BEST

dormakaba Group

BEST OFFLINE LOCKS

User Guide

Credits / Copyright

Information in this document is subject to change without notice and does not represent a commitment on the part of dormakaba USA Inc. The software described in this document are furnished under a license agreement or nondisclosure agreement.

This publication is intended to be an accurate description and set of instructions pertaining to its subject matter. However, as with any publication of this complexity, errors or omissions are possible. Please call dormakaba USA Inc. at 1-800-392-5209 if you see any errors or have any questions. No part of this manual and/or databases may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose, without the express written permission of dormakaba USA Inc.

This document is distributed as is, without warranty of any kind, either express or implied, respecting the contents of this book, including but not limited to implied warranties for the publication's quality, performance, merchantability, or fitness for any particular purpose. Neither dormakaba USA Inc., nor its dealers or distributors shall be liable to the user or any other person or entity with respect to any liability, loss, or damage caused or alleged to be caused directly or indirectly by this publication.

Written and designed by:
dormakaba USA Inc.
6161 East 75th Street
Indianapolis, IN 46250

T80946_Rev E February 2022

Contents

1 Overview

This manual is your guide to the Offline Locks System.

The information in this guide is presented in a linear manner; however, tasks to install hardware and software and configure the system for the first time do not necessarily progress in a linear manner. You will find a Setup Checklist at the end of this section to take you through the initial setup and configuration tasks in a logical sequence.

Online and Offline Diagram

The Offline Locks system is capable of being configured as both an online and an offline access control system. This means that with Offline Locks, you can manage any access control hardware, whether they are wired directly to a panel or not.

This diagram describes a typical combined online and offline system.

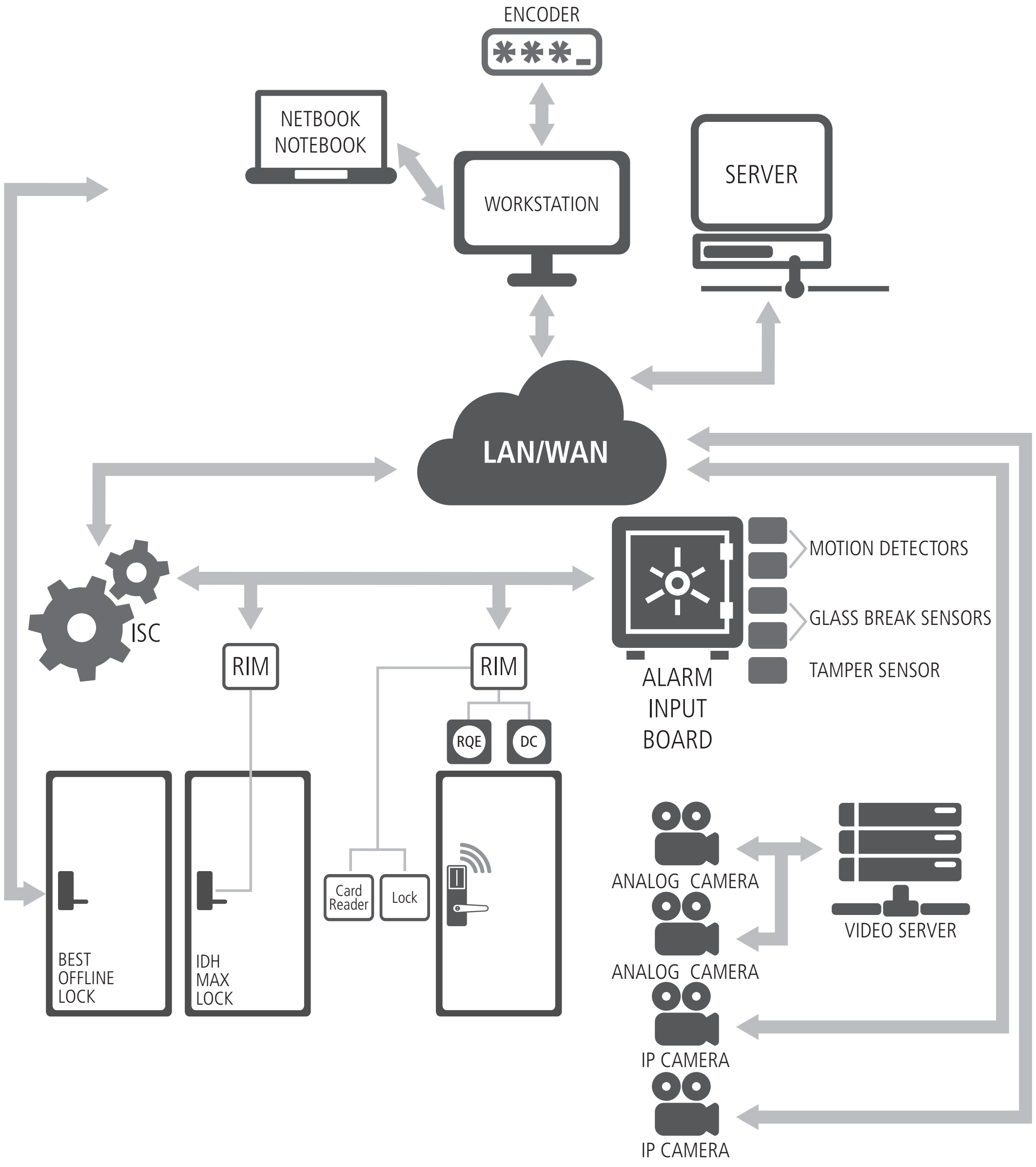


Figure 1 Online and offline diagram overview

How Offline Locks Readers Work

Offline G

Offline G locks are designed primarily for the college/university dormitories. However, they 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 functionality 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

Offline G allows a range of per-programmed badge numbers access into a locked unit that secures a dormitory room. These badge numbers are available for issue and reuse as students are assigned to their dormitory accommodations. The badge number is automatically issued to a student 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 student for use in his or her assigned room.

New students may be assigned access to a particular room by using badge IDs from the same range without ever needing to reprogram 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 Offline G locks use to achieve the guest functionality.

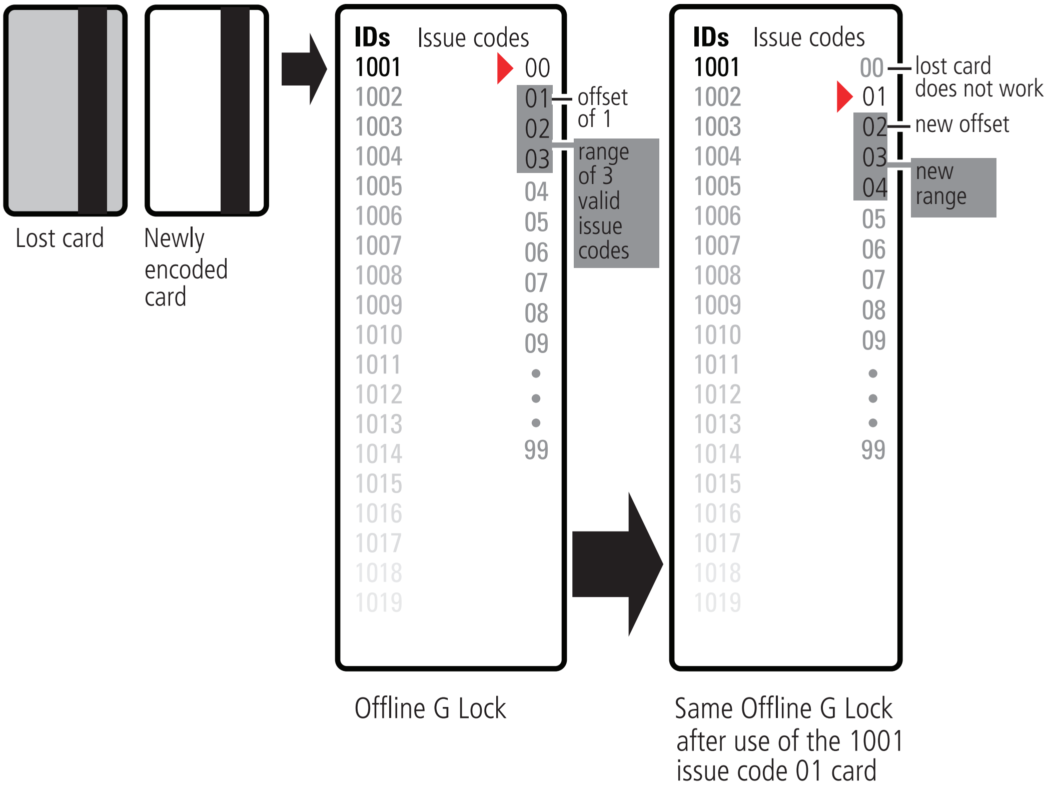


Figure 2 Guest functionality diagrammed

The diagram uses the following issue code look ahead values:

Look ahead function	Value
Offset	1
Range	3
Number of issue code digits	2

The next diagram shows what happens when the issue code has reached its limit. The issue code look ahead values remain the same.

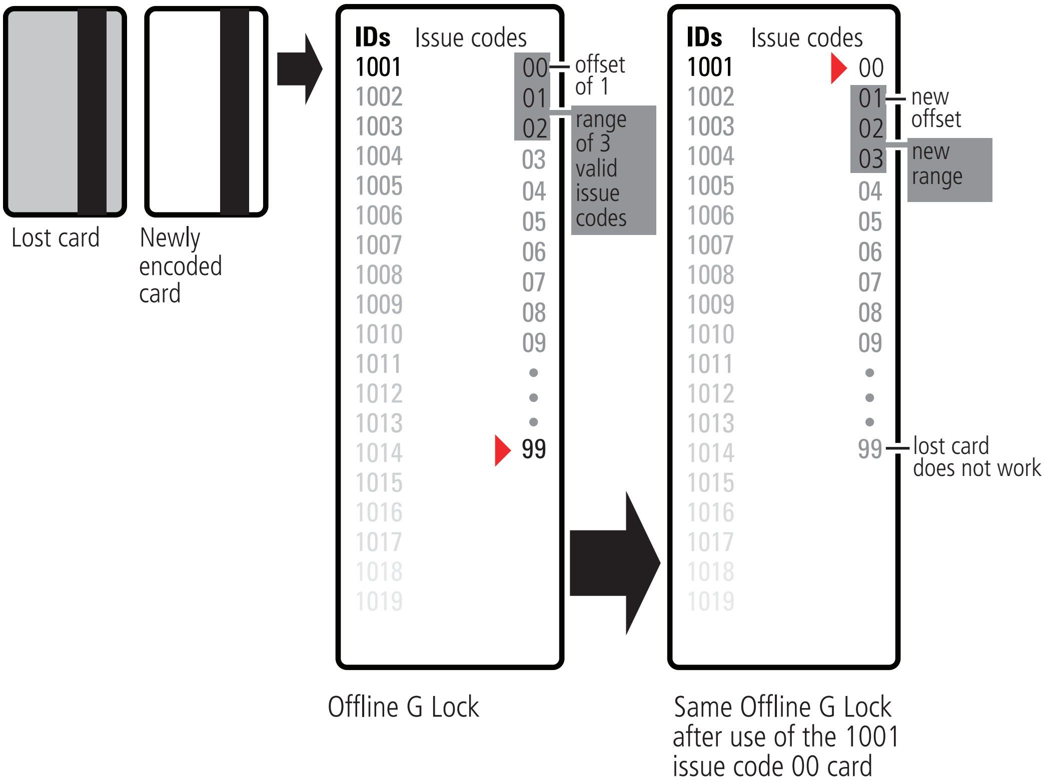


Figure 3 Guest functionality diagrammed

Offline V

Offline V locks are designed to include all functions of Offline G (including Guest Functionality as described in previous section), plus upgraded features. On the following page, the ‘Feature Comparisons of Offline G and V' table compares the systems.

Feature Comparisons of Offline G and V

Feature	Description	G	V
Guest (dormitory feature)	Provides the ability to issue pre-created badge IDs to students. This supports the assignment of one reader directly to the badge. Other readers may be assigned to the badge through normal access level assignment.	■	■
Look ahead	Issue code look ahead feature through offset and range fields.	■	■
Encoding	Provides the ability to encode both magstripe.	■	■
Passage mode	Allows the cardholder to place the reader into an unlocked mode. This status is cleared only by another passage mode attempt or reader mode change occurrence.	■	■
Deadbolt override	Allows the cardholder to retract the deadbolt	■	■
Key override event	An event logged into history whenever the key override feature is used in a mortise lock. Not supported in Cylindrical.	■	■
Use activation date	Determines if the lockset will use the activation date field stored in the cardholder record when validating. This option has no impact on Dormitory functionality.		■
Use deactivation date	Determines if the lockset will use the deactivation date field stored in the cardholder record when validating. This option has no impact on Dormitory functionality.		■
Two card control	Requires that two valid users must present their cards in order to unlock the door.		■
Enforce use limit	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.		■
Denied attempts	Includes attempts count and time out duration. Sometimes referred to as 'Three strikes you're out'.		■
Logging (grant denies, status)	Provides the ability to filter the displaying/logging of history events. This feature is implemented at the Management System level.	■	■
Daylight savings time	Support for all OS world time zones.	■	■
128K RAM	5000 Users/History	■	■
Card formats (8)	Support for up to eight card data formats per reader. Facility codes are assigned through card formats.	■	■
Magnetic	5 bit ABA data only.	track 3	track 1&2
Wiegand	Any valid Wiegand format.		■
Online mode	Automatic (time zone control of reader mode), Facility Code, Card Only, Unlocked, Locked, Card and Pin, and Card or Pin.	■	■
Reader mode (automatic unlock/ relock)	This feature provides the ability to change (automatic operational modes at specified periods through unlock/relock) time zone control. The current modes would be Facility Code, Card Only, Unlocked, Locked, Card and Pin, Card or Pin, and First Card Unlock.	2	32
Unlock duration	The amount of time that the lock set will remain unlocked for a valid access grant.	■	■
Extended unlock	This feature provides the ability to extend the unlock duration for certain cardholders.	■	■
Chassis type	Cylindrical & Mortise with support for a user defined type 'Custom'.	■	■
Automatic Chassis Volume	Chassis volume automatically corresponds to the chassis type chosen.		
Holidays	Special days of the year can be categorized as one of the eight types.	8	32
Time Zones	Time Zones are necessary for the use of Access Levels. A time zone can be comprised of up to six intervals.	4	32
Access levels	Access Level assignment to readers.	■	■
Battery warning/alarm	Reported through the activation of LED's and the lock internal sounder.	■	■

Panel password	Communication password is configured at the Access Panel level.	■	■
Diagnostics (Netbook/Notebook)	The Netbook/Notebook will support the capability of performing diagnostics on the lock set.	■	■
Cycle count/reset	The lock set will maintain a current count of access grants. The count can be reset by the user.	■	■
Diagnostics code	This code provides some feedback of the lock set's status.	■	■
Backup battery level	Displays the current level of the backup battery.	■	■
Electronics level	Displays the current level of the main battery.	■	■
Unlock once	This feature allows for the unlocking of the door for the unlock duration.	■	■
Reader mode	This feature allows for the setting of the current operating mode directly to the reader through the Netbook/Notebook. This action would override the online mode set at the management system level. All online reader modes are supported.	■	■
Reader support	Dual Validation	■	■
	Magstripe	track 3	track 1&2
	HID Proximity		■
	Motorola Proximity		■
Batch Update	This feature allows for the bulk updating of Activation/Deactivation Dates.	■	■

Setup Checklist

In the next chapter you will find complete step-by-step instructions for the first-time installation and configuration of an Offline Locks system. Listed below are the major steps of that process.

- Task 1: Install Offline Locks Software
  See page 15.
- Task 2: Install Encoder
  See page 15.
- Task 3: Define Card Formats
  See page 19.
- Task 4: Define Badge Types
  See page 22.
- Task 5: Define Offline Access Panels
  See page 25.
- Task 6: Define Guest Locks/Readers
  See page 27.
- Task 7: Install Offline Locks Transport
  See page 38.
- Task 8: Install Offline Locks Transport on Netbook/
  Notebook See page 48.

2
Installation and Configuration

This chapter will guide you through performing the following tasks: Task

1 — Install Offline Locks Software

Task 2 — Install Encoder

Task 3 — Define Card Formats

Task 4 — Define Badge Types

Task 5 — Define Offline Access Panels

Task 6 — Define Guest Locks/Readers

Task 7 — Install Offline Locks Transport

Task 8 — Install Offline Locks Transport on Netbook/Notebook

Needed Components

The following describes the hardware and software that it takes to create an Offline Locks system.

Components include:

- Offline ET691 software, or higher
- Dedicated computer or ‘workstation’ (consult your dormakaba representative for complete details)
- Offline G or V lock(s), includes cylindrical, mortise or exit hardware trim models
- Netbook/Notebook. See **https://dhwsupport.dormakaba.com/hc/en-us** for supported models
- Encoder
    - Magnetic Stripe encoder: Unitech Model MSR206
- Cables
    - Netbook or Notebook to lock (requires USB to Serial programming cable, Null Modem Serial Cable-female to female, and programing cable). See “Figure 94 Connecting the Netbook/Notebook to a lock”

Task 1: Install Offline Locks Software

For complete Offline Locks software installation and configuration, see the Offline Locks Installation and Setup User Guide. Contact your dormakaba representative for a copy or visit **https://dhwsupport.dormakaba.com/hc/en-us**.

Task 2: Install Encoder

One types of encoder is available for the Offline Locks system:

- Magnetic Stripe encoder: Unitech Model MSR206

The card encoder or some type of encoding device (that is, an encoder or a printer with a built-in encoder) is intended for Offline G locks. So the following instructions are required for Offline G functionality, but optional for Offline V. For a comparison of Offline G and V, see “Feature Comparisons of Offline G and V” on page 10. The following instructions are for a stand-alone encoder.

Perform the following steps to set up the encoder:

1 Click Start > Programs > BEST ET > 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.

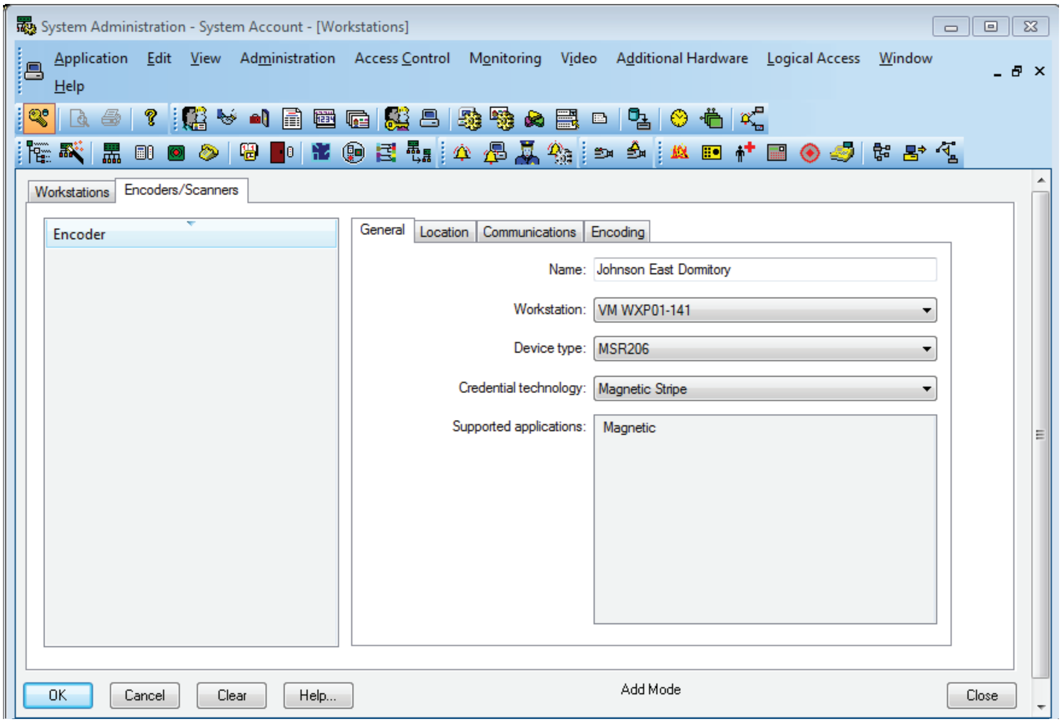
7 Click OK.

8 Click the Encoders/Scanners tab.

9 Select the General tab and name your encoder under the encoder settings.

10 Make sure that your workstation is selected under the Workstation setting.

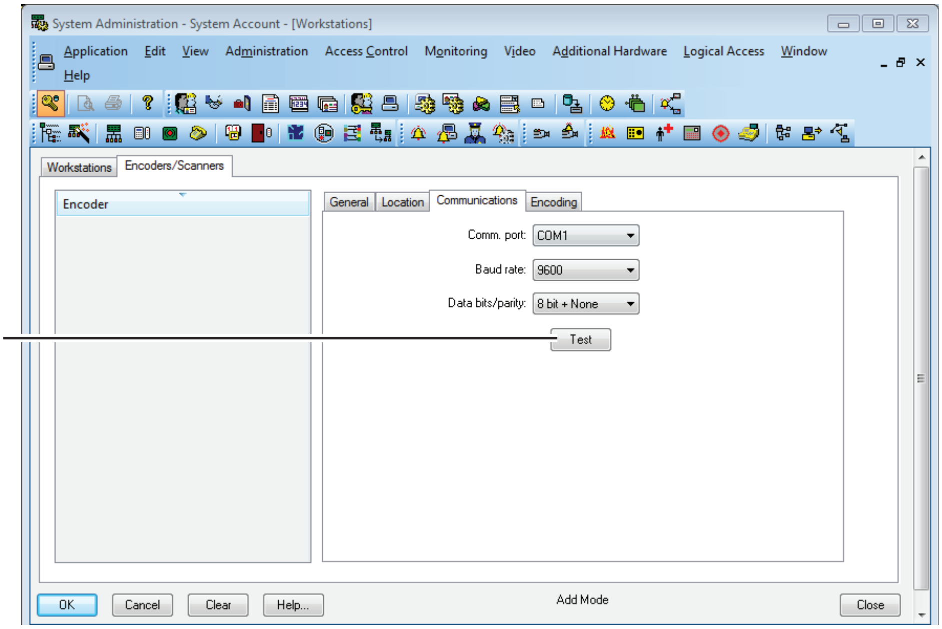
11 Under Device type, select your device. Credential technology should automatically select Magnetic.



Name: Johnson East Dormitory
Workstation: VM WXP01-141
Device type: MSR206
Credential technology: Magnetic Stripe
Supported applications: Magnetic

Figure 4 Device type

12 Confirm that the encoder is physically connected to a COM port on the computer, by selecting the Communication tab.



Comm. port: COM1

Baud rate: 9600

Data bits/parity: 8 bit + None

Click to test whether the encoder is online

Figure 5 Configuring 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. The corecitivity setting must be selected as "High" on the Encoding tab.

14 Click OK.

Defining the system

To define an Offline system, you need to configure:

- Card Formats
- Badge Types
- Guest Readers
- Offline Access Panels
- Timezones
- Access Levels
- Adding a cardholder

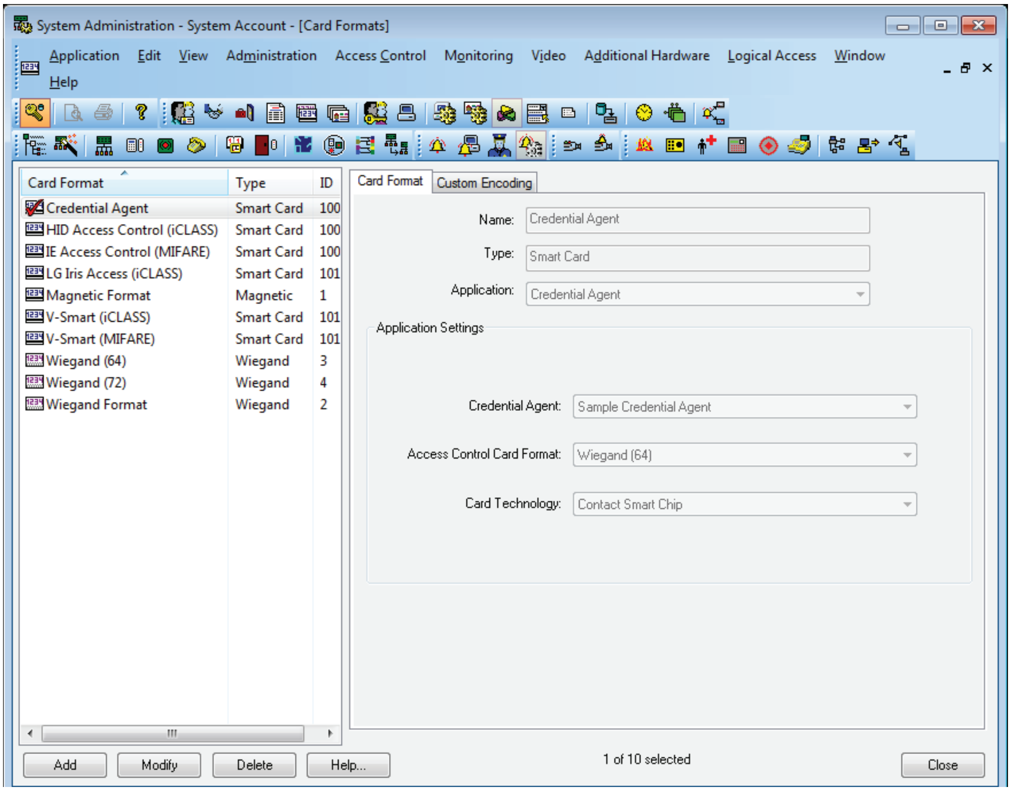
Although Offline locks are offline (stand-alone) and are not managed by access control panels, you must define Access Panel settings for the locks. In effect, you define access control panels for the locks. More than one lock – called a *reader* in Offline Locks — can share the same panel configuration. However, these locks (readers) must all:

- be managed by the same Server or Workstation
- share the same password
- be located in the same time zone
- use the same daylight savings time setting.

