
<td></td>
<td>□</td>
</tr>
<tr>
<td>Batch update</td>
<td>This feature allows for the bulk updating of Activation/Deactivation Dates.</td>
<td>□ □</td>
</tr>
</tbody>
</table>
What is Guest Access Control?

Both B.A.S.I.S. G and V locks support Standard and Guest Access Control with the proper license.

Guest access control can be effectively used in any application where a room has continuous occupancy change over a period of time, or where the lock location is remote or isolated enough that going out to reprogram the lock becomes undesirable.

Guest access control then is the lock feature that enables you to add and delete users to and from the lock without having to go out and visit the lock to reprogram it.

Operation

Guest access control allows that a range of badge numbers be pre-programmed into the lock unit securing a room. These badge numbers are available for issue and reuse as individuals are assigned to their room accommodations. The badge number is automatically issued to an individual when the lock for the room is chosen in the cardholder setup screen. The card number from the assigned range can then be encoded and presented to the individual for use in his or her assigned room.

New individuals may be assigned access to a particular room by using badge IDs from the same range without ever needing to re-program the lock. By taking advantage of the issue code look ahead feature, a badge ID issued with an incrementally higher issue code will deactivate any other like badge ID for the lock.

The following diagram describes the design and process that B.A.S.I.S. offline locks use to achieve the guest access control.
The diagram uses the following issue code look ahead values:

<table>
<thead>
<tr>
<th>Look ahead function</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offset</td>
<td>1</td>
</tr>
<tr>
<td>Range</td>
<td>3</td>
</tr>
<tr>
<td>Number of issue code digits</td>
<td>2</td>
</tr>
</tbody>
</table>

Also instructive is to see what happens when the issue code has reached its limit. Let’s look at another diagram to see what happens in this case. The issue code look ahead values remain the same.
Figure 2.2  Guest functionality in rollover diagrammed

Lost card  Newly encoded card

B.A.S.I.S. Offline Lock

Auto update

Same B.A.S.I.S. Offline Lock after use of the 1001 issue code 00 card

Lost card does not work

Notes

Issue codes
1001 00
1002 01
1003 02
1004 03
1005 04
1006 05
1007 06
1008 07
1009 08
1010 09
1011
1012
1013
1014 99
1015
1016
1017
1018
1019

Issue codes
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019

Offset of 1
Range of 3 valid issue codes

New offset
New range

1001 issue code: 99
1001 issue code: 00

B.A.S.I.S. G Lock
Same B.A.S.I.S. G Lock after use of the 1001 issue code 00 card
Installing the B.A.S.I.S. Software

You are now ready to start setting up your B.A.S.I.S. offline system. The following tasks do not include installation of the locks themselves. The installation of B.A.S.I.S. G or B.A.S.I.S. V locks are fully described in the following instruction documents.

<table>
<thead>
<tr>
<th>Title</th>
<th>Doc number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Instructions for Electronic Stand-alone Cylindrical Locks</td>
<td>T61835</td>
</tr>
<tr>
<td>Installation Instructions for Electronic Stand-alone Mortise Locks</td>
<td>T81627</td>
</tr>
<tr>
<td>Installation Instructions for Electronic Stand-alone Exit Hardware Trim</td>
<td>T61828</td>
</tr>
</tbody>
</table>
Notes

Make sure that the B.A.S.I.S. offline locks are on site and ready to be programmed. Locks may be programmed before installation.

Before you start, confirm that you have the B.A.S.I.S. CDs, a hardware key and a license file.

Overview

This chapter will take you through step by step instructions on how to properly install the B.A.S.I.S. software for a server configuration. It will cover:

- Confirming computer specifications
- Checking for and loading missing prerequisites
- Installing the license key
- Installing the B.A.S.I.S. software
- Installing the license file
- Setting up the database
- Logging into B.A.S.I.S. for the first time

There are two installation types that can occur with the B.A.S.I.S. software: Server and Client.

A server is required for every installation. A server installation supplies the ability to install the necessary access control programs, services and a database.

A client installation provides only the necessary access control programs that will connect to an existing database.

Confirming computer specifications

Refer to current price book for computer specifications.

To confirm computer specifications

1. Insert Disc 2 in a CD drive

   Supplementary Materials Disc screen will appear.
Chapter 3: Installing the B.A.S.I.S. Software

2 Check the current system requirements to ensure compatibility.

3 Write down the computer name for future reference.

Checking for and loading missing prerequisites

Check the appropriate area for the prerequisite software. You should look for the most current versions of the following programs:

- Adobe Acrobat Reader
- Microsoft Data Access
- Microsoft DirectX

To check for and load missing prerequisites

1 Identify missing software (if any) and/or the need to upgrade to a higher version of software.

2 Follow the instructions on how to load the software from the Supplementary Materials Disc.
Notes

Installing the license key

Each hardware key or dongle has a unique serial number that is keyed to a license file.

If the license key is located at the individual workstation as a USB Ultra Pro drive, you will need to install the hardware prior to loading the B.A.S.I.S. software.

If you are connecting to a license key located on a network, skip this step but make sure you know the location of the license key.

To install the license key

1. Plug the USB Ultra Pro drive into an active USB port.
   
   You will see an icon pop up on the lower right hand corner of the monitor and the New Hardware Wizard should automatically start.

2. Choose Install the software automatically (Recommended) and click Next. The wizard will search for the hardware.
   
   In most cases, the wizard will not be able to find the hardware and the following screen will appear.

   ![Figure 3.2  Found New Hardware](Image)

   Click Cancel.
Chapter 3: Installing the B.A.S.I.S. Software

3 If this screen appears, clear (uncheck) the “Don’t prompt me again to install this software.” and click Cancel.

**Caution:**
Remove the dongle from the workstation then proceed to step 4.

4 On the Supplementary Materials Disc, select the Rainbow Drivers link.

*The Rainbow drivers installation link will appear.*

**Figure 3.4  Rainbow Drivers**

5 Click Install Now.

6 Sentinel System Driver Wizard will appear. Click Next.

7 Accept the license agreement and click Next.

*The Sentinel install wizard will appear.*
Chapter 3: Installing the B.A.S.I.S. Software

Notes

8 Choose Complete set-up type and click Next.
9 Remove the USB license key from the computer.

Caution
If you haven’t already, remove the USB license key from the computer.

10 Click Install.
11 Follow any onscreen instructions. Click Finish.
12 Restart the computer.
13 Plug the USB Ultra Pro into the computer.
14 New Hardware Wizard should appear again. Choose Install the software automatically (Recommended) and click Next.
15 The wizard will search for the hardware and should install the software needed for the drive.
16 Click Finish.

