



BEYOND SECURITY

KABA[®]

E-Plex[®] Enterprise Software (Version 3.1) User Guide

Fourth Edition (for V3.1):	March 2013
Third Edition (for V3.0):	May 2011
Second Edition (for V2.x):	December 2010
First Edition (for V1.x):	August 2009

The *E-Plex Enterprise System Software User Guide* is a publication of Kaba Access and Data Systems.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without prior written permission from Kaba Access Control.

The information contained in this publication is accurate to the best of Kaba Access Control's knowledge. Specifications are subject to change without notice.

Trademarks

The following items are trademarks or registered trademarks of Kaba Ilco in the United States and/or other countries.

E-Plex

LectroBolt

Technical Support

Please call Kaba Access Control's Technical Support phone line at (800) 849-8324 or (336) 725-1331 between 8:00 a.m. and 5:00 p.m., Monday through Friday (except holidays), Eastern Standard Time.



Kaba Access Control
2941 Indiana Avenue
Winston-Salem, NC 27105
Phone: (800) 849-8324 or (336) 725-1331
Fax: (800) 346-9640 or (336) 725-3269
www.kabaaccess.com

Document: **PKG 3288 0313**

© 2013 Kaba

Table of Contents

1	About the E-Plex Enterprise	1-1
	System Components	1-3
	For Wireless Enabled Lock Systems Only	1-3
	E-Plex “Enterprise” Locks	1-4
	PINs, Tokens and Token/Card Enrollers	1-5
	E-Plex Enterprise Software (Server and Client modules)	1-6
	Portable PC M-Unit (Netbook/Laptop) and PC M-Unit Software	1-6
	System Definitions	1-7
	Host PC System Operator Classifications	1-8
	Operator Rights when Wireless Configuration is Enabled	1-8
	Door Groups & Doors.....	1-9
	Access Schedules.....	1-9
	Holiday/Vacations	1-10
	Access Groups.....	1-10
	Lock User Personnel Classifications – Departments & Users	1-11
	The E-Plex Enterprise Software Packages	1-12
2	Getting Started	2-13
	E-Plex Enterprise System Requirements.....	2-14
	Additional Requirements for Wireless Lock System	2-15
	Basic System Setup & Quick Start Tips	2-15
	[Software Installation & Registration – described in Appendix].....	2-15
	Quick Start Tips.....	2-16
	Starting the E-Plex Enterprise Software on a Standalone PC	2-17
	Main Menu and Toolbar	2-20
	Main Menu	2-21
	Toolbar	2-22
	Online ZigBee (wireless) Network.....	2-25
3	Using the E-Plex Enterprise Software.....	3-1
	System Setup Menu	3-2
	Changing Systems Settings.....	3-2
	Changing Systems Settings – for Wireless.....	3-4
	Managing Operators (Add/Modify/Delete)	3-9
	Database Management (Backup/Restore).....	3-13
	Managing Schedules.....	3-16
	Adding a Schedule	3-17
	Editing a Schedule	3-18
	Deleting a Schedule.....	3-19
	Managing Holidays/Vacations.....	3-21
	Adding a Holiday/Vacation.....	3-22
	Editing a Holiday/Vacation	3-23
	Deleting a Holiday/Vacation.....	3-24

Managing Online ZigBee Network	3-26
Discover Device.....	3-27
Configuring an E-Plex Gateway	3-27
Configuring an E-Plex Router.....	3-34
Enable E-Plex Gateway to “Join On” Mode.....	3-36
Disable E-Plex Gateway from “Join On” to “Join Off” Mode.....	3-38
Configure Previously Configured Gateway(s) or Router(s).....	3-38
Managing Door Groups.....	3-40
Adding a Door Group.....	3-41
Editing a Door Group.....	3-44
Managing Door Group Managers	3-45
Deleting a Door Group.....	3-45
Managing Doors.....	3-47
Adding a Door [Standalone / Non-wireless]	3-48
Adding a Door [Wireless].....	3-54
Editing a Door	3-58
Deleting a Door.....	3-59
Managing Access Groups.....	3-61
Adding an Access Group.....	3-61
Editing an Access Group	3-64
Deleting an Access Group.....	3-68
Managing Departments.....	3-69
Adding a Department.....	3-69
Editing a Department.....	3-70
Deleting a Department.....	3-71
Managing Users.....	3-73
Adding a User.....	3-74
Both Prox and Smartcard Enrollment	3-77
Batch Enrollment (without an Enroller).....	3-80
Reading a User’s Card	3-82
Editing a User.....	3-84
Deleting a User.....	3-85
Managing Access Assignment.....	3-86
Assigning Users to Lock with Privileges	3-86
Importing Users.....	3-91
Viewing/Printing/Exporting Reports	3-95
Viewing Reports.....	3-95
Printing Reports.....	3-97
Exporting Reports	3-97
Access schedules Report	3-99
Holidays/Vacations Report	3-100
Audits from Downloaded Door.....	3-101
Cards Status Report	3-102
Door Groups Report	3-103
Doors Report	3-104
Doors for a User Report	3-105
Access Groups with Doors Info Report	3-106
Access Groups with Users Info Report.....	3-106
Operators Report.....	3-107

Systems Activity Log Report	3-108
Departments Report	3-109
Users Report	3-109
Users for a Door Report	3-110
Users without an Active Card Report	3-111
(Wireless) Lock Status Report	3-112
Offline Wireless Locks Report	3-112
Wireless Network Map Report	3-113
4 Operating the E-Plex Lock at its Keypad	4-1
Overview of the Lock	4-2
States of the Lock	4-2
Battery Life and Replacement	4-3
Sequence of Operations	4-4
Configuring the Lock Functions	4-4
Default Values of the E-Plex Lock Programmable Parameters	4-5
Initial Programming of the Lock	4-5
Entering Pushbutton Programming Mode	4-5
Modifying the Master User PIN	4-6
Additional Pushbutton Keypad Commands	4-7
Resetting the Lock	4-9
Performing ZAC (ZigBee Access Code) Operation on Lock	4-10
Activate/Deactivate Emergency Lockdown	4-10
Put Lock back in Normal State from Emergency State	4-10
Activate/Deactivate Emergency Passage	4-10
Summary of Pushbutton Programming Commands	4-11
Visual Feedback Message Definitions	4-12
5 Programming and Auditing Locks	5-1
M-Unit User Definition	5-1
Portable PC M-Unit with Kaba's IrDA Kit	5-2
PC M-Unit Software Installation	5-4
Manual PC/M-Unit Sync (Data Transfer with PC M-Unit via a USB flash drive)	5-8
Automatic PC/M-Unit Sync (Data Transfer within the same "Integrated" Laptop PC which acts as both Host PC & PC M-Unit)	5-9
Wireless Data Transfer between Host PC and Locks via Gateway(s) and Router(s)	5-11
Commissioning of a Wireless Lock	5-11
Remote Control & Maintenance of a Wireless Lock	5-14
Scheduled Auto Programming of Wireless Locks	5-17
Emergency Lockdown & Emergency Passage of Wireless Lock(s)	5-17
Initiating Emergency Commands via a Wireless Lock's Keypad	5-22

6 Appendix: Software Installation.....	6-1
Software Registration and Licensing	6-2
Software Registration.....	6-2
Option 1: Standalone/Express Installation.....	6-6
Option 2: Server/Client Networked Installation	6-14
Server PC related Installation	6-15
Client PC(s) related Installation including PC M-Unit	6-15

1

About the E-Plex Enterprise

All E-Plex Wireless Locks & System related info are highlighted in this turquoise color background for easy reference.

The **E-Plex lock series** that can be operated by the Enterprise 3.0 software system are the following lock series, plus all their wireless twins with the Wireless option installed:

E3200, E5200 & E5200 SAC (Standalone Access Controller):

PIN based Single credential locks,

E3700, E5700, & E5700 SAC

PIN & Prox card based (125 KHz RFID) Dual credential locks,

E3600, E5600, & E5600 SAC:

PIN & Smart card based (ISO 14443A/B 13.56 MHz RFID)
Dual credential locks.

Important: If you have already used the E-Plex Enterprise 1.x or 2.x software and its compliant E-Plex locks in your facility, you will find the 3.x software version to be almost exactly the same, if the locks are not wireless. In this case, you can skip all wireless related features in this manual. However, if you have the wireless E-Plex locks, and/or a mix of non-wireless and wireless locks in your facility, you must read and use all wireless related features described in this manual.

The E5x00 lock series are “standard” door locks for regular doors and the E3x00 lock series are the “narrow stile” locks, which are designed to be installed typically on a narrow door frame, such as the frame encompassing an aluminum glass door.

Each above lock model is designed to control entry or access to an area or premises through one or more of three ways, depending of the model -> by PIN only access, by presentation of a Prox or a Smart ID card (contactless), or by PIN followed by the presentation of the ID card.

The contactless **Prox RFID** card must be an HID compatible card with its card number data format ranging between the "Standard" Wiegand 26 bits, and from the non-standard 27 through 84 bits. The Enterprise software is designed to read the Card Number (Facility code + card ID) of the Prox card if it is a standard 26 bit wiegand format card.

The contactless **Smart RFID** card can be either, an industry standard (i) a Mifare card, (ii) a DESFire card, or (iii) an HID iClass card. The Enterprise software is designed to read only the Card Serial Number (CSN) of the Mifare and the DESFire cards, and only the unique ID of the HID iClass card contained within its application ID field.

The above different lock models are designed to work in conjunction with the E-Plex Enterprise system software along with the use of a mini Laptop (Netbook) PC with an IrDa (Infra-Red) communications interface to program and audit the lock. You can also use the same laptop where the main Enterprise applications software is installed to do the lock programming and auditing functions, instead of a separate Netbook PC.

"LearnLok" Option: All card ID based lock series such as the E3600, E3700, E5600, E5600 SAC, E5700 and E5700 SAC can also be used without the Enterprise software, if desired by programming it right at the lock's keypad using Kaba's patented "LearnLok" feature.

Note 1: From now on in this manual, *when we refer to a "card", it means either a Prox based token or a Smart card based token such as Mifare, DESFire or iClass.*

Note 2: *Also, from now on the portable mini Laptop/Netbook PC that is used as a lock programming & auditing device will be referred to as the M-Unit (Maintenance Unit) because its primary function is to perform lock <-> PC data transfer maintenance. This is required only for all non-wireless E-Plex locks.*

The items explained in this chapter include the following:

System Components

System Definitions

The E-Plex Enterprise Software Package

System Components

The E-Plex Enterprise system contains the following system components:

- E-Plex Enterprise compliant locks and controllers and also their wireless twins: E3200, E3600, E3700, E5200, E5200 SAC, E5600, E5600 SAC, E5700 and E5700 SAC.
- For Prox card based locks: HID compliant Prox card tokens (125 KHz RFID) and a Prox card enroller
- For Smart card based locks: Smart card compliant tokens (13.56 MHz RFID) and a Smart card enroller
- Microsoft OS compatible PC running the E-Plex Enterprise system software
- Mini Laptop / Netbook portable PC to run E-Plex Enterprise M-Unit software, mandatory for all non-wireless locks (but not needed for wireless locks). The M-Unit device will be capable communicating with the lock via Kaba's IrDa Communications Interface kit.

[Start]

- **For Wireless Enabled Lock Systems Only:** Kaba's wireless *E-Plex Gateway*, minimum one Gateway unit is required. Optionally you may also require one or more wireless *E-Plex Routers* – the quantities will be based on your facility's requirement after your site survey. The Gateway and the Router are actually the same hardware unit, but will be configured either as a Gateway or as a *Router* in the Enterprise software during initial setup.

E-Plex Gateway / Router unit with Front & one Side view:



USB Cable between Host PC & Gateway/Router

AC Adapter of Gateway/Router



Type-A Type Mini-B

[Type-A to Host PC and Mini-B to Gateway/Router] [5 VDC /300mA minimum, w/ Mini-B]

Important: You must first complete a **wireless site survey** to install the E-Plex **wireless locks** in your facility using Kaba's "**Wireless E-Plex Lock Site Survey Guide**".

[End]

E-Plex “Enterprise” Locks

The above mentioned E-Plex Enterprise compliant locks can be operated by the Enterprise software. The standalone battery operated lock will grant access if an authorized user presents one of the three valid credentials at the lock front housing: PIN only, or Card only or PIN followed by Card. The lock can store up to 3,000 unique users who can be mix of regular Access users, Manager users, Guest users, Service users and M-Unit users. There is one (and only one) global Master User per lock. The lock can store the last 30,000 transactions (audited events) in the lock’s memory.

Lock Modes

You can access the E-Plex lock by one of the following four modes at a given time:

Default Factory Mode – The lock is shipped from the factory in Default Factory Mode with a default factory Master PIN. In this mode, the lock can only be opened with the Default Factory Master User PIN of “12345678” and no other PIN or Card credential will be recognized by the lock as valid.

Access Mode by “LearnLok” – This mode refers to the lock that is operational for user access after the factory default Master PIN of 12345678 is changed to something else. When the lock enters the LearnLok Access Mode, the Master (and Manager users) can add or delete regular users in the lock simply by entering relevant command codes at the lock keypad. Please refer to the “**E-Plex Card Based 36xx/37xx/56xx/57xx Lock Series Operations Manual**” for details.

Access Mode by Software – This mode refers to a lock that is operational for user access, after it is programmed, (i) either by the portable M-Unit for non-wireless locks, or (ii) after it is programmed remotely from the Host/Client PC via wireless commands for wireless enabled locks. “Lock programming” here means that the lock/user configuration data is downloaded from the E-Plex Enterprise system software to the lock. When the lock enters the Software Access Mode, the method of lock access is either by, (i) PIN only, or by (ii) Card only, or by (iii) PIN followed by the associated Card. Note: The Service users can have PIN only access any time and no cards are associated with them.

Pushbutton Programming Mode – This mode is typically used to program or audit the lock using the M-Unit handheld device. In this mode, the Master User, or the Manager(s), or the M-Unit User(s) can enter one or more command sequences to program and configure the lock, or download the lock audits.

For more information about using the lock in these modes, refer to **States of the Lock** in Chapter 4, **Operating the E-Plex Lock at its Keypad**.

Lock Access Methods

You can open a lock using one of the following three access credential methods. For Service users only, the access method is by PIN only access; for the rest of the User types, it can be either PIN only, or Card only or PIN & Card access, depending on the specific Access Schedule set during that time. You can set up the lock with specific access schedules for each day, for example PIN only access during morning shift; PIN & Card access during evening shift etc so as to require different access credential methods for users.

PIN Only

Only entering of a valid PIN (Personal Identity Number) is required to access the lock.

Important: The global user PIN length is configurable from 4 to 8 digits, but the first 4 digits *must be* unique for security reasons.

Card Only

Only the presentation of a valid Card is required to access the lock.

PIN and Card

The entry of a valid PIN followed by the presentation of a valid associated ID Card is required to access the lock. The access method through PIN and Card is referred to as “Dual Credential” access.

PINs, Tokens and Token/Card Enrollers

An authorized E-Plex Enterprise system Operator must enroll all users in the system database who need to access the E-Plex locks in the facility. The operator must enter the name etc for each enrolled user and assign a PIN which is automatically generated by the system but can be modified manually by the operator. Additionally, the operator must also enroll a valid token for the user if s/he will require access to a token based lock such as an E3600, E3700, E5600, E3600 SAC, E5700 and/or an E3700 SAC, for either wireless or non-wireless models. This is done by using a Card Enroller/Reader – there is one specific model to enroll Prox ID based tokens and another specific model for Smart ID based tokens, depending on your lock models in your facility.

Important: In a few cases where your facility is migrating from one token (and lock) type to another type, for example, from legacy Prox cards to more secure Mifare/DESFire/iClass Smart cards, you will need to use both types of card Enrollers with the Enterprise software system until the migration from legacy to new cards (and locks) is complete.

The enroller is connected to the PC via the USB port interface. The enroller simply reads the card ID data from the token and this ID is assigned to this user in the system. Both enrollers are read-only type enroller and so no writing is performed on the card.

Token Types: ***For Prox-> Card, Tag or FOB; For Smart-> Card, Tag or Key***

The user ID tokens that can be used in the applicable E-Plex locks come in various forms as shown below. It can be either in a “card” form, or in a “FOB” form that can be carried in a key-ring. It can be also in the form of a 25 cent coin (mini disc) called a “Tag”; this can be affixed to an existing non Prox or non Smartcard ID badge of a user with picture so as to work in the E-Plex card locks.



HID Prox compliant Tokens



Smart compliant Tokens (Ex: iClass)

The use of a Prox enroller for Prox token based locks and a Smart card enroller for Smart token based locks are mandatory (see below) for all token based E-Plex locks. As specified earlier, the Smart token or card can be either a Mifare, or a DESFire or an iClass.

The enroller only reads, either (i) the pre-encoded Prox user card number data from the token, or (ii) the pre-encoded Smart user card Serial Number (CSN) data from the token and stores it the system software. An authorized user with a valid ID (the above enrolled user ID)

► *About the E-Plex Enterprise*

will be granted access in all the programmed Prox card and/or Smart card based lock(s) in the facility. The following two pictures show the Prox and the Smart token enrollers that are used in the E-Plex Enterprise system with their USB connectors.



“RFIdeas” HID Prox compliant Enroller



“RFIdeas” Smartcard compliant Enroller

For the reading (enrolling) of a token, you just need to place the token on top of the enroller for a second or so. The small red light on the enroller will turn green momentarily indicating a successful read. The ID data will be read by the enroller and transferred to the E-Plex Enterprise and stored in the database instantly. The example shown here is for the Prox token enroller; it will be the same procedure for the Smart token based enroller.



E-Plex Enterprise Software (Server and Client modules)

The E-Plex Enterprise software when installed allows you to manage your door locks and the associated user data from one standalone PC. It also offers auditing and reporting capabilities. The software consists of the “Server” and the “Client” parts/modules which can both be installed on a single Standalone PC along with the SQL server database.

Optionally, you can install the server related modules and the SQL database on a separate Server PC only, and then install the Client related modules on one or more individual Client PCs in a networked configuration. In this networked configuration, you must have the right card enroller connected to each client PCs if you use card/token based E-Plex locks.

Portable PC M-Unit (Netbook/Laptop) and PC M-Unit Software

The E-Plex “universal” PC M-Unit software is installed on either, (i) the same PC where the main Enterprise applications software is installed or (ii) on a separate mini Laptop / Netbook PC. In either case, the M-Unit software will work in conjunction with **Kaba’s PC M-Unit IrDa Communications Kit** to program and audit the locks.

This portable PC M-Unit device, in addition to letting you program and audit the lock, allows for the downloading of Users/Locks configuration data from the PC to the M-Unit, and also the uploading of the lock audits data from the M-Unit back to the PC for Reports at the PC.

[Start]-----

For Wireless: As stated earlier, the portable M-Unit is not required for programming and/or auditing a wireless lock since these operations are performed remotely via wireless communications. However, if for some reason your wireless network is down, you will either need to ensure that it has come back “online” before programming/auditing the wireless locks remotely, or must use a portable PC M-Unit with its software to program/audit the wireless locks that are currently in “offline” mode.

[End]-----

System Definitions

This section contains system definitions for the following items:

PC System Operator Classifications

Door Groups and Doors

Access Schedules

Holidays/Vacations

Access Groups

Lock User Personnel Classifications (Departments & Users)

Host PC System Operator Classifications

- Three types of operators can use and operate the E-Plex Enterprise software:

Operator Rights when Wireless Option is Not Enabled:

Level 1 Operator – The software system can have up to 255 Level 1 Operators. The global Master user of the system will automatically become the very first Level 1 Operator. All Level 1 Operators will have the highest system authorization and will have access to all operational functions of the E-Plex Enterprise software. Any Manager user can also be assigned as Level 1 Operator (or as Level 2 but not as Level 3).

The Level 1 Operator can add Level 2 or Level 3 Operators to the Enterprise system. The Level 1 Operator can add a maximum of 255 Level 2 and Level 3 Operators combined to the system. When a Level 2 or Level 3 Operator is added to the system, this Operator's Logon Name and Password must also be established.

Level 2 Operator – Can be a maximum of 255. Level 2 Operators can perform all functions of Level 1 Operators, with the exception of the following:

- Adding, modifying, or deleting any other operators
- Adding, modifying, or deleting any managers
- Modifying the site's software "Private ID"
- Will not be able to view any user's access PIN

Level 3 Operator – Can be a maximum of 255. Level 3 Operators can be M-Unit and/or Access users only and can perform all functions of Level 1 Operators, with the exception of the following:

- Adding, modifying, or deleting any other operators
- Adding, modifying, or deleting any managers
- Modifying the site's software "Private ID"
- Will not be able to view any user's access PIN
- Cannot perform a system database restore operation
- Can only change her/his own Password in the *System Setup*.