Task 3: Define Card Formats

Defining a card format is the starting point to configure guest access control. 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. Perform the following steps:

1 From System Administration, click Administration > Card Formats.



Card Format	Type	ID
Credential Agent	Smart Card	100
HID Access Control (iCLASS)	Smart Card	100
IE Access Control (MIFARE)	Smart Card	100
LG Iris Access (iCLASS)	Smart Card	101
Magnetic Format	Magnetic	1
V-Smart (iCLASS)	Smart Card	101
V-Smart (MIFARE)	Smart Card	101
Wiegand (64)	Wiegand	3
Wiegand (72)	Wiegand	4
Wiegand Format	Wiegand	2

Name: Credential Agent

Type: Smart Card

Application: Credential Agent

Application Settings

Credential Agent: Sample Credential Agent

Access Control Card Format: Wiegand (64)

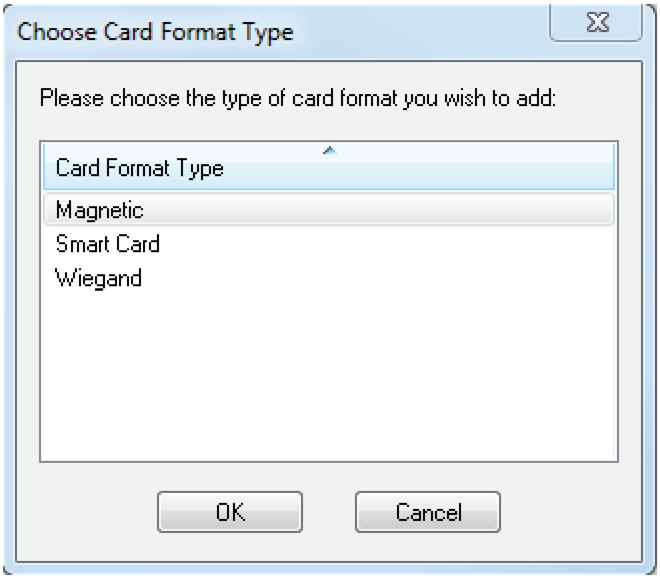
Card Technology: Contact Smart Chip

1 of 10 selected

Figure 6 Card format

2 Click Add.

The Card Format form displays:

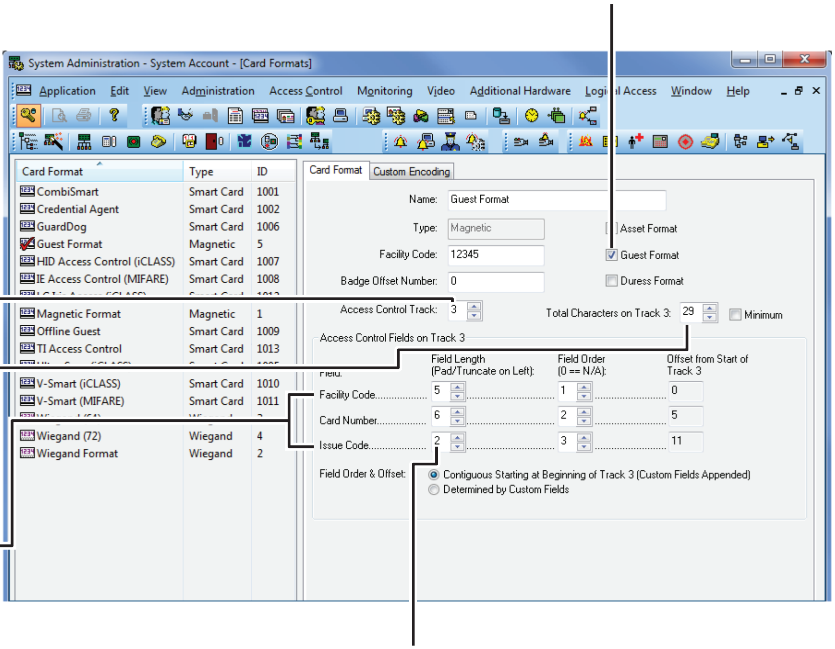


Please choose the type of card format you wish to add:

Card Format Type
Magnetic
Smart Card
Wiegand

Figure 7 Choose card format type

3 Choose the appropriate card format and click OK.



Card Format	Type	ID
CombiSmart	Smart Card	1001
Credential Agent	Smart Card	1002
GuardDog	Smart Card	1006
Guest Format	Magnetic	5
HID Access Control (iCLASS)	Smart Card	1007
IE Access Control (MIFARE)	Smart Card	1008
Magnetic Format	Magnetic	1
Offline Guest	Smart Card	1009
TI Access Control	Smart Card	1013
V-Smart (iCLASS)	Smart Card	1010
V-Smart (MIFARE)	Smart Card	1011
Wiegand (72)	Wiegand	4
Wiegand Format	Wiegand	2

Name: Guest Format

Type: Magnetic

Facility Code: 12345

Badge Offset Number: 0

Access Control Track: 3

□ Asset Format

☑ Guest Format

□ Duress Format

Total Characters on Track 3: 29 □ Minimum

Access Control Fields on Track 3

Field:	Field Length (Pad/Truncate on Left):	Field Order (0 == N/A):	Offset from Start of Track 3
Facility Code	5	1	0
Card Number	6	2	5
Issue Code	2	3	11

Field Order & Offset:
● Contiguous Starting at Beginning of Track 3 (Custom Fields Appended)
○ Determined by Custom Fields

When the guest format check box is selected, the data is offset from the start of the card by the fact that the activation and deactivation dates are encoded onto the card.

Set access control track to 3.

Make sure to adjust the total characters on the track to the correct access control data length.

Field Length and Field Order for Facility Code, Card Number, and Issue Code is required. A 2 digit code should be used.

A two-digit issue code is preferred for Offline G.

Figure 8 Defining card formats

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

5 Complete all appropriate fields including field length and field order for facility code, card number, and issue code.

Task 4: Define Badge Types

To use Offline G lock basic functionality, 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.

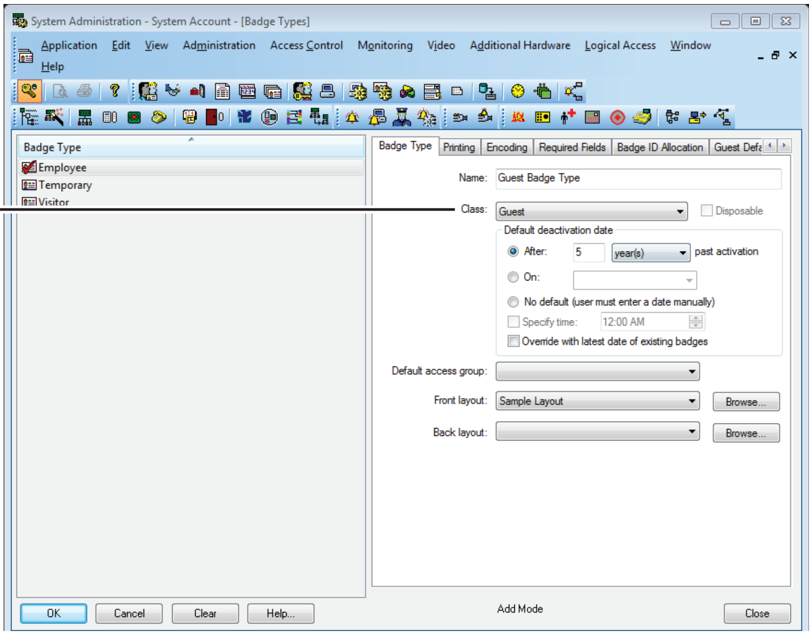
Note A badge type could be used to allocate a pool of badge numbers for a dormitory from which smaller blocks of numbers could be obtained for the individual dormitory units.

Perform the following steps:

1 From System Administration, click Administration > Badge Types.

2 Click Add.

The modify badge type window displays.



Name: Guest Badge Type

Class: Guest ☐ Disposable

Default deactivation date

● After: 5 year(s) past activation

○ On:

○ No default (user must enter a date manually)

☐ Specify time: 12:00 AM

☐ Override with latest date of existing badges

Default access group:

Front layout: Sample Layout

Back layout:

Choosing the Guest classification enables the features of the Badge ID Allocation tab

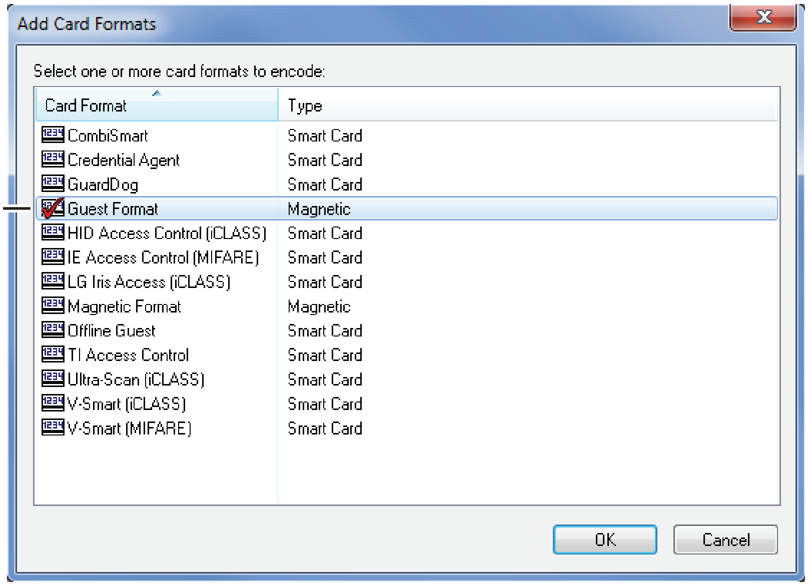
Figure 9 Selecting the Guest class for Offline G badge type

3 Select the Guest class from the drop down box.

4 Complete all other necessary information on the tab.

5 Click the Encoding tab > Click Add

6 Select the appropriate card format to be encoded for the badge type by clicking the icon to the left of the “Guest Format”. A red arrow will appear over the card illustration > Click OK



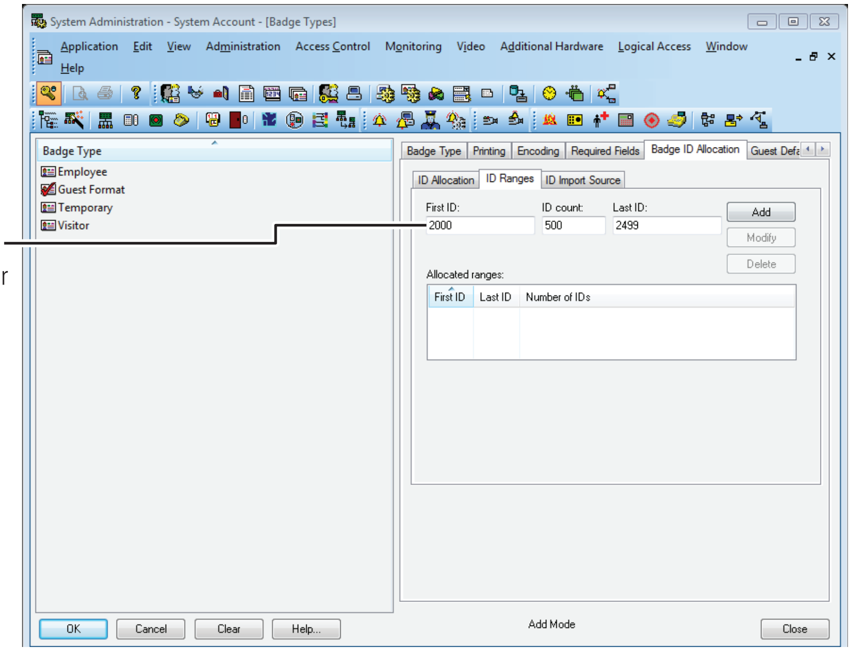
Select one or more card formats to encode:

Card Format	Type
CombiSmart	Smart Card
Credential Agent	Smart Card
GuardDog	Smart Card
✓ Guest Format	Magnetic
HID Access Control (iCLASS)	Smart Card
IE Access Control (MIFARE)	Smart Card
LG Iris Access (iCLASS)	Smart Card
Magnetic Format	Magnetic
Offline Guest	Smart Card
TI Access Control	Smart Card
Ultra-Scan (iCLASS)	Smart Card
V-Smart (iCLASS)	Smart Card
V-Smart (MIFARE)	Smart Card

Make sure that the Guest format is selected for encoding Guest Badge Types.

Figure 10 Add card formats

7 Click the Badge ID Allocation tab and then click the ID Ranges tab.



Badge Type
- Employee
- Guest Format
- Temporary
- Visitor

First ID: 2000

ID count: 500

Last ID: 2499

Allocated ranges:

First ID	Last ID	Number of IDs

Add Mode

Enter the appropriate range of badge IDs for your application.

Figure 11 Entering the range of Badge IDs

8 Enter the First ID number in the badge range that you want to create

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.

9 In the ID Count field, enter the number of Badge IDs that you want to create.

10 Click Add.

11 Click OK.

Task 5: Define Offline Access Panels

Although Offline Locks are offline (stand-alone) locks and are not managed by access control panels, you must define Virtual Access Panel settings for the locks. Using the access panel concept allows the programming of guest locks to follow the same conventions as Offline Locks online products. Up to 64 locks (called readers) can share the same panel configuration. However, these readers must all:

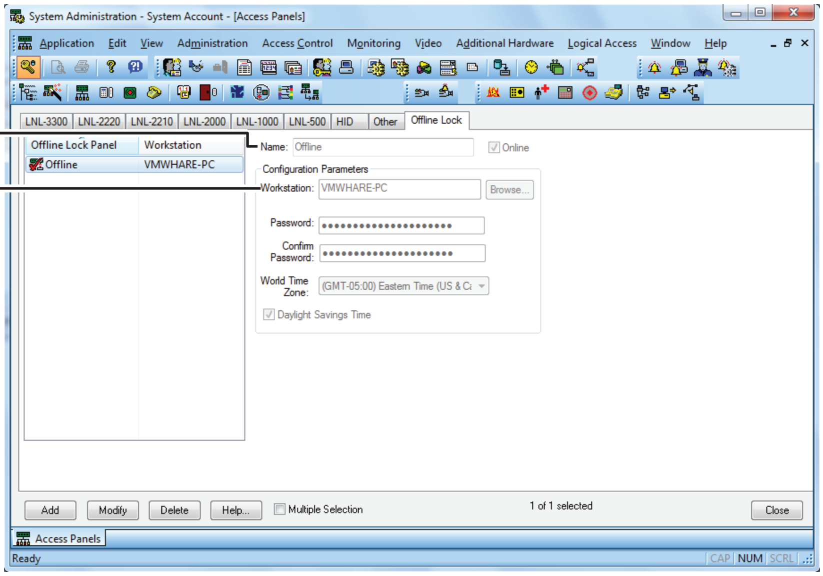
- be managed by the same Server or Workstation
- share the same password
- be located in the same time zone
- use the same daylight saving time setting.

Note The default password is 'BEST.' Care should be given to faithfully document any changes to this password since the password cannot be viewed from anywhere in the application software.

Perform the following steps:

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.



Name the offline lock access panel appropriately for all of the possible 64 locks that it controls.

The workstation name refers to the technical name of the computer to which the Netbook is attached

System Administration - System Account - [Access Panels]
Application Edit View Administration Access Control Monitoring Video Additional Hardware Logical Access Window Help
LNL-3300 LNL-2220 LNL-2210 LNL-2000 LNL-1000 LNL-500 HID Other Offline Lock
Add Modify Delete Help... Close
Access Panels
Ready
CAP NUM SCRL

Offline Lock Panel	Workstation
Offline	VMWHARE-PC

Name: Offline ☑ Online

Configuration Parameters

Workstation: VMWHARE-PC Browse...

Password: ••••••••••••••••••••

Confirm Password: ••••••••••••••••••••

World Time Zone: (GMT-05:00) Eastern Time (US & Ca

☑ Daylight Savings Time

□ Multiple Selection

1 of 1 selected

Figure 12 Naming the offline lock access panel.

4 In the Name field, type the name of the access control panel.

5 Click OK.

6 Repeat steps 3 and 4 as necessary.

Task 6: Define the Guest Locks/Readers

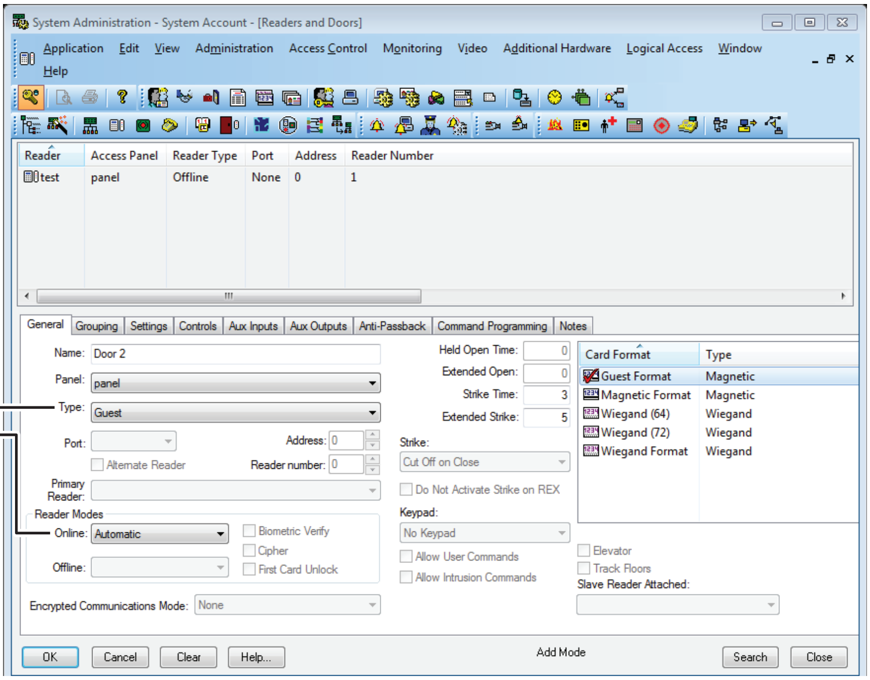
In the Offline Locks software, locks are referred to as readers to conform and maintain consistency with online terminology conventions.

You can define up to 64 readers for each 'virtual' offline access control panel. And each reader will accept up to eight different card formats. It would be highly unusual to use this many formats in one lock. Perform the following steps:

1 From System Administration, click Access Control > Readers and Doors.

2 Click Add.

The Add Reader window displays.



Reader	Access Panel	Reader Type	Port	Address	Reader Number
test	panel	Offline	None	0	1

Name: Door 2

Panel: panel

Type: Guest

Port:

Address: 0

□ Alternate Reader

Reader number: 0

Primary Reader:

Online: Automatic

Offline:

□ Biometric Verify

□ Cipher

□ First Card Unlock

Encrypted Communications Mode: None

Held Open Time: 0

Extended Open: 0

Strike Time: 3

Extended Strike: 5

Strike: Cut Off on Close

□ Do Not Activate Strike on REX

Keypad: No Keypad

□ Allow User Commands

□ Allow Intrusion Commands

Card Format	Type
Guest Format	Magnetic
Magnetic Format	Magnetic
Wiegand (64)	Wiegand
Wiegand (72)	Wiegand
Wiegand Format	Wiegand

□ Elevator

□ Track Floors

Slave Reader Attached:

Selecting the Guest reader type enables the assignment of a subset of badge numbers from the larger range of numbers configured for a Badge Type.

The automatic setting for 'online reader mode' allows the lock to use time zone control and token control when programmed for both.

Figure 13 Defining offline guest readers

3 In the Name field, type the name of the reader.

4 In the Panel field, select the virtual offline access control panel that controls the reader.

5 In the Type field, select Guest.

6 Select the appropriate reader mode.

7 Under the Card Format section, select the Guest Card Format.

Note Selecting the ‘Offline Guest’ reader type refers to an Offline G configuration.

8 Make any other selections as necessary.

9 Click OK.

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

10 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 only 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.

Define Other Guest Reader Features

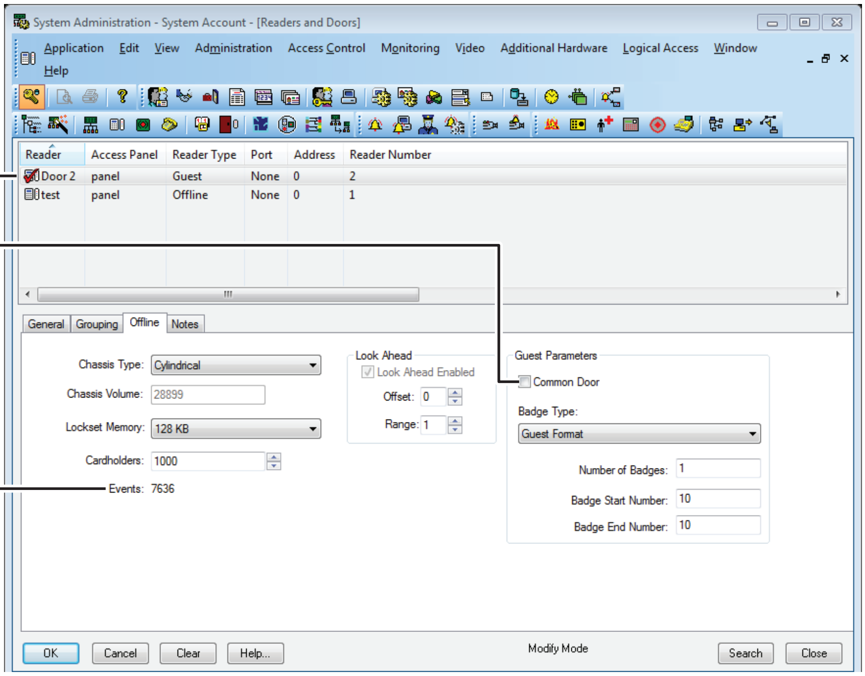
1 From System Administration, click Access Control > Readers and Doors.

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

3 Click the Offline tab.

4 Click Modify.

The Modify Offline Reader window displays.



Reader	Access Panel	Reader Type	Port	Address	Reader Number
Door 2	panel	Guest	None	0	2
test	panel	Offline	None	0	1

Chassis Type: Cylindrical

Chassis Volume: 28899

Lockset Memory: 128 KB

Cardholders: 1000

Events: 7636

Look Ahead

☑ Look Ahead Enabled

Offset: 0

Range: 1

Guest Parameters

☐ Common Door

Badge Type: Guest Format

Number of Badges: 1

Badge Start Number: 10

Badge End Number: 10

Make sure that the correct reader is selected when selecting offline features.

The common door feature allows duplication of a badge range between locks.

The number of events is automatically calculated based on the amount of lock memory and the number of cardholders allocated.

Figure 14 Defining the offline reader

5 In the Chassis Type field, select the chassis type that the lock/reader has.

Note 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 Offline G locks, the offset is set to 1 and the range to 3.

8 The Guest Parameters section, select whether the 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 21.

10 In the Number of badges field, enter the number of guest badges to be allocated to this 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 reader. The badge end number is automatically calculated from the numbers entered.

12 Click OK.

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

Define Timezones

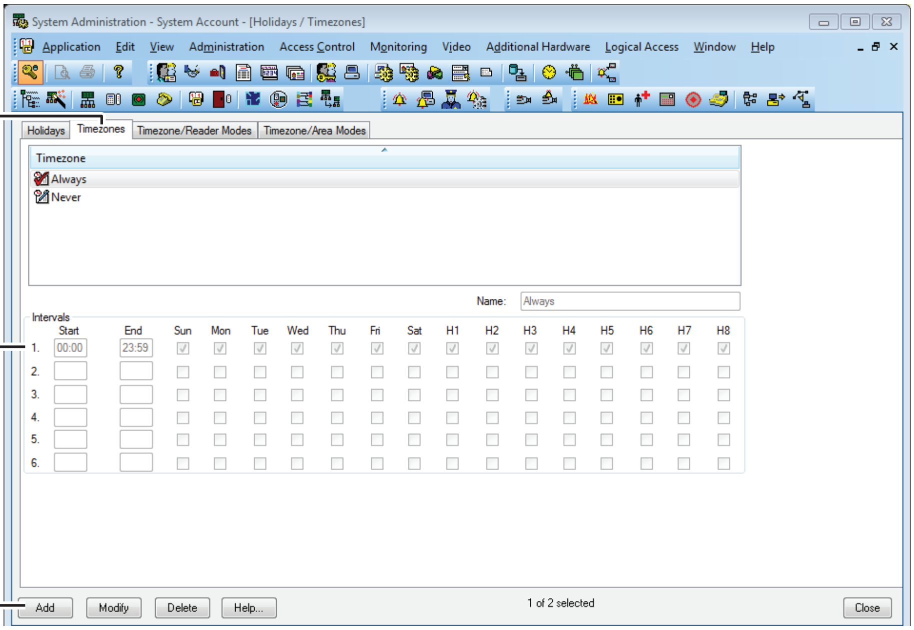
A timezone is a block of time that a particular activity or function is allowed to occur. These blocks of time are represented by intervals.