The Found New Hardware message should appear in the lower right hand corner of your monitor. The USB License Key is ready to go and will remain plugged into the computer from now on.

17 Restart the computer.
Install the B.A.S.I.S. Software

Now you are ready to begin the installation of the B.A.S.I.S. software.

**To install the B.A.S.I.S. software**

1. Insert Disc 1 into the CD drive.
   
   *The installation wizard will automatically appear.*

   **Figure 3.7  B.A.S.I.S. Installation Wizard**

   2. Accept the license agreement.

   3. Click on the appropriate type of installation: Client > or Server >. The following steps will show you a typical Server installation.

**Selecting Components & Program Location**

*You will begin by selecting components for the system type.*
Notes

1. Choose Complete or Custom System. Custom install allows you to install only the programs and services you select and/or have license to use.

2. Select the appropriate type of database.

3. Click Next.  
   
   Program location selection screen will appear.

4. Use the default installation location unless instructed otherwise by the customer. The License Server location is the name of the workstation.

   Note: You wrote down the workstation name at the beginning from the Supplementary Materials Disc.
Chapter 3: Installing the B.A.S.I.S. Software

Note  Do not change the port number. Use the default port 8189.

Note  Database location will either be on the workstation or on the network. Make sure you know the location prior to installation.

5  To find or change database location, click Browse...

   A browse window will appear.

Figure 3.10  Browse for Computer

6  Navigate to the database location. Click OK.

Note  It is recommended to browse for the location versus manually entering the information because it ensures the path is correct.

7  Click Install.

8  There will be several progress windows active during the installation. Follow any onscreen instructions.

Database Installation Utility

   The next screen will confirm the database name and location setup.
Chapter 3: Installing the B.A.S.I.S. Software

Notes

Figure 3.11  Database Installation Utility

1. Enter the database name or use the default name.
2. Click Browse... to find the correct path to copy the database files or use the default path.
3. Click OK.

Note  A DOS window will appear for a few moments.
4. Installation is complete. Click Finish.
5. Restart the computer.

Setting up a license file

A new license file will need to be installed prior to launching B.A.S.I.S.

To setup a license file
1. Click Start > Programs > B.A.S.I.S. > License Administration

The menus will appear on the monitor.
Figure 3.12 Navigate to License Administration

Click Start > Programs > B.A.S.I.S. > License Administration.

Windows Explorer windows will appear.

Figure 3.13 License Administration Log In

Enter Username and Password.

Click Log In.

2 Enter the user name and password.

Username: admin
Password: admin

3  Click Log In.
       *The license file menu will appear.*

Figure 3.14  Install New License

Note
Changing the password is optional.

4  Click Install New License.
       *Step 1 of 3 will appear.*

Figure 3.15  Choose License File

Step 1: Choose License File
1  Click Browse...
2  Navigate and locate the license file.
3  Select the file and click Open. The path to the license file will show up the box.
4  Click Next.
Step 2: View the License
This screen allows you to view the entire license.

1. Scroll to the bottom of the page.
2. Click Next.

Step 3: Read License Agreement
1. Select Yes.
2. Click Finish.
3. License installation is complete. Click Log Out.
4. Close the Windows Explorer window(s).

Testing the B.A.S.I.S. installation
It’s time to find out if you’re ready to open the B.A.S.I.S. program.

To test B.A.S.I.S. installation
1. Click Start > Programs > B.A.S.I.S. > System Administration.

   Error 1: Could not add columns to table

   Figure 3.16 System Administration Error 1

   Click OK.

2. Click OK.

   Error 2: Database cannot be opened or is not compatible

   Figure 3.17 System Administration Error 2

3. Click OK.
Notes

If you receive these errors, the database has to be setup. If you do not receive any errors and the B.A.S.I.S. login screen appears, skip to “Logging into B.A.S.I.S. for first time”.

Setting up a database

In most cases, you will need to setup a new database for the customer.

To setup a database

1. Click Start > Programs > B.A.S.I.S. > Database Setup.
2. Click Continue.

   The login screen will appear.

3. Enter the Login ID and password.
   
   Login ID: lenel
   
   Password: multimedia

4. Click OK. A weak password notification will appear.

   Note

   Changing the password is optional.

5. Click Continue.

6. Select Create new database and click Continue.

   Setup Finished Successfully message appears.
Chapter 3: Installing the B.A.S.I.S. Software

Notes

7 If you want to view the setup log, click Continue.
8 To finish, click Exit.

Logging into B.A.S.I.S. for the first time

You should now be able to log into the B.A.S.I.S. software.

To log into B.A.S.I.S.

1 Click Start > Programs > B.A.S.I.S. > System Administration.

   The B.A.S.I.S. login screen appears.

2 Enter the user name and password.
   User name: sa
   Password: sa

3 Click OK.

   Password change required screen will appear.
Chapter 3: Installing the B.A.S.I.S. Software

Notes

You must change the password or B.A.S.I.S. will not allow access to the program. Make sure you pick a password and communicate that to the customer or use a customer-provided password.

4 Click Yes.

5 Type in old password (sa) and enter the new password twice.

6 Click OK.

7 A Successfully Changed message will appear. Click OK.

8 The login screen will appear again. Use the same username (sa) and the new password to login.

9 Click OK.

Depending on the new password, you may or may not see an error message.

10 Click OK.

If you followed these steps, the B.A.S.I.S. program should successfully launch and the opening screen for System Administration should appear. Click on a menu to ensure the program is functioning properly.
This chapter describes the next steps in setting up your B.A.S.I.S.® offline system. Make sure that the B.A.S.I.S. G or V locks are at least on site and ready to be programmed. Locks may be programmed before installation.

Installing the PDA

The Personal Digital Assistant (PDA) is your link from the B.A.S.I.S. workstation to the B.A.S.I.S. G or V lock.

With the help of your computer network administrator, if necessary, perform the following steps to set up the connection between the PDA and the B.A.S.I.S. workstation.

To install Microsoft ActiveSync
1. Connect the PDA to the B.A.S.I.S. workstation.
2. Install Microsoft ActiveSync.
Chapter 4: Installation of Peripherals

**Notes**

3 When prompted, set up a partnership with this computer and remove all check marks associated with programs.

4 Restart the computer after ActiveSync completely installs.

5 Test the encoder and confirm ActiveSync connectivity before proceeding. To test the encoder, see page 4-4.

**Note** When ActiveSync is running, the ActiveSync icon, shown in the taskbar on the PC’s desktop, is green. When ActiveSync is not running, the icon is gray.