Note 1: An M-Unit user can be assigned only as a Level 3 Operator; this user cannot login to the E-Plex Enterprise (Client) software but can login to the PC M-Unit software to program/audit locks.

Note 2: An Access user can be only a Level 3 Operator; s/he can login to the Enterprise software but cannot perform any M-Unit software functions to program/audit locks.

Note 3: The Guest and Service users cannot be assigned any Operator status – Level 3, 2 or 1.

[Start]-----

Operator Rights when Wireless Configuration is Enabled:

- **Level 1: (Same rights as in non-wireless Client above), plus**
 - Can wirelessly Activate/Deactivate Global Emergency Lockdown, or Global Emergency Passage/Open of all locks (or locks selected by Door Groups) on the site,
 - Can perform a wireless remote unlock of one individual lock at a time,
 - Can "Page" a lock,

- Can wirelessly Activate/Deactivate Passage mode of one individual lock at a time, but only if this Level 1 operator has already been programmed in this lock as a user, &
 - Can wirelessly Activate/Deactivate the Lockdown of one individual lock at a time, but only if this Level 1 operator has already been programmed in this lock as a user.
- **Level 2: (Same rights as in non-wireless Client above), plus**
 - Can wirelessly Activate/Deactivate Global Emergency Lockdown, or Global Emergency Passage/Open of all locks (or locks selected by Door Groups) on the site, only if configured in Systems Settings to allow,
 - Can perform a wireless remote unlock of one individual lock at a time,
 - Can “Page” a lock, and
 - Can wirelessly Activate/Deactivate Passage mode of one individual lock at a time, but only if this Level 1 operator has already been programmed in this lock as a user.
 - **Level 3: (Same rights as in non-wireless Client above), plus**
 - Can wirelessly Activate only Global Emergency Lockdown, or Global Emergency Passage/Open of all locks (or locks selected by Door Groups) on the site, only if configured in System Settings granting these rights,
 - Can perform a wireless remote unlock of one individual lock at a time,

[End]-----

Door Groups & Doors

You can define up to a maximum combination of 10,000 door groups and doors in the system database. A door group represents a group of physical doors that contain the E-Plex locks operated by the Enterprise system. For example you can have a couple of door groups called “DG-Factory” and “DG-Offices”, each containing many doors (locks) belonging to them.

For Wireless Mix: If your facility has a **mix of** both non-wireless (standalone) and **wireless** E-Plex locks, it is highly recommended that you place these two types of lock series in two different main Door Groups. For example, one main group called “DG-Wireless” where you place all your wireless locks and the other one called “DG-NonWireless” where you place all your non-wireless locks. This segmentation makes it easier to manage the two different mixes of lock types.

In each door group, you must assign one (and only one) Door Group (DG) Manager user. However you can assign many regular Manager users to each door group. The DG Manager will have complete access to all the doors in this door group without any restrictions. This is very similar to the global Master user having complete access to all the door groups and doors in the facility, the difference here being that this DG Manager will have complete access only to her/his doors in this door group rather than the doors in the entire facility.

Access Schedules

You can define an unlimited amount of access schedules in the system database. However, you can define only up to 16 access schedules in a lock. When assigning access schedules to a user, you may only use the access schedules that have been assigned to the lock. There is a default access schedule, “Always” (24 hours per day, seven days per week), that is built into the system software and cannot be changed or deleted.

An access schedule is a defined time period during the span of a week during which users are granted access to a door. Operators using the E-Plex Enterprise software at the PC define the access schedules by selecting the days of the week that the schedule is active and by specifying the schedule’s start time and end time for the days specified. You can define a descriptive schedule name for each access schedule. Once defined, you can assign access

schedules to a door with what credential type to use (PIN, card or PIN & card) during that schedule in the **Manage Doors** menu of the software dialog. A maximum of 16 access schedules can be assigned to a single door.

Because you may specify whether the door access credential method is either PIN only, Card only or PIN followed by Card, the different access schedules in the system cannot overlap.

If you have a need for periods of time where access for certain groups of users overlaps partially, you will need to break those time periods into separate access schedules. Also, an access schedule cannot bridge a time period between two consecutive days. If you have an access schedule that needs to start before midnight and end after midnight, you must set this up as two separate access schedules.

Example

During the week, say you have three shifts at your company:

First Shift – 7:00 a.m. to 3:00 p.m.

Second Shift – 2:00 p.m. to 11:00 p.m.

Third Shift – 10:00 p.m. to 8:00 a.m.

These three shifts will need to be broken into seven access schedules so they do not overlap:

7:00 a.m. to 2:00 p.m. – First shift

2:00 p.m. to 3:00 p.m. – First and second shift overlap

3:00 p.m. to 10:00 p.m. – Second shift

10:00 p.m. to 11:00 p.m.– Second and third shift overlap

11:00 p.m. to 12:00 a.m. – First part of third shift (first day)

12:00 a.m. to 7:00 a.m. – Second part of third shift (next day)

7:00 a.m. to 8:00 a.m. – Third and first shift overlap

By default, all user types (except the global Master user) are not assigned any access to the lock. These user types include the Manager users, the Access users, the Guest users and the Service users. One or more of the access schedules must be assigned to these user types who must have access to the affected doors/locks .

Choose from access schedules that have been previously defined for the door, which means that the maximum number of access schedules that can be assigned to a user for a particular door is the number of access schedules defined for the door, up to 16.

Holidays/Vacations

You can define an unlimited amount of holidays/vacations in the system database. However, you can define only up to 32 holidays/vacations in a lock.

A holiday/vacation template is a defined time period during which users will NOT be granted access to a door. By default, there will be no access allowed to a door/lock during a defined holiday/vacation period, except for the global Master user and all Manager user(s) of the system. The Access, Guest and Service Users who are assigned a “privilege” in the software to override the holidays/vacations will also have access during the holiday/vacation period.

Access Groups

An Access Group is setup when you define a collection of doors WITH an Access Schedule assigned AND an access credential method during this schedule (PIN only, card only or PIN

& card access) to each one of these doors. This makes it easy when the operator wants to add a new user in the system database that should have access to many doors at various schedules very quickly, saving enormous keyboard entry time.

Lock User Personnel Classifications – Departments & Users

- In addition to the Master, up to five different types of users can perform various operations at the lock – both at the pushbutton keypad of the non-wireless and the wireless locks. For wireless enabled locks, there are certain additional operations that the Manager and Access users can perform as stated separately below.

Master User – The Master User is the top-level user who performs the initial lock setup activities and can program all lock functions. There is only one (global) Master User per facility (all door groups and all doors) whose credential will be accepted in all locks in the entire facility. The Master User is the only user who has “Always” access to any lock, and has all the access privileges all the time and cannot be locked out. The global Master user’s credential acts just like an emergency mechanical override key. The Master User’s PIN is always eight digits in length.

Manager & Door Group (DG) Manager Users – A regular Manager User is a second-tier administrator who can program most of the lock functions as the Master user and these are specified in a Table in *Chapter 4*, the “*Summary of Pushbutton Programming Commands*” at the lock keypad. A lock can have up to 3,000 Manager Users.

The Door Group (DG) Manager on the other hand is just like the global Master user, except that her/his credential is always valid without any restrictions only in the doors belonging to her/his Door Group. All locks/doors belonging to a Door Group must contain one and only one Door Group (DG) Manager, though you can have multiple regular Manager users in the same door group.

Manager, when Programmed in one or more Wireless Locks on-site: If this Manager user is also either a Level-1 or Level-2 type Operator in the system software, s/he can perform a Global Emergency Lockdown or a Global Passage of all these wireless locks at the lock keypad. However, these commands can only be returned back to normal (cancelled) by Level 1 or 2 Operators using the system software.

Access User – An Access User has only the ability to open locks. Each lock may have up to 3,000 Access Users and these are considered permanent users.

Access, when Programmed in one or more Wireless Locks on-site: If this Access user is also a Level-3 type Operator in the system software, s/he can perform a Global Emergency Lockdown or a Global Passage of all these wireless locks at the lock keypad; but cannot cancel these commands.

Guest – A Guest user is just like an Access user, except the maximum expiry for a Guest user is one year. Each lock may have up to 3,000 Guest Users, which are temporary and last between 1 day and 365 days (1 year).

Service User – The Service user’s credential is always PIN only. A Service User has authorization any time of day to a lock for a specified period of time -> either one-time entry (“one shot”) only; or from 1 hour to 96 hours access only from the first time s/he presents the credential; or can have 24/7 access with no expiry, thus enabling the service user to gain entry just with PIN only access, even during a card only or PIN & card access schedule period in the lock, overriding any schedules assigned to the door.

M-Unit User – An M-Unit User does not have access to open any locks. The M-Unit User can only perform maintenance on locks using the portable M-Unit handheld, as well as any lock programming and auditing. Each lock may have up to 3,000 M-Unit Users.

Note: All of the user types, including Manager Users, can have one or all of the following three privileges:

-
- *Override holidays/vacations*
 - *Override deadbolt privacy*
 - *First entry passage authorization*
-

The E-Plex Enterprise Software Packages

There are three (3) software packages/kits available from Kaba to be used with the E-Plex Enterprise system as described below:

(1) **Kit #1: E-Plex Enterprise Software CD Kit**

This kit includes the following items:

- E-Plex Enterprise Software installation CD.*
- E-Plex Enterprise Getting Started Sheet.*
- E-Plex Enterprise Software User Guide (this guide) in electronic form on the CD.*

(2) **Kit #2: E-Plex Enterprise Implementation Kit**

- This package combines the *E-Plex Enterprise Software CD Kit (Kit #1)* above and the *E-Plex PC M-Unit Communications Kit (Kit #3)* below).
- Kit #2 is the only kit you will need to run the Enterprise software system in your facility. You need this whether your PC M-Unit part of software module runs on the same laptop PC where the main Enterprise applications software is also running or that you are planning to use a dedicated/separate Netbook/Min laptop PC to run the PC M-Unit software.

(3) **Kit #3: E-Plex PC M-Unit Communications Kit**

A Laptop or a Netbook PC does not have a built-in IrDA interface. This kit will provide that interface when connected to the M-Unit PC's USB port to "talk" to the lock via IrDa communications. This kit includes the following items:

- A USB Flash drive, pre-loaded with the *PC M-Unit Software* and the *PC M-Unit User Guide*.
- *E-Plex PC M-Unit Getting Started Sheet*.
- An IrDA-to-USB adapter and a USB extension cable.



USB Flash Drive with M-Unit Software



IrDA Adapter with extension Cable

2

Getting Started

All E-Plex Wireless Locks & System related info are highlighted in this turquoise color background for easy reference.

The contents of this chapter are intended to assist you with installing and setting up your E-Plex Enterprise system software.

The items explained in this chapter include the following:

- System Requirements
- Software Installation and Registration (via **Appendix**)
- Basic System Setup
- Starting the Software
- Main Menu Functions with Toolbar Icons

E-Plex Enterprise System Requirements

PC & OS Requirements

Standalone PC (for “Express” Install)

- MS Window’s compatible PC with minimum Pentium-III 500+MHz processor
- Minimum 1 GB of RAM.
- Minimum of 4 GB of free hard disc space when using smaller SQL database
- SVGA Monitor with minimum resolution of 1024 x 768
- CD-ROM drive for software installation
- Minimum of 2 USB ports in PC to connect the Prox Enroller and the M-Unit PDA
- One of the Microsoft Operating Systems below:
 - MS Windows XP Professional (SP 3 or higher),
 - MS Windows 7 Premium – 32 or 64 bit versions
 - MS Windows 8 – 32 or 64 bit versions
- MS SQL Express 2005 (SP3 or higher) or 2008 – supplied with Enterprise software

Networked PCs (for “Custom” Install)

- **Client PC:** Same requirements as Stand Alone PC above, except the MS SQL
- **Server PC:** Same requirements as Stand Alone above, except
 - Recommended 2+GB of RAM when using larger SQL database
 - Recommended 10+GB free hard disc space for larger SQL database
 - MS Windows Server 2003 & 2008 OS (if not using XP, VISTA or Windows 7)

Maintenance Unit (M-Unit) Requirements

- **Standard Laptop PC:** Same requirements as Standalone PC above, or
- **Mini Laptop (Netbook) PC:** Microsoft XP Home or higher OS and minimum 1MB of RAM, minimum 1024 x 600 screen resolution, 4GB of storage memory (flash or hard-drive), 1 available USB port. Optionally, wired or wireless LAN interface for network communications via IP address to host PC

Note 1: Either of the above M-Unit PCs requires Kaba’s **E-Plex PC M-Unit Communications Kit** as an accessory containing a USB Flash drive with PC M-Unit program pre-loaded & a USB <-> IrDa adaptor for PC to/from Lock communications.

For Wireless: If you have only wireless locks on your site, you do not need a portable M-Unit since the lock programming & auditing can be done remotely via wireless data transfer.

Card Enroller Requirement (**Mandatory* for card based E-Plex locks*)

- **RFIdeas pcProx** [RDR-6018KU, or BSE-PCPRX-U] 125 KHz HID Prox token Enroller with USB interface – to be used with E37xx and E57xx Prox card lock series, or/and
- **RFIdeas AIR ID** [RDR-7082AKU-KA] 13.56 MHz Smart token (Mifare, DESFire or iClass) Enroller with USB interface – to be used with E36xx & E56xx Smartcard lock series.

[Start]

Additional Requirements for Wireless Lock System

- **E-Plex Gateway** (mandatory; minimum one; more only if your Site Survey warrants it)
- **E-Plex Router** (optional; one or more, based on your Site Survey requirements)
- **Kaba's wireless Site Survey Unit (SSU)** – (required only during your Site Survey)

[End]

Basic System Setup & Quick Start Tips

Complete the following steps in this order prior to setting up the system for use:

Note: In this example, it is assumed that you will be using one standalone laptop to run the E-Plex Enterprise Server/Client applications software, and again use the same laptop to operate it as a portable M-Unit device to program/audit locks.

1. The actual **Software Installation section** is found at the very end of this manual under “**Appendix**”. Please continue to read this section and then jump to the *Appendix* section to actually install the applications software from the E-Plex Enterprise software CD on your laptop.
2. Ensure that you have the administrative rights to install the software on the PC. If you do not, you will require your IT personnel's help in installing the software. During installation, you will be required to register the E-Plex Enterprise software with Kaba so as to activate and use the software.
3. Connect your **Card ID Enroller** – Prox token based or Smart token based as appropriate, to the PC through a USB port. The enroller is plug-n-play and no driver installation is required.
4. **(Standalone) Express Installation:** For most situations, you will be installing the software (which consists of the Server, Client & M-Unit parts of the modules) on one standalone PC. Select the “Standalone / Express” install option which will automatically install all Enterprise software modules without any user/operator intervention, **OR**

(Custom) Network Installation: If on the other hand, you are going to be using a separate Server PC and one or more Client PCs in a networked environment, please check with your IT/Network Administrator for software installation rights, SQL password details etc. Typically, all Server related Prerequisites, followed by the Server part of the software module and the E-Plex SQL database module will need to be installed on the Server PC; you will be registering the software with Kaba during the Server part of the installation only, once. Then on each Client PC, you must install all Client related Prerequisites, the Client part and the M-Unit part of the software – as specified in the “(Software) Install Procedure” document on the CD. You must also connect a Card ID enroller to desired Client PC(s) to enroll your facility's user ID badges.

Software Installation & Registration

- Please refer to the **Appendix** at the end of this user guide on how to install the software. You will be also required to register the E-Plex Enterprise software with Kaba to receive the registration/activation key to be able to install and use the software.

Quick Start Tips

You can follow these useful tips to quickly set up and use the E-Plex Enterprise system and the associated E-Plex locks in your facility:

- Click the **E-Plex Enterprise Client** icon on your PC desktop to launch the software.

► *Getting Started*

1. Set up the global Master User for the application and if it is you, remember your new Level 1 Operator Name and Password for future login sessions. Change the default “Your Private ID” number from 99999999 to a different 8-digit number. This Private ID combined with an internal unique number in your software is used as your unique *Customer Security key*. This unique key is encrypted and passed back and forth between the PC software, the M-Unit and the locks during their data communications. Refer to **Logging On for the First Time** in this chapter for more information.
2. Change the default 8-digit Master PIN 12345678 (to be used in the locks by the global Master) to a different 8-digit Master PIN and remember this important PIN.
3. On the *System Setup* window, change any default parameters, such as all users’ PIN length, date/time format etc, if desired.
4. **[Start]**-----

For Wireless:

Enable the wireless communication/configuration option and configure all required wireless locks and ZigBee network related parameters for your facility. Only Kaba certified Access Control Dealers are eligible to enable the wireless configuration parameters by entering their Dealer ID.

Additionally, configure your *E-Plex Gateway* unit via USB connection with your Server PC (or Server/Client PC if they are on the same PC) so as to let all your wireless locks (doors) on your site to “join” this wireless ZigBee network when ready.

Important: Enabling the wireless option in the software can only be done by a Kaba certified access control Dealer/Integrator who has undergone Kaba’s E-Plex Wireless certification training with Kaba. The authorized Dealer/Integrator must enter her/his “Kaba authorized” Dealer ID & Activation key to get validated by the software which will then enable (turn on) the wireless option in the system.

[End]-----

5. Your unique 10-digit Software License number is displayed on the **Help | About** window. You will need to refer to this License number when contacting Kaba’s technical support team to receive any technical support.
6. Ensure that the card enroller is connected to your PC.

Migration from Prox to Smartcard: If your facility is migrating from an older Prox card technology to the newer, more secure Smart card technology, you will need to use both types of card enrollers to enroll these two different types of ID cards in the Enterprise system till the transition is complete.

7. Create your *Access Schedules* – assigning each schedule with period of time for each day when users should have entry access.
8. Optional: Create your *Holidays and Vacation blocks*.
9. Create your *Door Groups*.
10. Create your *Doors*, one door at a time – assigning each door with its various configuration parameters.

For Wireless: Configure additional required door parameters for wireless enabled doors.

11. Optional: Create your *Access Groups* – assigning each access group with door or doors with schedules attached to each door.
12. Create your *Departments* (referred to as *User Groups* in Enterprise 1.x software)).
13. Create your *Users*, one user at a time – assigning each user with various user parameters such as a PIN, user type etc and optionally import user’s photo. You will also need to enroll the user’s ID card, if this user will have access to any card based E-Plex locks in the facility.
14. For each user, you can also assign an Access Group, if you had already created a few access groups earlier, Or

Access Assignment: If you did not create any Access Groups in the system, you can assign the user to a door for access under the Access Assignment menu. Select a previously created door and assign schedules and access credential required (PIN only, card only or PIN & card) during each schedule, holidays/vacations and assign users for this door who should have access. Additionally, assign schedules to each user in this door including any user Privileges, if desired.

14. Repeat Steps 12 through 13 above for other users created in the system for door(s) access.

Important: Ensure that the actual E-Plex lock on the door to be programmed is properly installed and initialized and its Lock Function is configured (for Privacy and/or Residence locks only), according to the Lock Function Setup Instructions that came with the lock in the box.

For Wireless: Ensure that each wireless lock has its wireless hardware kit installed correctly onto the lock, that the RF antenna connection has been tested per the kit instructions, and that all wireless locks on the doors are installed properly.

15. *Transfer/download* your locks <-> users configuration data from the PC database to the *M-Unit* part of the database so as to be able to *program the locks* with the M-Unit.
16. Take the M-Unit (the same laptop or a separate Netbook PC) to each of the desired doors/locks and program them, one at a time. Repeat this step to program all locks in your facility.

For Wireless: Configure your E-Plex (ZigBee) wireless *Gateway* which will act as the main hub of your wireless network. Optionally, if required for your site, configure your wireless *Router(s)* which will act as Repeater(s).

Activate all your wireless locks, ie., make each wireless lock “Join” your ZigBee wireless network by entering a “ZigBee Access Code [ZAC]” at each lock’s keypad; the ZAC process will also automatically program the lock remotely. From now on, you can re-program the wireless locks anytime remotely from your Host PC without having to physically visit each wireless door/lock.

17. Similarly, you can go to the desired locations and *audit the required locks* in your facility for later uploading back to the PC for viewing/printing the lock audit Reports.

For Wireless: Audit the wireless locks remotely from your PC without having to physically visit each wireless lock (door). You will be also able to monitor all wireless lock and system events remotely from your Host PC in real time.

Starting E-Plex Enterprise Software on a Standalone PC (or, on a Client PC in Networked Configuration)

Note: Ensure that your applicable card ID enroller (Prox or/and Smartcard) is connected to your (Client) PC through the USB port and is recognized by the PC, if you will be using card based E-Plex locks on your site.