Offline Locks Access Control system can be configured for up to 255 timezones limited by the feature set of each product.

Add a timezone

1 From System Administration, click Access Control > Timezones

The Timezones window displays



Name: Always

Intervals

	Start	End	Sun	Mon	Tue	Wed	Thu	Fri	Sat	H1	H2	H3	H4	H5	H6	H7	H8
1.	00:00	23:59	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
2.			□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
3.			□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
4.			□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
5.			□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
6.			□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

1 of 2 selected

Timezones tab

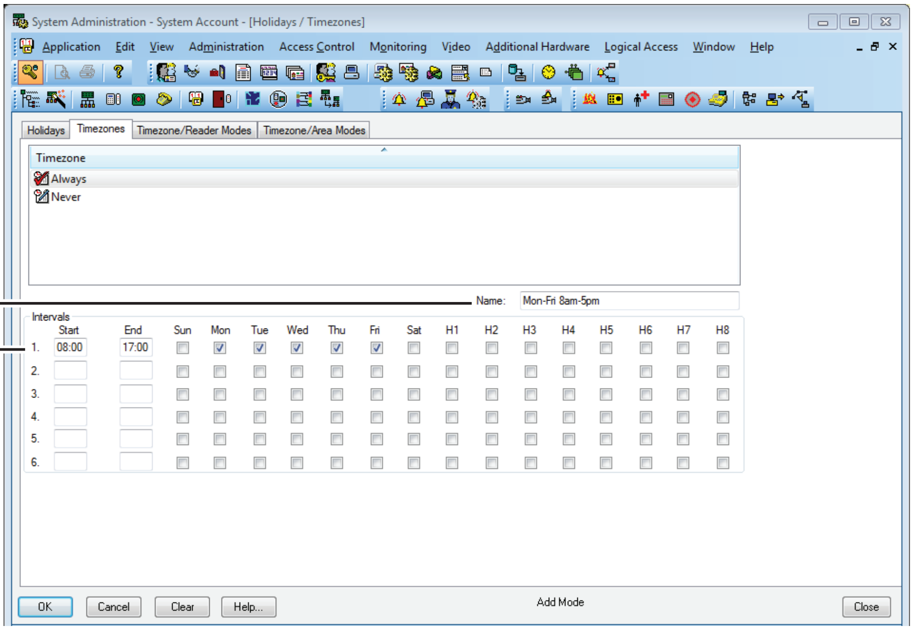
Default "Always" schedule

Click Add to create a new timezone

Figure 15 Timezone window displaying 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.



Name: Mon-Fri 8am-5pm

Intervals

	Start	End	Sun	Mon	Tue	Wed	Thu	Fri	Sat	H1	H2	H3	H4	H5	H6	H7	H8
1.	08:00	17:00	☐	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐
2.			☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
3.			☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
4.			☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
5.			☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6.			☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Enter the timezone name

Enter the time interval(s) start, end, and the days of the week when it is to be active

Figure 16 Adding a timezone

4 Choose a name for the timezone and enter the choice in the Name field.

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

6 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.

7 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-H8 represent holidays that allow for the exceptions to each interval. These holidays, or exception days, are configured on the Holiday tab.

Offline Locks 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 eight types. A holiday type can contain more than one configured exception period.

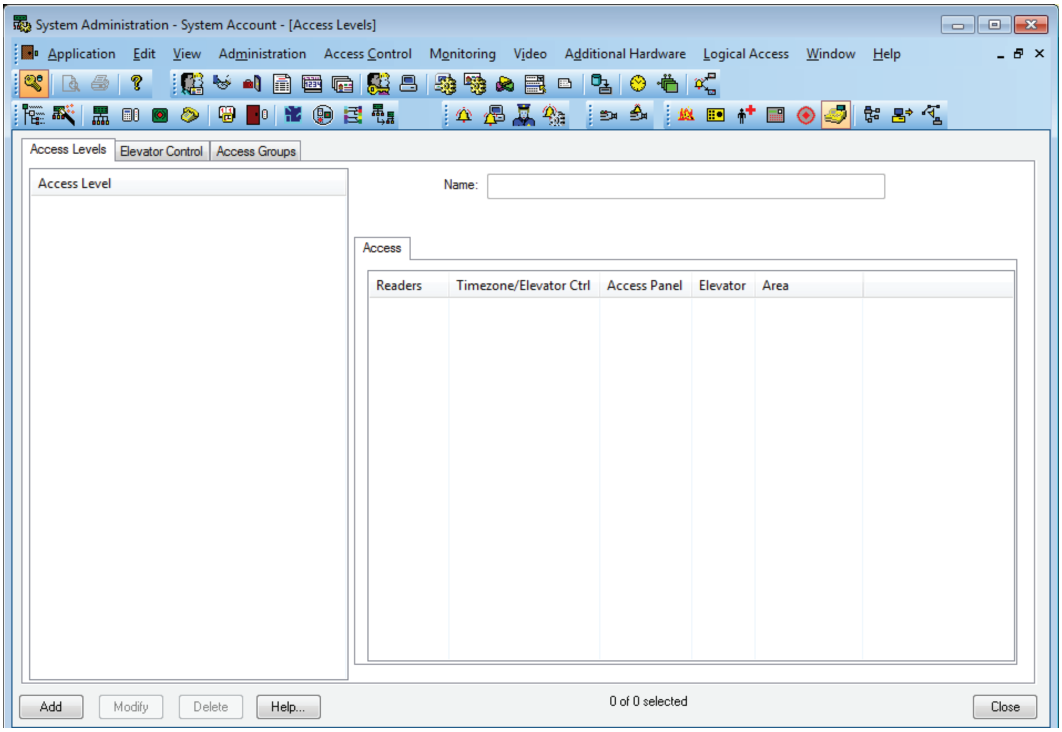
Access Levels

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.

Add access levels

1 From System Administration, click Access Control > Access Levels

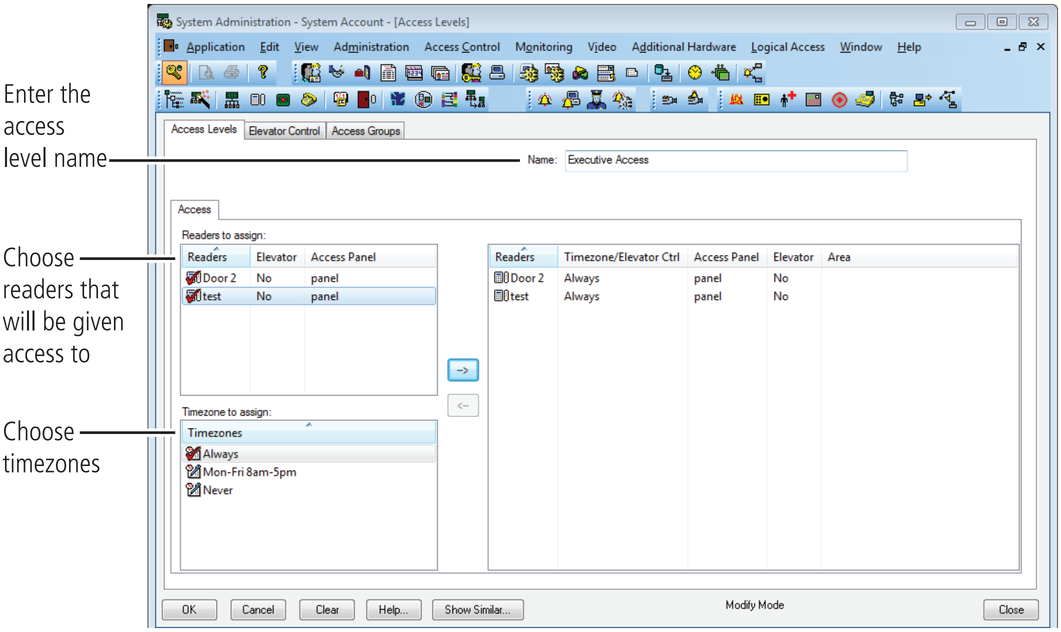
The Access levels window displays



System Administration - System Account - [Access Levels]
Application Edit View Administration Access Control Monitoring Video Additional Hardware Logical Access Window Help
Access Levels
Elevator Control
Access Groups
Access Level
Name:
Access
Readers
Timezone/Elevator Ctrl
Access Panel
Elevator
Area
Add
Modify
Delete
Help...
0 of 0 selected
Close

Figure 17 Access level

2 Click Add to create an access level.



Name: Executive Access

Readers to assign:

Readers	Elevator	Access Panel
Door 2	No	panel
test	No	panel

Timezone to assign:

Timezones
Always
Mon-Fri 8am-5pm
Never

Readers	Timezone/Elevator Ctrl	Access Panel	Elevator	Area
Door 2	Always	panel	No	
test	Always	panel	No	

Figure 18 Access level

3 Choose a name for the access level and enter the choice in the Name area.

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

5 Click on arrow button to the right to move the reader and timezone selections to the right side of the form.

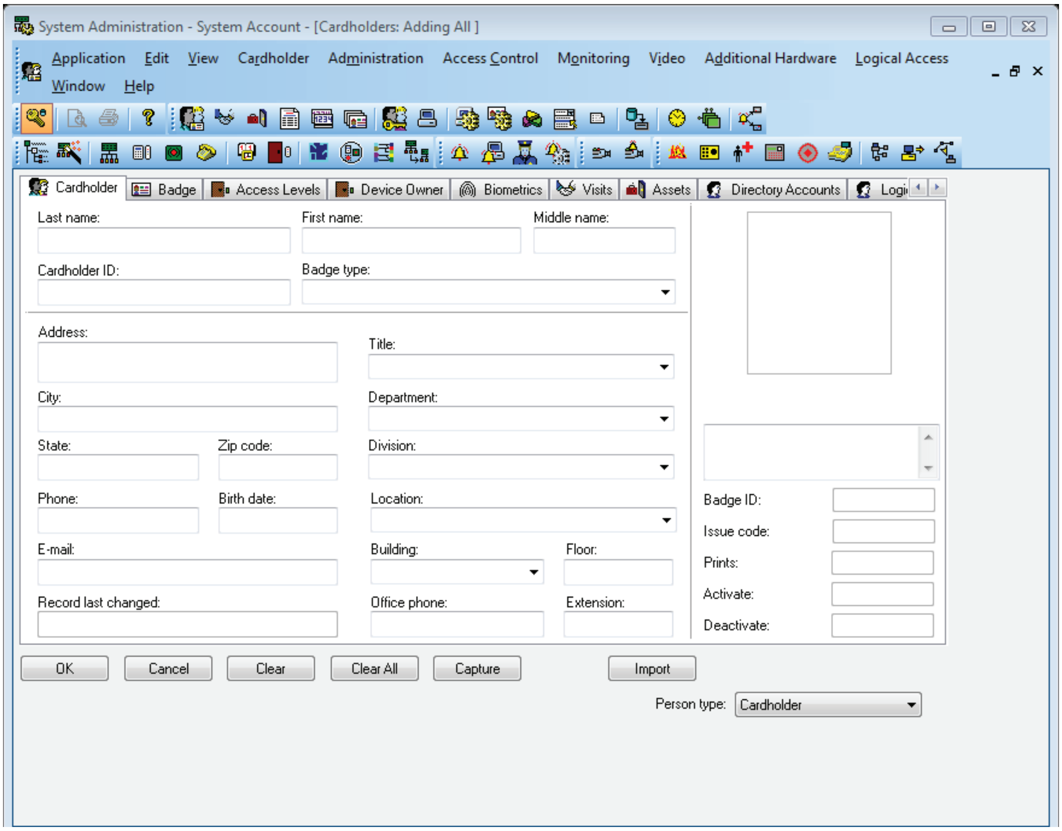
6 Click OK to save the record.

Adding a Cardholder for Standard Access Control

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.



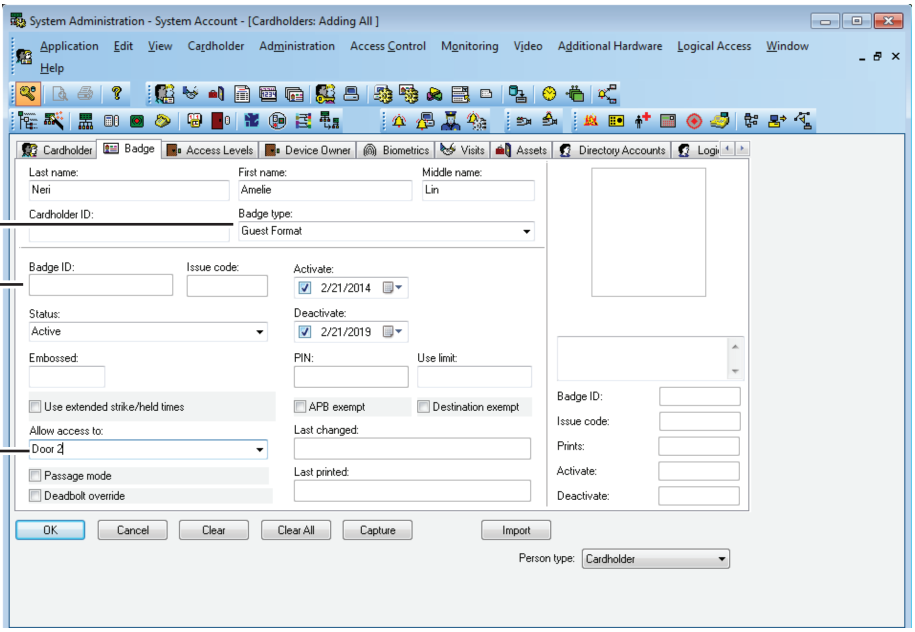
System Administration - System Account - [Cardholders: Adding All]

Person type: Cardholder

Figure 19 The cardholder general information screen

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

3 Click the Badge tab.


System Administration - System Account - [Cardholders: Adding All]
Application Edit View Cardholder Administration Access Control Monitoring Video Additional Hardware Logical Access Window Help
Cardholder Badge Access Levels Device Owner Biometrics Visits Assets Directory Accounts Logi
OK Cancel Clear Clear All Capture Import

Last name: Neri

First name: Amelie

Middle name: Lin

Cardholder ID:

Badge type: Guest Format

Badge ID:

Issue code:

Activate: ☑ 2/21/2014

Status: Active

Deactivate: ☑ 2/21/2019

Embossed:

PIN:

Use limit:

□ Use extended strike/held times

□ APB exempt

□ Destination exempt

Allow access to: Door 2

Last changed:

□ Passage mode

□ Deadbolt override

Last printed:

Badge ID:

Issue code:

Prints:

Activate:

Deactivate:

Person type: Cardholder

Choose badge type

Enter badge ID if the field will accept the data

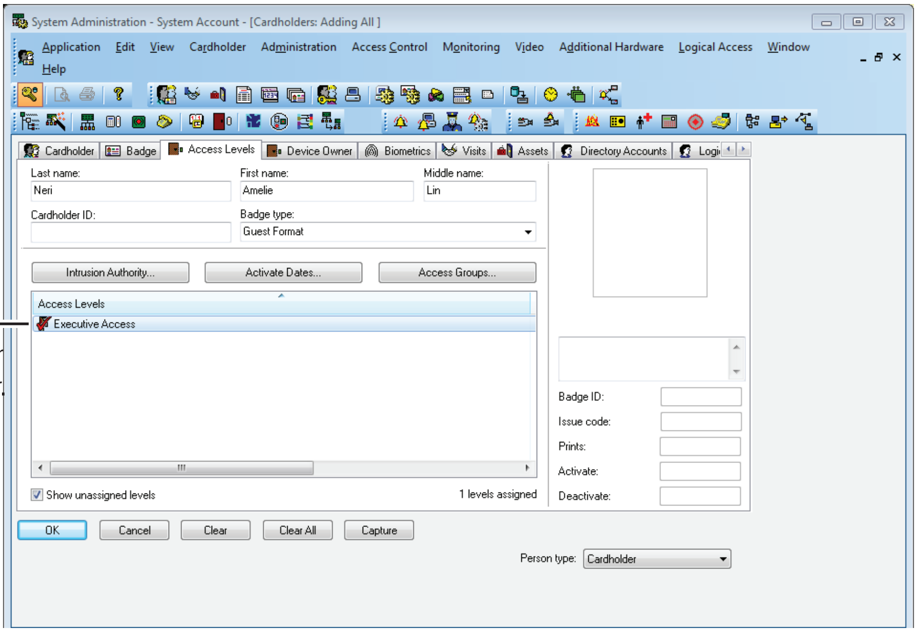
Choose access doors

Figure 20 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.



Last name: Neri

First name: Amelie

Middle name: Lin

Cardholder ID:

Badge type: Guest Format

Access Levels

☑ Executive Access

☑ Show unassigned levels

1 levels assigned

Badge ID:

Issue code:

Prints:

Activate:

Deactivate:

Person type: Cardholder

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

Figure 21 The cardholder, access level information screen

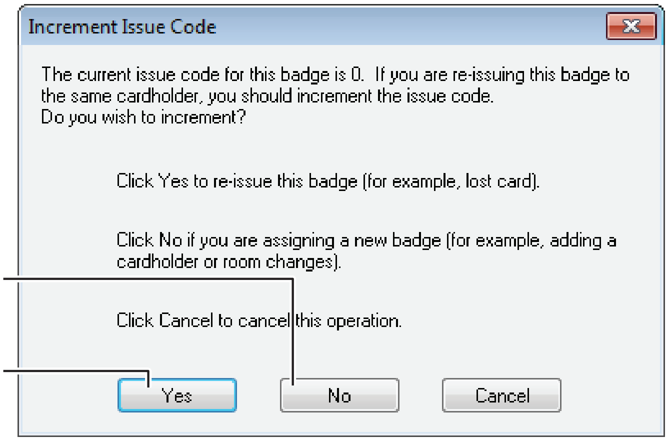
7 Select the appropriate access levels for the cardholder.

Note Only the access levels accompained 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 is at zero, the following confirmation is displayed



The current issue code for this badge is 0. If you are re-issuing this badge to the same cardholder, you should increment the issue code.
Do you wish to increment?

Click Yes to re-issue this badge (for example, lost card).

Click No if you are assigning a new badge (for example, adding a cardholder or room changes).

Click Cancel to cancel this operation.

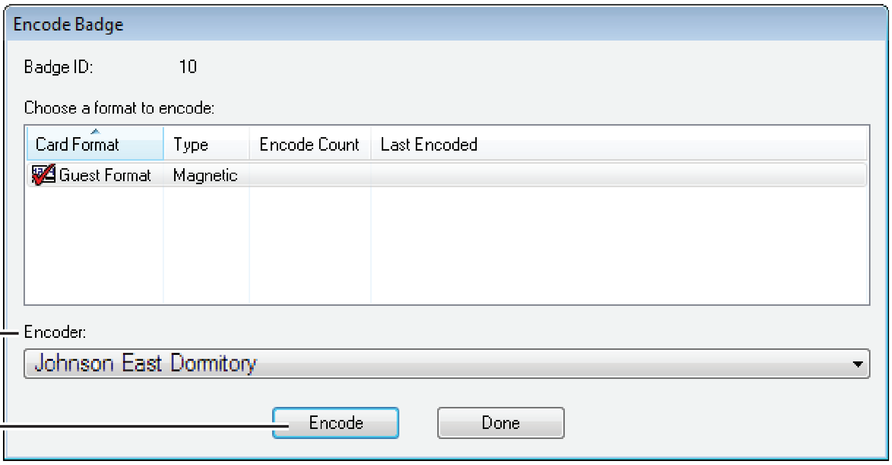
Click No, if you are assigning a new badge.

Click Yes, if the card is lost or stolen.

Figure 22 Question regarding the issue code

10 Click No.

The Encode Badge window displays



Encode Badge

Badge ID: 10

Choose a format to encode:

Card Format	Type	Encode Count	Last Encoded
☑ Guest Format	Magnetic		

Encoder:

Johnson East Dormitory

Choose the encoder.

Click the Encode button to start the encoding process.

Figure 23 Choosing a card format to encode

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

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

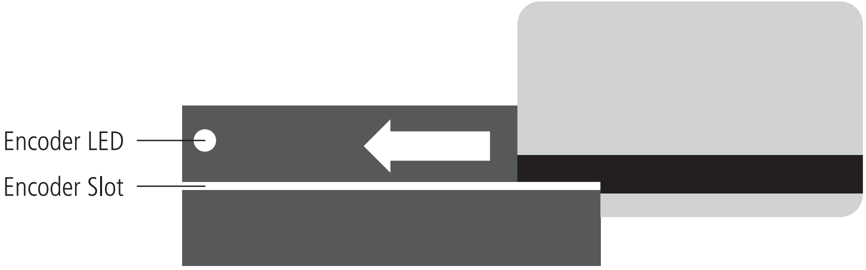


Figure 24 Swiping the magstripe card through the encoder

13 Confirm that the encoding is complete.

Offline G reader programming is now complete

If you have finished the tasks up to this point, you have completed all steps necessary for the programming of Offline G functionality or basic functionality for Offline V. Please see the Offline Locks System Administration User Guide on the dormakaba website: **https://dhwsupport.dormakaba.com/hc/en-us** for more information on configuring time zones, holidays, access panels, cardholder management and other additional features.

Task 7: Install BEST Access Transport

The BEST Access Transport software provides communication between your offline locks and your Offline Locks workstation. With the help of your computer network administrator, if necessary, perform the following steps to set up the BEST Access Transport software.

First, confirm that the following requirements are met for running BEST Access Transport.

- Offline Locks System Administration is installed.
- Offline Locks Communication Server is installed.

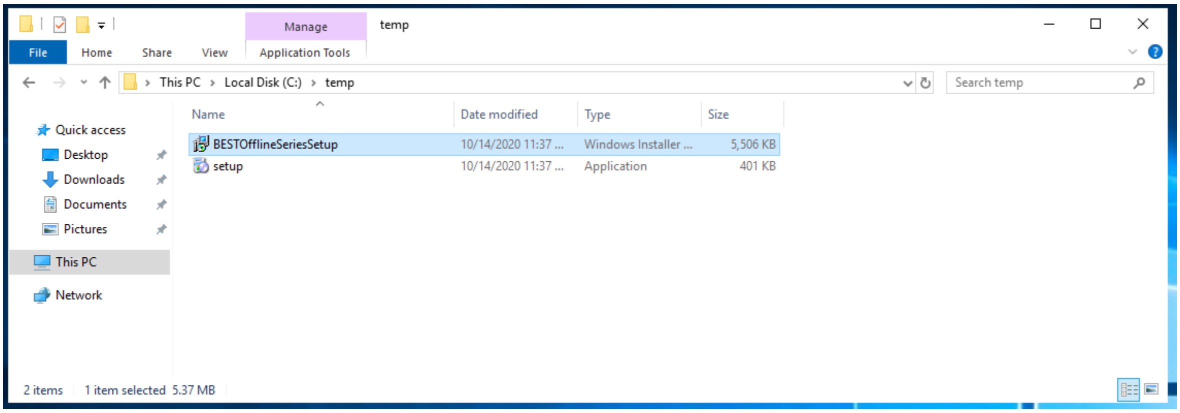
BEST Access Transport Server (Tray)

The BEST Access Transport Tray displays information that is downloaded/uploaded to/from the Transport database. General use of the Transport Tray Application can be performed by a user with only “User” rights. Perform the following instructions to install BEST Access Transport Tray:

1 Working on the PC where BEST Access is installed stop the communications server.

2 Navigate to the BEST Transport Tray installation folder:

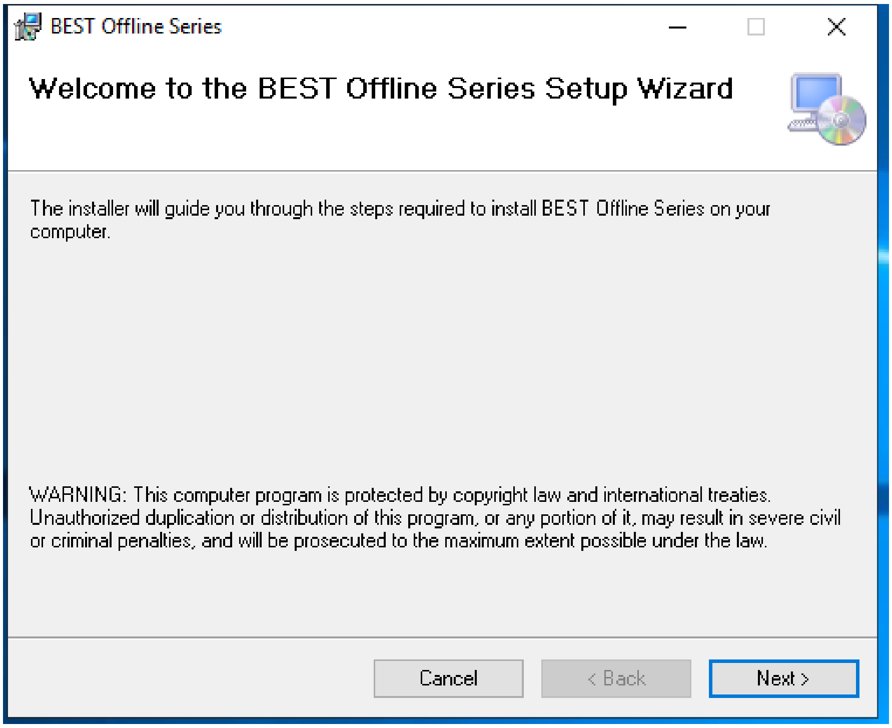
3 Right click setup.exe and run as Administrator



Name	Date modified	Type	Size
BESTOfflineSeriesSetup	10/14/2020 11:37 ...	Windows Installer ...	5,506 KB
setup	10/14/2020 11:37 ...	Application	401 KB

2 items   1 item selected 5.37 MB

Figure 25 setup.exe



Welcome to the BEST Offline Series Setup Wizard

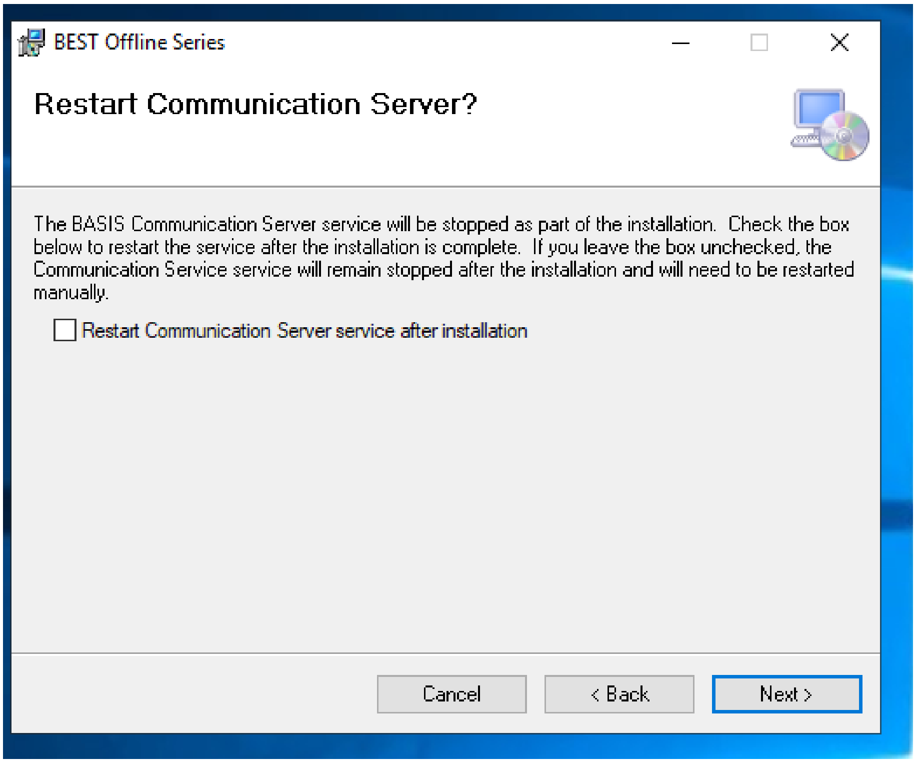
The installer will guide you through the steps required to install BEST Offline Series on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Figure 26 Welcome window

4 Click Next.

5 The Offline Locks communication Server service will stop as part of the installation. Deselect the box to automatically start the communication server after installation. The communications server will manually restart after SW installation has been completed.