**Installing B.A.S.I.S. Transport**

Confirm that the following requirements are met for running B.A.S.I.S. Transport. For detailed instructions see the B.A.S.I.S. Installation & Configuration User Guide.

- B.A.S.I.S. System Administration is installed.
- B.A.S.I.S. Communication Server is installed.
- Microsoft ActiveSync is installed.
- A connection is established between the PDA and the PC using ActiveSync.

**Note** Before you can install B.A.S.I.S. Transport, you must establish a connection between the PDA and the B.A.S.I.S. PC.

**To install B.A.S.I.S. Transport**

You install B.A.S.I.S. Transport from the B.A.S.I.S. CD #1 onto the PDA from the host with a connection established through ActiveSync.

1 Open an Explorer window for B.A.S.I.S. CD #1. Stop the auto-run of the B.A.S.I.S. installation wizard if it starts.

2 Navigate to the B.A.S.I.S. Transport folder.

3 Double-click the Transport executable (program) file.

   *The B.A.S.I.S. Transport Setup wizard appears.*

4 Follow the on-screen instructions.

**Installing the encoder**

One type of encoder is available for the B.A.S.I.S. Offline system:

- Magnetic stripe encoder
  - Unitech model MSR206
  - part number MSR206-33
The card encoder or some type of encoding device (that is, an encoder or a printer with a built-in encoder) is required for guest access control locks. So the following instructions are required for guest access control, but optional for standard access control. For a comparison of B.A.S.I.S. G and V, See “Feature comparison of B.A.S.I.S. G and B.A.S.I.S. V” on page 2-1.

These instructions assume a stand-alone encoder.

**To set up the encoder**

1. Click Start > Programs > B.A.S.I.S. > System Administration.
2. At the login window type your user name and password and then click OK. If you do not know your user name or password, see your System Administrator.
3. Click Administration > Workstations.
4. From the Workstation tab, confirm that the name of your computer is in the list. If your computer is not in the list, add your workstation by using the browse button and select your workstation.
5. Click Add.
6. Type the name of your computer or click the browse button and browse the network for your computer.
7. Click OK.
8. Click the Encoder tab.
9. Confirm that the encoder is physically connected to a COM port on the computer, preferably COM1, and is powered on.
10. Click Add.
11 Under Encoder Settings, in the name field, type a name for the encoder.

12 In the Encoder Type field, select the appropriate model number for the encoder.

13 Click Test.

**Note**  The encoder can be tested at any time by returning to the Encoder tab. **You do not need to put the encoder in modify mode to test the encoder.**

14 Click OK.

15 Close System Administration.
Initial Configuration

This chapter describes the next steps in setting up your B.A.S.I.S.® offline system.

General system configuration

Overview

To define a B.A.S.I.S.® G or B.A.S.I.S. V general system configuration, you need to configure:

- Card formats
- Badge types

Although B.A.S.I.S. locks are offline (stand-alone) and are not managed by access control panels, you must define Access Panel settings for the locks. In effect, you define ‘virtual’ access control panels for the locks. More than one lock – called a reader in B.A.S.I.S. – can share the same panel configuration. However, these locks (readers) must all:
Notes

- be managed by the same B.A.S.I.S. PC
- share the same password
- be located in the same timezone
- use the same daylight saving time setting.

Defining card formats

1 Defining a card format is the starting point to configuring guest access control. But if guest access control is not needed, a standard card format can be used or configured for a reader assignment through access levels. Badges using standard formats on compatible tracks can only be assigned readers through access levels. For more information on access levels, see page 7-4

To define a card format for guest access control

1 From System Administration, click Administration > Card Formats.

   The Card format form displays

2 Click Add.

   The Choose Card format type window displays

   [Image of Choose Card Format Type window]

   Choose the appropriate card format

3 Choose the appropriate card format and click OK.

   The modify card format window displays
4 Type the name of the card format. A typical name for the guest format is ‘Guest format.’

5 Complete all appropriate fields including facility code, access control track, total characters on track, and the guest format check box.

**Defining badge types**

To use guest access control, you must define a guest badge type. This badge type allows you to define and allocate a range of badge ID numbers that will be programmed into the lock. Badge type is an ID Credential Center function used in the configuration of Guest products and determines the block or pool of badge numbers to be allocated to a group of locks. Also, badge type determines the card format to be encoded on the badge. In this instance think of the badge type as a way of allocating a block of badge numbers to a facility, building, or other group of related guest locks.
A badge type could be used to allocate a pool of badge numbers for a building from which smaller blocks of numbers could be obtained for the individual room units.

**To define a guest badge type**

1. From System Administration, click Administration > Badge Types.

   *The Badge Types form displays*

2. Click Add.

   *The modify badge type window displays*

Figure 5.2 Selecting the Guest class for B.A.S.I.S. G badge type

<table>
<thead>
<tr>
<th>Steps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Select the Guest class from the drop down box.</td>
</tr>
<tr>
<td>4</td>
<td>Complete all other necessary information on the tab.</td>
</tr>
<tr>
<td>5</td>
<td>Click the Printing/Encoding tab</td>
</tr>
</tbody>
</table>

*The Printing/Encoding tab badge type displays*
Select the appropriate card format to be encoded for the badge type.

Make sure that a check mark appears next to the selected card format.

Click the Badge ID Allocation tab.

*The Badge ID Allocation window displays*
Enter the First ID number in the badge range that you want to create.

Application note
Make sure to allocate a range of badge numbers that will facilitate the future growth of a group of locks. The size of the range will determine the length of the reader list in the ‘Allow Access To’ drop-down selection on the Badge tab under Cardholders.

10 Enter the number of Badge IDs that you want to create.

11 Click Add.

12 Click OK.
Hardware Configuration

This chapter describes configuration of the hardware that will allow setup and communication with the B.A.S.I.S. offline locks.

Defining ‘virtual’ offline access panels

Using the virtual access panel concept allows the programming of guest locks to follow the same conventions as B.A.S.I.S. online products. Up to 64 locks (called a ‘reader’ in B.A.S.I.S.) can share the same panel configuration.

Caution

The default password is ‘BEST.’ Care should be given to faithfully document any changes to this
password since the password cannot be viewed from any-
where in the B.A.S.I.S. application software.

To define a 'virtual' offline access panel
1 From System Administration, click Access Control >
   Access Panels.
2 Click the Offline Lock tab.
3 Click Add.

   The Offline Lock Access Panel window displays

Figure 6.1  Naming the offline lock access panel

4 In the Name field, type the name of the ‘virtual’ access
   control panel.
5 Click OK.
6 Repeat steps 3 and 4 as necessary.