► Getting Started

You can start the E-Plex Enterprise on the PC by clicking the **E-Plex Enterprise** icon on the desktop.



Note: Do not delete the default desktop icon or modify it in any way.

Logging On for the First Time

When you have clicked the **E-Plex Enterprise (Client)** icon on the desktop for the very first time, the software displays the **Define First Master Operator** window as shown on the left hand side, below.

The screenshot shows the 'Define First Master Operator' window with the following fields and options:

- Site:** Site Name (empty), Site PrivateID: 99999999
- Site Credentials:** PIN Only (3200, 5200 locks), Prox Card (3700, 5700 locks), SmartCard (3600, 5600 locks)
- SmartCard Type:** (Dropdown menu)
- Master User:** Last Name (empty), First Name (empty), Master PIN: 12345678, Department: Global, User Type: Master
- Master Operator:** Operator Name (empty), Password (empty), Verity Password (empty), Operator Level: 1
- Prox Card Bit Format:** Standard Wiegand (26-Bit), Other
- Smart Card Bit Format:** Standard Wiegand (26-Bit), Other

Instructions at the bottom: "Enter a Name for your Site where the locks will be installed and used. Change the default site PrivateID 99999999 to a different 8-digit PrivateID and the factory default Master PIN 12345678 to a different 8-digit Master PIN. Enter an Operator Name (Login name) and Password. The password must be between 6 and 10 characters." Buttons: OK, Cancel.

The screenshot shows the 'Define First Master Operator' window with the following fields and options:

- Site:** Site Name: KabaAccessControl, Site PrivateID: 11111111
- Site Credentials:** PIN Only (3200, 5200 locks), Prox Card (3700, 5700 locks), SmartCard (3600, 5600 locks)
- SmartCard Type:** (Dropdown menu showing CLASS, MIFARE, DESFire)
- Master User:** Last Name: Thomas, First Name: Java, Master PIN: 87654321, Department: Global, User Type: Master
- Master Operator:** Operator Name: lico, Password: (masked), Verity Password: (masked), Operator Level: 1
- Prox Card Bit Format:** Standard Wiegand (26-Bit), Other
- Smart Card Bit Format:** Standard Wiegand (26-Bit), Other

Instructions at the bottom: "Enter a Name for your Site where the locks will be installed and used. Change the default site PrivateID 99999999 to a different 8-digit PrivateID and the factory default Master PIN 12345678 to a different 8-digit Master PIN. Enter an Operator Name (Login name) and Password. The password must be between 6 and 10 characters." Buttons: OK, Cancel.

- As shown in the picture on the right hand side, enter your **Site Name** (your company or facility name) which will be displayed on your system reports.
- Change the default “*Site Private ID*” value from 99999999 (ie., 8 nines) to any other number. The system will use this number in conjunction with a unique internal factory number to generate an encryption/decryption key in the database. This combined (but hidden) value will be your unique Customer Security Key which will be used in (i) protecting your Enterprise database, and (ii) in communicating lock/user configuration data between the PC, M-Unit and the E-Plex locks.
- Enter the following information in the **Master User** fields for the global Master user of all the locks in your facility:
 - Last Name
 - First Name
 - New Master PIN number – must be 8 digits long.

Note: The default factory Master PIN number is 12345678. You must change to a different 8-digit PIN number which you must enter and remember it (or write it down and store it in a safe place) for future routine use.

- Enter the following information in the **Master Operator** fields who will be the first Level-1 (highest) system administrator/operator to manage the Enterprise software system on the PC:

(Master) *Operator Name*: this is the Enterprise system's Login name – typically the Master (PC Login) operator in the system and the global Master user in the lock is one and the same person.

Important: The operator login name “kaba”, or “Kaba”, or “KABA” etc cannot be used; if you try to create this login name, you will get an error message.

Password: this must be minimum 6 alphanumeric characters

Verify Password by re-entering

Click **OK**. The software displays the Main Menu for the E-Plex Enterprise.

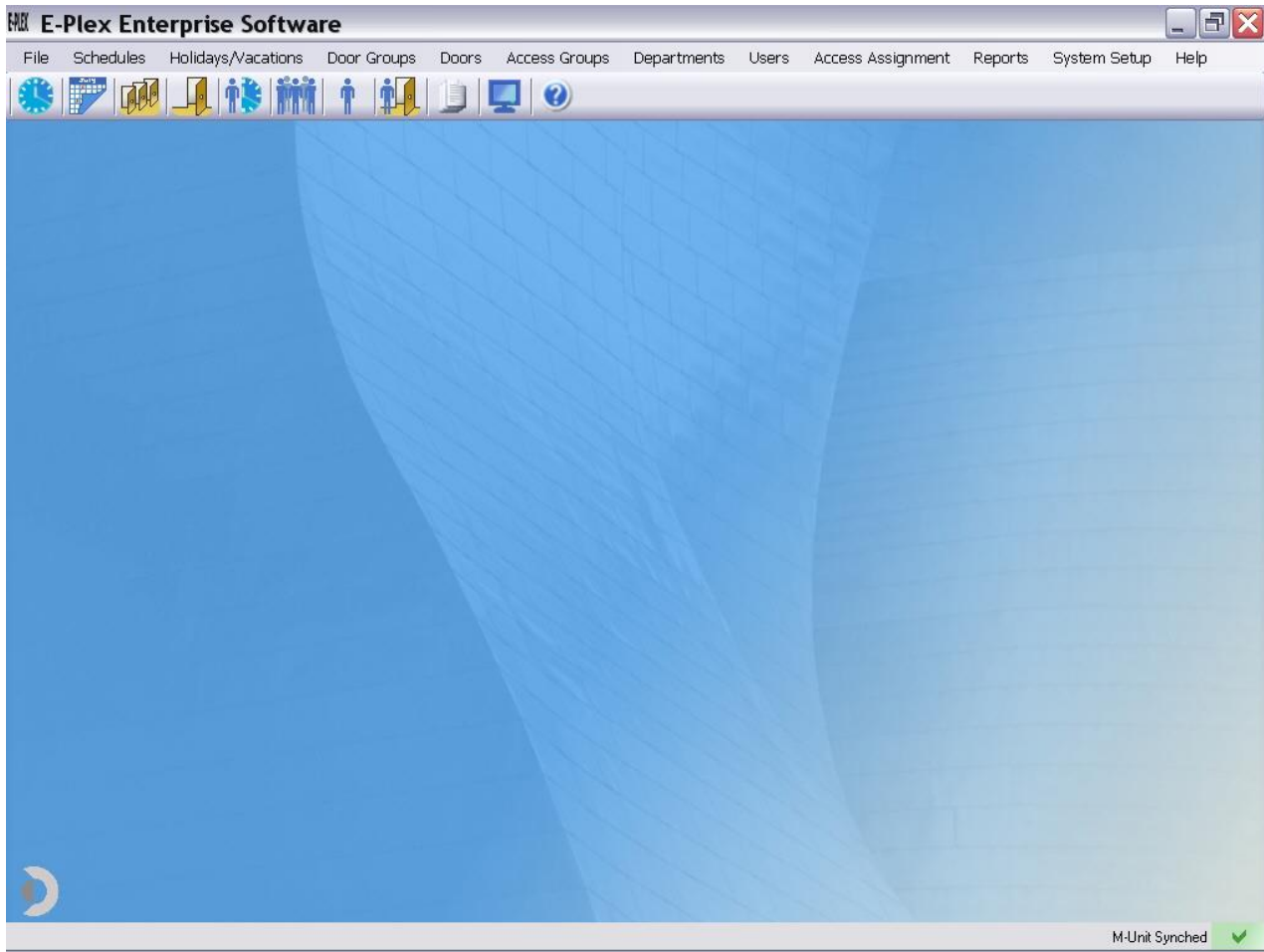
Note: From now on, must use this newly created logon credentials (operator name and password) to logon to the Enterprise software.

- Check the relevant box(es) for the **Site Credentials**; ie., what kind of E-Plex locks are being used in your facility. If you are going to be using PIN only lock series (E32xx and E52xx), you need to check that box only; no card credentials and relevant ID card enroller(s) are required.
- If you selected smartcard locks, you must also specify what type of smart card/credential you will be using in your facility (one type only) -> iClass, Mifare or DESFire. The smartcard lock series are E36xx and/or E56xx.
- Prox Card Bit Format: If you selected earlier Prox card based locks, you must also specify the Prox card bit format -> either as 26 bit Standard Wiegand or “Other” (27 through 84 bits). The Prox card lock series are E37xx and/or E57xx.
- Smart Card Bit Format: The same applies if you had selected a Smartcard based lock but using the iClass credential (not Mifare or DESFire). Click **OK** when done.

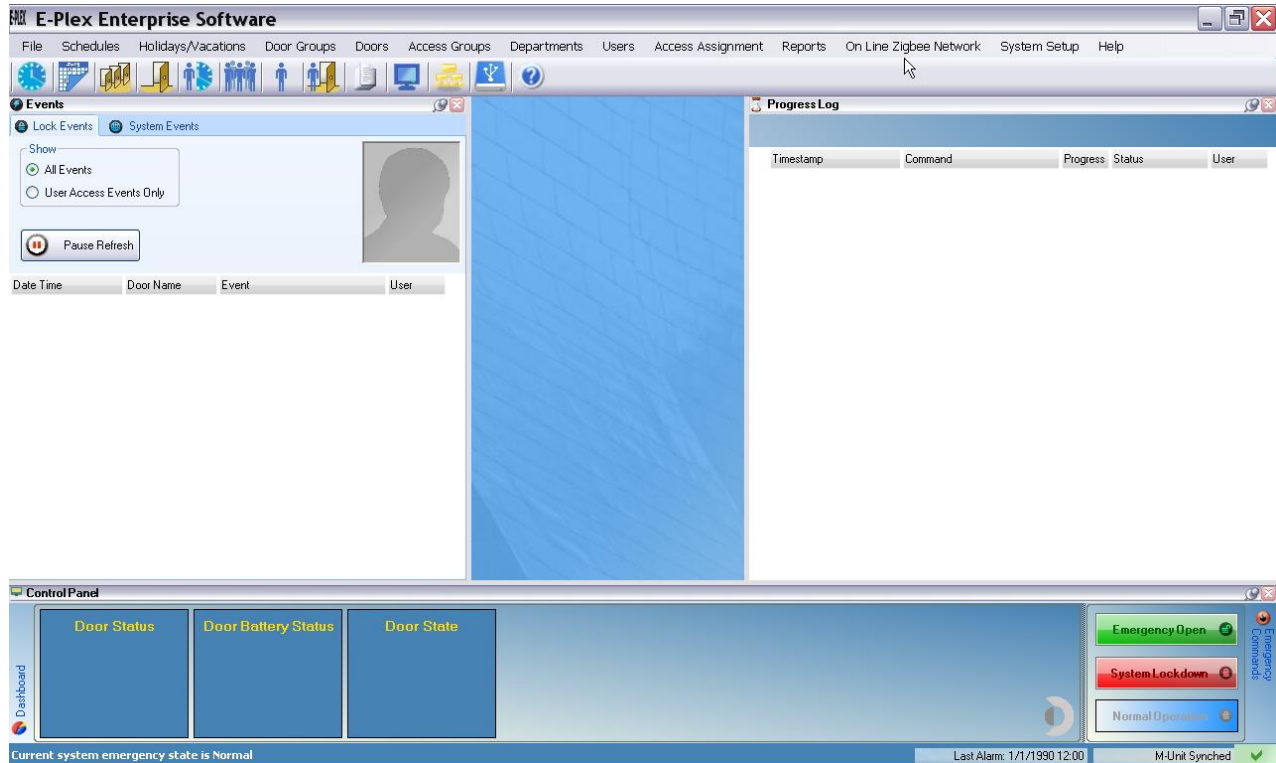
Recovering Forgotten (Master) Password

- Click “*Forgot Password*” and follow the screen instructions to recover your Master password. You will need to contact Kaba's Technical support line to recover your forgotten or lost Master login password.

Main Menu and Toolbar



(Or, after **Wireless** option is enabled in *System Settings*)



This section describes the Main Menu and Toolbar, which are the primary points to access the functions of the E-Plex Enterprise.

Main Menu

The Main Menu provides access to all functions and displays the available menu options.



The following 12 drop-down menus are available from the Main Menu:

File

Schedules

Holidays/Vacations

Door Groups

Doors

Access Groups

Departments

(Note: In the first release Enterprise 1.x software version, this field was called *User Groups*, it means one and the same !)

Users

Access Assignment

Reports

Online ZigBee Network

(For Wireless option enabled system only)

System Setup

► Getting Started

Help

Please refer to the appropriate sections in the manual in **Chapter 3** for more detail on each of the options that are available from the drop-down menus. These menu options are also available from the Toolbar as shown below.

Toolbar

The Toolbar is located directly below the Main Menu and displays the icons for the Main Menu options.

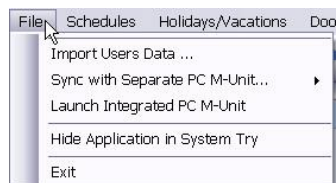


(Or, if **Wireless** option is enabled)



You can select an icon on the toolbar by positioning the mouse pointer on the icon and clicking the left mouse button one time. The menus available from the Enterprise Main Menu and the corresponding Toolbar icon (if applicable) are described in the following sections.

File Menu



From the **File** menu, you can either (i) Import users (basic info such as names, PINs and Prox or iClass card ID numbers in 26-bit Standard format, if available), (ii) Manually sync locks/users configuration data and locks' audited data between the (Client) PC and a separate PC M-Unit (Netbook) device, (iii) automatically sync the above configuration data between the PC and the M-Unit, if the Enterprise and M-Unit software modules are "integrated" and reside within the same PC, (iv) hide/minimize the E-Plex Enterprise software application in the System Tray screen area of the PC and (v) Exit from the software.

Schedules



From the **Schedules** menu, you can add, edit, or delete unlimited number of access schedules in the system database. Note: You can assign a maximum of 16 schedules in each lock out of the total number of schedules in the system database. An access schedule is a defined time period during the span of a week in which users can be granted access to the door. One of the 16 schedules will have an "Always" (24/7) access schedule that is built into the system software; this schedule cannot be changed or deleted.

Holidays/Vacations



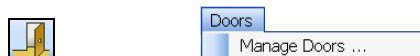
From the **Holidays/Vacations** menu, you can create unlimited number of holidays/vacations in the system database but can set up a maximum of 32 holiday and vacation schedules per lock. When a holiday or a vacation period (ie., one day or a consecutive block of days) is assigned to a door, the door will NOT grant access to any Users during that period. Holidays/vacations can be overridden by any users – Manager, Access, Guest and/or Service, if they are given this holiday override “Privilege” in the software.

Door Groups



From the **Door Groups** menu, you can add, edit, or delete any number of door groups. Each Door Group must contain one (and only one) Door Group Manager.

Doors



From the **Doors** menu, you can add, edit, or delete any number of physical doors with associated E-Plex lock configuration parameters. You must select and assign to each door one or more (up to 16) Access Schedules from previously created Access Schedules in the system including the Credential Type to be used (PIN only, Card only or PIN & Card) during each schedule period. You must ensure that these access schedules do not overlap, but if you do, the system will prompt you to correct this scenario. Optionally, you can also select and assign from previously created Holidays/Vacations in the system, from one to 32 holiday/vacation periods to each door. Free passage is disabled in the lock by default but you can enable one of three Passage mode options for each schedule period – (i) Manual passage (at lock keypad), (ii) Automatic Schedule based Passage, or (iii) First authorized user access Passage.

For Wireless: Additionally, you must also configure all wireless lock/door related parameters for all wireless enabled locks.

Access Groups



From the **Access Groups** menu, you can add, edit, or delete any number of access groups which contain the doors with their schedules and associated users. An access group can consist of one or more doors, each with a schedule and the credential type to use during that schedule for each door. You can also assign one or many users in each access group you created. Additionally, each access group can be “cloned” as a new access group; this cloned access group can be edited to add or remove door(s) and/or user(s) from it very quickly instead of trying to create a new one from scratch, thus saving enormous operator data key entry time. Optionally, you do not need to create any access groups in the system if you have only a handful of locks/doors and only limited users who will need access in your facility. If this is the case, you can configure your facility’s door/user access assignment setup under the **Access Assignment** menu instead of doing it here.

Departments



From the **Departments** menu, you can add, edit, or delete any number of Departments (user groups). The use of Department in the software is for your convenience only to define and organize each department containing your users belonging to that department or user group. However, the Department field data is not recognized by the E-Plex locks.

Users



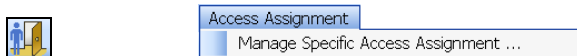
From the **Users** menu, you can add, edit, or delete any number of users in the database but up to 3,000 users and their associated PINs in a lock. You can also enroll (add), if required and available, each user's ID card, or remove it, if previously assigned from the database. If you have a deck of the Standard 26-bit format HID Prox or iClass cards, you can "batch enroll" all these hundreds of cards/users in the system in one operation. This assumes that each card contains the same 3-digit Facility code on each card and the card numbering on each card is sequential. Additionally in this menu, you can assign to each newly created user an existing Access Group (of doors), thus assigning all these doors with their access schedules to the user in one quick operation.

- There are five (5) types of users that an E-Plex lock can recognize:

- (1) Manager: Lock programming/auditing rights; schedule based access with optional privileges; no expiry
Door Group Manager: One (and only one) DG Manager in all locks belonging to her/his Door Group; 24/7 lock programming/auditing rights and 24/7 access with all privileges; ie., same functionality as the Global Master, except applies to her/his Door Group locks only
- (2) Access: Schedule based access with optional privileges; no expiry
- (3) Guest: Schedule based access with optional privileges; 1 year max expiry
- (4) Service: 24/7 access from first access with various expiry options: either one time entry only, or 1 – 96 hours expiry, or no expiry
- (5) M-Unit: 24/7 lock programming/auditing rights only but no access; no expiry

Refer to the **Summary of Pushbutton Programming Commands** table in **Chapter 4, Operating the E-Plex Lock at its Keypad** for detailed lock programming & auditing rights of the global Master, Manager(s) and the M-Unit(s) users. Additional information on the M-Unit(s) users is at the beginning of Chapter 5.

Access Assignment (includes assigning user Privileges)



Note: Everything related to door <-> users access control info is tied together in this menu, just like in the Access Groups menu.

From the **Access Assignment** menu, you must select a door that you want to populate with valid users for access. For each user, select and assign required access schedules from the available door schedules that were previously assigned to this door from the Manage Doors configuration menu.

- Also, for each user type, you can optionally assign any one or more of the following three (3) Privileges:

(1) Override holidays/vacations: By default, assigned to a Manger user but can be changed

(2) Override deadbolt privacy: Applies to Privacy locks only

(3) First user passage entry: By default, assigned to a Manger user but can be changed

After this access assignment process, the lock configuration data is set up and prepared to be synchronized with the M-Unit for uploading to lock(s).

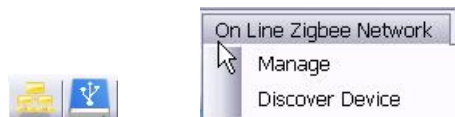
Reports



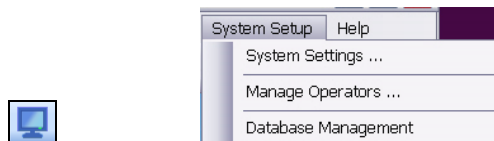
From the **Reports** menu, you can generate many useful reports from the E-Plex Enterprise system database for viewing and/or printing. The reports can also be exported in PDF, Word, Excel etc file formats, if desired.

For Wireless: Only when this option is enabled in *System Settings* by Kaba certified dealer/integrator, the "Online ZigBee Network" menu option below will be available.

Online ZigBee Network



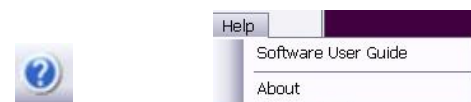
System Setup



From the **System Setup** menu, you can (i) set up and maintain all important Enterprise system configurations, (ii) manage system Operators and their passwords, and (iii) perform routine system database maintenance like backup and restore operations.

For Wireless: Additionally, in "System Settings" you must also enable the wireless system option (can be enabled by Kaba certified dealers/integrators only), and configure all wireless system related parameters such as Emergency Lockdown etc.