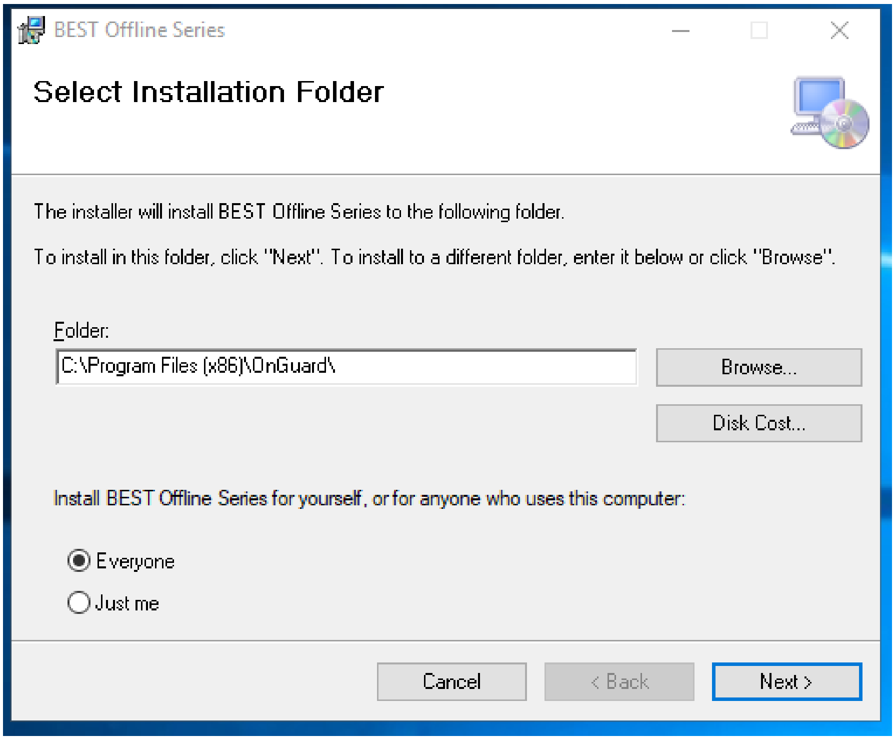
Restart Communication Server?

The BASIS Communication Server service will be stopped as part of the installation. Check the box below to restart the service after the installation is complete. If you leave the box unchecked, the Communication Service service will remain stopped after the installation and will need to be restarted manually.

□ Restart Communication Server service after installation

Figure 27 Restart Communication Server

6 Click Next and the Select Installation Folder window will appear.



Select Installation Folder

The installer will install BEST Offline Series to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files (x86)\OnGuard\

Install BEST Offline Series for yourself, or for anyone who uses this computer:

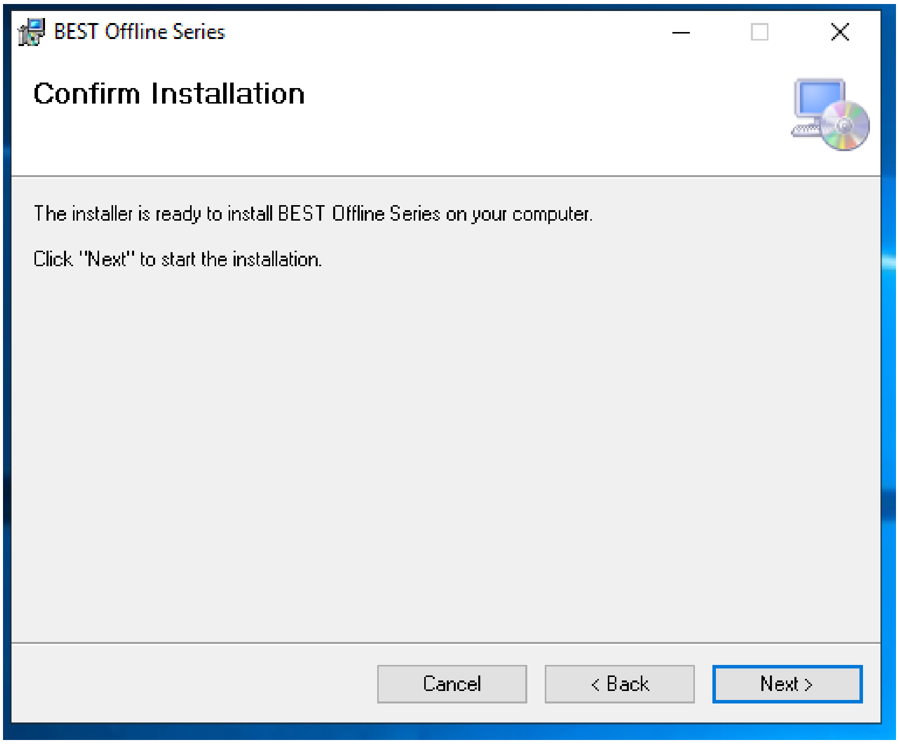
● Everyone

○ Just me

Figure 28 Select Installation Folder

7 The Installation Folder will automatically install on your program file drive, unless you specify otherwise. Make sure to select “Everyone” to enable use of the Transport Tray application.”.

8 Click Next.


BEST Offline Series

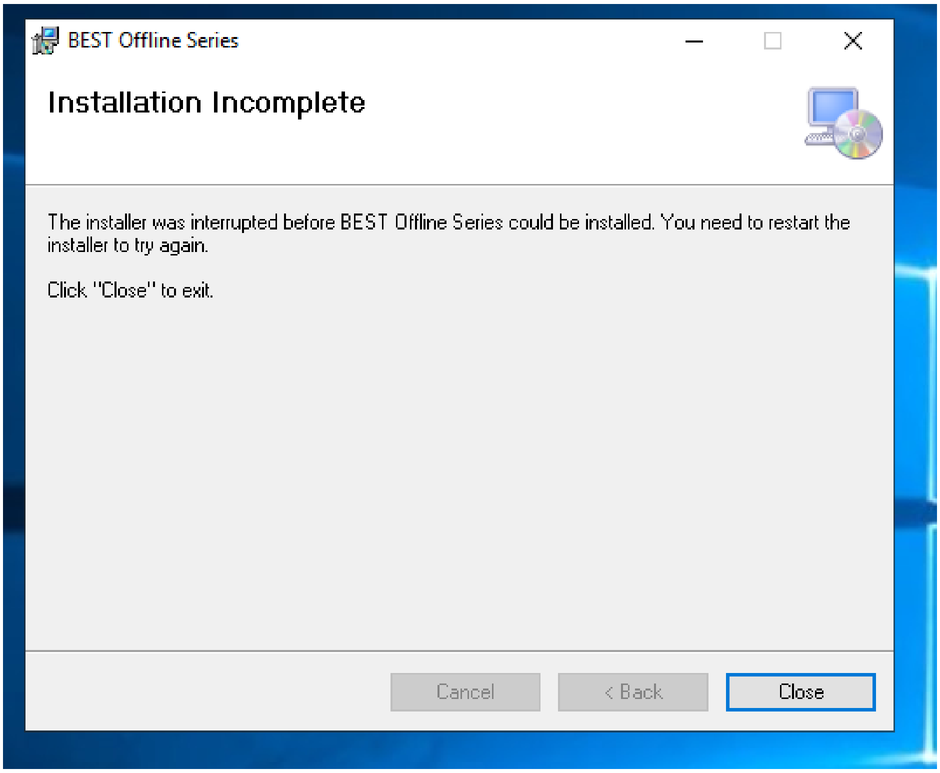
Confirm Installation

The installer is ready to install BEST Offline Series on your computer.

Click "Next" to start the installation.

Figure 29 Confirm Installation

9 Click Next and installation will begin. Once the Installation Complete window pops up, click Close.



BEST Offline Series

Installation Incomplete

The installer was interrupted before BEST Offline Series could be installed. You need to restart the installer to try again.

Click "Close" to exit.

Figure 30 Installation Complete

Initial Configuration of Transport Tray

After the Offline Locks Transport Tray has successfully installed onto your workstation, you will need to set up the location of the SQL Server CE Offline Locks Transport database file that is used to store offline information. This configuration is required before installing any Offline Locks Transport software for a Netbook. Three options exist for the configuration location of the Transport Database location:

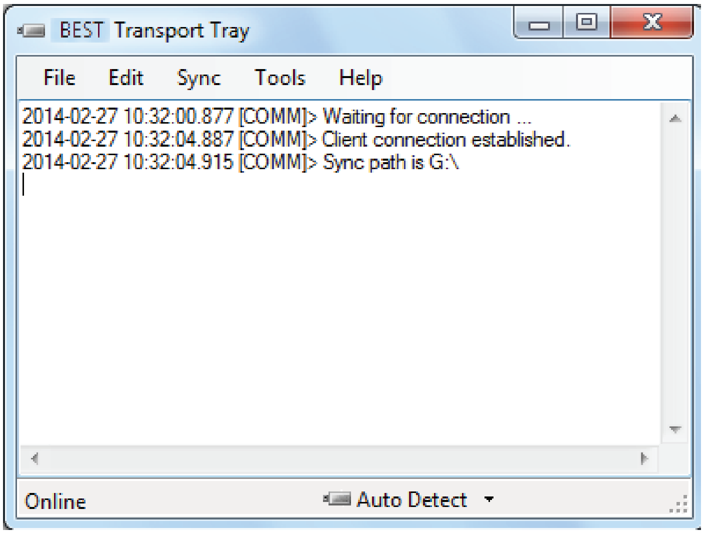
- **Removable Media Device** — USB Flash Drive
- **Known Directory** — simple directory

Removable Media Device

The Removable Media Device option can be used to store the database if the user has a USB Flash Drive that will be used by the client during reader programming. The flash drive can be inserted into the server's USB port to store the database file. Once a panel download is complete, the device can be removed and inserted into the client computer to allow access to all lock set information during programming activities. History will automatically be uploaded when the device is reconnected to the server and communication server is running If retrieved from the lock. Perform the following steps:

1 Go to Start > Programs > BEST Access > BEST Transport > BEST Transport Tray menu item.

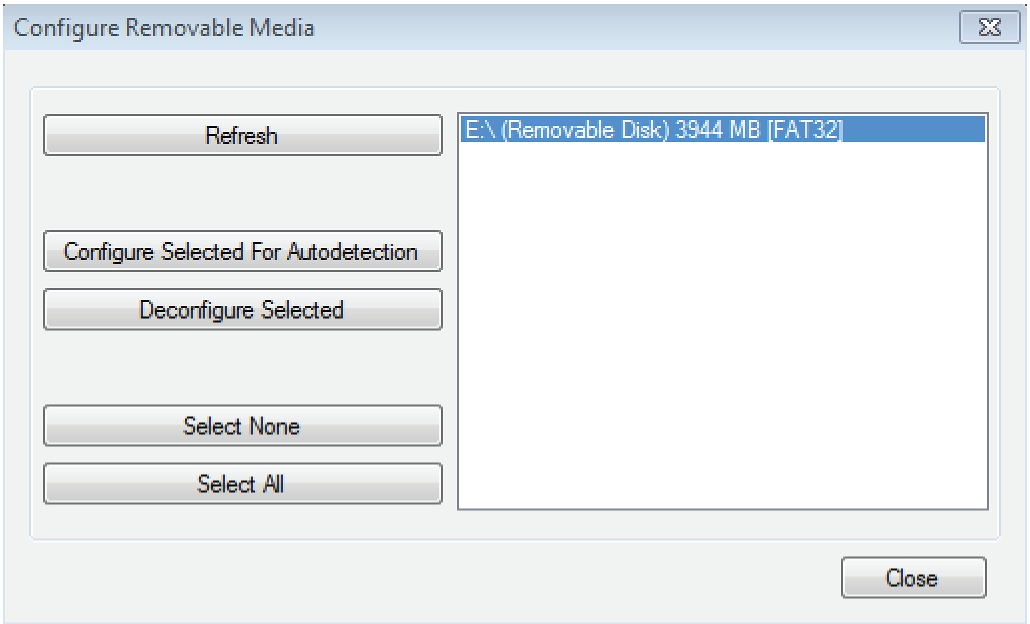
2 The Transport Tray home page will open and an icon is displayed in the task tray.



```
2014-02-27 10:32:00.877 [COMM]> Waiting for connection ...
2014-02-27 10:32:04.887 [COMM]> Client connection established.
2014-02-27 10:32:04.915 [COMM]> Sync path is G:\
```

Figure 31   Transport Tray

1 Select“Tools > Configure Removable Media menu item.


Configure Removable Media
Refresh
Configure Selected For Autodetection
Deconfigure Selected
Select None
Select All
Close

E:\ (Removable Disk) 3944 MB [FAT32]

Figure 32 Configure removable media

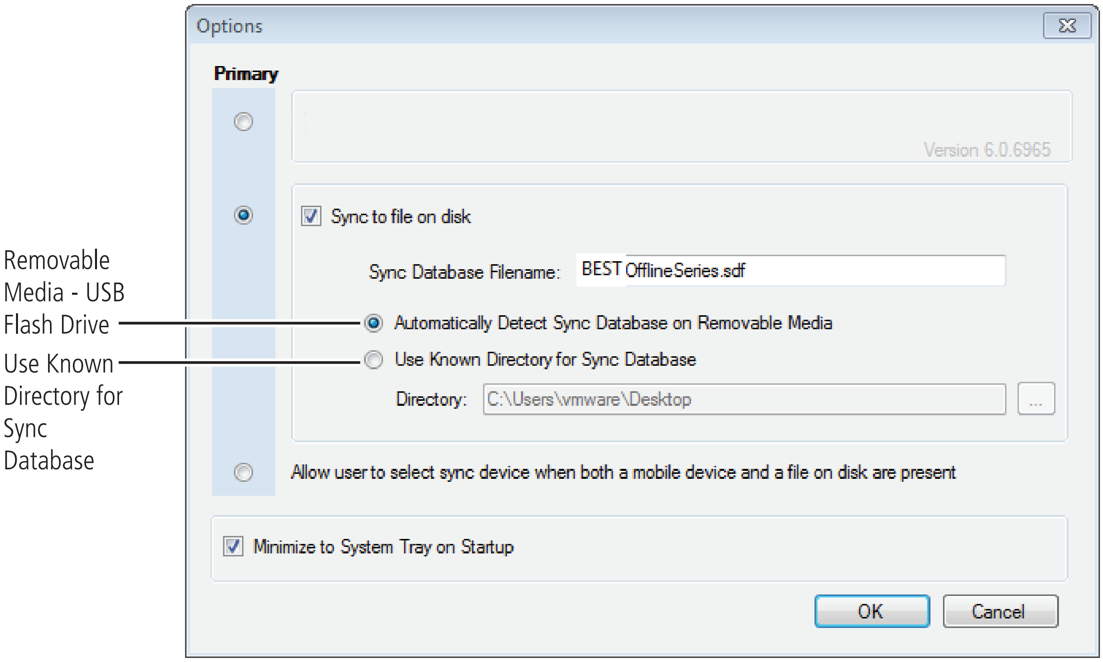
2 Figure 32 will show all available removable devices on the system and the following table provides the definition of each option under the ‘Configure Removable Media’ window.

3 Click the USB flash drive to highlight it.

4 Click "Configure Selected For Autodetection" button to configure the USB Flash drive.

Removable Devices	Definition
Refresh	Refreshes the list of removable devices.
Configure selected for autodetection:	Configures the selected media for auto detection. The **BESTTransportSync.dat** and **BESTOfflineSeries.sdf** files are placed on the root drive of the device. When the device is plugged in and BEST Communication Server and the transport tray application are running, history will automatically be uploaded to Offline Locks A “{DETECTABLE}” string will appear next to the removable device once configured.
Deconfigure Selected	Deconfigures the selected device for auto detection and removes the _BESTTransportSync.dat file from the device
Select None	Select no removable media
Select All	Select all removable media

5 Select Tools > Options. User can select primary transport method.



Options

Primary

○ Version 6.0.6965

● ☑ Sync to file on disk

Sync Database Filename: BEST OfflineSeries.sdf

● Automatically Detect Sync Database on Removable Media

○ Use Known Directory for Sync Database

Directory: C:\Users\vmware\Desktop

○ Allow user to select sync device when both a mobile device and a file on disk are present

☑ Minimize to System Tray on Startup

Removable Media - USB Flash Drive

Use Known Directory for Sync Database

Figure 33 Options

6 Select box to sync to file on disk and check the “Automatically Detect Sync Database on Removable Media” option. This will ensure the application auto detects devices.

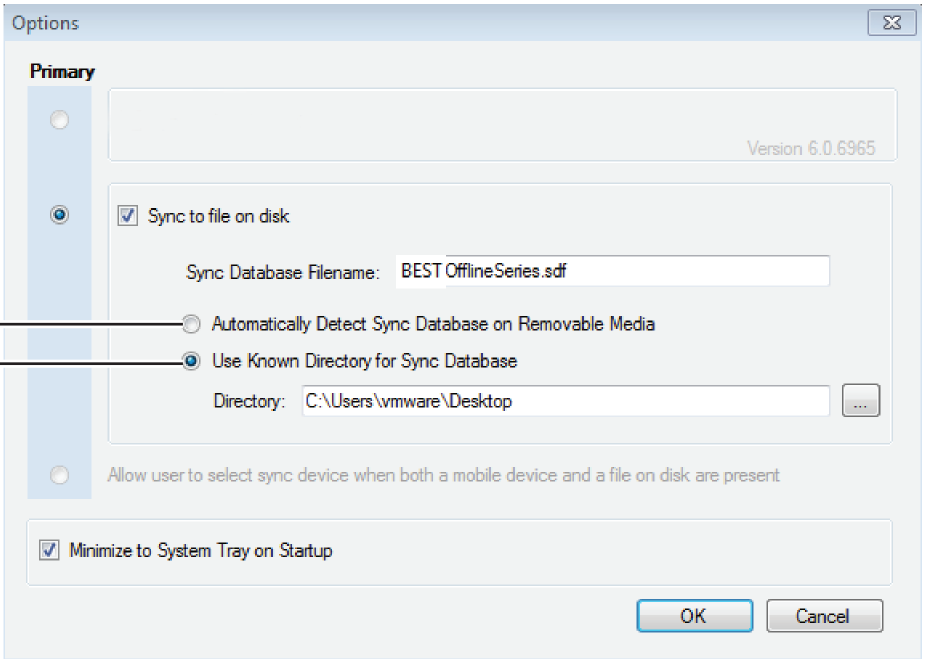
Note You are able to select both the "Sync to Mobile Device" and "Sync to file on disk".

7 Click the “OK” button.

Known Directory

If a Removable Media device is not used, a simple directory can be used that is shared on the network. It can also be a shared drive if the client and server are on the same computer. Perform the following steps.

1. Go to the Transport Tray home page.
2. Select Tools > Options. The following window will appear.



Options

Primary

○

Version 6.0.6965

● ☑ Sync to file on disk

Sync Database Filename: BEST OfflineSeries.sdf

○ Automatically Detect Sync Database on Removable Media

● Use Known Directory for Sync Database

Directory: C:\Users\vmware\Desktop ...

○ Allow user to select sync device when both a mobile device and a file on disk are present

☑ Minimize to System Tray on Startup

OK Cancel

Removable Media - USB Flash Drive

Use Known Directory for Sync Database

Figure 34 Options

3. Select box to sync to file on disk and check the “Use Known Directory for Sync Database” option. Then select the location for the directory. This will ensure the application uses this directory to store the database.
4. Click the “OK” button.

Task 8: Install Offline Locks Transport for Netbook/Notebook

The Offline Locks Transport application is used to download information to the reader and upload history from the reader to your Netbook/Notebook only. There are two components to the Transport Client software that needs to be installed:

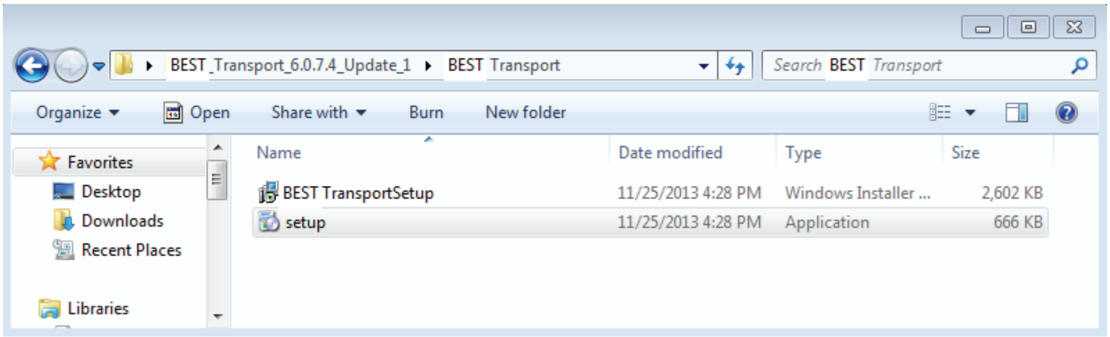
- **SQL Server 3.5 Compact** — relational database for applications that run on mobile devices and desktops
- **Setup.exe** — Transport Client (Netbook/Notebook) software

Offline Locks Transport Installation

To install Transport software, complete the following steps:

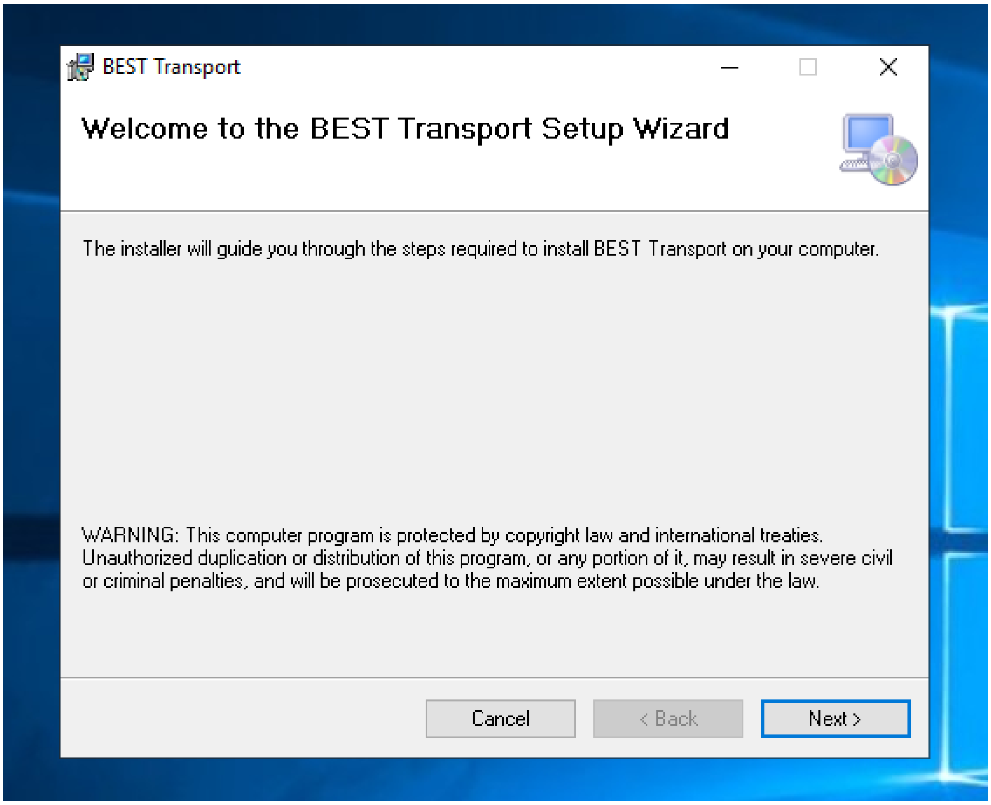
1 Navigate to the Transport folder.