Defining the offline reader/lock

In the B.A.S.I.S. software locks are referred to as readers to
conform and maintain consistency with B.A.S.I.S. online ter-
minology conventions.
You can define up to 64 readers or locks for each ‘virtual’ offline access control panel. And each reader or lock will accept up to eight different card formats. It would be highly unusual to use this many formats in one lock.

In this section you will define an offline reader or lock.

**To define an offline reader/lock**

1. From System Administration, click Access Control > Readers.
2. Click the Reader tab – if not already on the reader tab.
3. Click Add.

   *The Add Reader window displays*

4. In the Name field, type the name of the reader.
5. In the Panel field, select the ‘virtual’ offline access control panel that controls the reader.
6. In the Type field, select Guest for B.A.S.I.S. G or V lock. Select Offline or Offline Guest for a B.A.S.I.S. V lock.
7. Select the appropriate reader mode.
8. Under the Card Format section, select the appropriate card format.
Selecting Guest in the reader type allows the lock to be configured for guest access control. All reader types support standard access control.

9 Make any other selections as necessary.
10 Click OK.

*The Reader is listed in the Reader listing at the top of the window.*

11 Repeat steps 3 – 10 for each additional lock/reader.

Now that you have defined the reader operation of the lock/readers, you now need to configure the software so that the correct chassis type is assigned to the lock/reader and other offline features are configured appropriately.

Before you can complete this section you must know:

- Chassis type of the lock/reader. The chassis type will most likely be either mortise or cylindrical.
- The maximum number of cardholders that will need to access the lock/reader. This includes both guest cardholders and those cardholders that access the reader by access levels.
- The number of guest badges that will be assigned from the pool of badge IDs (if guess access control is used).

**To define other guest reader features**

1 From System Administration, click Access Control > Readers.

2 Click the Offline tab.

3 Select the Reader that you want to define. Make sure that the check mark is next to the reader to be modified.

4 Click Modify.

*The Modify Offline Reader window displays*
5 In the Chassis Type field, select the chassis type that the lock/reader has.

The custom chassis type enables the modification of the chassis volume. The chassis volume is a value used by engineers that relates to the number of turns of the motor that is required to unlock the lock. Only use the custom chassis type at the direction of a technical support engineer or specific instructions enclosed with the lock.

6 In the Cardholders field, select the total number of cardholders that will need to access the lock/reader.

7 In the Look Ahead section, select the look ahead offset and range. Normally for B.A.S.I.S. offline locks, the offset is set to 1 and the range to 3. For more information on guest access control, see page 2-5 and page 6-1.

Note If you have chosen a configuration that includes a guest reader type, guest access control is available to configure.

8 In the Guest Parameters section, select whether the lock/reader will be a Common door.

9 In the Badge Type field, select a guest badge type from the list that was created. See page 5-3.
Chapter 6: Hardware Configuration

Notes

10 In the Number of badges field, enter the number of guest badges to be allocated to this lock/reader from the total pool of badge IDs.

11 **For a common door only:** In the Badge Start Number field, enter the starting badge number for the subset of numbers to be used in this lock/reader. The badge end number is automatically calculated from the numbers entered.

12 Click OK.

13 Repeat steps 3 – 12 for each lock/reader to be defined.

B.A.S.I.S. Offline Lock/reader programming is now complete

If you have finished the tasks up to this point, you have completed all steps necessary for the configuration of the B.A.S.I.S. system for offline locks. Now you can move onto programming for standard or guest access control in the next two chapters.
In this chapter, you will learn the final steps in programming standard access control for B.A.S.I.S. offline locks.

Standard access control is nothing more than solving the equation of who can go where when.
A timezone is a block of time that a particular activity or functionality is allowed to occur. These blocks of time are represented by intervals.

B.A.S.I.S. Access Control system can be configured for up to 255 timezones, but a B.A.S.I.S. offline lock is capable of only storing the number of timezones limited by the feature set of each product.

To add a timezone

1. From System Administration click Access Control > Timezones.

   The Timezones window displays

Figure 7.1 The Timezone window showing the ‘Always’ schedule.

2. Click the Timezones tab. A list of the existing timezones will be displayed.

3. Click Add to create a new timezone to the list.
4 Choose a name for the timezone and enter the choice in the Name field.

Choosing a name that actually represents the period of time for the timezone allows you to more efficiently retrieve a timezone from a long list. The timezone list can include up to 255 different timezones.

5 Enter the desired start and end times for each desired interval (time must be entered in a 24-hour format). Indicate by checking the check box on each day that you want the interval to be active.

6 Click OK.

*The new timezone has been added to the list.*

Notice the Timezones tab has additional headings for something other than standard days of the week. These H1 through H8 headings represent holidays that allow for the exceptions to each interval. These holidays, or exception days, are configured on the Holiday tab.

B.A.S.I.S. organizes these exception days into one of eight types. Those exception days that are to be treated the same would be organized into one of the eight types. A holiday type can contain more than one configured exception period.
Notes

Access Levels

An Access Level is nothing more than a list of relationships between readers and timezones. These access levels will become assigned to badges and will determine whether or not a badge will unlock a door during a specified time.

To add access levels

1. From System Administration click Access Control > Access Levels.

   The Access levels window displays

Figure 7.3

2. Click Add to create an access level.
Choose a name for the access level and enter the choice in the Name area.

4 Select the reader(s) and timezone configuration(s) to be included in the access level. Remember that a selection is not made unless a checkmark is observed.

5 Click Assign to move the reader and timezone selections to the right side of the form.

6 Click OK to save the record.

Adding a Cardholder for Standard Access Control

To add a cardholder for standard access control

1 Open System Administration and go to Administration, Cardholders.

A page with several tabs will be displayed. We are only concerned with the first three tabs of Cardholder, Badge, and Access Levels for common day-to-day entry.
2 Click Add on the Cardholder tab. Complete all appropriate fields on the form.

3 Click the Badge tab.

Figure 7.5 The cardholder, general information screen.

Figure 7.6 The cardholder, badge information screen.
4 Select the appropriate Badge Type from the drop-down list.

5 Enter a Badge ID for the corresponding badge only if the field will accept data. Sometimes a system is set to automatically generate badge ID’s and manual entry will not be required. Complete the rest of Badge tab as required by your organization.

6 Click the Access Level tab.

Figure 7.7 The cardholder, access level information screen

Choose the access level for this cardholder. You may need to choose more than one access level.