Help

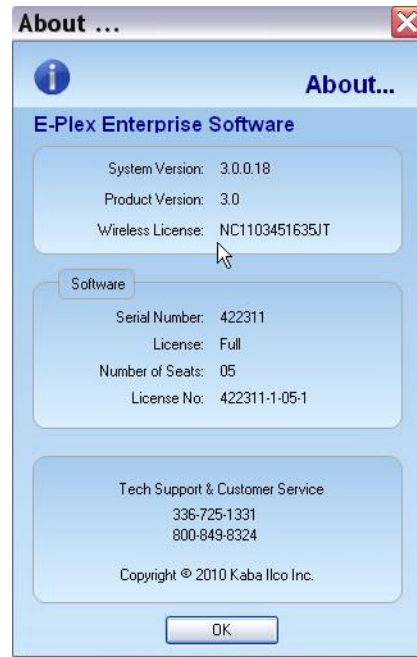


From the **Help** menu, you can (i) access the *Software User Guide* to view/print, and (ii) by clicking on *About*, you can display all product specific info such as: The Software Version number, Your (End user's) unique Site License number, your (Integrator's) unique Wireless License number (if enabled), Kaba's Technical and Customer Support Phone numbers etc as shown below:

If Wireless Option is Disabled:



If Wireless Option is Enabled:



(or)

3

Using the E-Plex Enterprise Software

All E-Plex Wireless Locks & System related info are highlighted in this turquoise color background for easy reference.

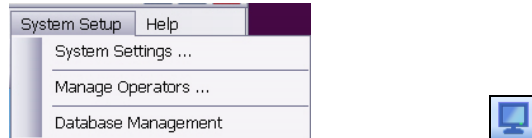
This chapter explains how to use the E-Plex Enterprise system software on a regular basis to suit your physical access control security needs. It typically involves the following items:

- System Setup Menu (additional setup for Wireless enabled lock system)
- Managing Access Schedules
- Managing Holidays/Vacations
- Managing Door Groups
- Managing Doors (additional setup for Wireless enabled locks)
- Managing Access Groups
- Managing Department
- Managing Users
- Managing Access Assignment
- Importing Users
- Viewing/Printing/Exporting Reports (additional setup for Wireless enabled lock system)

System Setup Menu

The **System Setup** menu allows you to define and maintain global system settings that, in most cases, you need to do this only during the initial system setup.

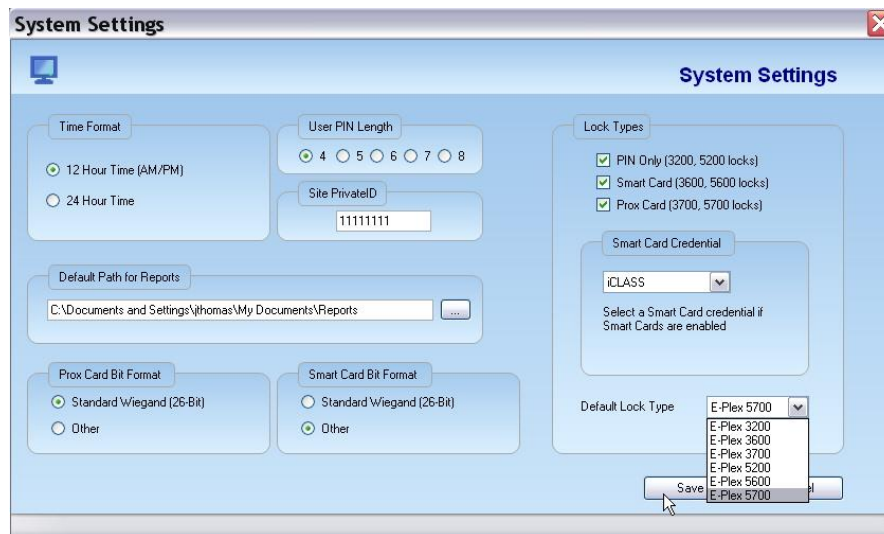
To access system settings, select an option from the **System Setup** menu or click the **System Setup** menu icon.



Changing System Settings

You should establish the system settings before you begin using the E-Plex Enterprise on a daily basis – typically you need to do this at initial install only. However, you can use this feature at any time if you need to update or add to the existing information.

From the System Setup menu, select **System Settings**. The system displays the **System Setup** window.



- Edit the following data areas as desired:

- **Time Format**

Select the display of **Time Format** for your system. The default is **12-Hour Time** (a.m. and p.m. display), and the other option is **24-Hour Time** display.

Note: The Enterprise software uses the start and end dates/times of the DST setup directly from your PC's Operating System. You must also ensure that the DST setup and the current date & time are setup correctly on your portable M-Unit device. The M-Unit automatically sends this information to the locks every time the lock is programmed so that the DST switching in the lock will occur automatically in Autumn and Spring.

- **User PIN Length**

Select the appropriate global **User PIN Length**—between four and eight digits—that you will be using in your system. The default user PIN length is four digits.

Important: The first 4 digits must be always unique when assigning PIN numbers for each user later in the software; this is for security reasons.

- **Site PrivateID**

The 8-digit Site PrivateID is combined with an internal unique factory to generate a unique hidden customer (your) encryption/decryption key. The customer key is used throughout the Enterprise system – database, M-Unit and locks in protecting data communications and the database.

Important: If in the future after deploying your system and locks, for some reason you need to change the value of the Site PrivateID, you must re-initialize and re-program all the E-Plex locks in your facility. This is because the original encryption/decryption communications key inside the locks will have to be changed again since it has been modified now in the software.

- **Default Path for Reports and PC Activity Log**

This field defines the default directory path to be used when generating and saving reports and archived data files. You can browse and select/change the path for reports to a CD-RW drive, network drive, jump drive or another similar type of drive.

- **Prox Card Bit Format & Smart Card) Bit Format (For E3700/5700 Prox locks & E3600/5600 iClass locks only)**

Select the appropriate Wiegand bit format for your Prox and/or iClass ID Cards that you will be using in your facility. The default value is **Standard Wiegand (26-Bit)**. If you select the non-standard **Other (= 27 to 84-Bits)**, you must use the applicable Prox card and/or the Smart card Reader/Enroller to assign the tokens/cards for the users. If you checked the “Other” option, the display of the card ID format in the Users dialog menu will not be in standard xxx-yyy (3 digit facility code – 5 digit card number) format, but will display as one long hexadecimal number only.

- **Lock Types**

Select one or all three types of locks that you will be installing on your site -> PIN only (E3200, E5200), and/or PIN & Smartcard (E3600, E5600), and/or PIN & Prox (E3700, E5700).

- **Smart Card Credential**

If you had selected PIN & Smartcard under “Lock Types” above, this sub-option will be enabled for you to further narrow it down to which of the following three Smartcard credentials you will be using -> DESFire, or iClass or Mifare.

Important: You can select only one of these three types of Smartcard credentials.

- **Default Lock Type**

Finally, you can select a (default) lock type that will be most used in your facility. Whenever to create a new door/lock in the database, this lock model will be automatically selected to speed up data entry, which if required can be changed to another lock type.

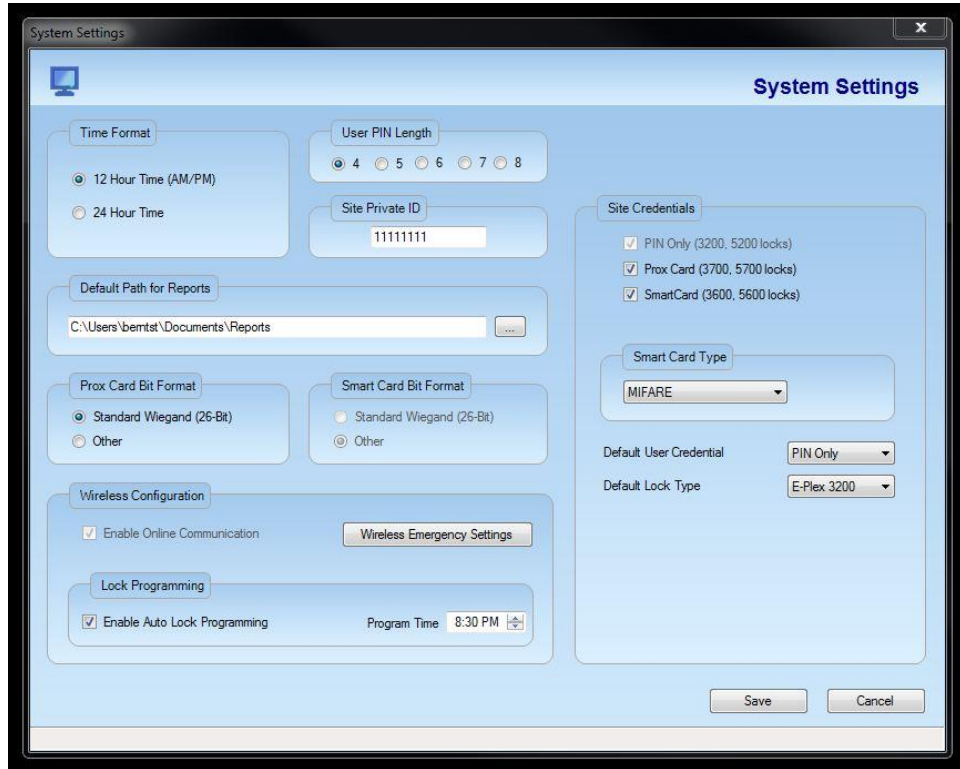
Once you have updated the desired fields, click **Save**. The software confirms that the changes saved successfully in the status bar of the window.

[Start]

For Wireless:

- **Wireless Configuration Setup**

- a. Additionally, you must check the box to “*Enable Online (wireless) Communication*” so as to configure all wireless system related parameters.

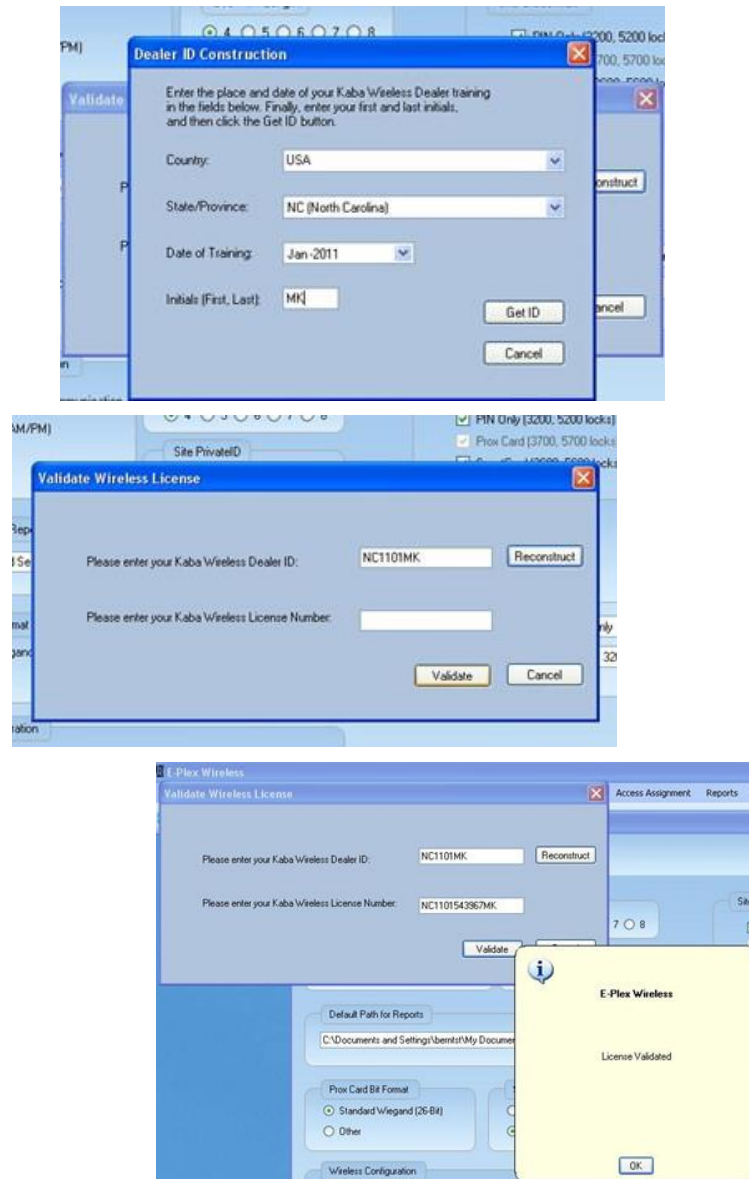


- b. ***Important:*** Only Kaba factory trained and certified Access Control Dealers, Integrators and/or Associates can enable/activate the wireless option in the software. Each certified dealer/integrator would have already received the two required wireless activation info [(i) ID and (ii) License #] from Kaba after successfully completing her/his E-Plex wireless certification training. Please contact Kaba Technical Support for further assistance.

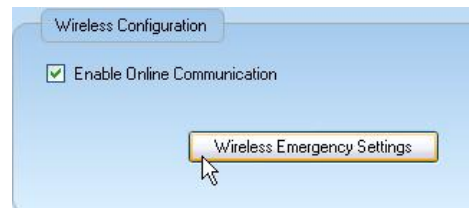
Please follow the screen prompts by entering your “Wireless Dealer ID” first (e.g.: NC1101MK) and then your “Wireless License Number” (e.g.: NC1101543967MK) as prompted by the software. Once validated, the software will activate (enable) the wireless settings option so that you will be able to configure the wireless locks/system parameters to suit your exact needs.

The following are a few sample screen shots of the user interface:





- c. Once validated, click on “**Wireless Emergency Settings**” to setup the two main Emergency commands -> (i) the Emergency Lockdown of your site, and (ii) the Emergency Passage/Open (for evacuation) of your site.



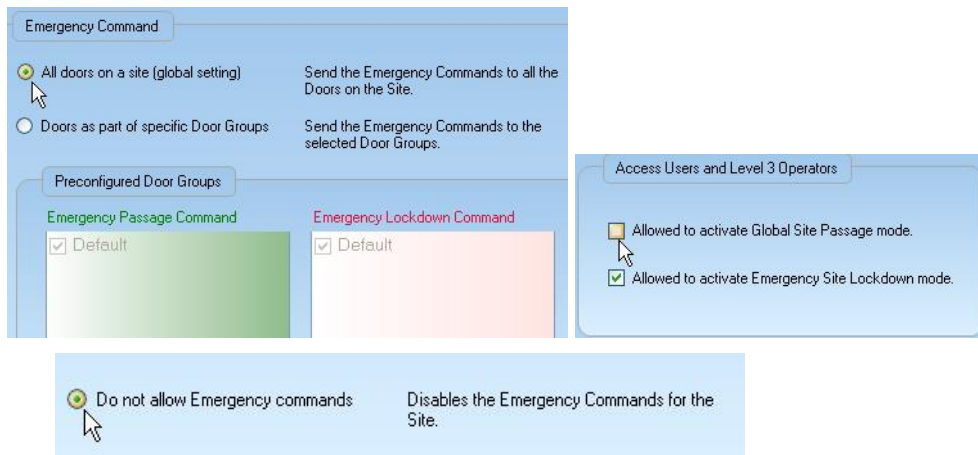
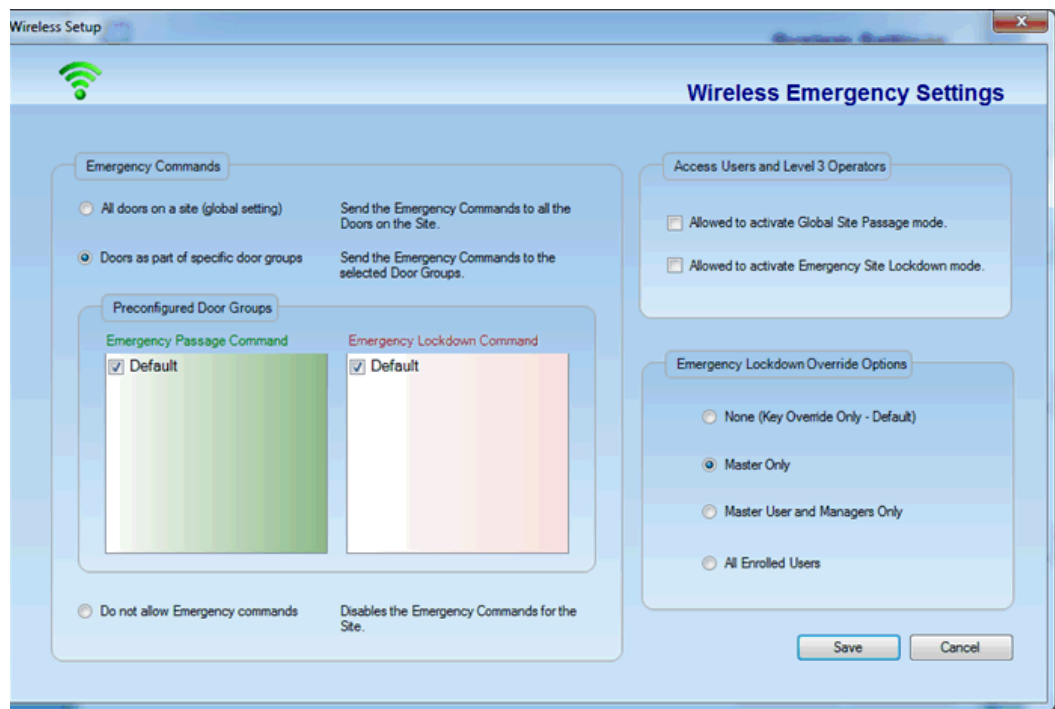
- d. You may either select the option to apply these commands globally to all doors on your site, or select only those applicable Door Groups that contain the doors that you want to be locked down or opened immediately during an emergency.

Important: The narrow stile **E-Plex 3x66 series wireless locks** cannot be put into global emergency lockdown or passage state due to their mechanical hardware constraints. Please ensure that you have installed the **E-Plex 3x65 or 5x00** type wireless locks if you want them to be able to accept the global emergency commands.

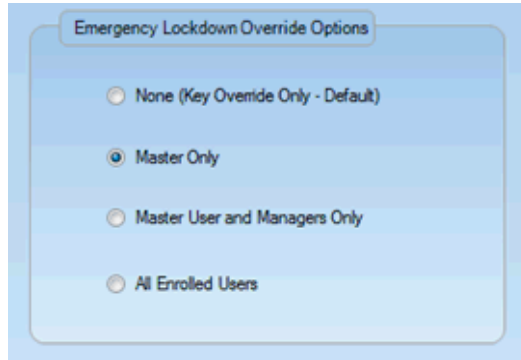
Initially, you will see only the “Default” Door Group listed, but after you populate your database with many door groups and doors, you can come back to this menu and select the applicable Door Groups(s) where the Emergency commands will take effect in doors contained within those selected Door Group(s).

Note: You may also choose to altogether disable these Emergency commands for your site. In this case, then nobody will be able to either accidentally or as a prank perform a global lockdown/opening of your wireless locks.

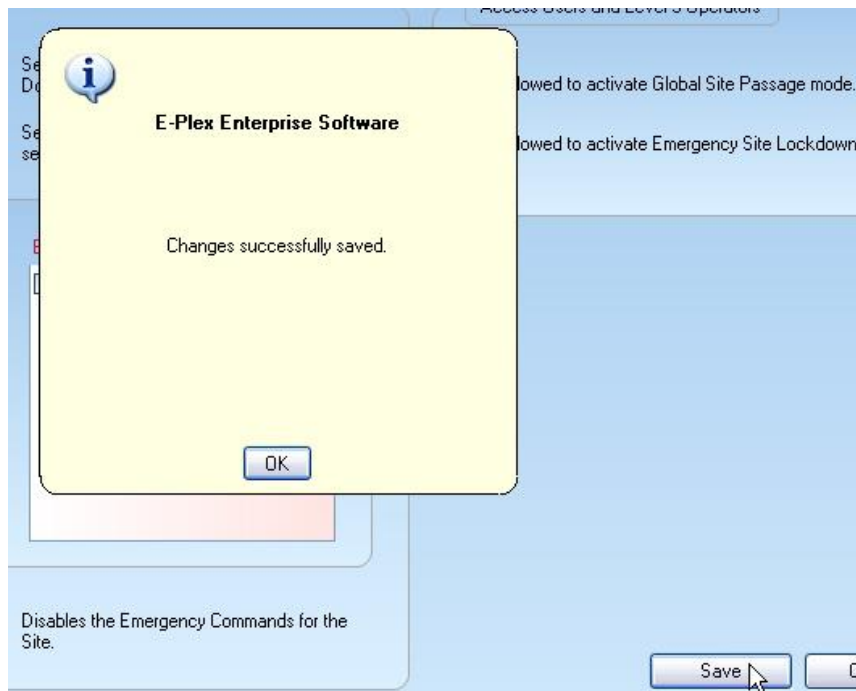
- e. You also have an option to give permission to either, regular “Access” type users and/or low level system Operators (Level-3) to perform these Emergency commands in the software and/or at the lock keypad. By default, only the Master, the Managers and the Level 1 & 2 Operators can perform these Emergency commands in the system or at the lock.
- The following are a few screens showing different optional settings of the “Wireless Emergency Settings”. Select the ones that are suitable for your site operation.