2 Right click setup.exe and Run as administrator.



Name	Date modified	Type	Size
BEST TransportSetup	11/25/2013 4:28 PM	Windows Installer ...	2,602 KB
setup	11/25/2013 4:28 PM	Application	666 KB

Figure 49 Setup



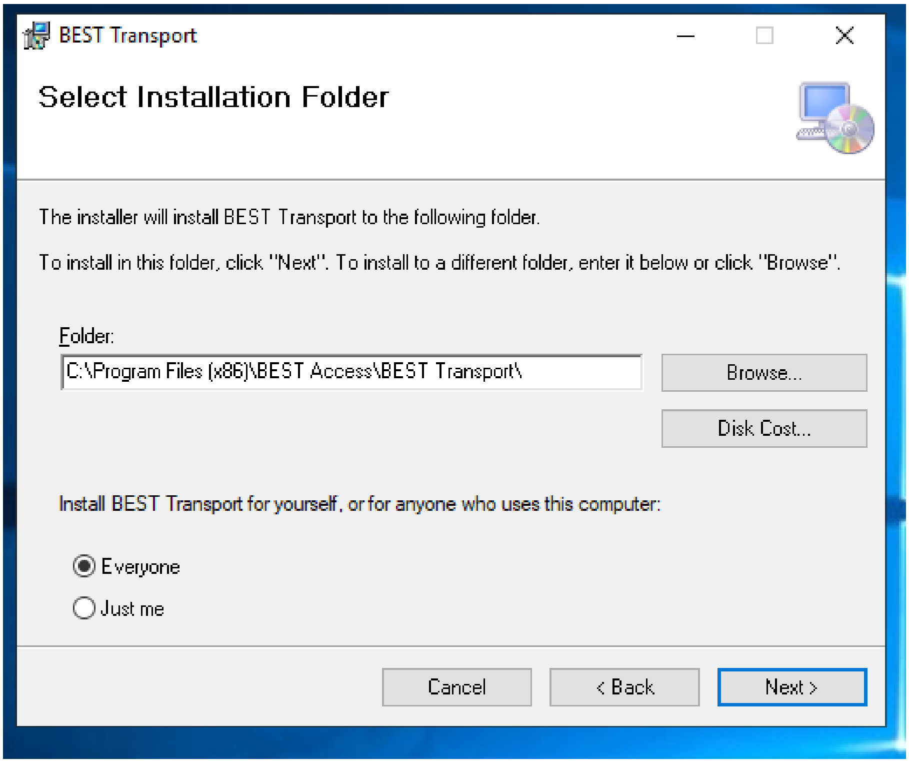
Welcome to the BEST Transport Setup Wizard

The installer will guide you through the steps required to install BEST Transport on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Figure 50 Setup Wizard

3 Click Next and the Select Installation Folder window will appear.


BEST Transport

Select Installation Folder

The installer will install BEST Transport to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files (x86)\BEST Access\BEST Transport\

Install BEST Transport for yourself, or for anyone who uses this computer:

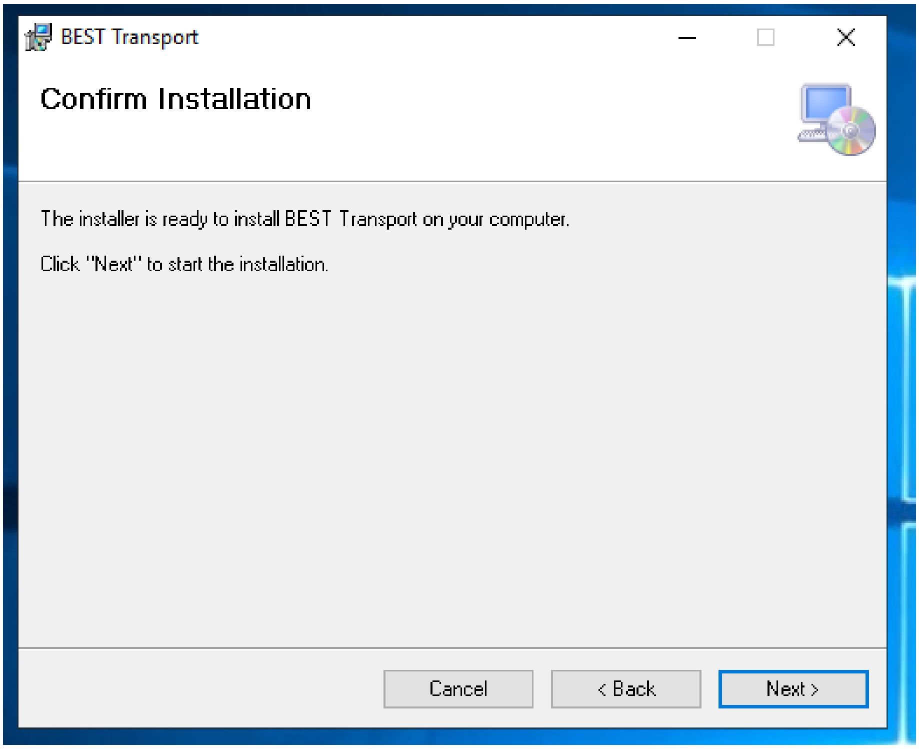
● Everyone

○ Just me

Figure 51 Select installation folder

4 The Installation Folder will automatically install on your program file drive, unless you specify otherwise. Make sure to select “Everyone” to enable use of the BEST Transport application.

5 Click Next.



BEST Transport

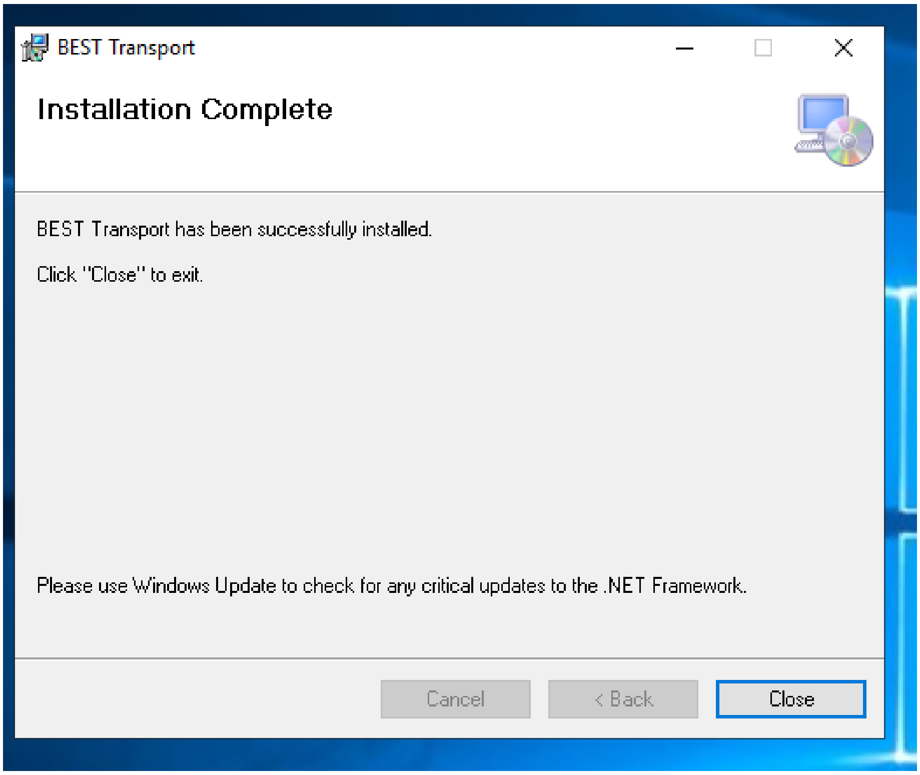
Confirm Installation

The installer is ready to install BEST Transport on your computer.

Click "Next" to start the installation.

Figure 52 Confirm installation

6 Click Next



BEST Transport

Installation Complete

BEST Transport has been successfully installed.

Click "Close" to exit.

Please use Windows Update to check for any critical updates to the .NET Framework.

Figure 53 Installation complete

7 Click Close

3
Set Up and Maintain Offline Locks

This section describes how to use your Offline Locks Transport software. The following topics are covered:

- Transferring reader configurations from Offline Locks System
- Administration to your Netbook/Notebook
- Connecting the Netbook/Notebook to the Lock
- Manually Changing the PIN in a Dual Validation Lock

Transferring Lock/Reader Configurations

At this point you have successfully completed the following for the Offline Locks System:

- Task 1: Install Offline Locks Software
  See page 15.
- Task 2: Install Encoder
  See page 15.
- Task 3: Define Card Formats
  See page 19.
- Task 4: Define Badge Types
  See page 22.
- Task 5: Define Offline Access Panels
  See page 25.
- Task 6: Define Guest Locks/Readers
  See page 27.
- Task 7: Install Offline Locks Transport
  See page 38.
- Task 8: Install Offline Locks Transport on Netbook/Notebook See page 48.

Now that you have installed and defined the Offline Locks System, you'll want to transfer your new configurations or changes to your locks/readers, using your Netbook/Notebook. Two steps are involved to complete the transfer:

- Workstation connection
- or Insert a USB flash drive into your workstation to transfer configurations to Netbook/Notebook
- Connecting your Netbook/Notebook to reader

Transferring Lock/Reader Configurations to the Netbook/Notebook

To transfer lock/reader configuration made through the BEST System Administration to your Netbook/ Notebook, perform the following steps:

Note The following presumes the user has successfully logged into BEST System Administration and the communication server is running. It is also presumed the USB to serial cable is connected and configured on the Netbook per the manufacturers instructions.

1 Connect a USB flash drive in the a USB port on your Netbook/Notebook and then open BEST Transport Tray.

2 In System Administration and working from the System Tree right click the reader to be programmed, and select Download.

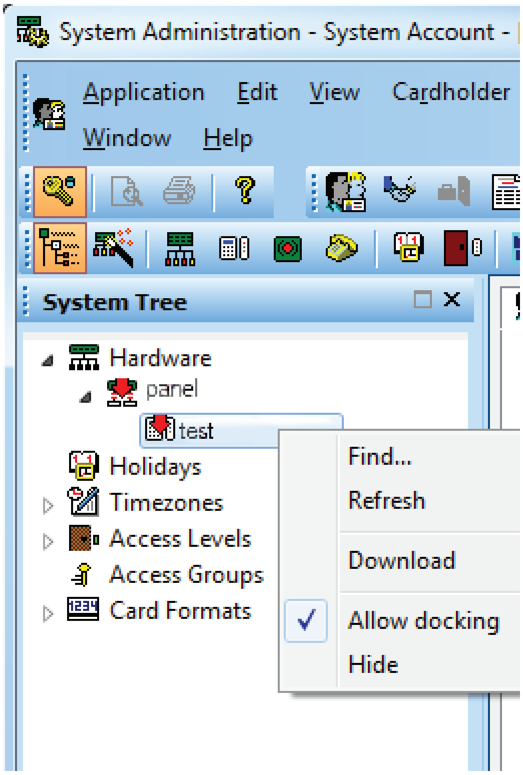
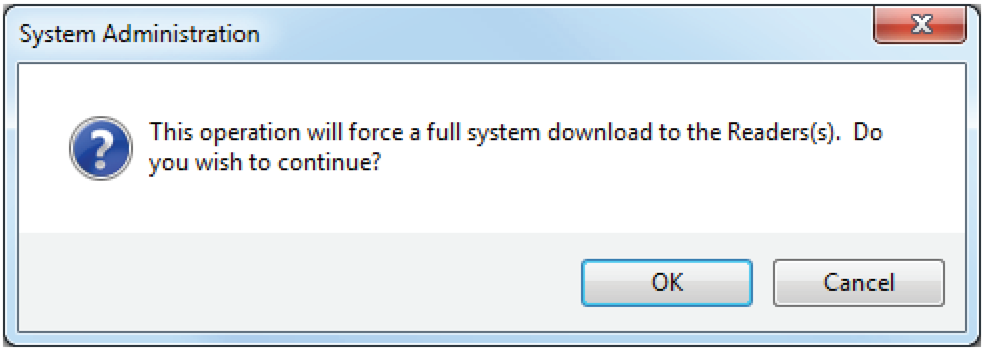


Figure 86 Reader Program Download

3 Click OK.

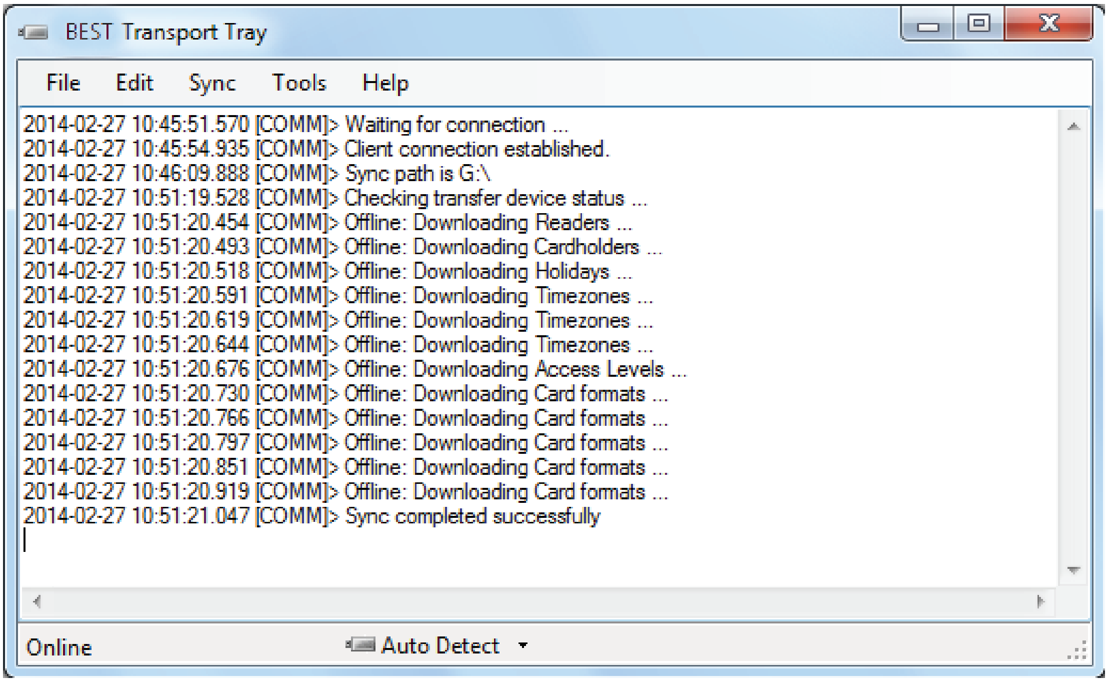


This operation will force a full system download to the Readers(s). Do you wish to continue?

Figure 87 Full System Download

4 Upon Sync successfully completed, eject and disconnect the USB flash drive from your workstation.

5 Connect the USB flash drive to the USB/com port on your Netbook/Notebook and connect the USB to serial cable.



```
2014-02-27 10:45:51.570 [COMM]> Waiting for connection ...
2014-02-27 10:45:54.935 [COMM]> Client connection established.
2014-02-27 10:46:09.888 [COMM]> Sync path is G:\
2014-02-27 10:51:19.528 [COMM]> Checking transfer device status ...
2014-02-27 10:51:20.454 [COMM]> Offline: Downloading Readers ...
2014-02-27 10:51:20.493 [COMM]> Offline: Downloading Cardholders ...
2014-02-27 10:51:20.518 [COMM]> Offline: Downloading Holidays ...
2014-02-27 10:51:20.591 [COMM]> Offline: Downloading Timezones ...
2014-02-27 10:51:20.619 [COMM]> Offline: Downloading Timezones ...
2014-02-27 10:51:20.644 [COMM]> Offline: Downloading Timezones ...
2014-02-27 10:51:20.676 [COMM]> Offline: Downloading Access Levels ...
2014-02-27 10:51:20.730 [COMM]> Offline: Downloading Card formats ...
2014-02-27 10:51:20.766 [COMM]> Offline: Downloading Card formats ...
2014-02-27 10:51:20.797 [COMM]> Offline: Downloading Card formats ...
2014-02-27 10:51:20.851 [COMM]> Offline: Downloading Card formats ...
2014-02-27 10:51:20.919 [COMM]> Offline: Downloading Card formats ...
2014-02-27 10:51:21.047 [COMM]> Sync completed successfully
```

Online

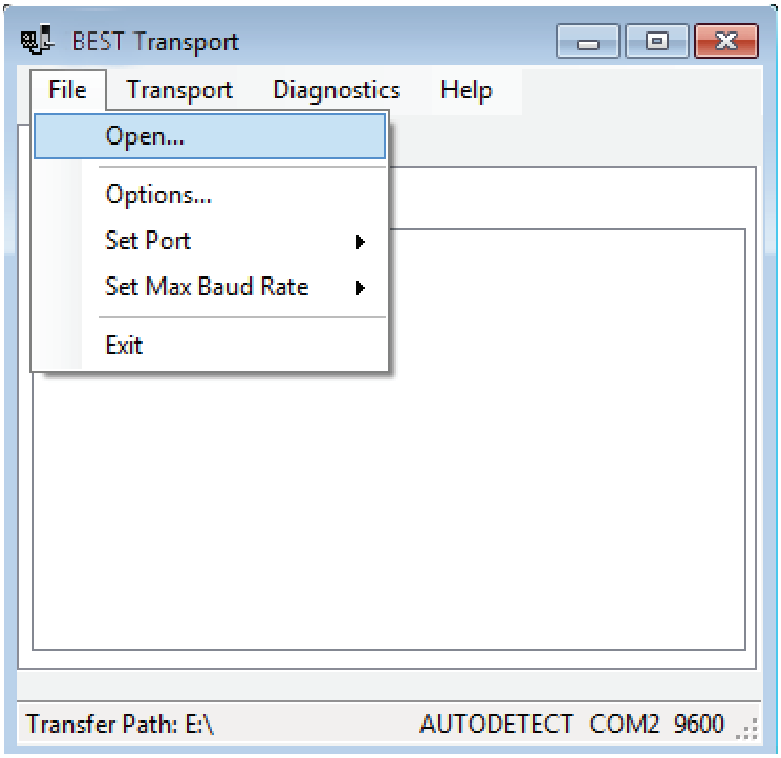
Figure 88 Transfer Completed

6 Open the BEST Transport application.

Opening a Panel/Reader Configuration on a Netbook

After saving the **OfflineSeries.sdf** file on your Netbook/Notebook from your USB flash drive, you'll need to upload all of your Offline Locks System Administration configurations to Transport Client. Perform the following steps:

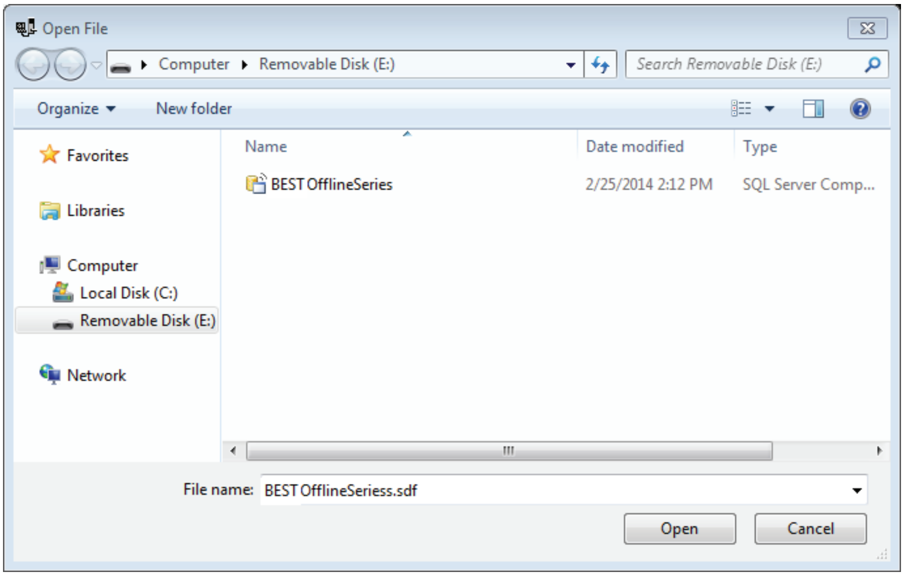
1. Go to the Transport home page by selecting Programs > BEST Access > BEST Transport > BEST Transport
2. Go to the File > Open…" menu item. The following window will appear.



Transfer Path: E:\ AUTODETECT COM2 9600

Figure 89 Open file

3 Select your **BESTOfflineSeries.sdf** file and Click Open.

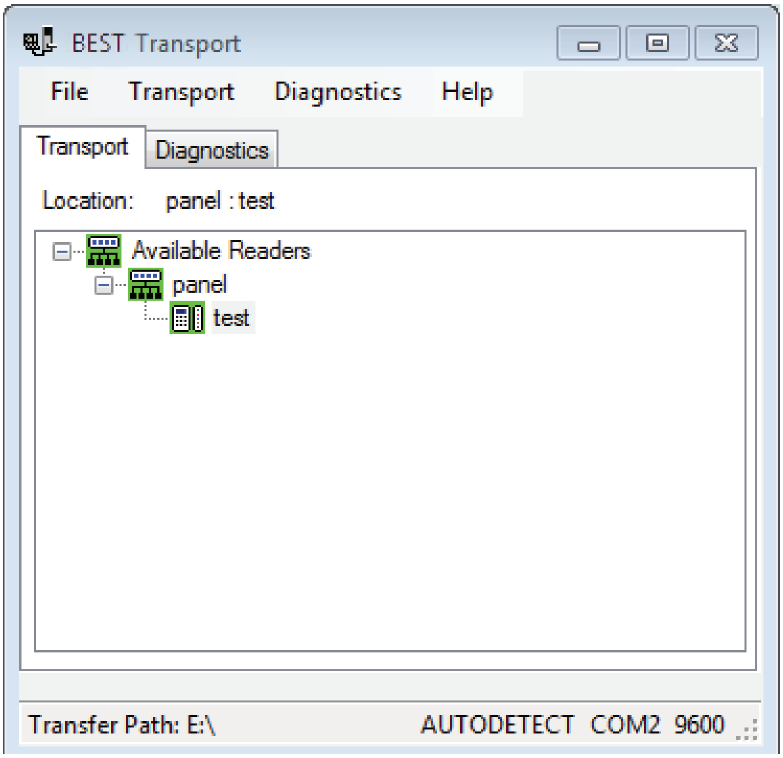


Name	Date modified	Type
BEST OfflineSeries	2/25/2014 2:12 PM	SQL Server Comp...