7 Select the appropriate access levels for the cardholder. **Only the access levels accompanied by a checkmark are selected for assignment.**

8 Click OK to save the record.

9 Click Encode if you are encoding badge ID’s for standard access control.
If the issue code is at zero, the following confirmation is displayed:

Figure 7.8 Question regarding the issue code

Click No, if you are assigning a new badge.
Click Yes, if the card is lost or stolen.

10 Click No.

The Encode Badge window displays:

Figure 7.9 Choosing a card format to encode

Click the Encode button to start the encoding process.

11 Make sure that the checkmark is on the card to be encoded, then click Encode.

The encoder is initialized and prompts you to encode the card:

Figure 7.10 The encoder is ready for the card swipe
12 Slowly swipe the card through the encoder as shown below.

Figure 7.11  Swiping the magstripe card through the encoder

13 Confirm that the encoding is complete.
Guest Access Control

In this chapter, you will learn how to program guest access control for B.A.S.I.S. offline locks.

Adding a Cardholder for Guest Access Control

This section will discuss the configurations that are necessary to implement guest access control. Many people refer to this type of programming as B.A.S.I.S. G programming, but as observed earlier, both B.A.S.I.S. V and G support this type of programming. In guest access control, we are doing nothing more than assigning a cardholder access to a single reader.
Notes

To add a cardholder for guest access control

1 Open System Administration and go to Administration, Cardholders.

A page with several tabs will be displayed. We are only concerned with the first three tabs of Cardholder, Badge, and Access Levels for common day-to-day entry.

Figure 8.1 The cardholder, general information screen.

2 Click Add on the Cardholder tab. Complete all appropriate fields on the form.

3 Click the Badge tab.
4 Select Guest Badge type from the drop down menu.

5 Click the drop down menu for Allow Access To. This lists the areas guest badge types have access. Choose the access area.

6 Click OK to save the record.

7 Click Encode.

   If the issue code is at zero, the following confirmation is displayed:

Figure 8.3  Question regarding the issue code

8 Click No.
The Encode Badge window displays:

Figure 8.4 Choosing a card format to encode

9 Make sure that the checkmark is on the card to be encoded, then click Encode.

The encoder is initialized and prompts you to encode the card:

Figure 8.5 The encoder is ready for the card swipe

10 Slowly swipe the card through the encoder as shown below.

Figure 8.6 Swiping the magstripe card through the encoder

11 Confirm that the encoding is complete.
Communicating with the Hardware

This section describes how to communicate with the offline locksets. The following topics are covered.

- Using B.A.S.I.S. Transport
- Transferring configurations to offline locks
- Retrieving history from offline locks and transferring to B.A.S.I.S. PC
- Running diagnostics on the offline locks

Introducing B.A.S.I.S. Transport

The B.A.S.I.S. Transport software application lets you:

- program B.A.S.I.S. G and B.A.S.I.S. V Locks by transferring reader configurations from B.A.S.I.S. System Administration to the locks
- transfer history records from B.A.S.I.S. Locks to System Administration
Notes

- view diagnostics information for B.A.S.I.S. Locks.

In addition, you can use Transport to unlock a B.A.S.I.S. Lock without using a card or PIN. You also can change the lock’s mode of operation.

Programming locks

To program a B.A.S.I.S. G or B.A.S.I.S. V Lock, you need to:

- Define an access control panel and reader configuration for the lock using B.A.S.I.S. System Administration. For more information, see page 6-1 of this guide as well as the B.A.S.I.S. System Administration User Guide.

- Transfer the reader configuration from the PC to the PDA. See the next section.

- Transfer the reader configuration from the PDA to the lock. See page 9-6.

Transferring reader configurations from the B.A.S.I.S. PC to the PDA

After you have used System Administration to create the reader configurations for the locks you want to program, you can transfer the reader configurations from the B.A.S.I.S. PC to the PDA. You can choose to transfer one, a few or all readers, based on activity, personnel, locations or any other pertinent information. Perform these steps:

To transfer reader configurations from the B.A.S.I.S. PC to the PDA

1 Establish an ActiveSync connection between the PDA and PC.

2 On the PDA, make sure B.A.S.I.S. Transport is not running. To exit Transport, see page 9-9.


4 From the System Administration main menu, click View, then System Tree. See Figure 9.1

Note

When ActiveSync is running, the ActiveSync icon, shown in the taskbar on the PC’s desktop, is green.
You can expand the entries in the System Tree to see the hierarchy of access control devices in your system. To expand an entry, click the plus sign (+) to the left of the entry. To collapse an entry, click the minus sign (−) to the left of the entry.

5 Expand the Hardware entry to view the access control panels defined for your system. Expand the access control panels to view the readers defined for your system. See Figure 9.2.

Figure 9.2 Expanding the System Tree to view readers

Note If a reader configuration has been created or updated at System Administration, but has not yet been sent to the PDA, a red “X” appears on the reader’s icon, as well as on the icon for the reader’s access panel.

6 Highlight the reader that you want to transfer to the PDA.
Notes

To highlight multiple readers, hold down the Ctrl key and click each reader.

7 Right-click on the selection in the System Tree.

The menu shown in Figure 9.3 appears.

Figure 9.3  Right mouse button menu for readers in the System Tree

8 Click Download Reader.

The PC begins transferring the highlighted reader configurations to the PDA.

9 If that reader or panel already exists on the PDA, the PDA will display a dialog requesting to overwrite the old version of the reader. Tap OK.

10 On the PDA, watch the messages indicating the progress of the transfer.

11 When the transfer is complete, a message appears stating, “Complete download successful.” On the PDA, tap OK.

12 To disconnect the PDA from the PC, disconnect the PDA from the ActiveSync connection.
Transferring a configuration from the PDA to a lock

The sections below provide instructions for sending a panel/reader configuration to a B.A.S.I.S. G or B.A.S.I.S. V Lock.

To connect the PDA to a lock
See Figure 9.4 and perform these steps:

1. Connect the serial cable to the PDA.
2. Connect the serial cable to the *programming cable*.
3. Connect the programming cable to the lock’s *communication port*. The connector snaps into place.
**Notes**

**To start B.A.S.I.S. Transport**

- On the PDA, tap Start, then Programs, then BAS, then Transport.

  *The Main window appears, as shown in Figure 9.5*

**Figure 9.5**  B.A.S.I.S. Transport Main window

**To transfer a panel/reader configuration to a lock**

1. Connect the PDA to the lock. See page 9-5.
3. From the B.A.S.I.S. Transport Main window on the PDA, tap View, then Transport.

   The Transport window shows the Panel/Reader Tree.