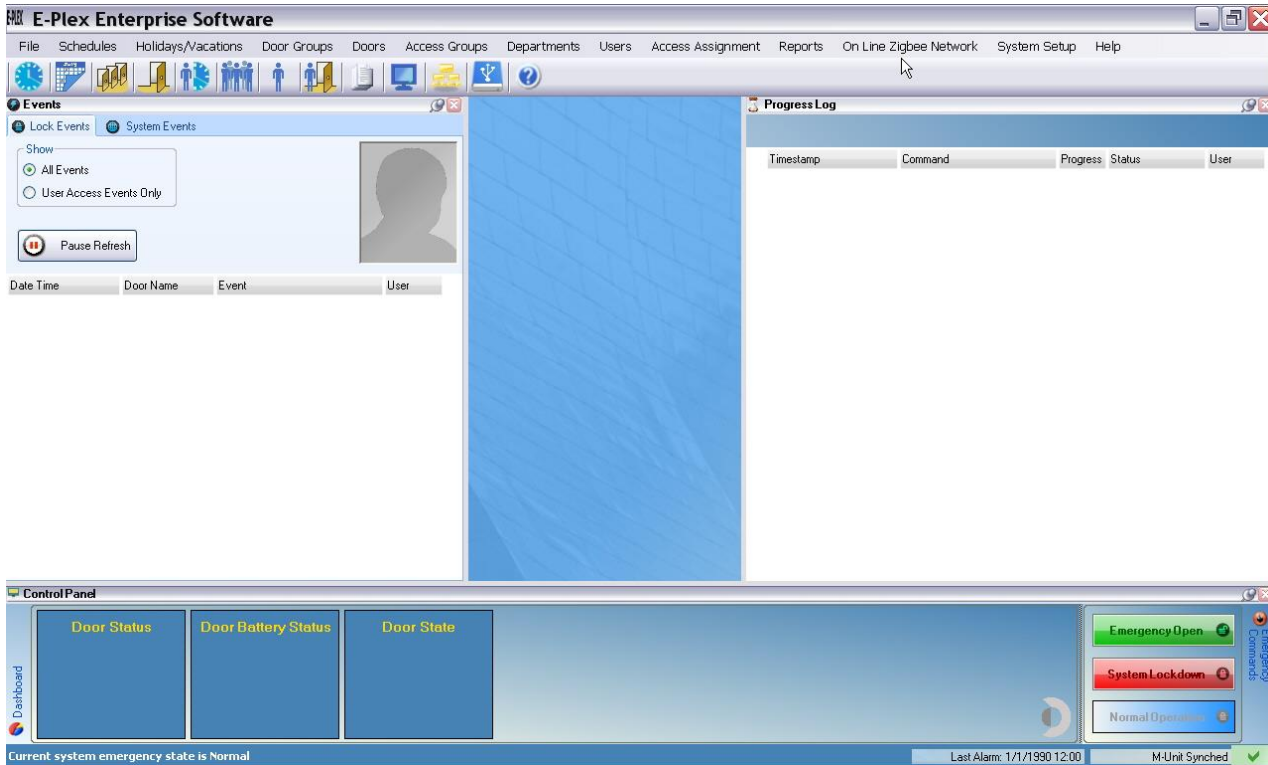
You can also customize the Emergency Lockdown Feature to tell the system who will have access during a Lockdown situation.



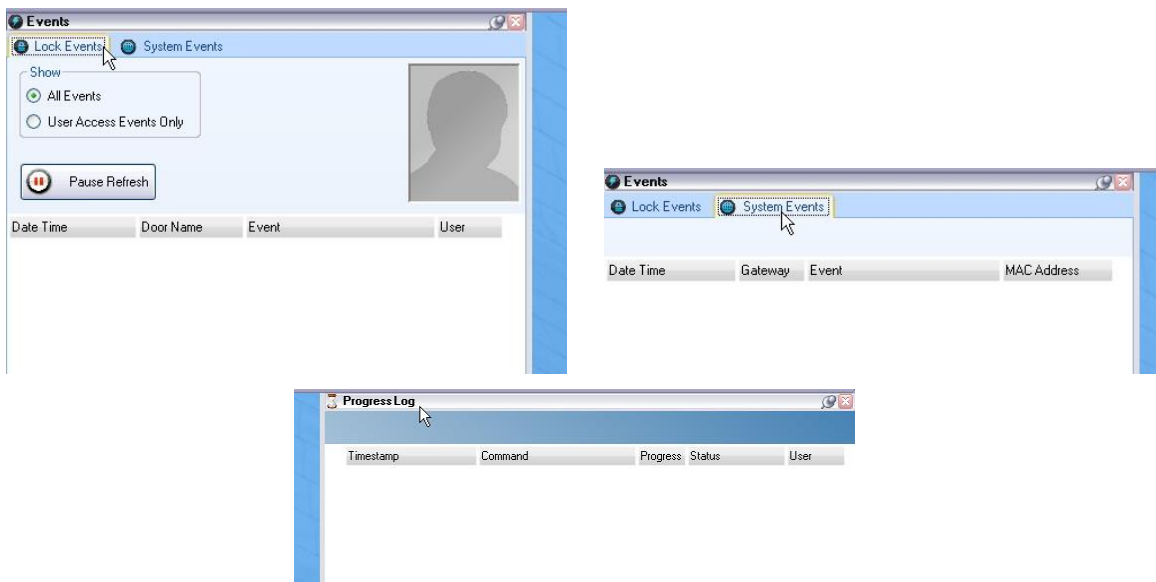
- Click "OK" and "Save" all the system setup parameters; close the **System Setup** window.

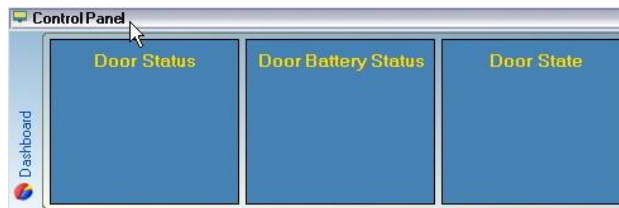


- Now the main menu will display a new wireless system related menu item called the **On Line ZigBee Network** and other wireless related screen info such as **Events**, **Progress Log** and **Control Panel**; the **Control Panel** is also referred to as the “**Dashboard**”.



- The following screen shots taken from the above main menu screen show the **Events**, **Progress Log** and the **Control Panel** (Dashboard status & Emergency Commands) parts of the main menu screen -> “clean” status (no events yet) of the Lock and System Events, the wireless commands and status Progress Log with no data yet, no doors info yet and the three emergency wireless command tabs for instant execution operator, when needed.





[End]

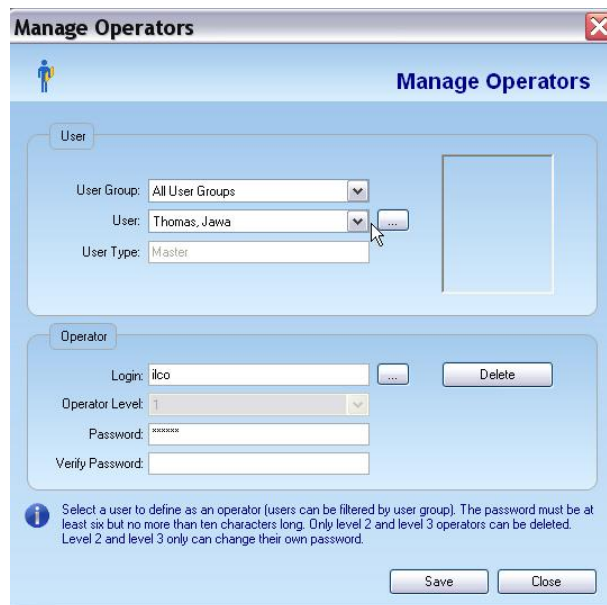
Managing Operators

The **Manage Operators** option allows you to create a new Operator and manage existing Operators in the system.

Important: The first Operator that you create in the software upon installation automatically becomes a Level 1 (highest authority) Operator. Only Level 1 Operators can add or delete other Level 2 or Level 3 (lowest authority) Operators. See **Chapter 1** for a detailed description of the E-Plex Enterprise **System Operator Classifications**.

Complete the following steps to manage Operators:

- From the **System Setup** menu, select **Manage Operators**. The software displays the **Manage Operators** window. **Note:** You must first create a few users in the system before hand under the "Managing Users" menu so as to assign one or more of them here as Operators of the Enterprise software system.



User Area:

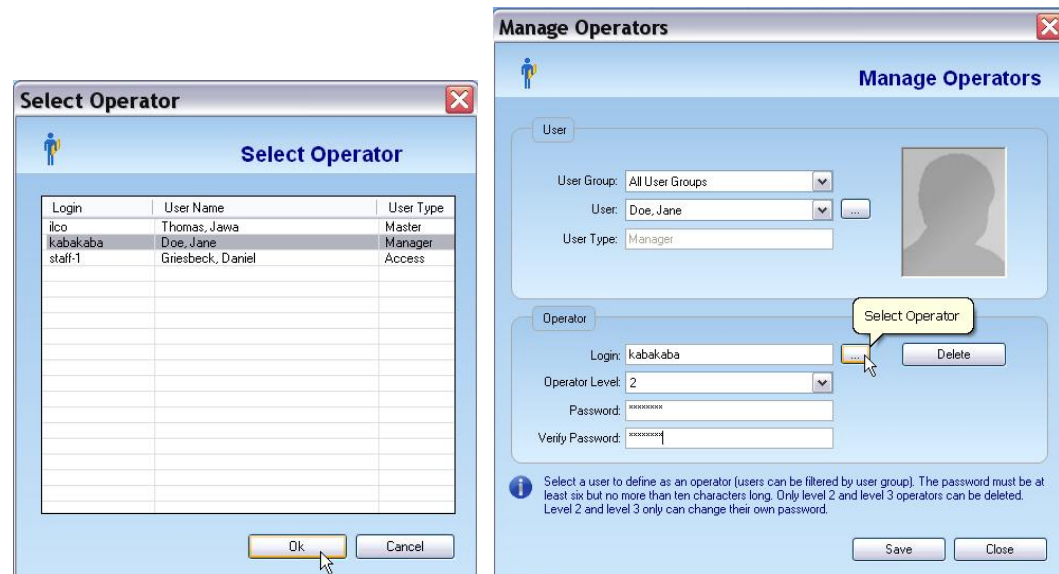
- From the **Department (User Group)** drop-down list, select the **Global** user group (by default, already exists in the system) or **All Departments**. To add, edit, or delete a user group, refer to **Managing Departments** in this chapter.
- From the existing **User** drop-down list, select the appropriate user whom you want to be

► *Using the E-Plex Enterprise Software*

an Operator of the software also. To add a user from this menu, click the ellipsis button and add a new user so as to assign her/him as an operator.

Operator Area:

- In the **Login** field, enter/edit the login name/ID for the selected operator. To select a different Operator, click the ellipsis button -> ...
- Select the Operator from the **Select Operator** window and click **OK**.



- In the **Operator Level** field, select 1 (highest authority), 2 or 3 (lowest) as the System Operator authority/privileges level. For details, please refer to “PC System Operator Classifications” described in Chapter 1.
- In the **Password** field, enter a Password for the selected Operator.

Note: The Password must be at least six but no more than ten (alphanumeric) characters long. Level 2 and Level 3 Operators can change their own password but cannot add or delete themselves.

- In the **Verify Password** field, re-enter the password.
- Click **Save**. The software displays confirmation that the changes were saved successfully.
- Click **Close** to exit the **Manage Operators** window.

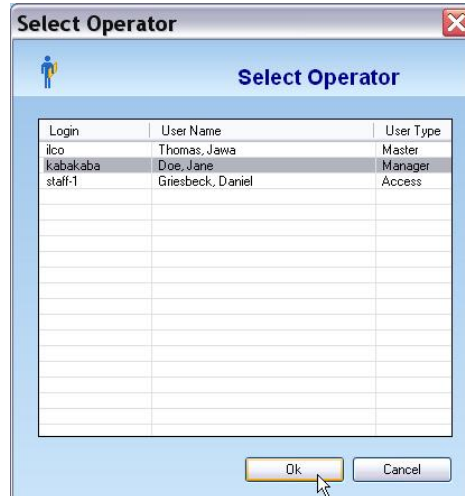
Changing an Operator Password

The **Change Password** option allows you to change an Operator’s password. Complete the following steps to change an Operator’s password:

- From the **System Setup** menu, select **Manage Operators**. The software displays the **Manage Operators** window.
- Select an Operator by clicking the ellipsis button in the Operator area of the window ->



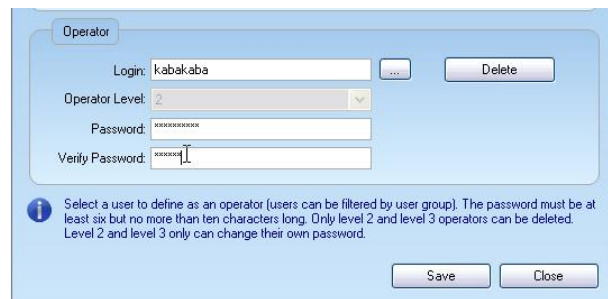
Select the Operator from the **Select Operator** window and click **OK**.



- In the **Password** field, enter a new password for the selected Operator.

Note: The Password must be at least six but no more than ten (alphanumeric) characters long. Level 2 and Level 3 Operators can change their own password but cannot add or delete themselves.

- In the **Verify Password** field, re-enter the password.



- Click **Save**. The software displays confirmation that the changes were saved successfully.
- Click **Close** to exit the **Manage Operators** window.

Deleting an Operator

The **Delete Operator** option allows you to delete an Operator from the system.

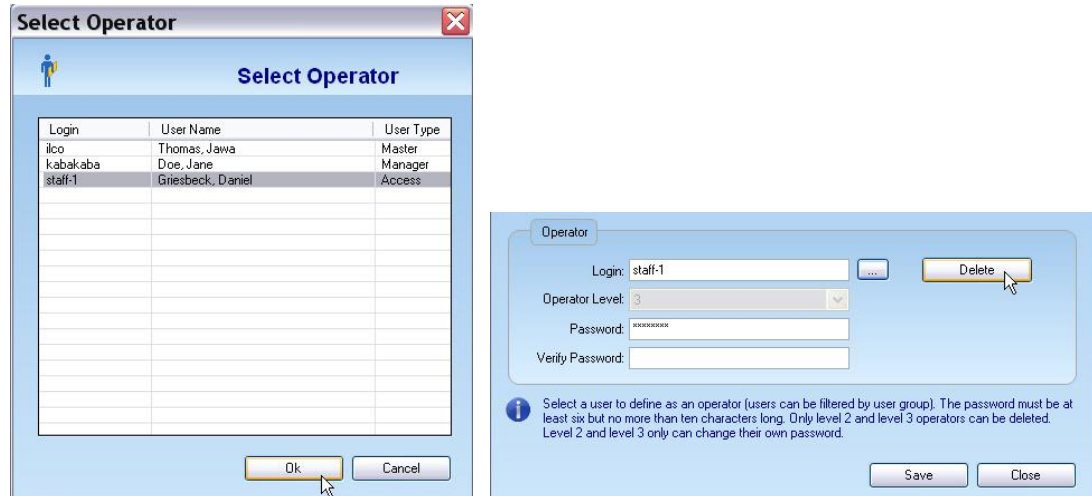
Note: Any Level 1 Operator can delete Level 2 and Level 3 Operators; Levels 2 & 3 Operators cannot delete any operators. A Level 1 Operator can be deleted only by another Level 1 Operator.

Complete the following steps to delete an Operator:

- From the **System Setup** menu, select **Manage Operators**. The software displays the **Manage Operators** window.
- Select an Operator by clicking the ellipsis button in the Operator area of the window ->



Select the Operator from the **Select Operator** window and click **OK**.



- Click **Delete**. The software prompts you for confirmation.



- Click **Yes**. The system deletes the operator.
- From the **Manage Operators** window, click **Save** and then **Close** to exit the window.

Database Management

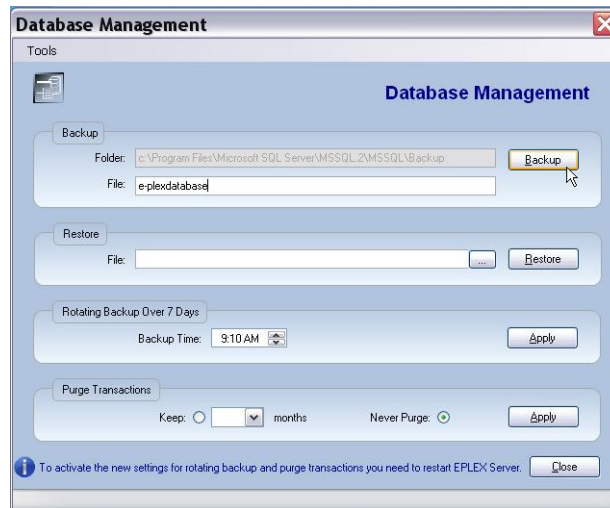
The **Database Management** feature enables you to periodically back up the Enterprise system database. You can also restore the last backed up database in case of corruption in the current database.

Important: It is highly recommended that you perform a periodic back up of your database.

Backing up the Database

Complete the following steps to back up the database:

- From the **System Setup** menu, select **Database Management**. The software displays the **Database Management** window.



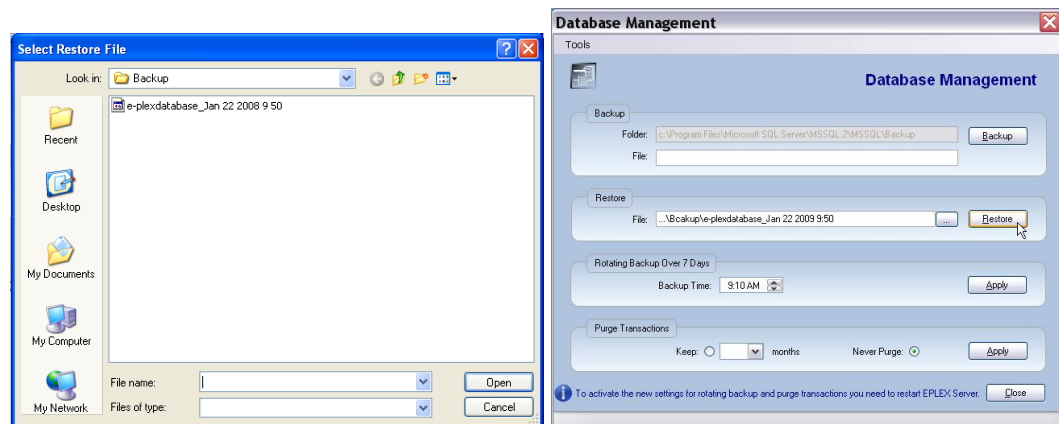
- Enter a file name in the **File** field of the **Backup** area.
- Click the **Backup** button to back up the database. The database will be backed up automatically in the secure Micro-Soft SQL system directory (by default) with date/time stamp for later retrieval, if need be. When the backup is complete, the system displays a message in the status bar of the **Database Management** window.

Backup Done: c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Backup\e-plexdatabase_Jan 22 2008 9 50

Restoring the Database

Complete the following steps to restore the database:

- Click the ellipsis button in the **Restore** area.
- The system displays the **Select Restore File** window. Choose the database that you want to restore and click **Open**. The system displays the file location in the **File** field of the **Restore** area.



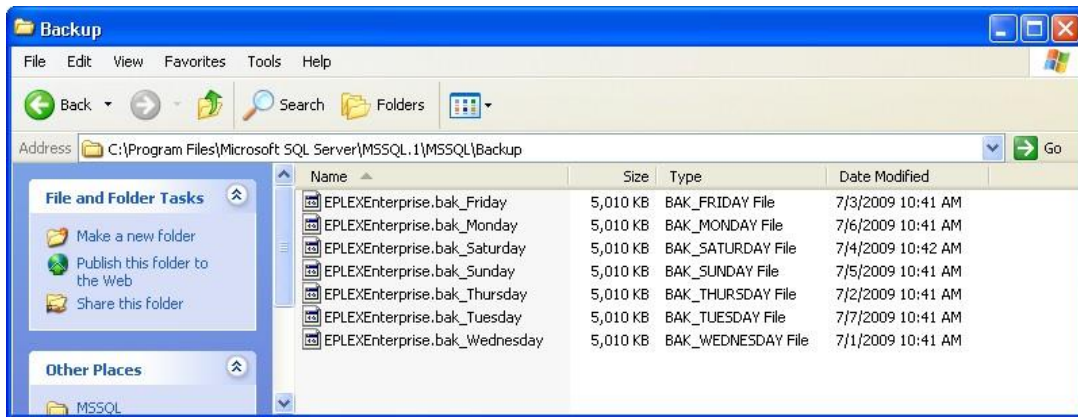
- Click **Restore**. The system prompts you for confirmation with a warning to say that this restore operation will overwrite your current database which will then be lost etc.
- Click **Yes** to continue or **No** to cancel.
- If you click **Yes**, the system restores the selected database and displays a message in the status bar of the **Database Management** window.