File name: BEST OfflineSeriess.sdf

Figure 90 Open file

4 The main window will refresh with the list of locks/readers.



Location: panel : test

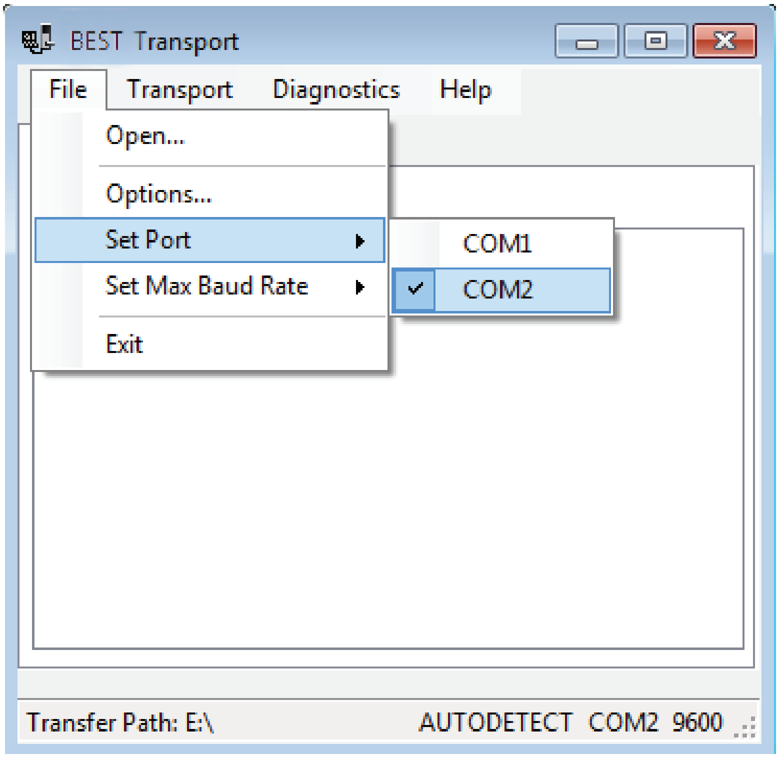
Transfer Path: E:\ AUTODETECT COM2 9600

Figure 91 List of locks/readers

Setting the USB/Communication Port

Once your panel has refreshed to reflect your **BESTOfflineSeries.sdf**, you must make sure that the correct com port is selected to continue with configuration. Perform the following steps:

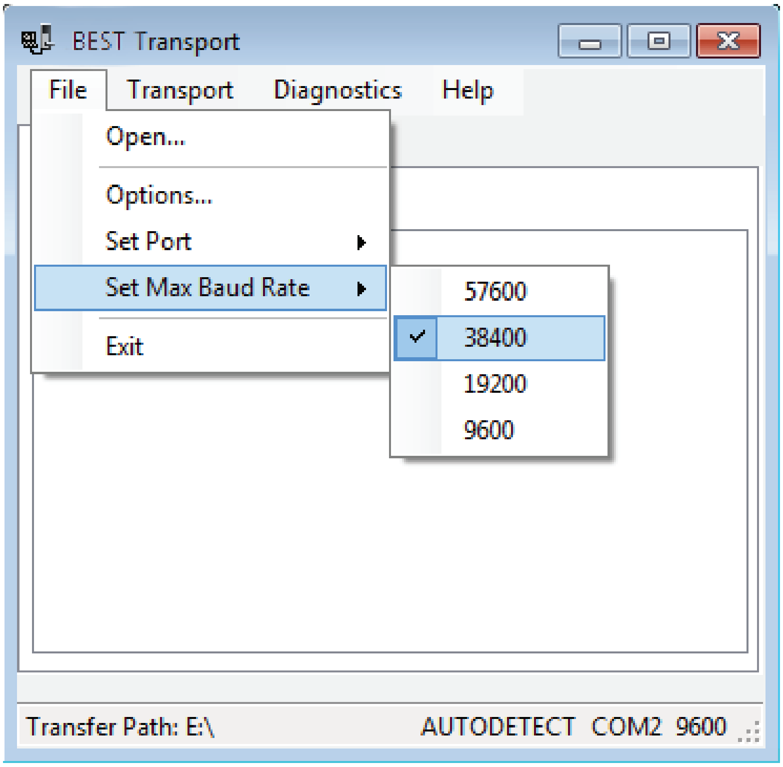
1 On the Transport home page, select File > Set Port > COM (port that is being used by the lock/reader). In this example, it is COM2.



Transfer Path: E:\ AUTODETECT COM2 9600

Figure 92 Set port

2 On the Transport home page, select File > Set Max Baud Rate > In this example, it is 38400.



Transfer Path: E:\ AUTODETECT COM2 9600

Figure 93 Set Max Baud Rate

Connecting the Netbook/Notebook to the Reader

To begin transferring configurations from your Netbook/Notebook to your lock, you must first properly connect the Netbook/Notebook to the reader. See Figure 94 and perform the following steps:

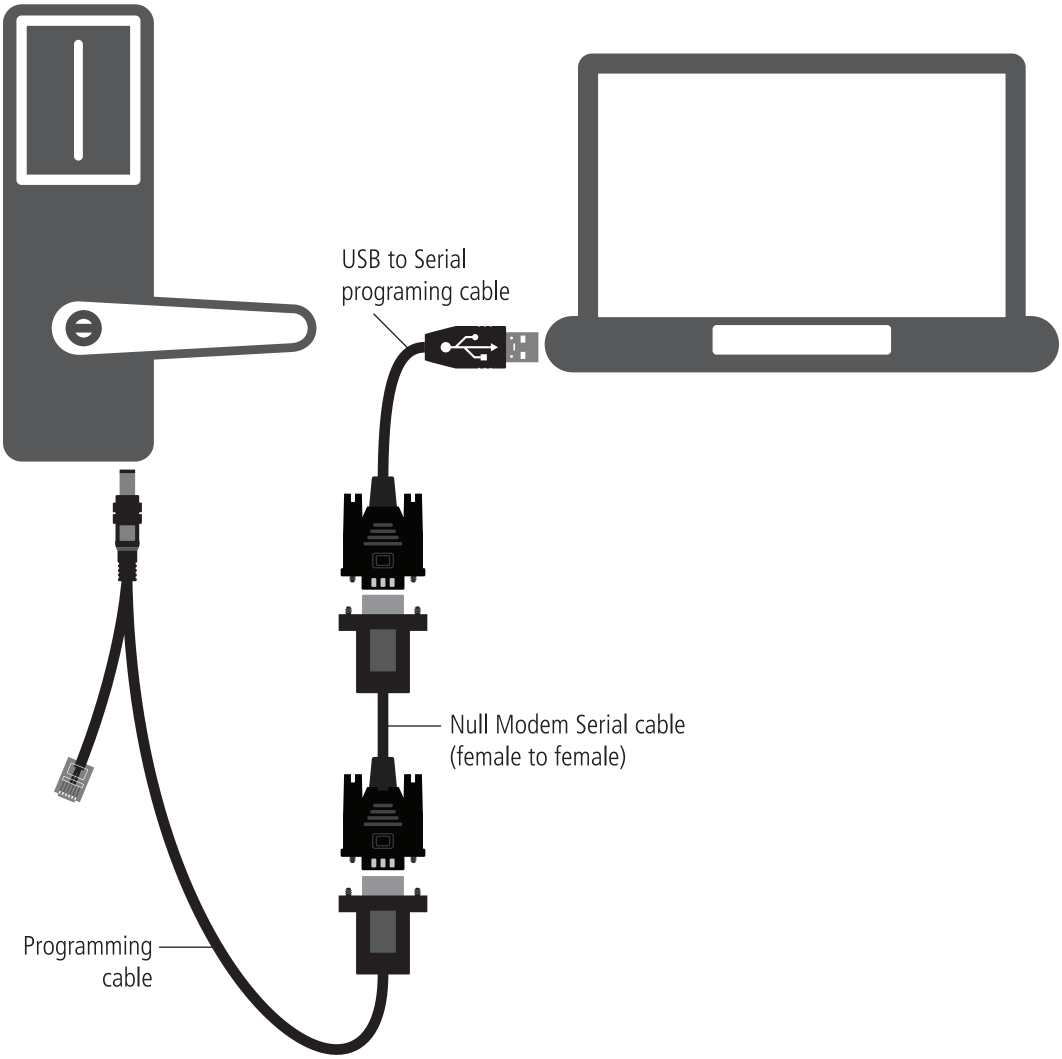

USB to Serial programing cable
Null Modem Serial cable (female to female)
Programming cable

Figure 94 Connecting the Netbook/Notebook to a lock

1. Connect the USB to Serial Programming cable to the USB port on your Netbook/Notebook.
2. Connect the USB to Serial Programming cable to the Null Modem Serial cable (female to female).
3. Connect the Null Modem Serial cable (female to female) to the Programming cable.
4. Connect the Programming cable to the lock’s Communication port. The connector snaps into place.

Note: Length of cables displayed in Figure 51 may be longer than illustrated.

Configure Lockset

The configure lockset option will allow you to configure a reader based on any configuration in System Administration. Perform the following steps:

Note: If this is the initial installation of the lock, you will need to run diagnostics first and set the Use Count to 0.

1 Return to the BEST Transport home page with the Transport tab selected and the list of locks/ readers present.

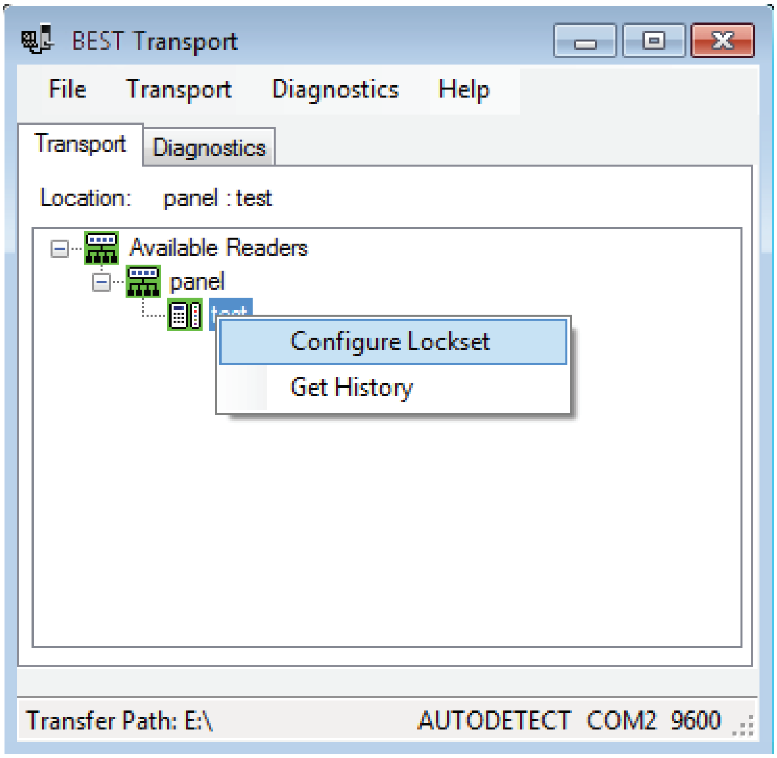


Figure 95 Configure lockset

2 Right-click on the desired reader configuration and select Configure Lockset. The following window will appear:

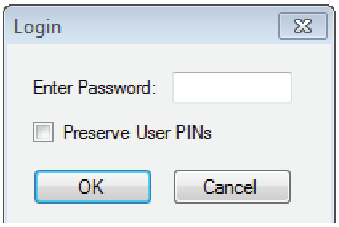
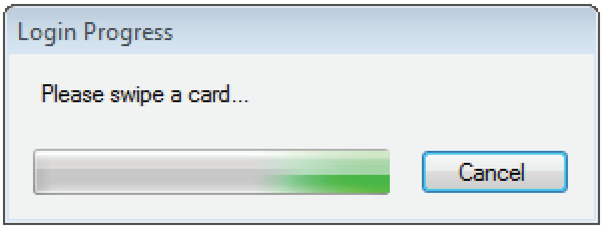


Figure 96 Enter password

Note The password for a lock is the password programmed in the virtual access control panel. You must enter the password exactly as it was entered in the Password field on the Offline lock tab in the Access Panels screen since it is case sensitive. If this is the initial time the lock is being programmed or if the lock was reset to its factory default setting, leave the password field blank and tap OK.

3 Enter the password and press the OK button. If you have a Dual Validation Lock (with keypad) and you wish to preserve pins at the reader during the configuration, select the "Preserve User PINs". Or, to reprogram the lock with the PINs stored in Offline Locks, remove the check from the Preserve user pins check box.

Warning ***If users have reprogrammed their PINs at the lock and you do not preserve the user PINs, users will no longer be able to access the lock. The ability to program PIN's is only available when using Card and PIN mode.***

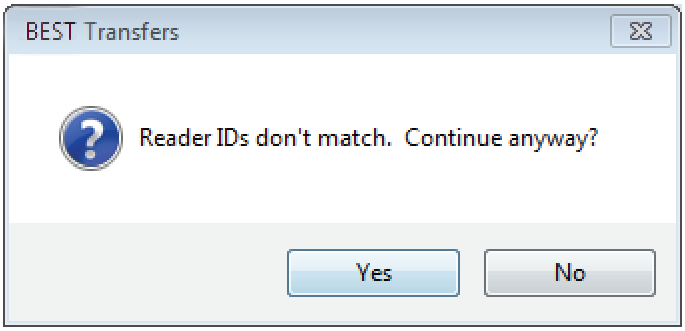


Please swipe a card...

Figure 97 Login process

4 Swipe a magnetic stripe card or proximity card through the reader. This will establish communications and begin the programming process. The following window may appear if this is the initial time the lock is programmed or if the lock has been reset to factory settings.

5 Click Yes.

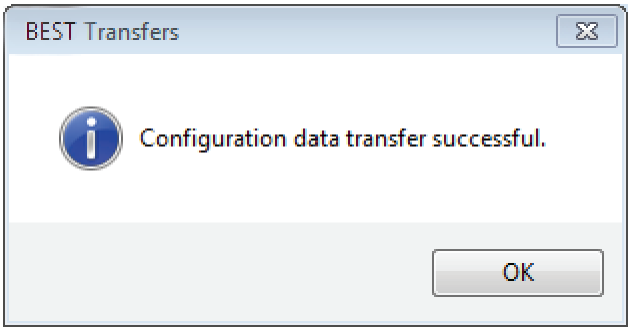


BEST Transfers

Reader IDs don't match. Continue anyway?

Figure 98 Offline Locks transfers

6 A window shows the download progress. Once the download is complete, the following window will appear.

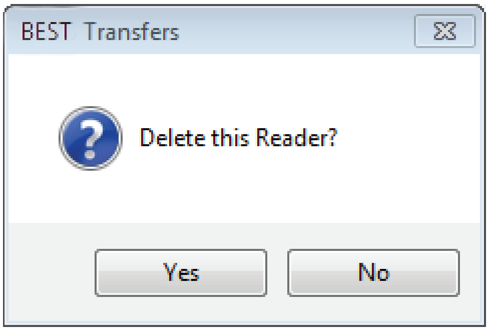


BEST Transfers

Configuration data transfer successful.

Figure 99 Configuration successful

7 Click OK and the following window will appear.



BEST Transfers

Delete this Reader?

Figure 100 Delete reader

8 If you wish to delete the reader from the list of readers, click the “Yes” button (recommended). Otherwise press the “No” button.

9 This completes the reader configuration.

Get History

The Get History option allows you to upload history from the lock.

1 Return to the BEST Transport home page with the Transport tab selected.

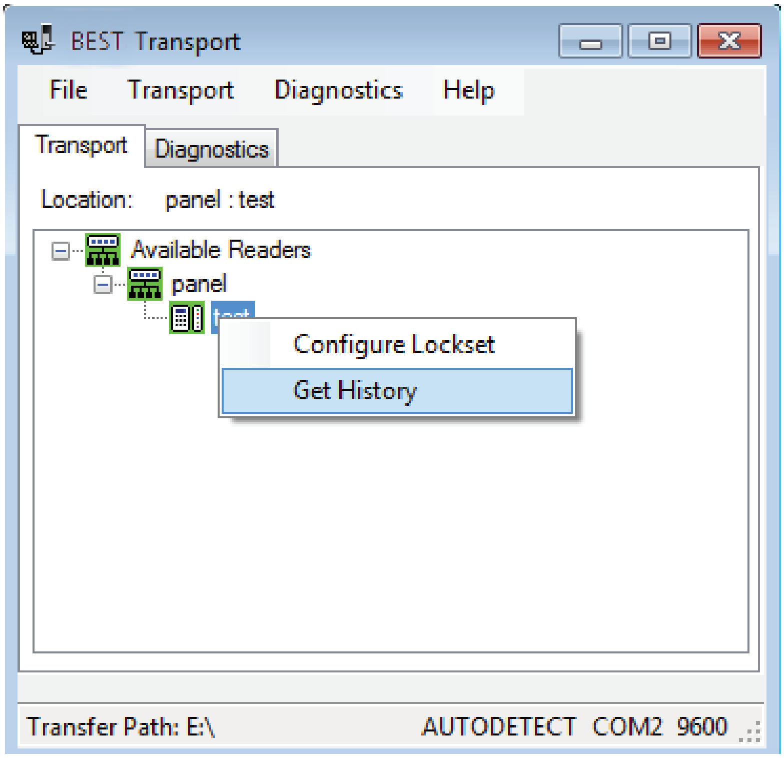


Figure 101 Get history

2 Right-click on the desired reader configuration and select Get History. The following window will appear.

Note The password for a lock is the password programmed in the virtual access control panel. You must enter the password exactly as it was entered in the Password field on the Offline lock tab in the Access Panels screen since it is case sensitive. If this is the initial time the lock is being programmed or if the lock was reset to its factory default setting, leave the password field blank and tap OK.

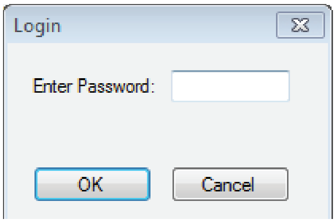
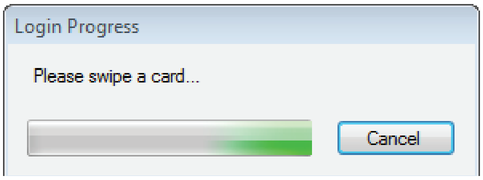


Figure 102 Login

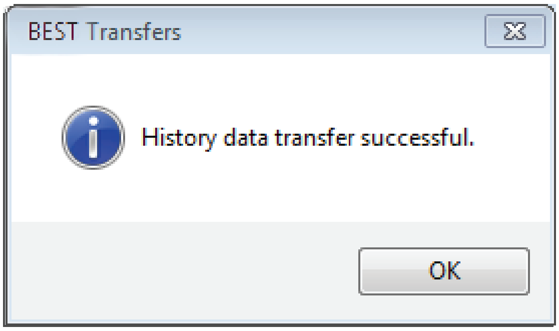
3 Enter the reader password and press the OK button.



Please swipe a card...

Figure 103 Swipe card

4 Swipe a magnetic stripe card or proximity card through the reader. This will establish communication and retrieve history events from the lock. A window shows the history upload progress. Once the upload is complete, the following window will appear.



History data transfer successful.

Figure 104 History data transfer successful

5 Click OK to exit.

Diagnostics

The Diagnostics view allows you to view information about the reader and configure options for your reader. The options include:

- Connect/Disconnect
- Set: Date/Time/DST enable, Reader Technology (Proximity, Magnetic, Dual Validation), and Online Mode
- Reset: Diagnostics Code/Use Count
- Unlock Once
- Deep Reset
- Download Firmware

Note: Some of the diagnostic options are only available if the Offline G or V lock is using a UVC board. If you are using a legacy Offline G or V lock, the options will appear gray and unable to program.

Connect

To connect to your reader through Transport, perform the following steps:

1 Go to Diagnostics > Connect.

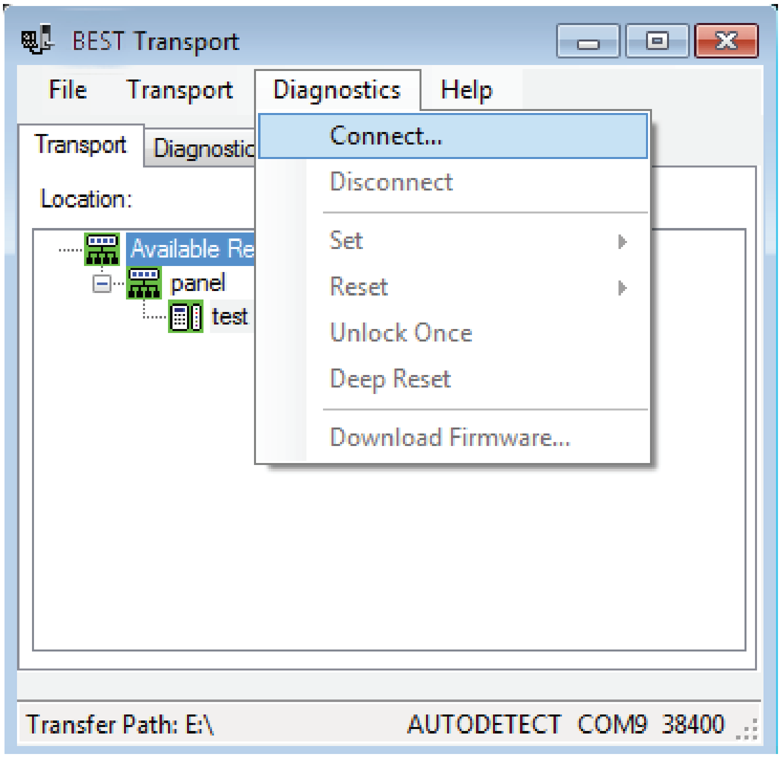


Figure 105 Diagnostic connect

Note The password for a lock is the password programmed in the virtual access control panel. You must enter the password exactly as it was entered in the Password field on the Offline lock tab in the Access Panels screen. The password is case sensitive. If this is the initial time the lock is being programmed or if the lock was reset to its factory default setting, leave the password field blank and tap OK.

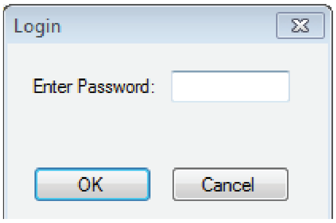
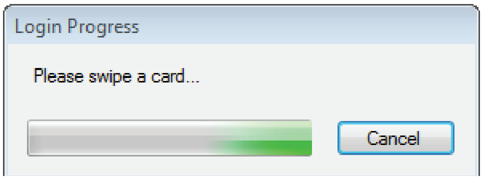


Figure 106 Login

2 Enter the reader password and press the OK button.

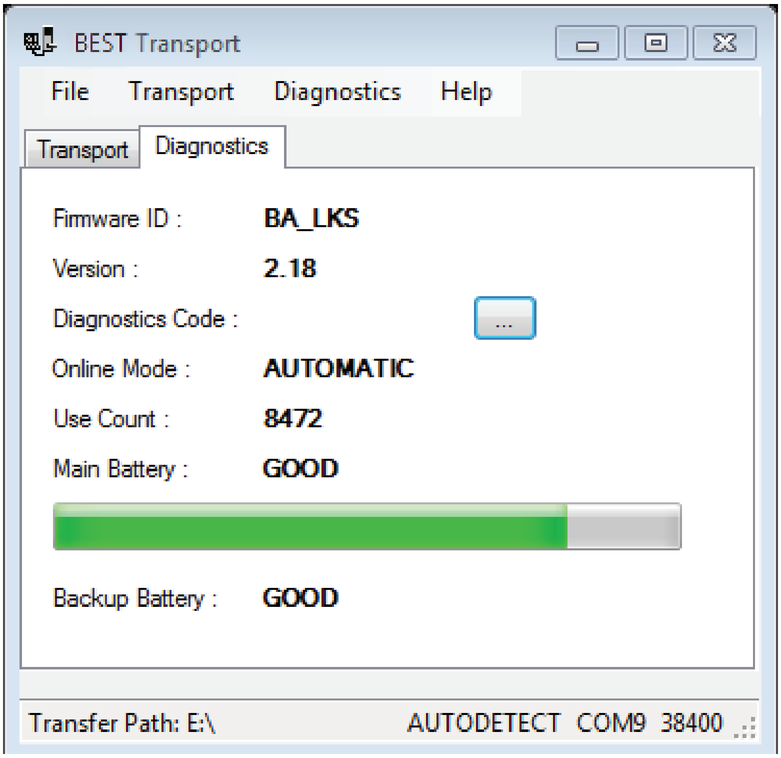


Please swipe a card...

Figure 107 Swipe card

3 Swipe a card.

4 Once connection is established, the reader diagnostics will display.



Firmware ID : BA_LKS

Version : 2.18

Diagnostics Code :

Online Mode : AUTOMATIC

Use Count : 8472

Main Battery : GOOD

Backup Battery : GOOD

Transfer Path: E:\ AUTODETECT COM9 38400

Figure 108 Diagnostics

The table below gives a definition for all of the fields in the Diagnostics window:

This Field...	Shows...
Firmware ID	ID indicating the type of firmware in the lock. Technical support personnel may ask you to provide this information.
Version	Version number of the lock's firmware. Technical support personnel may ask you to provide this information.
Diagnostics Code	Hexadecimal number indicating firmware conditions, such as firmware resets, that have occurred at the lock since the diagnostics code was last cleared. The code 0x00 means no conditions have occurred. To view the meaning of the code, click/tap the more button (...). The Diagnostics Code window shows each active diagnostics code and its meaning. Click/tap the close button (X) to close the window.
Online Mode	Whether the lock is under time zone control (Automatic) or set to a specific mode, such as Locked or Unlocked.
Use Count	Number of times access was granted since the use count was last reset.
Main Battery	Current power level of the lock's battery pack. No shading in the status bar indicates an Alarm condition. The batteries are dead and must be replaced. If the shading falls within the Warning range, the power level is 30% or lower. You should replace the batteries soon. If the shading falls within the Good range, the power level is between 30% and 100%.

Backup Battery	Current power level of the lock's coin cell battery, used to back up the lock's memory if the main battery pack dies or is disconnected. If the backup battery is Bad, you should replace it. Refer to the Electronic Stand-Alone Lock Service Manual and Keypad EZ Locks (T80935). **Note:** If using a Offline G or V lock with a UVC board, the backup battery is rechargeable and not replaceable.