You can expand the entries in the Panel/Reader Tree to see the hierarchy of access control panel/reader configurations on the PDA. See Figure 9.6
To expand a panel, tap the plus sign (+) to the left of the panel. To collapse a panel, tap the minus sign (–) to the left of the panel.

4 Highlight the reader configuration that you want to transfer to the lock.

5 Tap Transport, then Configure Lockset.

   The Login window appears, as shown in Figure 9.7.

Figure 9.7  Login window

6  *If you are programming the lock for the first time:*

   a  Leave the Enter Password field blank.

   **Note**  B.A.S.I.S. Locks do not have a factory-programmed default password.

   b  Ignore the Preserve user pins checkbox.

   c  Tap OK.
Notes

A message appears stating, “Attempting login . . . Please swipe a card . . .”

d Use the temporary operator card to activate the lock.

A message appears asking, “Reader ID’s don’t match. Continue anyway?”

7 Tap Yes.

The PDA begins transferring the selected reader configuration to the lock.

On the PDA, watch the messages indicating the progress of the transfer.
When the transfer is complete, a message appears stating, “Configuration data transfer successful.”

8 Tap OK.

A message appears asking, “Delete this reader?”

9 We recommend that you tap Yes to delete the reader configuration.

The reader configuration no longer appears in the Panel/Reader Tree.

Note If you want to use this reader configuration for another lock, tap No.

10 To return to the Main window, tap View, then Main.

11 To disconnect the PDA from the lock, press the button on the programming cable connector and unplug the programming cable from the lock’s communication port. See Figure 9.8
If you are updating the configuration for the lock:

1. Enter the lock’s password in the Enter Password field.

For instructions to use the PDA’s virtual keyboard, see the documentation provided with the PDA.

Note: The password for a lock is the password programmed for the reader in the virtual access control panel. You must enter the password exactly as it was entered in the Password field on the Offline Lock form in the Access Panels folder. Capitalization must be the same. The default password is ‘BEST.’

To exit B.A.S.I.S. Transport

□ From the B.A.S.I.S. Transport Main window on the PDA, tap View, then Exit.

Retrieving history records

History retrieval overview

To retrieve and view history records from a B.A.S.I.S. G or B.A.S.I.S. V Lock, you need to:

- Transfer the history records from the lock to the PDA. See the next section.
Chapter 9: Communicating with the Hardware

Notes

- Transfer the history records from the PDA to the B.A.S.I.S. PC. See page 9-12.
- Use System Administration to generate reports using the transferred records. See page 9-12.

You can retrieve history records from multiple locks and then transfer all of the records to the PC at the same time.

Transferring history records from a lock to the PDA

1. Connect the PDA to the lock. See page 9-5.
3. From the B.A.S.I.S. Transport Main window on the PDA, tap View, then Transport.

   The Transport window shows the Panel/Reader Tree.

   Note When transferring history records from the lock, you do not need to highlight a reader in the tree.

4. Tap Transport, then Get History.

   The Login window appears, as shown in Figure 9.9.

Figure 9.9 Login window

5. Enter the lock’s password in the Enter Password field. For instructions to use the PDA’s virtual keyboard, see the documentation provided with the PDA.

   Note The password for a lock is the password programmed for the reader configuration’s access control panel. You must enter the password exactly as it was entered in the Password field on the Offline Lock form in the Access Panels folder. Capitalization must be the same.

6. Tap OK.

   A message appears stating, “Attempting login . . . Please swipe a card . . .”
7 Use the temporary operator card to activate the lock. The lock begins transferring its history records to the PDA.

On the PDA, watch the messages indicating the progress of the transfer.

When the transfer is complete, a message appears indicating the number of history records that were transferred. See Figure 9.10.

Figure 9.10  History transfer completed message

8 Tap OK.

9 To return to the Main window, tap View, then Main.

10 To disconnect the PDA from the lock, press the button on the programming cable connector and unplug the programming cable from the lock’s communication port. See Figure 9.8 on page 9-9.

You can view the history records only after they have been transferred from the PDA to the PC. You cannot view the history records on the PDA.
Notes

To Transfer history records from the PDA to the B.A.S.I.S. PC


2. Establish ActiveSync connection between the PDA and the PC.

Note: When ActiveSync is running, the ActiveSync icon, shown in the taskbar on the PC’s desktop, is green.

When the connection has been established, the PDA automatically transfers all history records to the PC.

On the PDA, watch the messages indicating that the PDA is uploading history records to the PC.

When the history records have been uploaded, a message appears indicating the number of history records that were transferred.

Note: B.A.S.I.S. Transport does not need to be running during this process.

Viewing history records

After you have transferred lock history records from the PDA to the B.A.S.I.S. PC, you can use System Administration to generate reports using the records.

For example, you can use the All Events Over Time report to view and/or print all of the history events transferred from the locks. For instructions, see the B.A.S.I.S. System Administration User Guide.
Using diagnostics features

Diagnostics overview

Figure 9.11  B.A.S.I.S. Transport diagnostics window

You can use B.A.S.I.S. Transport to view diagnostics information for a lock. Figure 9.11 shows an example of the diagnostics information provided. The table below describes each of the fields in the Diagnostics window.

<table>
<thead>
<tr>
<th>This field</th>
<th>Shows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware ID</td>
<td>ID indicating the type of firmware in the lock. Technical support personnel may ask you to provide this information.</td>
</tr>
<tr>
<td>Version</td>
<td>Version number of the lock’s firmware. Technical support personnel may ask you to provide this information.</td>
</tr>
</tbody>
</table>
To view diagnostics information

1. Connect the PDA to the lock. See page 9-5.
3. From the B.A.S.I.S. Transport Main window on the PDA, tap View, then Diagnostics.
The Diagnostics window appears, with the fields blank.

4 Tap Diagnostics, then Connect.

The Login window appears.

5 Enter the lock’s password in the Enter Password field.
For instructions to use the PDA’s virtual keyboard, see the documentation provided with the PDA

Note The password for a lock is the password programmed for the reader configuration’s access control panel. You must enter the password exactly as it was entered in the Password field on the Offline Lock form in the Access Panels folder. Capitalization must be the same.

6 Tap OK.

A message appears stating, “Attempting login . . .
Please swipe a card . . .”

7 Use the temporary operator card to activate the lock.
The diagnostics information appears on the PDA, as shown in Figure 9.11 on page 9-13.

8 When you have finished using diagnostics features, tap Diagnostics, then Disconnect.

The PDA closes communications with the lock.