Restore Database Done

- Click **Close** to close the **Database Management** window.

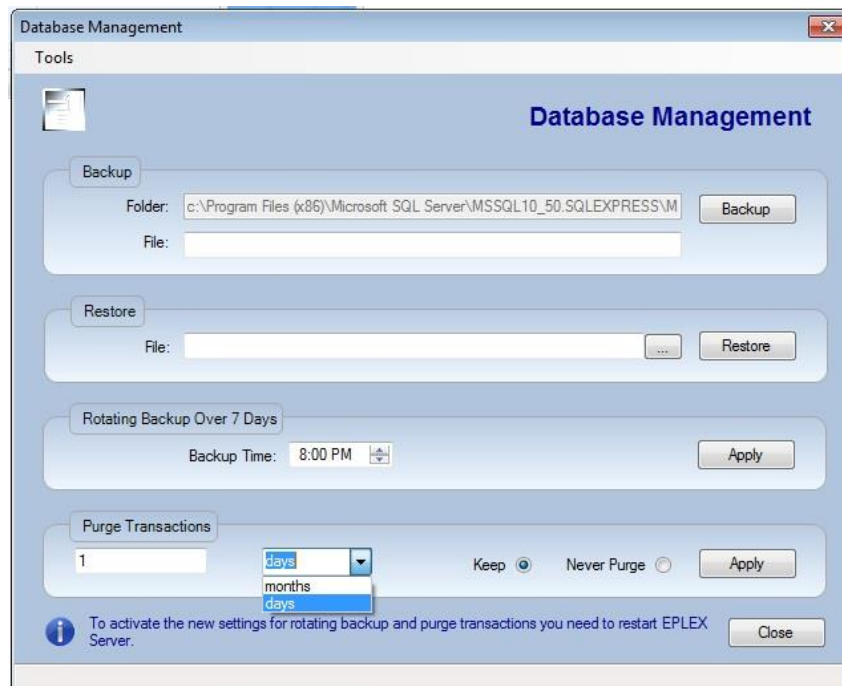
Rotating Backups Over 7 Days

- In this section, you can specify at which time a daily automated back-up will take place.
- Select the time you want the back-up to be taken and click **Apply**.
- A back-up will be performed daily at the specified time. The format of the saved files are as follows:



Purge Transactions

- In this section, you can specify how long in days or months to keep the record of operator activity that is logged in the Enterprise Database. This information is viewable via the “System Activity Log”, as described in the section called **Viewing / Printing / Exporting Reports**.
- You can choose either to **Keep** the logged transactions for the number of days or months you specify, or to **Never Purge** them. **In wireless systems with large quantities of stored transactions, a time limit in days or months should be specified to improve system efficiency and performance.**
- Make your selection and click **Apply**.

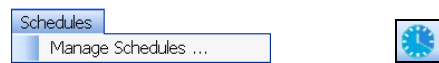


Managing Schedules

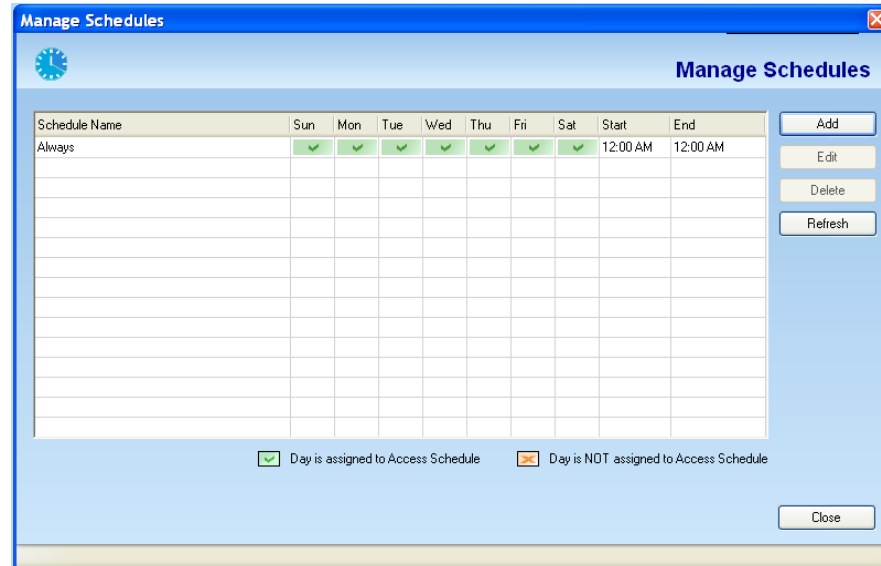
A schedule is a defined time period during the span of a week during which users are granted access to the door. The Enterprise software allows you to globally define schedules. Once you have defined schedules, you will assign them to doors and to the users who will access those doors. The software allows you to manage schedules through the **Schedules** menu.

Note: You can define up to 16 schedules in the lock but any number of them in the system software. However, the “Always” schedule is standard and is pre-defined in the system. It cannot be changed or deleted. The “Always” schedule allows 24/7 access to its associated doors and users.

- To manage access schedules, select **Manage Schedules** from the **Schedules** menu or click the **Manage** button.



- The software displays the **Manage Schedules** window.



- From this window, you can add, edit, or delete access schedules.

Adding a Schedule

Complete the following steps to manage schedules:

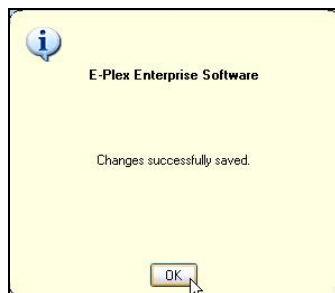
Note: You may add additional schedules at any time.

- From the **Manage Schedules** window, click **Add**. The software displays the **Add Schedule** window.

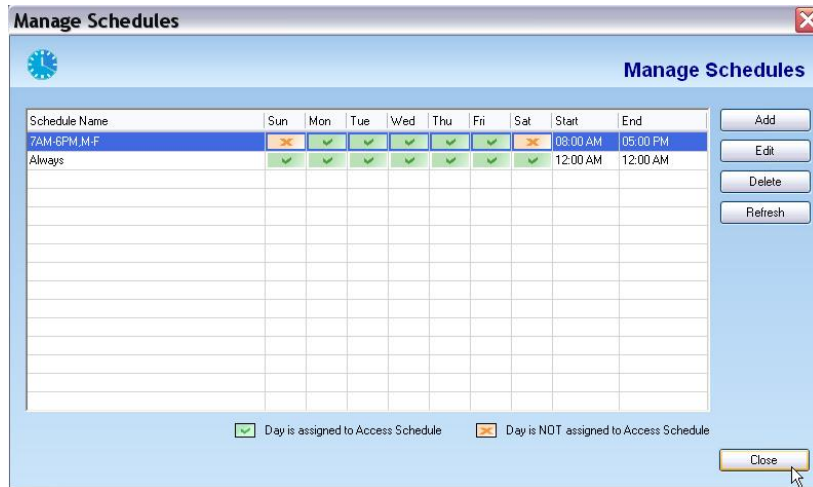
- In the **Schedule Name** field, type the name of the schedule you are adding – e.g. “Day-Shift” or “7AM-6PM, M-F” etc.

Note: The schedule name can be a maximum of 20 alphanumeric characters but no spaces and special characters are allowed, except the “-” character.

- Select the appropriate time range: **Week Only**, **Weekend Only**, or **Any Days**.
- Select the appropriate check box for the day(s) you want to add to the access schedule. These are the days that users will have access to a door.
- In the **Start Time** field, select a start time. This is the time that access begins each day.
- In the **End Time** field, select an end time. This is the time that access ends each day.
- Click **Save**. The software displays a **Changes Successfully Saved** message.



- Click **OK**. The system displays the new access schedule in the **Manage Schedules** window.



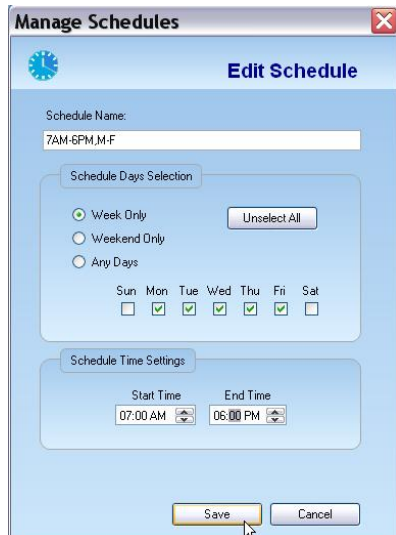
- Click **Close** to exit the **Manage Schedules** window.

Note: Once added, the access schedule becomes available in the **Schedule** drop-down list throughout the Enterprise software.

Editing a Schedule

Complete the following steps to edit access schedules:

- From the **Manage Schedules** window, highlight and click an access schedule you want to edit.
- Click **Edit button**. The software displays the **Edit Schedule** window.

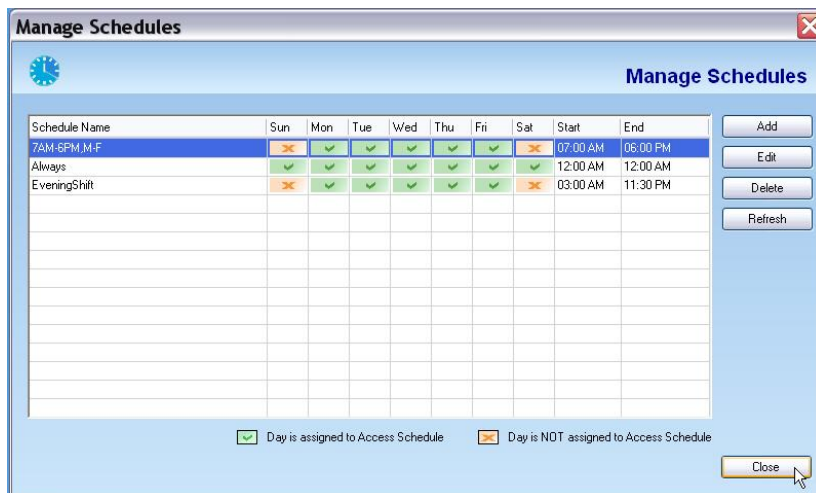


- In the **Schedule Name** field, change the name of the schedule, if necessary.
- Select the appropriate check box for the day(s) you want to change in the schedule. These are the days that users will have access to a door.
- In the **Start Time** field, change the start time, if necessary. This is the time that access begins each day.

- In the **End Time** field, change the end time, if necessary. This is the time that access ends each day.
- Click **Save**. The software displays a **Changes Successfully Saved** message.



- The system displays the updated schedule in the **Manage Schedules** window.



Note: You should update your locks if you modified any existing Access Schedules in those locks by transferring the changes to the M-Unit and programming/uploading the changed information to the locks. For more information, refer to **M-Unit Handheld** in Chapter 5, **Programming and Auditing Locks**.

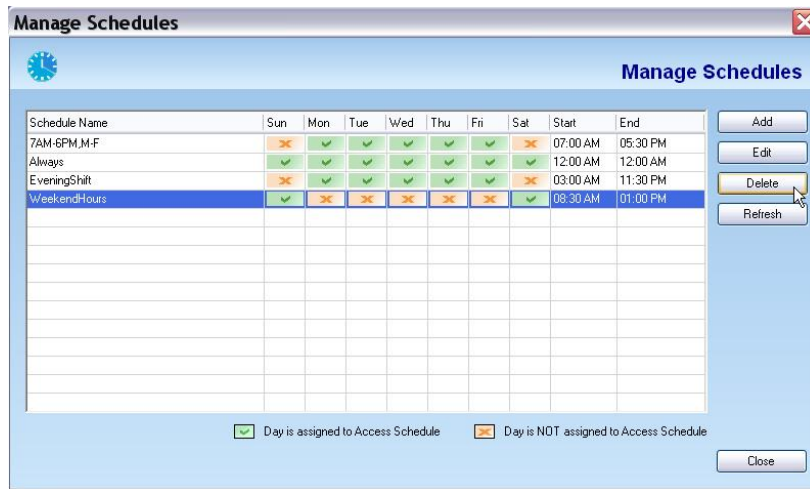
Deleting a Schedule

Complete the following steps to delete access schedules.

Note: You cannot delete an access schedule if it is already assigned to a door or doors.

- From the **Manage Schedules** window, highlight and click the access schedule you want to delete.

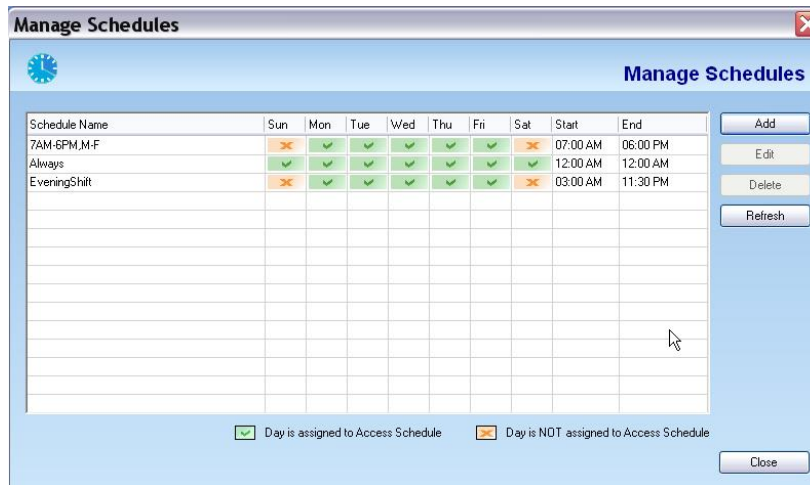
► Using the E-Plex Enterprise Software



- Click **Delete**. The software prompts you for confirmation.



- Click **Yes** to confirm the deletion. The system deletes the schedule from the database and returns to the **Manage Schedules** window.

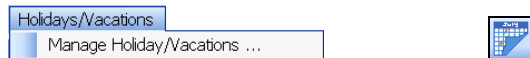


Managing Holidays/Vacations

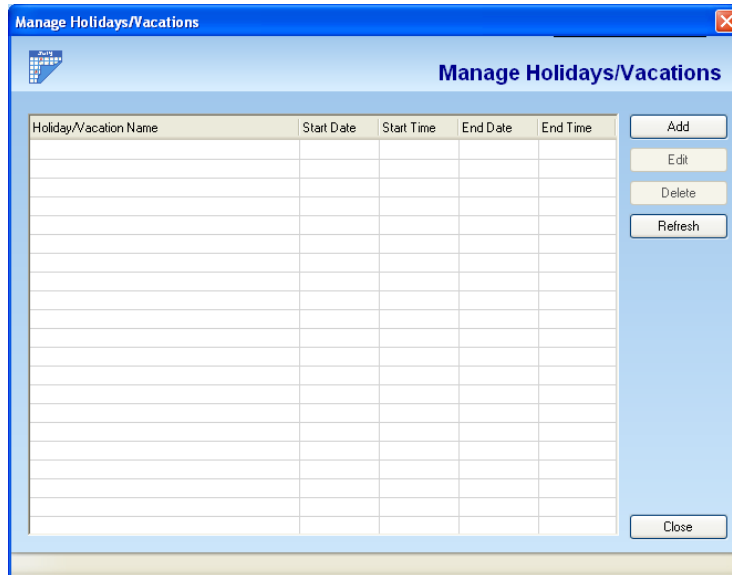
A holiday/vacation is a defined time period during which users will NOT be granted access to a door. By default, there will be no access allowed to a door/lock during a defined Holiday/Vacation period, except for any assigned “privileged” users in the system. By default, all Manager users have the privilege to override Holidays/Vacations.

Note: You can define a maximum of 32 holiday/vacation periods in the lock but any number of them in the system.

- To manage holidays/vacations, select **Manage Holidays/Vacations** from the **Holidays/Vacations** menu or click the **Manage Holidays/Vacations** button.



- The software displays the **Manage Holidays/Vacations** window.



- From this window, you can add, edit, or delete holidays or vacations.

Adding a Holiday/Vacation

Complete the following steps to add a holiday/vacation.

- From the **Manage Holidays/Vacations** window, click **Add**. The software displays the **Add Holiday/Vacation** window.

The screenshot shows a dialog box titled "Manage Holidays / Vacations" with a sub-header "Add Holiday/Vacation". It includes an information icon and a note: "11:59 PM (23:59) indicates end of the calendar day, which is actually 11:59:59 PM (23:59:59)". The form fields are: "Holiday/Vacation" (text box containing "Christmas"), "Start Date and Time" (date dropdown "12/25/2009" and time dropdown "12:00 AM"), "End Date and Time" (date dropdown "12/25/2009" and time dropdown "11:59 PM"), and a checked "All Day Event" checkbox. "Save" and "Cancel" buttons are at the bottom.

- In the **Holiday/Vacation** name field, type the name of the holiday (one day/24 hours only) or vacation block (a block of consecutive days within that year) you are adding.

Note: A holiday or vacation name can be a maximum of 16 alphanumeric characters and no spaces and special characters are allowed, except for the "-" character.

- Leave the **All Day Event** check box selected if you want a 24-hour period holiday, like New Year's Day.

Note: The **All Day Event** check box is selected by default. The **Start Time** and **End Time** fields will be grayed out if the **All Day Event** check box is selected.

- Uncheck the box if the holiday/vacation you are entering is a block of consecutive vacation days with specific start/end dates within that year.
- In the **Start Date** field, select the start date of the vacation block you want by using the drop-down arrow.

Note: 12:00 AM indicates midnight (start) or the **Start Time** of the calendar day which should not be modified.

- In the **End Date** field, select the end date of the vacation block you want by using the drop-down arrow.

Note: 11:59 PM indicates midnight (end) or the **End Time** of the calendar day which should not be modified.

Managing Online ZigBee Network

**** If you will NOT be using E-Plex Wireless locks & system, please skip this entire Section and go to the next Section, "Managing Door Groups". ****

[Start]-----

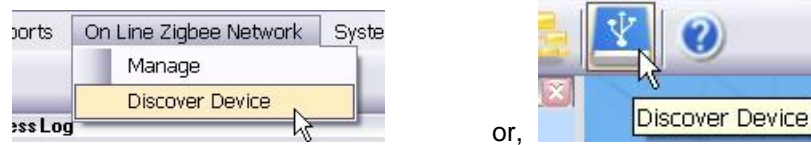
[Applies to Wireless Enabled E-Plex Locks & System only]

The system allows you to configure your E-Plex *Gateway (mandatory,)* and optionally one or more E-Plex *Router(s)* you may need in your facility to form your own E-Plex (ZigBee) wireless network. Later on, after creating all your wireless doors (locks) in the software database, you will "join" the locks to this wireless network for everyday wireless operation of your locks and the system.

Important: By now, you must have already completed a proper Site Survey of your facility using Kaba's portable Site Survey Unit (SSU) to ensure if you need any E-Plex wireless Routers, and also the optimum distance between each wireless door/lock and the Gateway and/or the Router(s) and the locations/placement of these hardware units in your facility for proper operation of your entire wireless network access control system. Please refer to the separate "**E-Plex Wireless Site Survey**" manual for further details.

Discover Device

Click **Online ZigBee Network** and then select **Discover Device** or click its equivalent icon.



The system will display the following screen. You must first configure your E-Plex Gateway unit so that it will communicate with your Server as a wireless “hub” to which all your wireless locks (and Routers, if any) will eventually communicate sending/receiving data.