Disconnect

1 To disconnect from the reader, go to the Diagnostics > Disconnect.

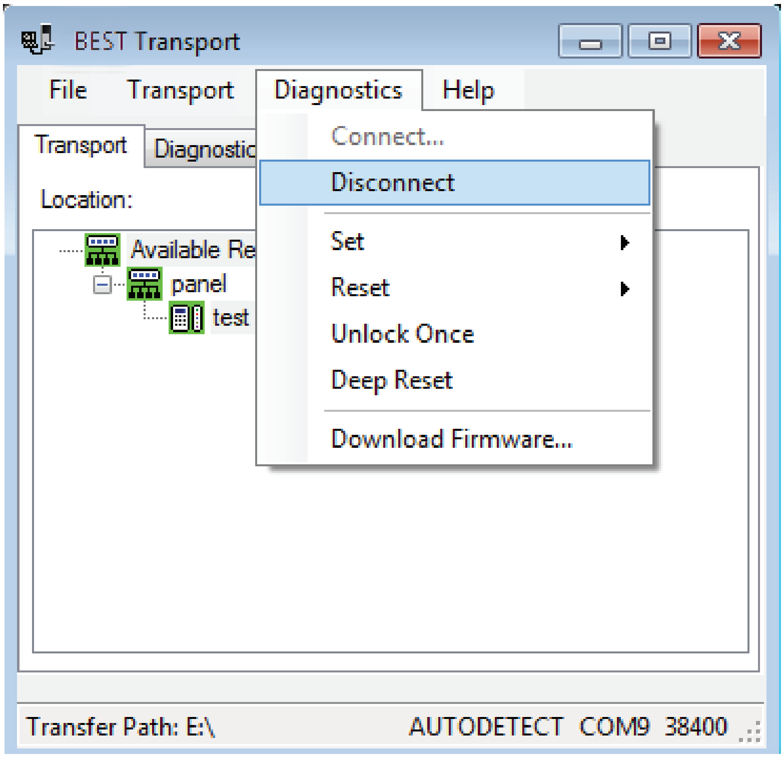


Figure 109 Diagnostic disconnect

Note The following diagnostic functions are performed while the Netbook/Notebook is already connected to the lock. You can exit diagnostics after performing any function by selecting Disconnect from the Diagnostic Menu.

Set

You have three options under the Set menu:

- Date/Time/DST enable
- Reader Technology
- Online Mode

Set: Date/Time/DST Enable

To set Day/Time to the current time, perform the following steps:

1 Select Diagnostics > Set > Date/Time/DST enable.

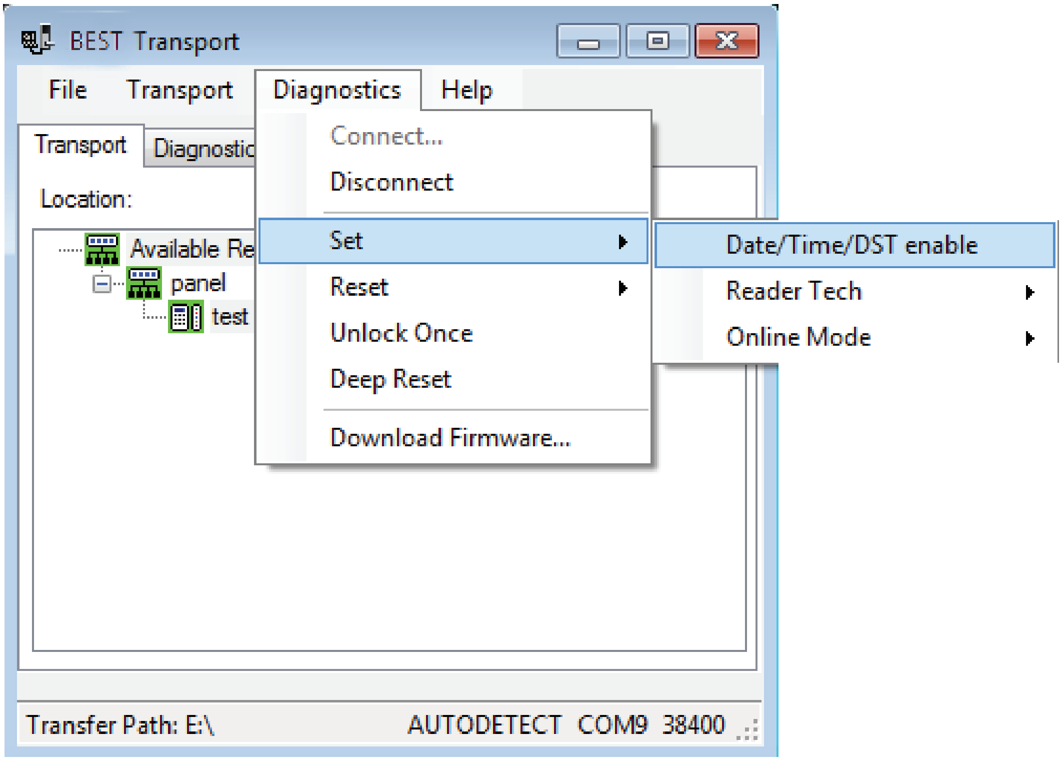
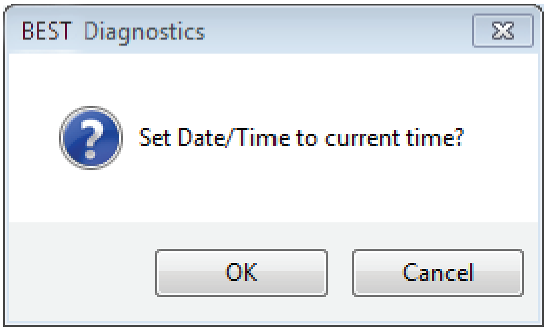


Figure 110 Date/Time


BEST Diagnostics

Set Date/Time to current time?

Figure 111 Set Date/Time

2 Click OK.

Set: Reader Technology

To set which reader technology the lock/reader is using, perform the following steps

1 Return to Diagnostics > Set > Reader Tech and select your choice of Proximity, Magnetic or Dual Val.

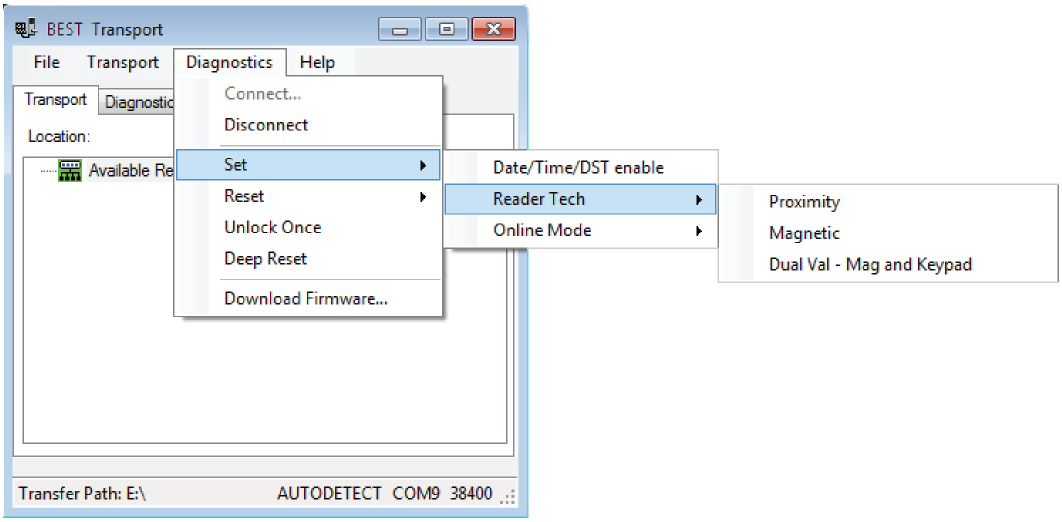


Figure 112 Set Reader Tech

Set: Online Mode

An offline lock mode of operation is determined by its programming. The diagnostics information for the lock indicates the locks current Online Mode setting.

For example, during an emergency you might set a lock’s online mode to Unlocked so that emergency personnel can access the room. When the event is over, you must return the lock to its original online mode setting to resume normal operation.

The online mode will change only after disconnecting from the lock.

The following online modes are available:

- **Automatic** — The lock is under time zone control.
- **Card** — Any valid card in the lock’s database can access the lock.
- **Card and PIN** — Any valid card and PIN combination programmed in the lock’s database can access the lock.
- **Card or PIN** — Any valid card or PIN programmed in the lock’s database can access the lock.
- **Facility Code** — Any card with a valid facility code can access the lock.
- **Locked** — The door is locked. All cards and PINs are denied access.
- **Unlocked** — The door is unlocked.

To override the current online mode of the reader, perform the following steps:

1 Return to Diagnostics > Set > Online Mode and select your choice of Automatic, Card, Card and PIN, Card or PIN, Facility Code, Locked, or Unlocked.

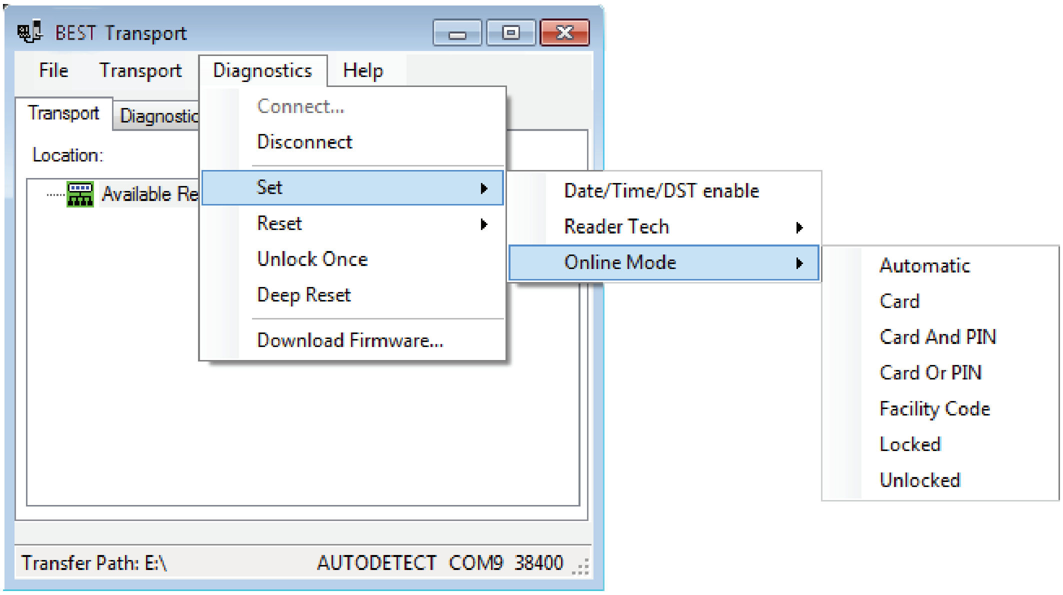


Figure 113 Online Mode options

Reset

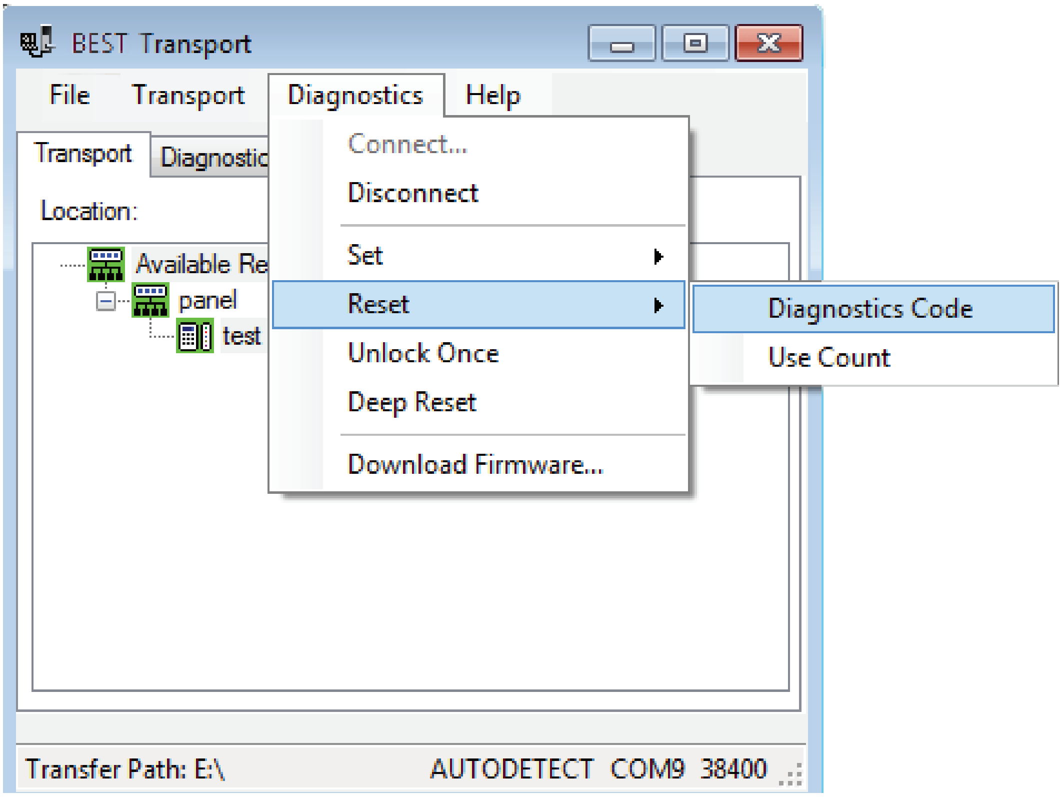
You have two options under the Reset menu:

- Diagnostics Code
- Use Count

Reset: Diagnostics Code

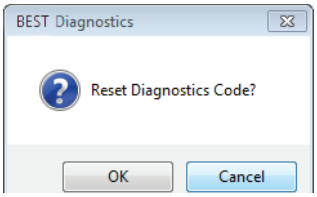
Diagnostic codes are used to help identify issues with the lock, such as low battery alarms that might have occurred since the diagnostics code was last cleared. Perform the following steps:

1 Return to Diagnostics > Reset > Diagnostics Code.



Transfer Path: E:\ AUTODETECT COM9 38400

Figure 114 Reset Diagnostics Code



Reset Diagnostics Code?

Figure 115 Reset Diagnostics Code

2 Click OK and the code will be reset to 0x0000.

Reset: Use Count

Every offline reader counts the number of times access has been granted to a card or pin since the use count was last reset. You can use this count to track how often a lock is accessed over time. Perform the following steps:

1 Return to Diagnostics > Reset > Use Count.

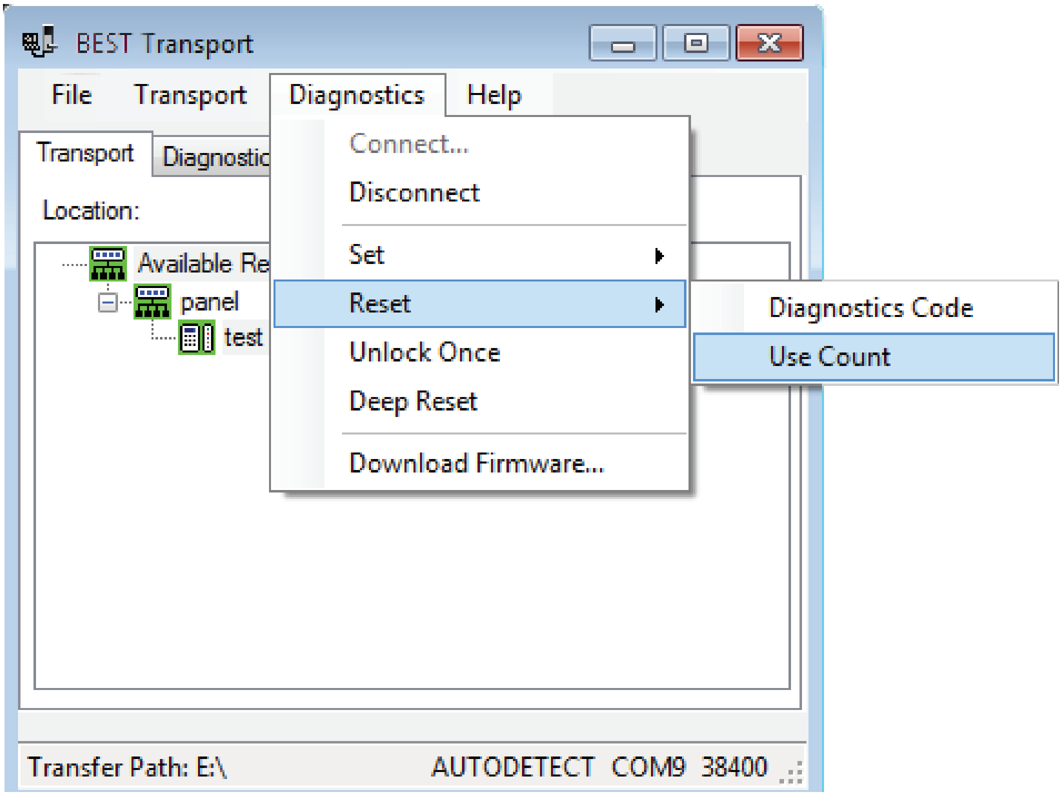
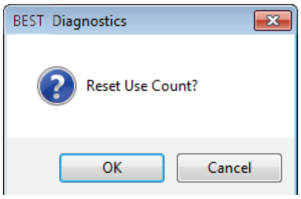


Figure 116 Reset Use Count



2 Click OK and the count will be reset to 0.

Unlock Once

You can use the Netbook/Notebook to unlock a door for the unlock duration programmed for a reader. This feature is useful when you need to access the inside of the door to replace the lock's batteries or perform other maintenance for the lock. Perform the following steps:

1 Go to Diagnostics > Unlock Once.

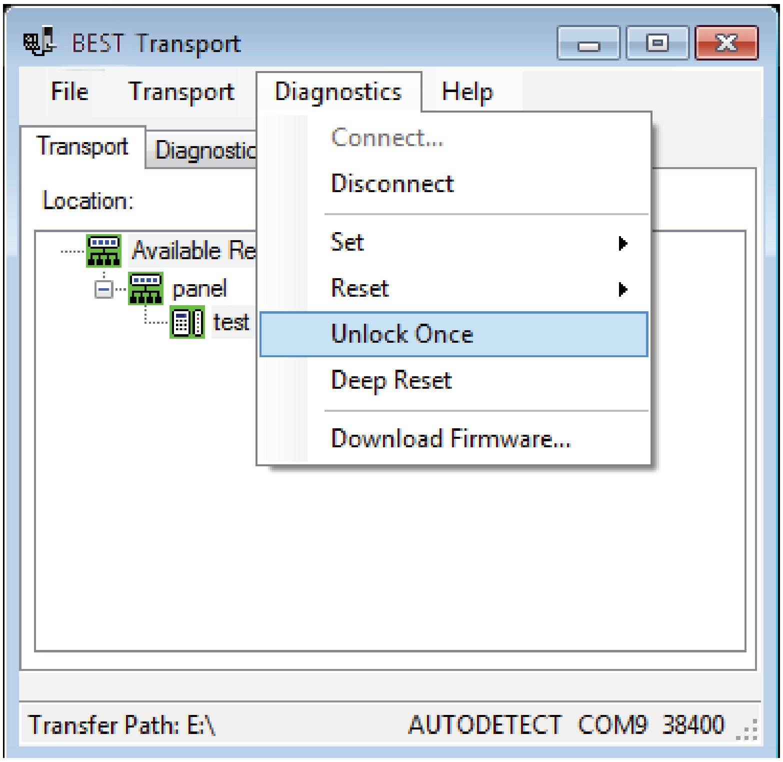
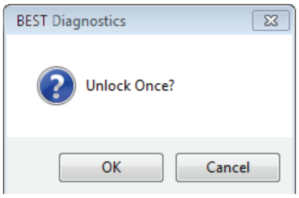


Figure 117 Unlock Once



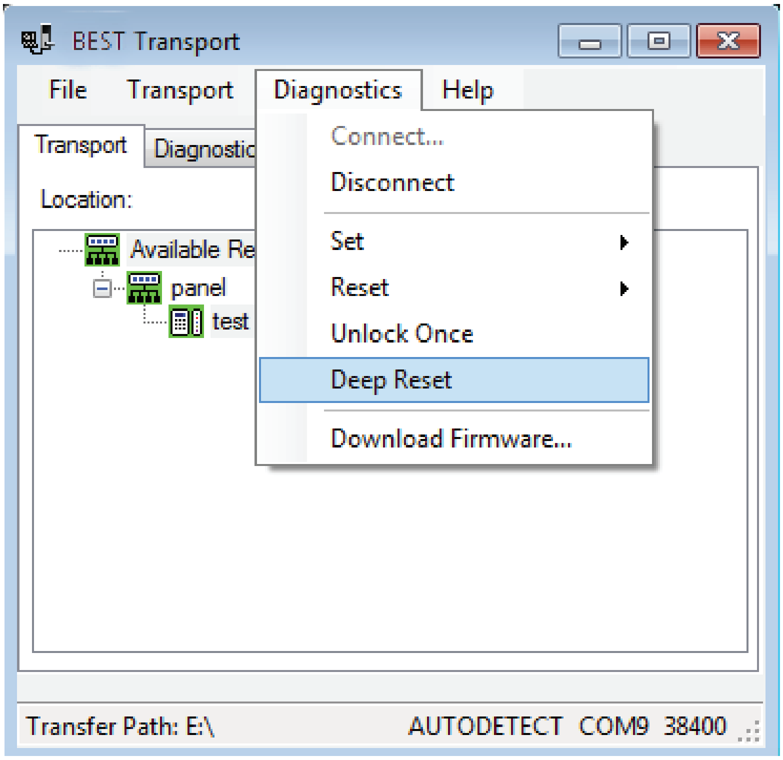
Unlock Once?

2 Click OK if you wish to unlock momentarily.

Deep Reset

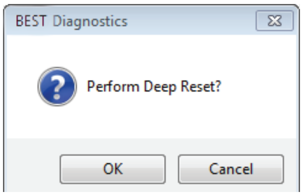
To reset the lock/reader to factory settings, perform the following steps:

1 Go to Diagnostics > Deep Reset.



Transfer Path: E:\ AUTODETECT COM9 38400

Figure 118 Deep Reset.



Perform Deep Reset?

2 Click OK to Deep Reset

Download Firmware

To download any Firmware updates to your Netbook/Notebook, perform the following steps:

Note A firmware download is only available if the lock is fitted with the UVC board.

1 Go to Diagnostics > Download Firmware.

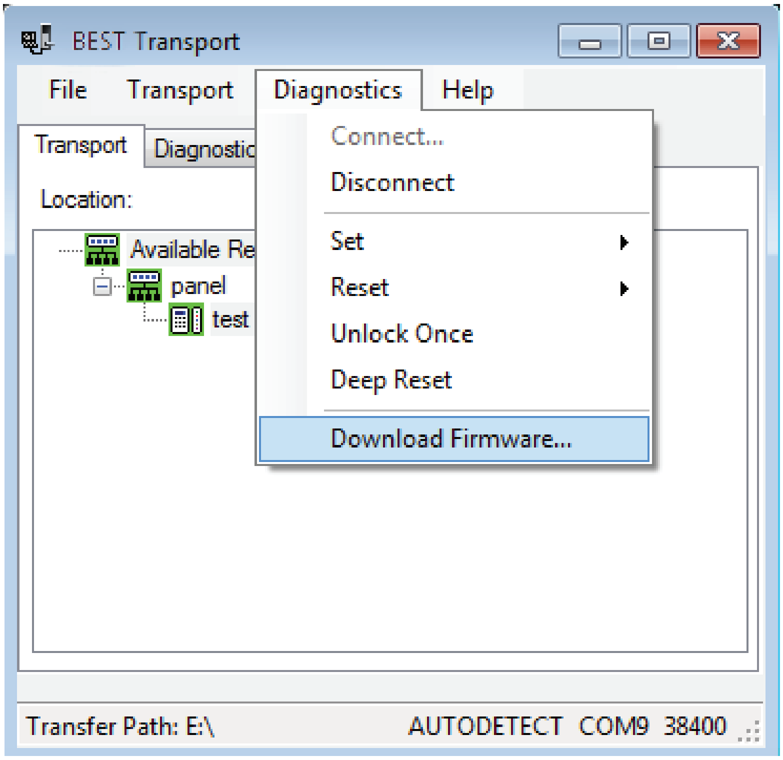


Figure 119 Download Firmware

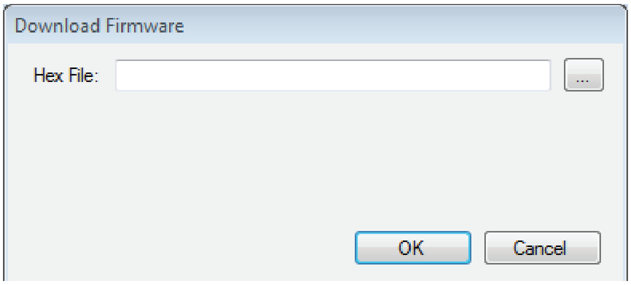
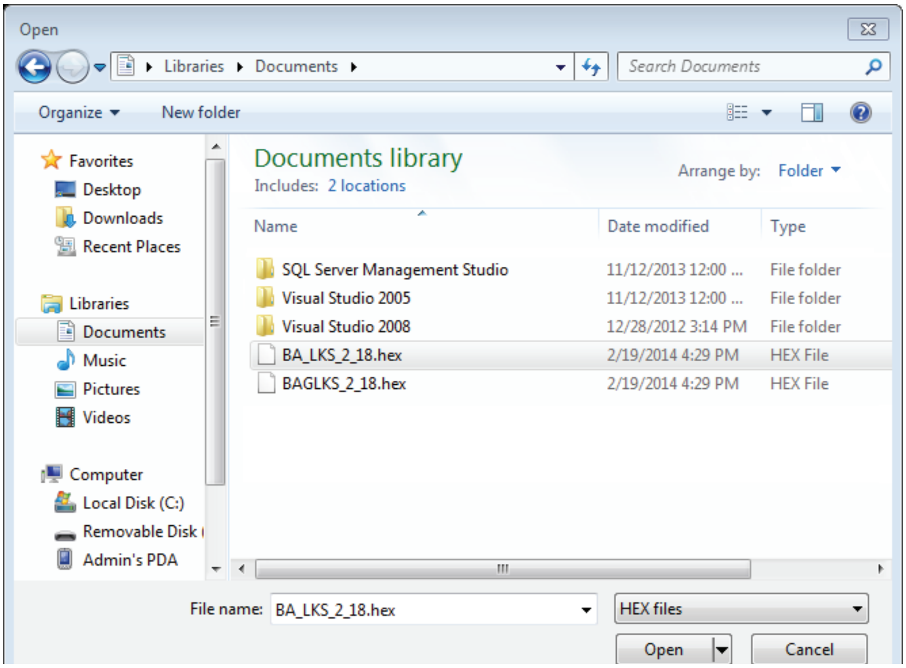


Figure 120 Hex file

2 Click on ... to browse for your firmware hex file.

Note Firmware files are available by contacting Technical Support at (800) 392-5209.