9 To return to the Main window, tap View, then Main.

10 To disconnect the PDA from the lock, press the button on the programming cable connector and unplug the programming cable from the lock’s communication port.
Managing Cardholders

Introduction

Use this section to understand how to manage cardholders for B.A.S.I.S. offline locks. Managing cardholders involves three activities:

- Editing cardholders
- Searching for cardholders
- Encoding cardholders’ badges

These activities form the bulk of day-to-day operations that are necessary for maintaining a B.A.S.I.S. System in good working order. This section will help you master these activities.
Notes

Editing cardholders

The first of the three activities, editing cardholders involves the following:

- Adding
- Modifying
- Deleting

Adding cardholders

Although it’s not required, to make the process of adding cardholders more efficient, we recommend using the List Builder feature of B.A.S.I.S. This feature allows you to build lists of departments names, building names, locations, and even custom cardholder information before actually creating the individual cardholder records.

In the cardholder screen, the following fields are drop-down lists that the user can pick from. If these lists are compiled before adding cardholders, users can create cardholders quicker and more consistently:

- Title
- Department
- Division
- Location
- Building
To create lists of cardholder data

1. From the System Administration application, click Administration > List Builder.

2. Click the List that you want to add to, so that check mark appears on the highlighted list.

3. Click Add.

4. Add the name of the building, department, etc, that will appear in the cardholder screen drop-down list.

5. Click OK.

6. Repeat steps 2 through 5 until all lists are completed.

Before you start adding cardholders, make sure that you compile all student, employee, contractor, and other records that will need badges.

If you have a large database of people that will need badges, you may want to consider using B.A.S.I.S. Data Exchange, a utility designed to make the process of importing large administration databases or meal card databases into B.A.S.I.S. See your local representative for more information.

But to individually create cardholders follow these steps.
To create a cardholder:

1. From System Administration, click Administration > Cardholders.
2. Click Add.

*The Add Cardholders window displays*

Figure 10.2  Adding cardholders

3. Complete all appropriate fields in the form.

**Note**

Completion of at least the last name field is required to temporarily save the cardholder record. Only complete those fields that are necessary for your business.

**Tip**

To more efficiently add cardholders, use the B.A.S.I.S. List Builder feature described on page 10-3.

4. Click the Badge tab.
The badge form displays

**Figure 10.3**

5 Complete all appropriate fields in the form. For a complete list of field definitions, see the System Administration Help or the Glossary.

**Note** Completion of at least the badge type field and, for B.A.S.I.S. G locks, the reader field (Allow access to) are required to temporarily save the cardholder record. Complete only those fields that are necessary for your business.

6 Click OK.

7 Click Encode.
If the issue code is at zero, the following confirmation is displayed:

Figure 10.4  Question regarding the issue code

Click No.

The Encode Badge window displays:

Figure 10.5  Choosing a card format to encode

Click the Encode button to start the encoding process.

9  Make sure that the checkmark is on the card to be encoded, then click Encode.

The encoder is initialized and prompts you to encode the card:

Figure 10.6  The encoder is ready for the card swipe
10 Slowly swipe the card through the encoder as shown below.

Figure 10.7  Swiping the magstripe card through the encoder

11 Confirm that the encoding is complete.

Modifying cardholders

When a cardholder’s name, location, title, or any other piece of data changes, use the modify function of the same cardholder forms that you used in adding a cardholder.

To be able to synchronize changes in other administration databases or meal card databases, you can use the Data Exchange application, the same utility used to import data.

For full import and export to and from ODBC compliant databases, including Odyssey’s CBORD meal card system, use B.A.S.I.S. Interface™.

To modify a cardholder

1  From System Administration, click Administration > Cardholders.

2  Search for the cardholder record that you want to modify. For more information on searching, see page 10-9.

3  Click Modify.
Chapter 10: Managing Cardholders

Notes

The Modify Cardholders window displays

Figure 10.8  Modifying cardholders

4  Select and change the field or fields that you want to change.

5  Click OK.

Deleting cardholders

To maintain a high degree of security, when someone graduates, retires, is transferred, resigns, or is terminated, that person’s computer record, along with the person’s badge, must be deleted or inactivated.

To delete a cardholder

1  From System Administration, click Administration > Cardholders.

2  Search for the cardholder record that you want to delete. For more information on searching, see page 10-9.

3  Click Delete.

4  Click OK.
Chapter 10: Managing Cardholders

A confirmation window displays

Figure 10.9  Confirming the cardholder to be deleted

5  Click Yes.

The cardholder record is deleted from the database.

Searching for cardholders

The search facility of B.A.S.I.S. is extensive and is an important function that can be used for many reasons. It's important to understand how to search if you’re:

- modifying a cardholder
- deleting a cardholder
- checking the status of a cardholder
- inquiring on a cardholder’s address, phone number, etc.

Search offers an efficient way to find a cardholder or a group of cardholder records using any known piece of the cardholder’s data.

To search for a cardholder or a group of cardholders

1  From System Administration, click Administration > Cardholders.

2  Click Search.

The Cardholder fields are cleared

The cardholder data fields are all cleared to enable you to search for any cardholder record, even if you know as little as one piece of cardholder data. Cardholders can be searched for using one, two or more fields. This enables you to narrow down the list of cardholder records. Once a cardholder or a group of cardholder records are displayed, you can page through the records one by one.

Tip  This is another reason for using the B.A.S.I.S. List Builder feature. Searching for List Builder items (title, department, division, etc.) enables the search facility to find all cardholders with like data because the data for those fields were entered
Notes

using consistent terminology. For more information on using the List Builder feature, see page 10-3.

3 Select the tab that you want to search from. You can search from any one of the following tabs. Each tab has its own unique search features:

- cardholder
- badge
- access levels
- biometrics
- visits
- directory accounts
- guard tours
- reports

4 Select and complete any one or any combination of fields. For example, to search for all students on the first floor of Johnson East dormitory, the following screen shows that two data fields are necessary:

Figure 10.10 Example of searching for all Johnson East, first floor residents

5 Click OK.
Use the search arrows to page through the records that met the search criteria.

**Encoding existing cardholders**

Once a cardholder has been added with the proper badge information, you’re ready to encode the card. For the complete encoder installation procedure, see page 4-2.

**To encode an existing cardholder’s badge**

1. From System Administration, click Administration > Cardholders.
2. Click the Badge form tab.
3. Search for the cardholder record that you want to encode. For more information on searching, see page 10-9.
The Encode badge form displays

Figure 10.12 Getting ready to encode a guest badge

4  Make sure that the checkmark selects the record that you want to encode.

5  Click Encode.

   If the issue code is at zero, the following confirmation is displayed:

Figure 10.13 Question regarding the issue code

6  Click No.
The Encode Badge window displays:

Figure 10.14 Choosing a card format to encode

Click the Encode button to start the encoding process.