There is one of two ways to configure the Gateway to communicate to the Server: either

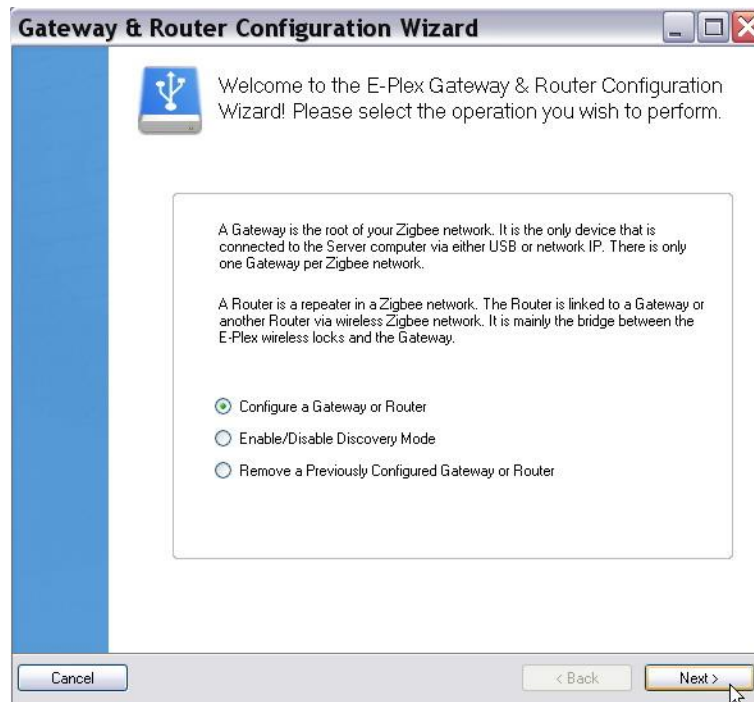
(i) via USB communications protocol, or

(ii) via TCP/IP communications protocol. **Important:** If it is going to be via TCP/IP, please consult with your IT/Network Administrator for your IP Address and related network settings etc that are specific to your facility.

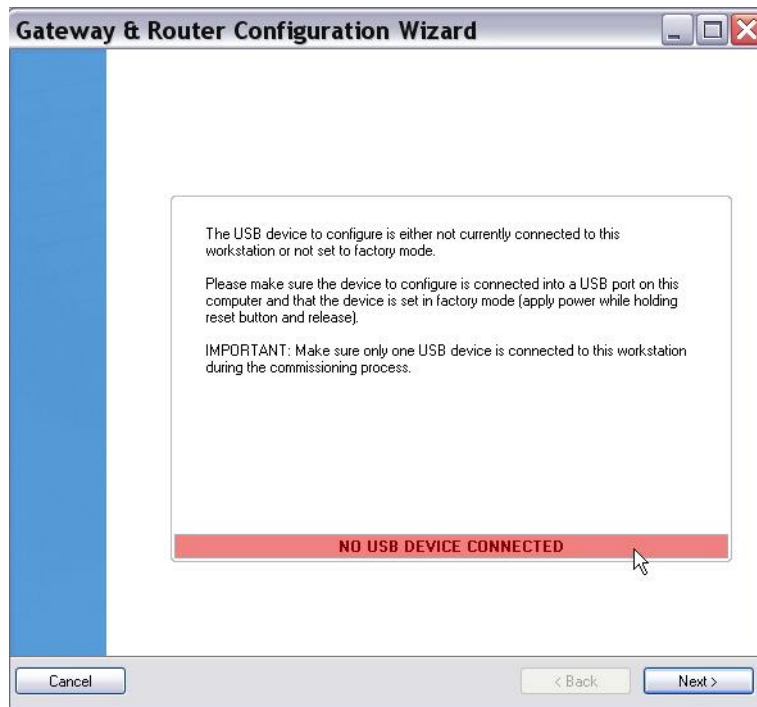
Important: In the following example of configuring the E-Plex Gateway, we will assume that it is USB protocol and that the Server/Client/PC and the M-Unit all reside on one standalone (same) PC which is non-networked. Use of an M-Unit handheld is not required for E-Plex wireless locks and system.

A-1: Configuring an E-Plex Gateway

From the “Gateway & Router Configuration Wizard” screen, select **Configure a Gateway or Router** and click **Next**.



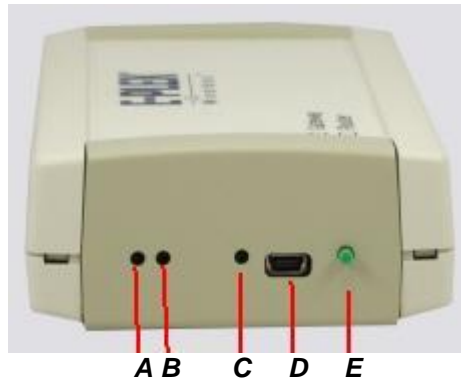
The system will display the following message “No USB Device Connected” with a red background on the Configuration Wizard screen.



A-1(i): Connect Gateway: Connect the E-Plex Gateway to the Host PC as follows: Connect the standard USB connector end of the “USB <-> USB Mini-B” cable to a USB port of the Host PC; depress the Green *Reset* button on the E-Plex Gateway unit and the *Reset* button still depressed, connect the other end of the USB cable (USB Mini-B connector) to the E-Plex Gateway unit, and then release the Green *Reset* button. This power up procedure ensures that the Gateway is in default factory reset mode, ready for wireless communication.

Gateway / Router: Top and Side Views with Ports & LEDs

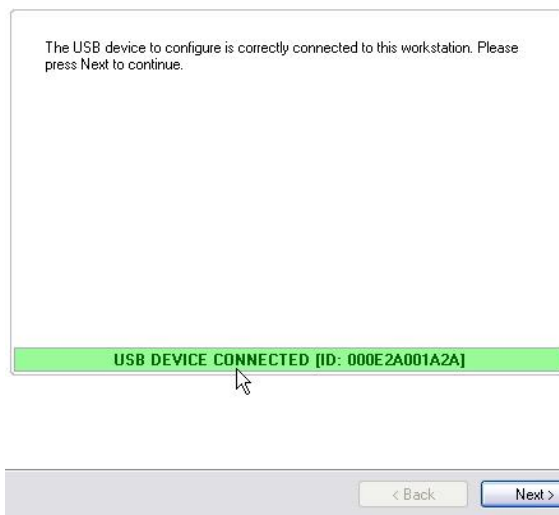




Where,

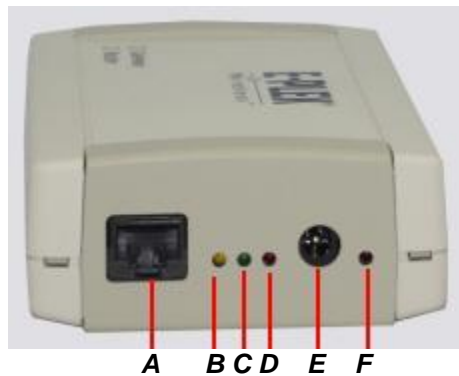
- A (Green) & B (Red) = Communications status light pair,**
- C (Red) = Power ON indicator light,**
- D = USB Mini-B type connector, and**
- E = Green Reset button**

On Gateway power up, the Green light closest to the USB Mini-B connector will come ON and stay ON. Also, the Red & Green light pair next to this will also turn ON for a few seconds, followed by the RED light going OFF but the Green light flashing ON/OFF every one second. This indicates that the E-Plex Gateway is ready to be configured by the Host PC's Enterprise software – this is also indicated by the “USB DEVICE CONNECTED” message on the Configuration Wizard screen of the PC with a green background.



Note: On the opposite side of the Green *Reset* switch of the Gateway box, you will see a single Red light staying ON which also indicates that the Gateway power is ON. You will also see three lights in a row -> Amber, Green and Red located between the Gateway's AC adapter jack and its CAT-5 Ethernet adapter jack flashing continuously every 2 seconds, if the Gateway is not connected to a network. If on the other hand, the Gateway is connected to your network via Ethernet connection and is configured and working properly, you will see the middle Green light flashing rapidly and continuously and the other Amber and Red lights staying ON permanently.

► Using the E-Plex Enterprise Software



Where,

- A** = Ethernet PoE (Power Over Ethernet) network cable jack,
- B (Amber), C (Green) & D (Red)** = Network Status indicator lights
- E** = 5VDC input jack (from AC adapter), and
- F (Red)** = Power ON indicator light,

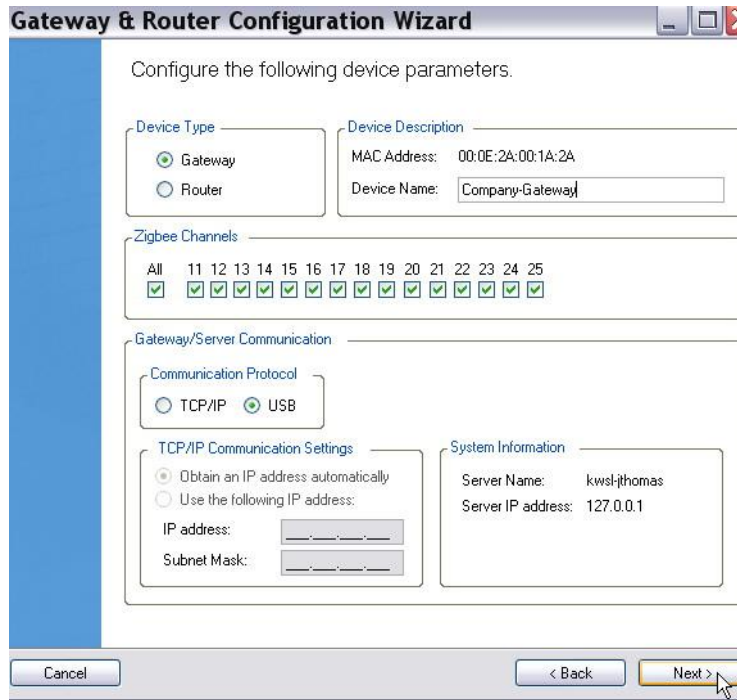
Click **Next**. The following message “This device is not currently configured in the system” will be displayed.



Click **OK** and then **Next**. The system will display the actual “Gateway & Router Configuration Wizard” screen where you must fill in all the required info in all applicable fields.

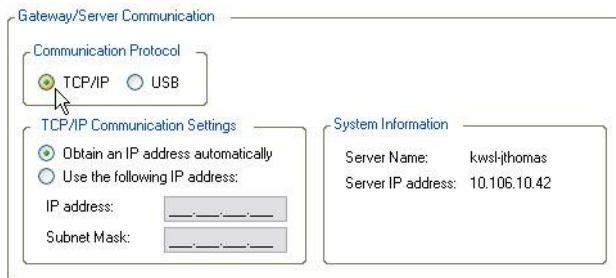
In the screen above, we will configure the following parameters of the E-Plex Gateway (example only):

- Device Type* = Gateway
MAC Address = [automatically retrieved by system and displayed here]
Device Name: = Company-Gateway
ZigBee Channels = Select All, unless you know that some channels are already being used by other wireless devices in your facility. If so, you must uncheck these specific channels to avoid any RF interference
Communication Protocol = USB
Server Name = [automatically retrieved by system from Windows OS on this PC and displayed here]
Server IP Address = [automatically displayed as 127.0.0.1 for a non-networked system]. Or, if this PC is networked consult with your IT/Network Administrator; in this case your Gateway/Server Communications protocol above must be set to TCP/IP (instead of USB).



Important for Network Environment: If your environment is (Server/Clients) networked, you will choose “TCP/IP” under “Gateway/Server Communication / Communication Protocol” option. Additionally, you may choose to either “*Obtain an IP address automatically*” or provide your specific IP address parameters (IP address & Subnet Mask) by choosing “*Use the following IP address*”.

If “Obtain an IP address automatically” is selected, the *Server Name* and the *Server IP address* info/values will be automatically detected and displayed by the software which cannot be changed. ***Please check with your IT Administrator to make sure*.**

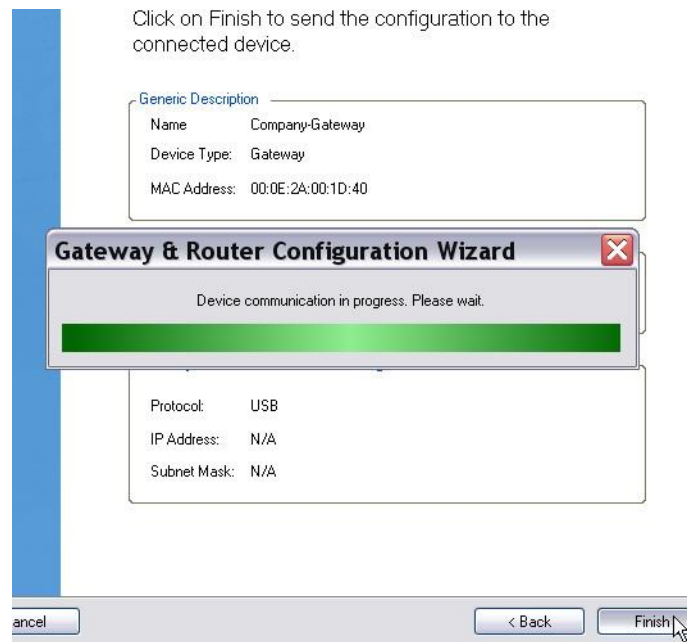


[Or],

If “Use the following IP address” is selected: ***You must consult with your IT Admin*.**



Click **Next** to configure the Gateway and on successful completion, click **Finish**.



Warning: At the end of the ZigBee commissioning process a pop up window appears informing you to disconnect the USB connected device. **Do NOT disconnect the gateway until the red led comes on and then goes out.** This indicates the configuration you selected has been written to the gateway.



Click **OK** to save and exit this Gateway configuration menu.

Important:

- (1) In this configuration setup, ie., USB Communication Protocol, you must permanently keep the USB cable connection between the Host PC and the Gateway unit and also the Host PC (Server/Client) power must be always ON for your ZigBee wireless network to be operational. If the power goes off, the wireless locks will still operate normally, except that you will not be able to see the locks' events "live" on the PC screen, nor will you be able to send any remote wireless commands to these locks (program, audit, momentary unlock, emergency lock down, passage etc).

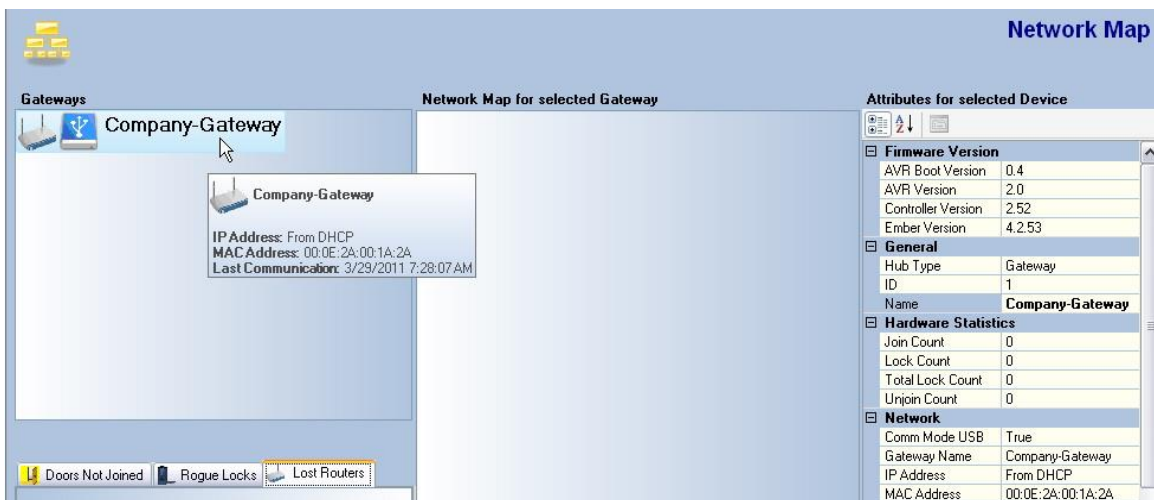
► Using the E-Plex Enterprise Software

- (2) If your Gateway configuration setup on the other hand was for TCP/IP Communication Protocol, you must disconnect the USB cable now and power up the Gateway with its AC adapter, unless you get the power through your PoE (Power Over Ethernet) network cable connection. You must connect an Ethernet network cable between the E-Plex Gateway and a network port of your facility's network jack; the Host PC should be already connected to your network environment.

From the Main menu, click **Online ZigBee Network** and then select **Manage** or click its equivalent icon.

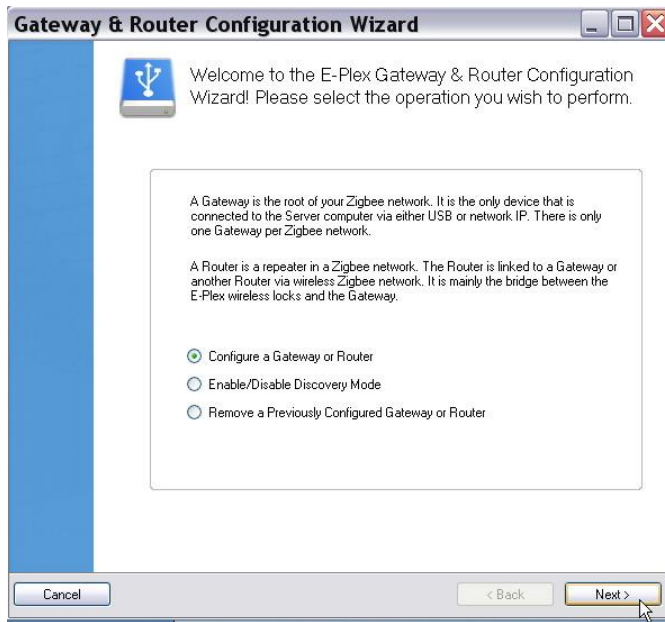


The system will display the following screen indicating that the E-Plex Gateway, named the "Company-Gateway" (which can be renamed anytime) of your wireless network has been configured properly. Later on after you finish creating all your E-Plex wireless locks/doors, access schedules, users etc in the database, you will make the wireless locks "join" this wireless network by, (i) sending software command from the Host PC over the wireless network and, (ii) by performing a ZAC (ZigBee Access Code") code entry process physically at each wireless lock/door.



A-2: Configuring an E-Plex Router

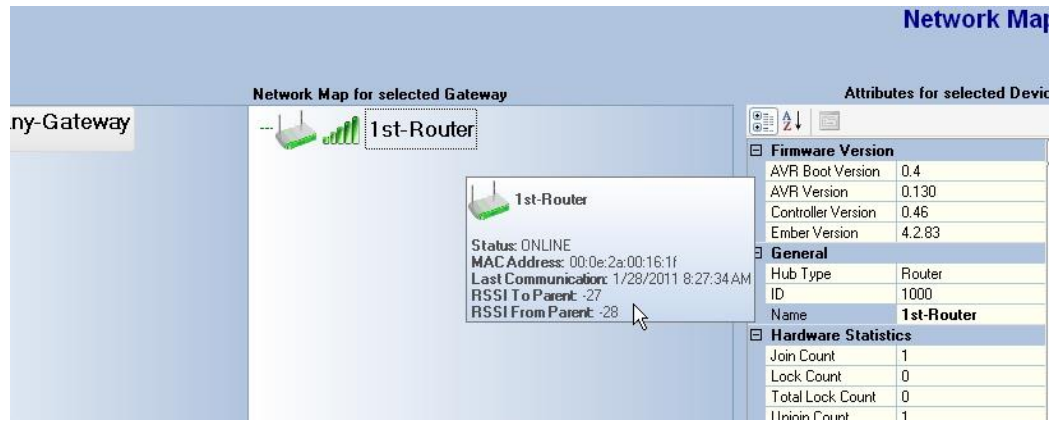
The procedure is similar to configuring an E-Plex Gateway described above but with much less parameters to setup for an E-Plex Router. The Router configuration is required only if your site is deemed to require one or more Routers after the site survey. As before, you must start with the following menu dialog to configure a Router.



The Router configuration does NOT require a USB connection like for a Gateway configuration. **Important:** You must put the Gateway in “Join On” mode first by selecting either the [B-1\(i\)](#) or the [B-1\(ii\)](#) Gateway Join-On method, as shown below in the next section. You must power up the Router with its AC adapter and then press the Green Reset switch of the Router to initialize. The Router will be successfully added to your E-Plex (ZigBee) wireless network.

After a successful configuration of each Router, the **Network Map** screen will display the status of each Router under “*Network Map of selected Gateway*” screen area with the Router’s retrieved MAC address, signal strength etc. You can rename the Router’s name from its default MAC address value name to a meaningful name such as “1st Router” as shown in this example screen.