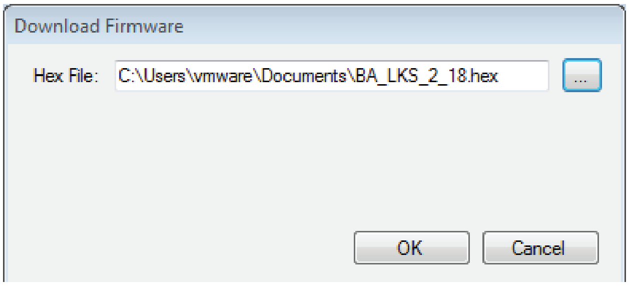
Name	Date modified	Type
SQL Server Management Studio	11/12/2013 12:00 ...	File folder
Visual Studio 2005	11/12/2013 12:00 ...	File folder
Visual Studio 2008	12/28/2012 3:14 PM	File folder
BA_LKS_2_18.hex	2/19/2014 4:29 PM	HEX File
BAGLKS_2_18.hex	2/19/2014 4:29 PM	HEX File

File name: BA_LKS_2_18.hex

HEX files

Figure 121 Open hex file

3 Select your Hex file and Click Open.

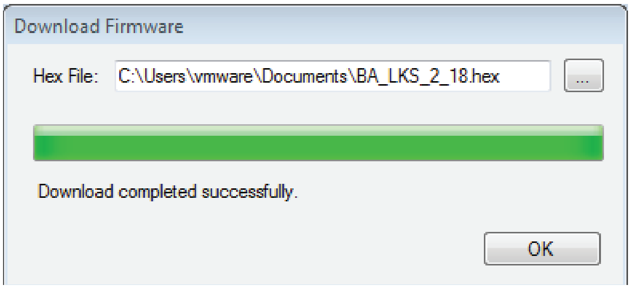


Hex File: C:\Users\vmware\Documents\BA_LKS_2_18.hex

Figure 122 Hex file

4 Click OK and the download will begin.

5 Once the download has completed, you should hear the reader make three beep sounds. This confirms that the reader has restarted to complete the Firmware download.



C:\Users\vmware\Documents\BA_LKS_2_18.hex

Download completed successfully.

Figure 123 Download completed successfully

6 Click OK to exit.

To Manually Change the PIN in a Dual Validation Lock

You can change your PIN only during a time period when both your card and PIN are required to unlock the door.

Warning: Do not write your PIN on your card or in a place where someone might see it.

1 Use your card at the lock.

2 From the lock keypad, immediately enter:

   * + your current PIN + #

   The red light remains on, indicating that you can change your PIN.

3 Immediately enter:

   your new PIN + #

4 Immediately re-enter:

   your new PIN + #

   The green light flashes to indicate that you successfully changed your PIN.

Note If you make a mistake re-entering your new PIN, three short tones sound and the red light turns off. Start over with step 1 and use your old PIN for step 2.

Example of changing your PIN

1 Use your card.

2 Enter * 1 2 3 4 #

3 Enter * 4 3 2 1 #

4 Re-enter * 4 3 2 1 #

Note If pin changes happen at the door for UVC users and a cardholder download is pushed, the pins are overwrittten by pins pushed during the download.

4 Managing Offline Locks Cardholders

Managing cardholders involves three activities:

- Creating cardholders
- Searching for cardholders
- Encoding cardholders’ badges

These activities form the bulk of day-to-day operations that are necessary to administer Offline locks. This section describes these activities.

Creating Cardholders

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

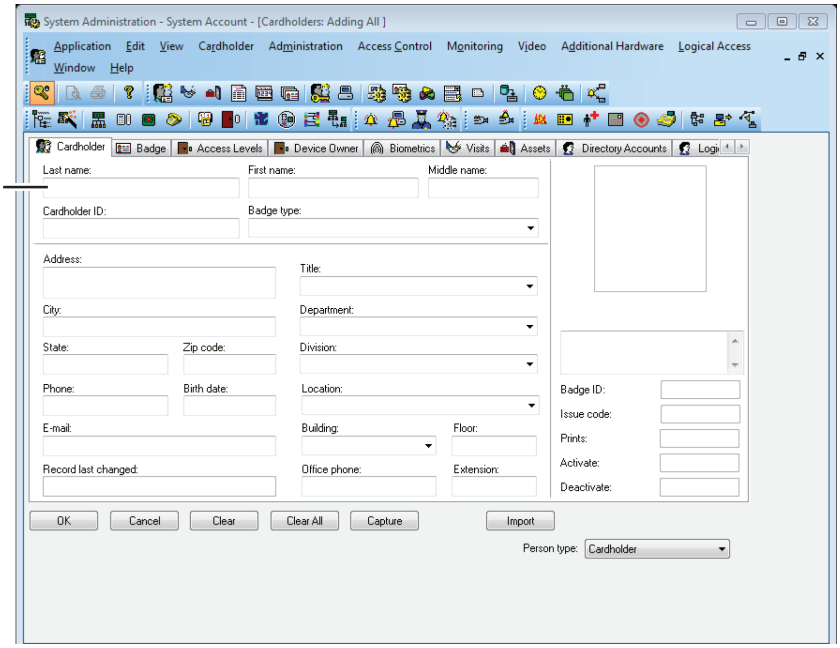
- Adding
- Modifying

To Create a Cardholder:

1 From System Administration, click Administration > Cardholders.

2 Click Add.

The Add Cardholders window displays



At a minimum, complete Last name, First name, and select a Badge type.

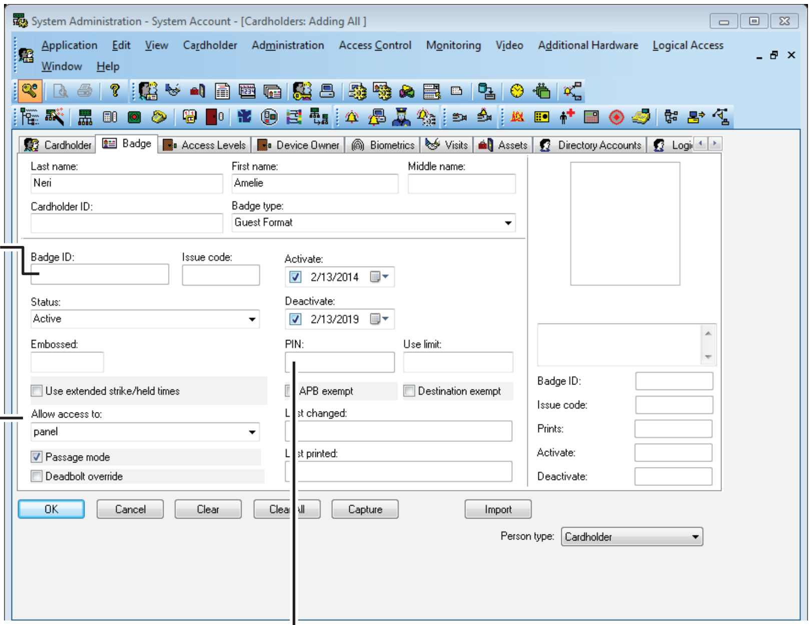
Figure 124 Adding cardholders

3 Complete all appropriate fields in the form.

4 Click the Badge tab.

The badge form displays:

Offline V locks: enter the badge number in the Badge ID field.
Offline G locks: select a reader from the Allow access to: field.



Last name: Neri
First name: Amelie
Middle name:
Cardholder ID:
Badge type: Guest Format
Badge ID:
Issue code:
Activate: ☑ 2/13/2014
Status: Active
Deactivate: ☑ 2/13/2019
Embossed:
PIN:
Use limit:
□ Use extended strike/held times
□ APB exempt
□ Destination exempt
Allow access to: panel
Last changed:
☑ Passage mode
□ Deadbolt override
Last printed:
Badge ID:
Issue code:
Prints:
Activate:
Deactivate:
Person type: Cardholder

The PIN field can be used with dual validation (magstripe/keypad) locks to allow access.

Figure 125 Badge Form

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

6 Click OK.

7 To encode the cardholders badge, see “Encoding Existing Cardholders” on page 90.

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.

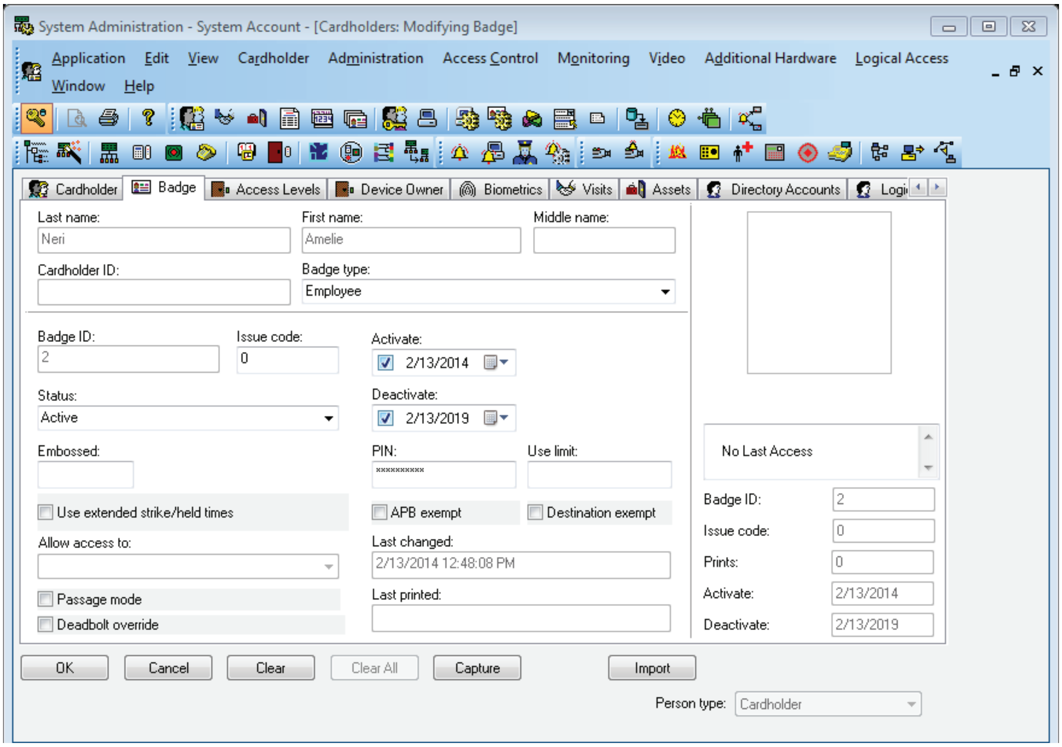
To Modify a Cardholder

1 From System Administration, click Administration > Cardholders.

2 Search for the cardholder record that you want to modify.

3 Click Modify.

The Modify Cardholders window displays



Last name: Neri

First name: Amelie

Middle name:

Cardholder ID:

Badge type: Employee

Badge ID: 2

Issue code: 0

Activate: ☑ 2/13/2014

Deactivate: ☑ 2/13/2019

Status: Active

Embossed:

PIN: **********

Use limit:

□ Use extended strike/held times

□ APB exempt

□ Destination exempt

Allow access to:

Last changed: 2/13/2014 12:48:08 PM

Last printed:

□ Passage mode

□ Deadbolt override

No Last Access

Badge ID: 2

Issue code: 0

Prints: 0

Activate: 2/13/2014

Deactivate: 2/13/2019

Person type: Cardholder

Figure 126 Modifying cardholders

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

5 Click OK.

Note: Modify mode will only allow you to make changes to the specific tab that you selected Modify in. Complete all necessary changes before selecting other tabs to be modified.

Searching for Cardholders

The search module of Offline Locks 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
- checking the status of a cardholder
- inquiring about 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.

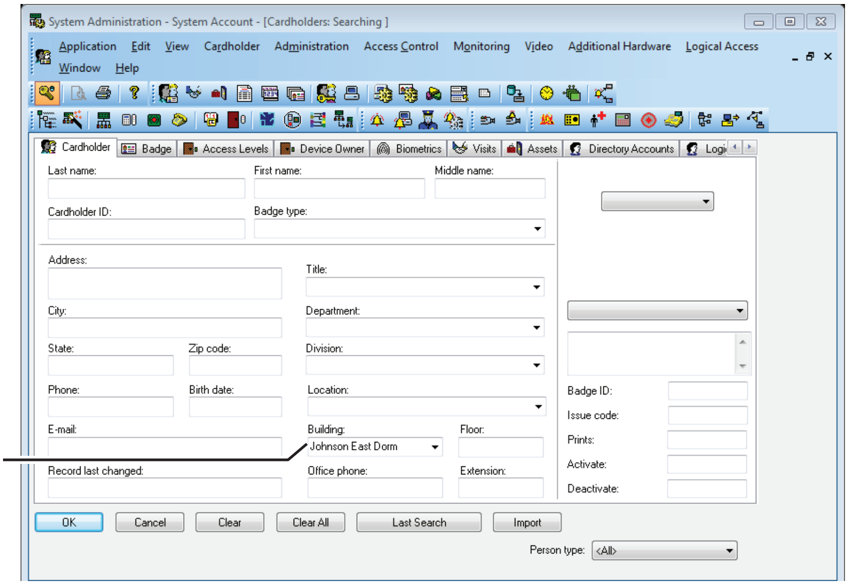
The Cardholder fields are cleared

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 groups of cardholder records are displayed, you can page through the records one by one.

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

4 “Select and complete at least one field to search on.” For example, to search for all students in the Johnson East dormitory, the following screen shows the required data selection:



Building: Johnson East Dorm

Person type: <All>

Searching specifically for rstudents of Johnson East Dormitory.

Figure 127 Example of searching for all Johnson East, dormitory students

5 Click OK.

The search arrows appear in the lower right-hand corner of the screen.

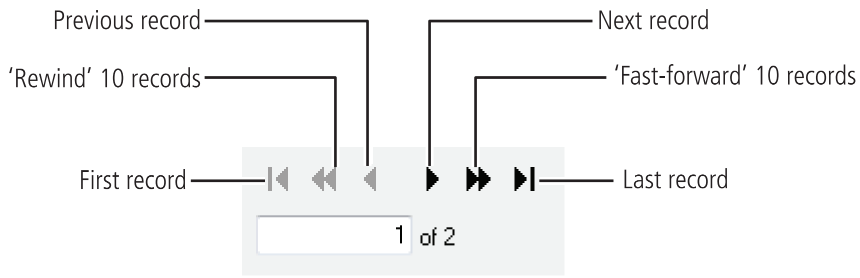


Figure 128 Search arrow definitions

6 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.

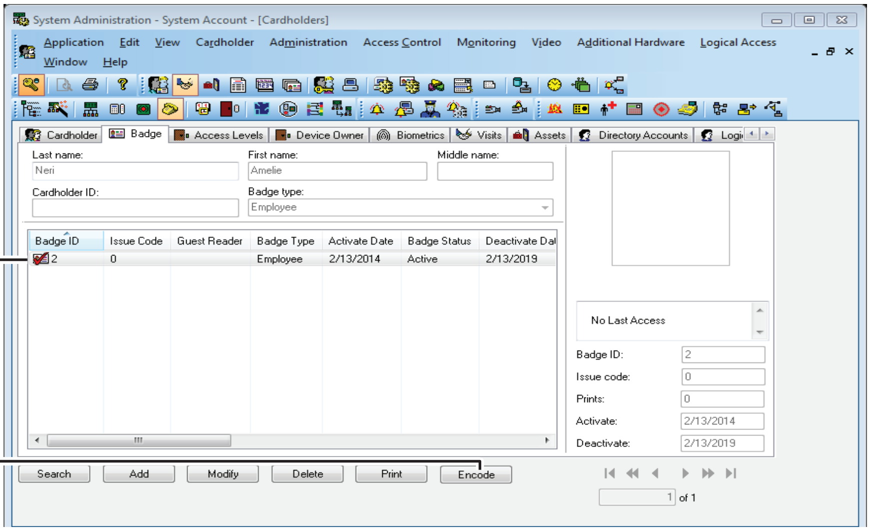
To encode an existing cardholder's badge

1 From System Administration, click Administration > Cardholders.

2 Click the Badge tab.

3 Search for the cardholder record that you want to encode. For more information on searching, see page 88.

The Encode badge form displays:


System Administration - System Account - [Cardholders]
Application Edit View Cardholder Administration Access Control Monitoring Video Additional Hardware Logical Access
Window Help
Cardholder
Badge
Access Levels
Device Owner
Biometrics
Visits
Assets
Directory Accounts
Logi
Search
Add
Modify
Delete
Print
Encode
1 of 1

Last name: Neri

First name: Amelie

Middle name:

Cardholder ID:

Badge type: Employee

Badge ID	Issue Code	Guest Reader	Badge Type	Activate Date	Badge Status	Deactivate Dat
✓ 2	0		Employee	2/13/2014	Active	2/13/2019

No Last Access

Badge ID: 2

Issue code: 0

Prints: 0

Activate: 2/13/2014

Deactivate: 2/13/2019

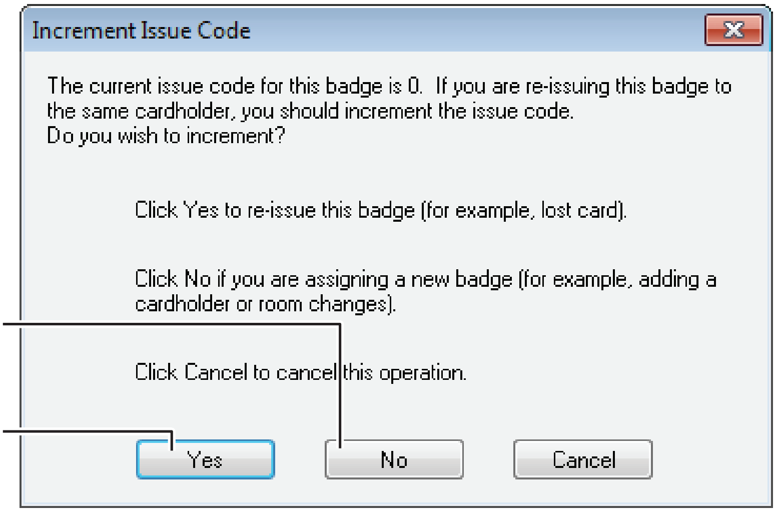
Make sure that a check-mark selects the cardholder record to be enclosed

The encode button is available when a guest badge is selected.

Figure 129 Getting ready to encode a guest badge

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

5 Click Encode.


Increment Issue Code

The current issue code for this badge is 0. If you are re-issuing this badge to the same cardholder, you should increment the issue code.
Do you wish to increment?

Click Yes to re-issue this badge (for example, lost card).

Click No if you are assigning a new badge (for example, adding a cardholder or room changes).

Click Cancel to cancel this operation.

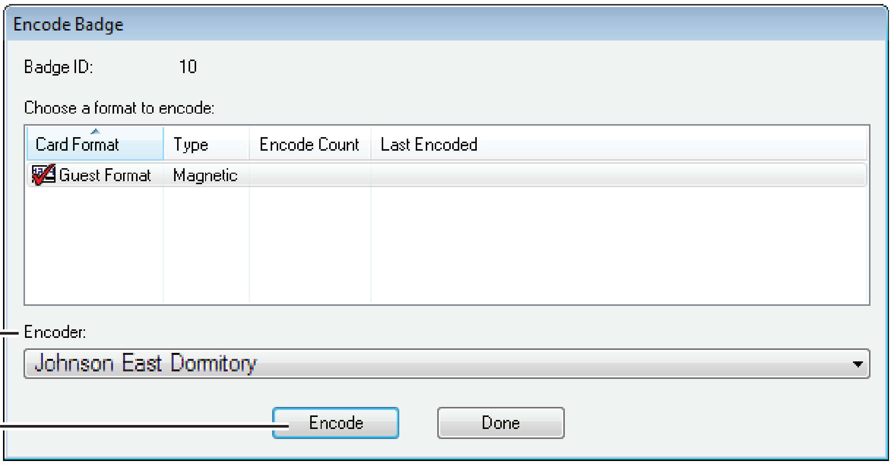
Click No, if you are assigning a new badge.

Click Yes, if the card is lost or stolen.

Figure 130 Question regarding the issue code

6 Click No.

The Encode Badge window displays:


Encode Badge

Badge ID: 10

Choose a format to encode:

Card Format	Type	Encode Count	Last Encoded
☑ Guest Format	Magnetic		

Encoder: Johnson East Dormitory

Choose the encoder.

Click the Encode button to start the encoding process.

Figure 131 Choosing a card format to encode

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

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

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

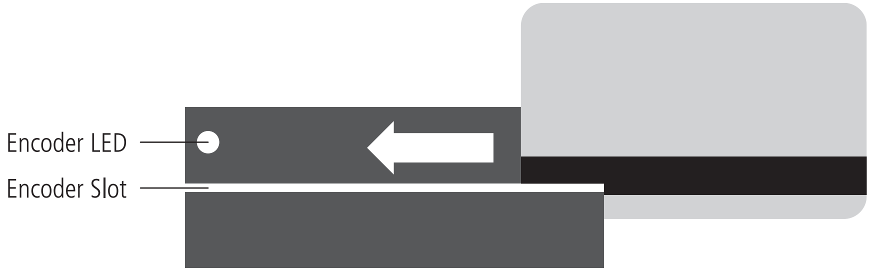


Figure 132 Swiping the magstripe card through the encoder

Glossary

access level An access control relationship made between a reader or readers and a time zone or time zones. 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 A circuit board with on-board memory that is responsible for making most of the decisions in an access control system.

activation/deactivation date The date that a credential becomes active or expires.

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 to 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 token. This information, usually numerical, is unique to a particular credential holder.

badge type Used in Offline Locks 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.

BEST Transport The application that runs on a Netbook/Notebook designed to update Offline locks and retrieve lock history.

battery alarm The diagnostic code that an Offline Lock displays when the main batteries are low.

battery warning The diagnostic code that BEST Transport displays when the main batteries must be replaced.

card format The way that data is arranged and ordered on the card.

cardholder An individual who is issued a particular credential.

chassis type The designation that defines the physical lock type. Three types exist: cylindrical, mortise, or exit hardware. See those terms for more information.

communication server The server application designed to provide network services to access panels, readers, and PCs.

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

cylindrical Lock chassis that installs into a circular bore in the door.

deadbolt override The ability for an authorized credential to retract both the spring latch and the deadbolt when the dead bolt is engaged.

diagnostic code The code in BEST Transport that identifies the processing error.

encoder The device, connected to a PC running Offline Locks, used to encode magnetic stripe cards or smart cards.

ethernet The most common networking standard in the world, formally known as IEEE 802.3.

exit hardware Lock chassis type that supports exit hardware trim lock.

extended unlock The extra period of time the lock will unlock 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 organization.

guest 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.

IP address The numeric address (like 192.168.1.1) that identifies each device in a TCP/IP network. input A hardware connection point used for status reporting of a particular sensor.

input A hardware connection point used for status reporting of a particular sensor.

intelligent system controller (ISC) See access panel.

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.

look ahead 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.

mortise A lock chassis that installs into a mortised cavity in the edge of a door.

netbook/notebook A small laptop computer that is designed primarily for accessing Internet-based applications.

output An Offline Locks on-board relay or switch that is configurable to follow the status of an input, system condition, or a time zone.

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..

programming cable The cable used to connect the mobile device to the Offline Lock.

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.

request to exit A sensor usually installed on the non-secure side of the door that will mask the door position switch upon activation.

time interval A specific range of time, which corresponds to a particular day or days of the week. A time zone can be comprised of several, individual intervals.

timezone A defined range of time for assignment to various access control activities. A time zone 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 The time that the lock momentarily unlocks.

use limit A configuration limiting a credential to a defined number of uses.