7 Make sure that the checkmark is on the card to be encoded, then click Encode.

The encoder is initialized and prompts you to encode the card:

Figure 10.15 The encoder is ready for the card swipe

8 Slowly swipe the card through the encoder as shown below.

Figure 10.16 Swiping the magstripe card through the encoder

9 Confirm that the encoding is complete.
Glossary of Terms

Use this glossary as a reference and whenever you see a word in italic type, like this:

*timezone*
<table>
<thead>
<tr>
<th>Terms</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>access level</td>
<td>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.</td>
</tr>
<tr>
<td>access panel</td>
<td>A circuit board with on-board memory that is responsible for making most of the decisions in an access control system. Also called Intelligent System Controller/ISC.</td>
</tr>
<tr>
<td>activation/deactivation date</td>
<td>The date that a credential becomes active or expires.</td>
</tr>
<tr>
<td>Active-Sync</td>
<td>A Microsoft utility designed to synchronize the data between a PC-based application and a PDA application. ActiveSync is used to synchronize the data between B.A.S.I.S. and B.A.S.I.S. Transport.</td>
</tr>
<tr>
<td>badge</td>
<td>The credential or token that carries a cardholder’s data.</td>
</tr>
<tr>
<td>badge ID</td>
<td>Part of the access control information that is encoded to a token. This information, usually numerical, is unique to a particular credential holder.</td>
</tr>
<tr>
<td>badge type</td>
<td>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.</td>
</tr>
<tr>
<td>B.A.S.I.S. Transport</td>
<td>The application that runs on a PDA designed to update B.A.S.I.S. locks and retrieve lock history.</td>
</tr>
<tr>
<td>card format</td>
<td>The way that data is arranged and ordered on the card.</td>
</tr>
<tr>
<td>cardholder</td>
<td>An individual who is issued a particular credential.</td>
</tr>
<tr>
<td>chassis type</td>
<td>The designation that defines the physical lock type. Three types exist: cylindrical, mortise, or exit hardware. See those terms for more information.</td>
</tr>
<tr>
<td>common door</td>
<td>A configuration setting that allows for the allocation of duplicate badge ID ranges in separate offline locks.</td>
</tr>
<tr>
<td>communication port</td>
<td>The connector on the bottom of the B.A.S.I.S. Lock that allows the lock to be connected to a PDA running B.A.S.I.S. Transport.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>communication server</td>
<td>The server application designed to provide network services to access panels, readers, PCs and PDAs.</td>
</tr>
<tr>
<td>credential</td>
<td>A physical token, usually a card or fob, encoded with access control information.</td>
</tr>
<tr>
<td>cylindrical</td>
<td>Lock chassis that installs into a circular bore in the door.</td>
</tr>
<tr>
<td>deadbolt override</td>
<td>The ability for an authorized credential to retract both the spring latch and the deadbolt when the deadbolt is engaged.</td>
</tr>
<tr>
<td>diagnostics code</td>
<td>The code in B.A.S.I.S. Transport that identifies the processing error.</td>
</tr>
<tr>
<td>dongle</td>
<td>See hardware key.</td>
</tr>
<tr>
<td>encoder</td>
<td>The device, connected to a PC running B.A.S.I.S., used to encode magnetic stripe cards or smart cards.</td>
</tr>
<tr>
<td>exit hardware</td>
<td>Lock chassis type that supports the B.A.S.I.S. exit hardware trim lock.</td>
</tr>
<tr>
<td>extended unlock</td>
<td>The extra period of time the lock will unlock when an authorized credential with extended unlock privileges is presented.</td>
</tr>
<tr>
<td>facility code</td>
<td>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 organization.</td>
</tr>
<tr>
<td>guest access control</td>
<td>A feature that enables you to add and delete cardholders to and from a lock without having to go out to a lock to reprogram it.</td>
</tr>
<tr>
<td>hardware key</td>
<td>Security mechanism that connects directly to the computer that has the license file installed, usually the server. The hardware key connects via a parallel port or USB.</td>
</tr>
<tr>
<td>holiday</td>
<td>A special period of time, where the timezone is to behave differently. An exception to the normal workings of a timezone.</td>
</tr>
<tr>
<td>issue code</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Appendix A: Glossary of Terms

<table>
<thead>
<tr>
<th>Notes</th>
<th>look ahead</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>mortise</td>
</tr>
<tr>
<td></td>
<td>A lock chassis that installs into a mortised cavity in the edge of a door.</td>
</tr>
<tr>
<td></td>
<td>passage mode</td>
</tr>
<tr>
<td></td>
<td>The ability to double present an authorized credential within the unlock duration to unlock an opening. The lock is returned to its original status by a second, double presentation of an authorized credential.</td>
</tr>
<tr>
<td></td>
<td>PDA</td>
</tr>
<tr>
<td></td>
<td>Personal Digital Assistant.</td>
</tr>
<tr>
<td></td>
<td>programming cable</td>
</tr>
<tr>
<td></td>
<td>The cable used to connect the PDA to the B.A.S.I.S. Lock.</td>
</tr>
<tr>
<td></td>
<td>reader</td>
</tr>
<tr>
<td></td>
<td>Readers equate to locks in the B.A.S.I.S. software to conform and maintain consistency with the B.A.S.I.S. online terminology conventions.</td>
</tr>
<tr>
<td></td>
<td>standard access control</td>
</tr>
<tr>
<td></td>
<td>Solves the equation of who can go where when. (When + Where + Who = Access)</td>
</tr>
<tr>
<td></td>
<td>System Tree</td>
</tr>
<tr>
<td></td>
<td>The screen that displays all hardware devices allowing you to directly control them.</td>
</tr>
<tr>
<td></td>
<td>timezone</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>two card control</td>
</tr>
<tr>
<td></td>
<td>The requirement for the presentation of two separate, authorized credentials in order to gain entry through an access controlled opening.</td>
</tr>
<tr>
<td></td>
<td>unlock duration</td>
</tr>
<tr>
<td></td>
<td>The time that the lock momentarily unlocks.</td>
</tr>
<tr>
<td></td>
<td>use count</td>
</tr>
<tr>
<td></td>
<td>Number of times access was granted since the use count was last reset.</td>
</tr>
<tr>
<td></td>
<td>use limit</td>
</tr>
<tr>
<td></td>
<td>A configuration limiting a credential to a defined number of uses.</td>
</tr>
</tbody>
</table>
Appendix A: Glossary of Terms