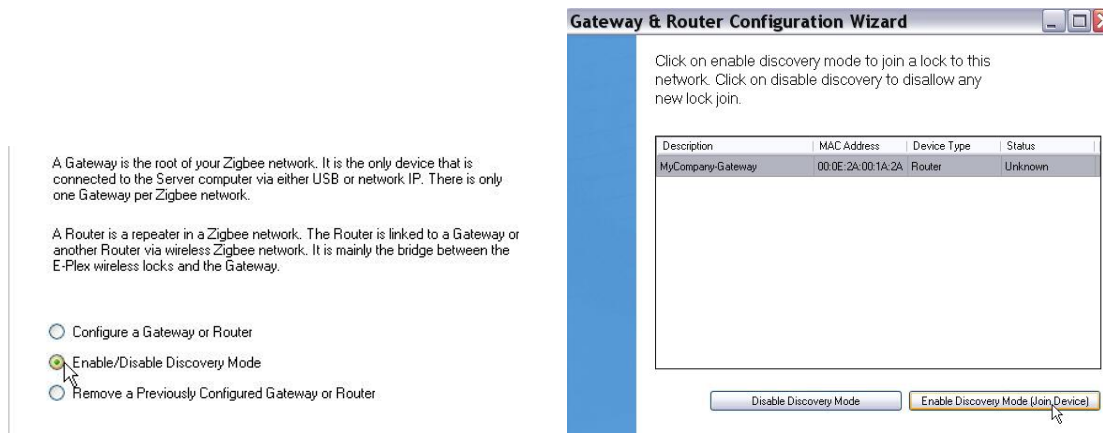


B-1: Enable E-Plex Gateway to “Join On” Mode

You can make the wireless locks and any Routers on site part of the E-Plex ZigBee wireless network by “joining” them to your E-Plex Gateway by one of 3 methods as described below. When the Gateway enters the “Join On” mode, it will be indicated by the simultaneous flashing of the Red and Green lights pair every second for a few seconds.

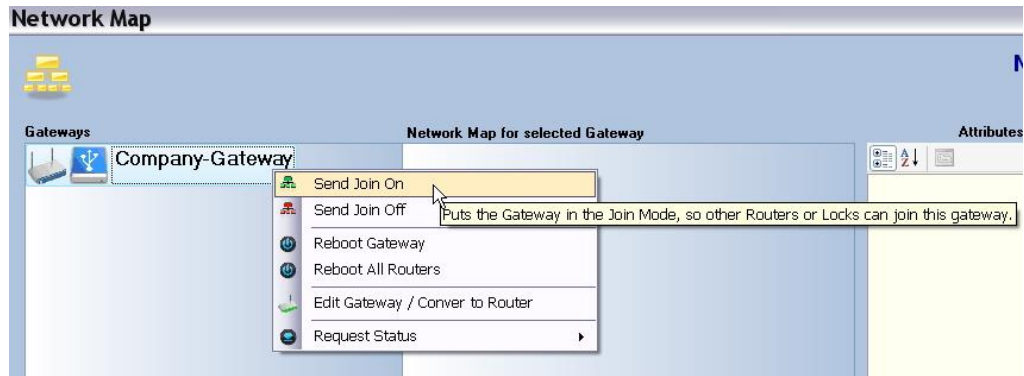
The locks and/or the routers can “join” the E-Plex wireless Gateway, either:

B-1(i): From this menu by enabling the join mode of the Gateway,



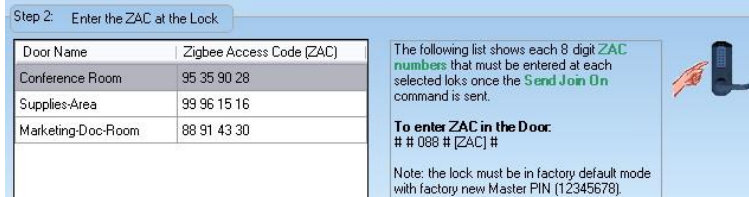
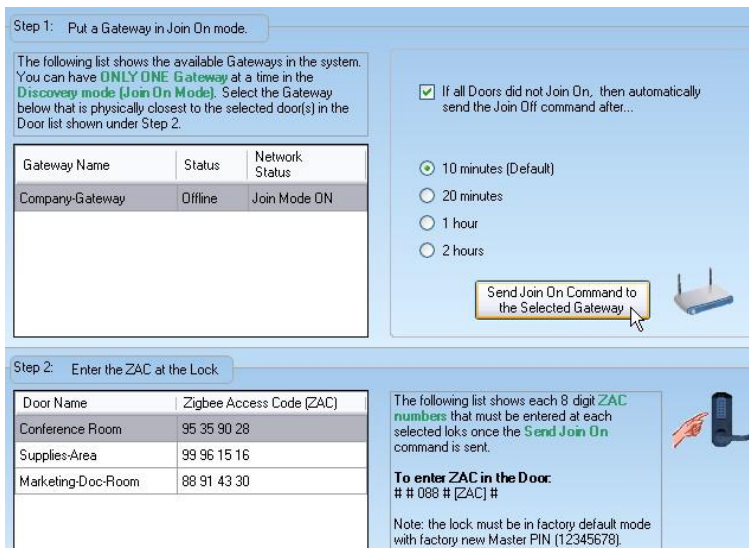
[Or,]

B-1(ii): From the **Network Map** menu under the **Gateways** panel where you select and highlight the Gateway’s name, right click and click “*Send Join On*”,



[Or,]

B-1(iii): From the **Manage Doors** menu, select and highlight the wireless lock(s), click “*Discover & ZAC*”. First as per *Step 1* in the screen menu, select and highlight your configured Gateway and then click “Send Join On Command to the selected Gateway”.



Once the “Join On” command is sent to the Gateway by either one of the above three methods, the Gateway “join” symbol will turn from “Off” (blue background) to “On” (green background) as shown below, indicating that it is ready to accept wireless locks and Routers in its ZigBee network.



When E-Plex Gateway is in “Join On” Mode:



Important: After sending the “Join On” command from the Host PC by either one of the above three methods -> B-1: (i), (ii) or (iii), you (actually, one of your associates) will need to be physically present at the wireless lock/door to enter this lock’s 8-digit unique ZAC (ZigBee Access Code) number at the lock’s keypad, as shown above in B-1(iii) under Step 2. The exact ZAC sequence for a wireless lock is described later under the section **Manage Doors**.

The above two combined actions – the wireless Gateway “join on” command at the Host PC and the ZAC’ing of the lock at the lock’s keypad will make the selected wireless lock(s) join and be part of the E-Plex wireless network.

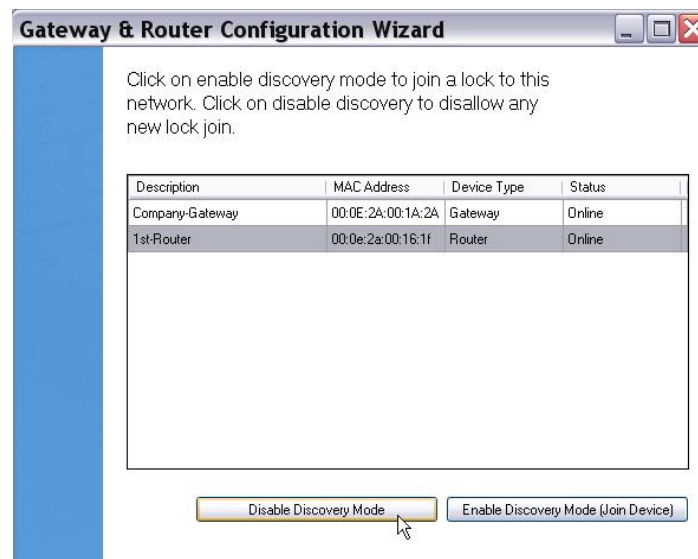
B-2: Disable E-Plex Gateway from “Join On” to “Join Off” Mode

You can disable the E-Plex Gateway from “Join On” to “Join Off” mode from your site’s wireless locks and any wireless Routers, if required by selecting and clicking “Disable Discovery Mode”.

A Gateway is the root of your Zigbee network. It is the only device that is connected to the Server computer via either USB or network IP. There is only one Gateway per Zigbee network.

A Router is a repeater in a Zigbee network. The Router is linked to a Gateway or another Router via wireless Zigbee network. It is mainly the bridge between the E-Plex wireless locks and the Gateway.

- Configure a Gateway or Router
- Enable/Disable Discovery Mode
- Remove a Previously Configured Gateway or Router

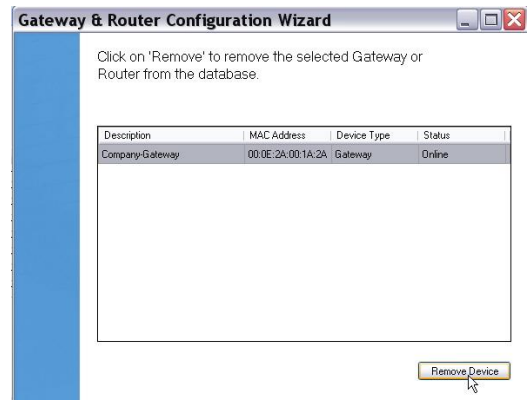


C: Remove Previously Configured Gateway(s) or Router(s)

You can remove your previously configured Gateway and/or Router(s) from the system database, if required, say due to temporary servicing of the unit(s) etc. This is done by selecting “Remove a Previously Configured Gateway or Router” and then highlighting the device(s) to be removed and clicking the “Remove Device” button.

Warning: If you remove a working E-Plex Gateway from the system database, you will not be able to perform any wireless commands and will not be able to monitor wireless events from your Host PC. However, the wireless locks will still work and grant/deny access to users as if they are in standalone mode.

- Configure a Gateway or Router
- Enable/Disable Discovery Mode
- Remove a Previously Configured Gateway or Router



Important: When you are ready again for wireless operation, you must reconfigure your Gateway and Router(s), if any as described above in steps A-1 and A-2 and must re-join all your wireless locks again to the ZigBee network.

[End]

Managing Door Groups

Door groups provide a way to manage multiple doors at a site. The Enterprise software allows Operators to group doors according to any criteria.

For example, your site may be a small college campus where you will be installing Enterprise driven E-Plex locks in say, three different buildings. In this case, you can create three different door groups and name them Admin Bldg, Library and Supplies Depot. Or, if you prefer you can create many different door groups within one building – for example, door groups named Staff Offices, Common Area, Recreation Center, Theater, Labs etc inside the Admin Bldg.

[Start]

For Wireless Mix: If your facility has a **mix of** both non-wireless (standalone) and **wireless** E-Plex locks, it is highly recommended that you place these two types of lock series in two types of main Door Groups, for example, one main group called “DG-Wireless” where you can place all your wireless enabled locks and the other called “DG-NonWireless” or “DG-Standalone” etc where you place all your non-wireless locks. This segmentation makes it easier to manage all your doors/locks in your facility.

[End]

The system allows you to manage door groups from the **Door Groups** menu.

Important: When creating a new door group, you will be prompted to assign one (and only one) Door Group Manager for this door group. The DG Manager will have complete control over all the locks/doors belonging to this door group, ie., the DG Manager will be just like the global Master user, but in this door group only.

Note: You can define any number of door groups in the database.

- To manage door groups, select **Manage Door Groups** from the **Door Groups** menu, or click the **Manage Door Groups** button.



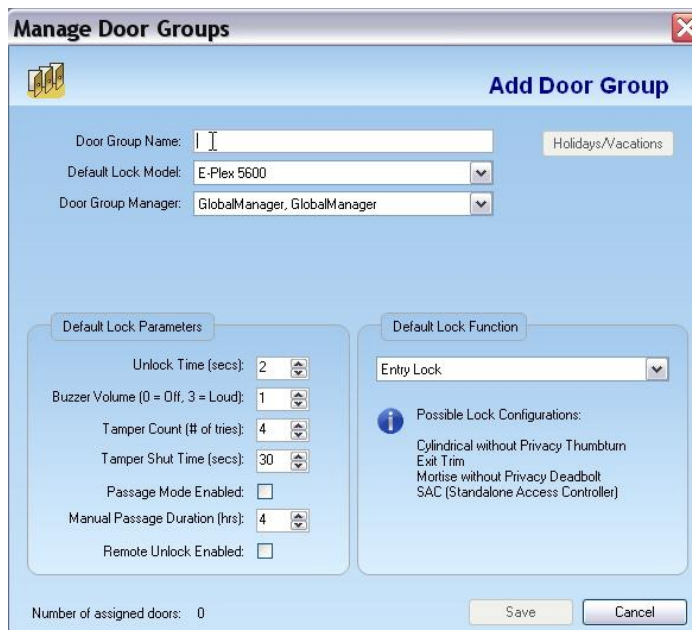
- The software displays the **Manage Door Groups** window. From this window, you can add, edit, or delete door groups. By default, there already exists a Door Group called “Default” belonging to a default Door Group Manager called “GlobalManager”. You can edit the name of this Door Group (and this Manager’s name under Users menu, shown later) to suit your site’s needs.



Adding a Door Group

Complete the following steps to add a door group:

- From the **Manage Door Groups** window, click **Add**. The software displays the **Add Door Group** window as shown below.



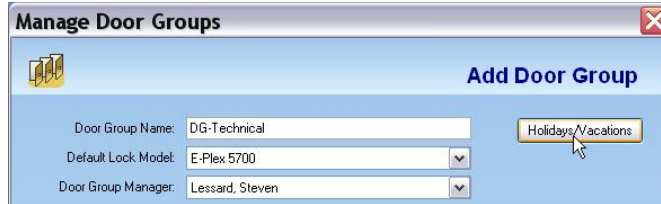
- In the **Door Group Name** field, type the name of the door group you are adding.

Note 1 : The door group name can be a maximum of 20 alphanumeric characters and no spaces and special characters are allowed, except for the “-“ character.

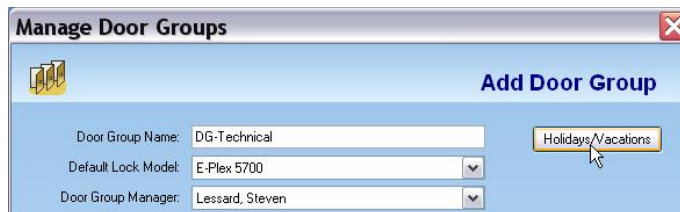
Note 2: When you create a new door group, you will be also creating various default parameter values of all the doors/locks that will belong to this door group. However, these default lock parameters can be changed to suit individual door/lock requirement when you create the individual doors later that will belong to this door group.

► Using the E-Plex Enterprise Software

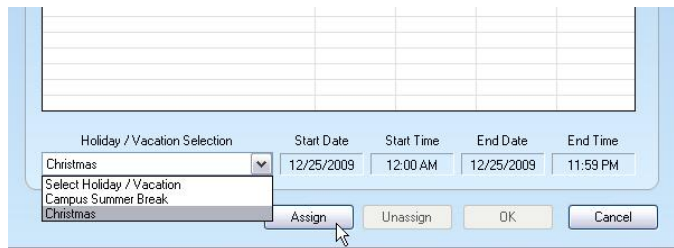
- You may keep the Default Lock Model as is (configured in System Settings earlier) or change it to another lock model from the pick list.
- Select the (single) **Door Group Manager** from the drop-down list; in the very beginning you will have only the default door group manager to choose from the pick list -> GlobalManager. As stated earlier, there can be only one Door Group Manager for this door group from the available any one of the normal Manager users in the system.



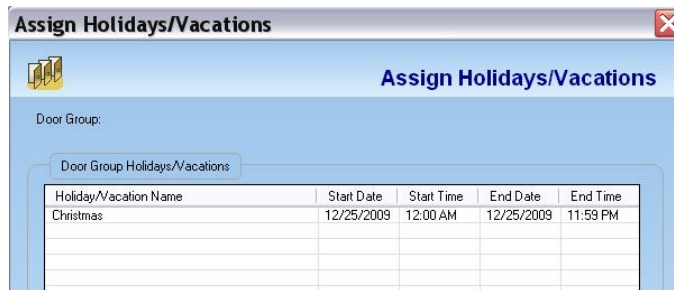
- Click **Holidays/Vacations** to select the holidays and/or vacations to be applied to this door group, if desired. The software displays the **Assign Holidays/Vacations** window.



- Select the desired holiday or vacation block from the **Select Holiday/Vacation** drop-down list at the bottom of the window including the Start and End Dates and Times.



- Click **Assign**. The system displays the assigned holiday or vacation block in the **Door Group Holidays/Vacations** area.



- Click **OK**. The software returns to the **Add Door Group** window. You can assign more holidays/vacation blocks if desired.
- Finally, adjust the following default lock parameters for all locks in this door group, as appropriate, using the up and down arrows:
 - Unlock Time (secs)
 - Buzzer Volume (0 = Off, 3 = Loudest)
 - Tamper Count (# of tries)

- Tamper Shut Time (secs)
- Manual Passage Duration (hrs)
- Select **Passage Mode Enabled** option, if you want your locks in this door group to be manually (by the Master and/or by a Manager) or automatically activated/de-activated for free passage at the lock keypad.

Note: The Passage Mode is automatically and permanently enabled for a lock with “Residence Lock function” and so the passage mode option will be grayed out if the lock function selected is Residence.

- Select **Remote Unlock Enabled** option, if you need. **Note:** For this option to work, you must have an E-Plex lock that is electronically pre-configured as such from the factory.
- Select the **Lock Function** from the drop-down list: for an E5xxx series lock as – either Entry (default), Residence or Privacy; and for an E3xxx series lock as – Latch/Exit/Swingbolt.

Note 1: The Remote Unlock is automatically disabled for a lock with Residence lock function and so this option will be grayed out if the lock function selected is Residence.

Note 2: For instructions on how to setup a Lock Function in an actual E-Plex lock and what each Lock Function means, please refer to the “**E-Plex 5x00 (and 3x00) Lock Function Setup Guide**” that came with the lock in the lock box. By default, all locks come out of the factory whose lock function is pre-configured as “Entry (5x00) or Latch (3x00)” lock function.

- Click **Save**. The system saves the changes and displays a confirmation message.
- Click **OK**. The software displays the updated **Manage Door Groups** window.



- Click **OK**. The software displays the updated **Manage Door Groups** window.

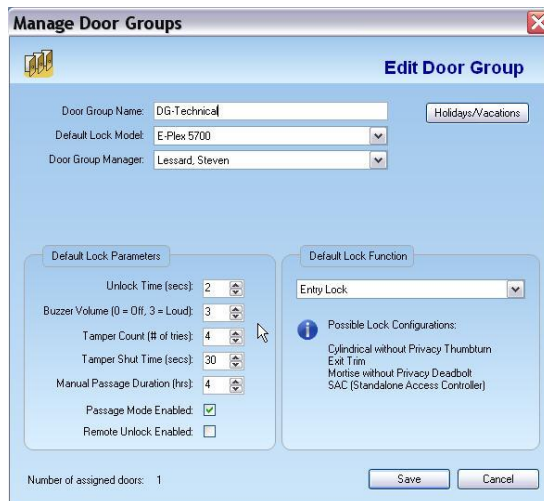


Note: You can add additional door groups at any time.

Editing a Door Group

Complete the following steps to edit a door group:

- From the **Manage Door Groups** window, select a door group to edit.
- Click **Edit**. The software displays the **Edit Door Group** window.



- Edit any or all required fields that you want changed.
- Click **Save**. The system saves the changes and displays a confirmation message.



- Click **OK**. The software displays the updated **Manage Door Groups** window.

Note: You should update your locks whose parameters have been modified, first by downloading the affected locks' configuration data to the M-Unit and then by programming / uploading this information to the locks.

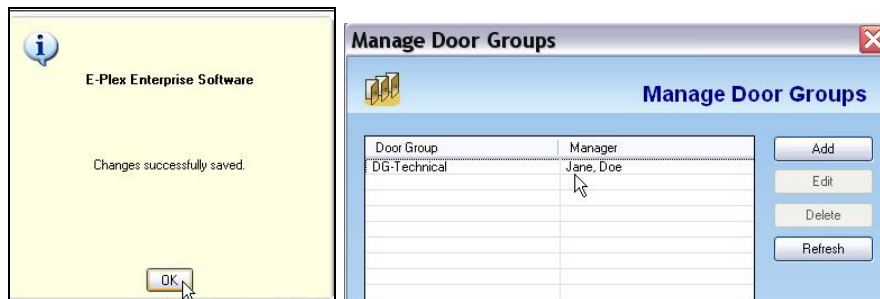
Managing Door Group Managers

Complete the following steps to manage door group managers:

- From the **Manage Door Groups** window, select the Door Group name where you want to change the DG Manager from the current person to a different person and then click **Edit**. Select the Manager you want to assign as the (one and only) DG Manager for this entire Door Group.



- Click **Save** and then **OK**. The software displays the updated **Manage Door Group Manager** window.



- Click **Close** to exit from this dialog.

Deleting a Door Group

Complete the following steps to delete a door group:

- From the **Manage Door Groups** window, select a door group to delete and then click **Delete**. If there is a door or doors that still belong to this door group, you will get the following warning message.



Note: You cannot delete a door group if it contains locks/doors within this group. You must either unassign all these doors from this door group and move them to a different door group, or must delete them all from the database. Only after this will you be able to delete this particular door group from the database.

- Perform operation(s) as per the message above, if required and then perform the delete operation of this door group.
- The software prompts you for confirmation.



- Click **Yes**. The software displays the updated **Manage Door Groups** window.
- Click **Close** to exit the **Manage Door Groups** window.

Note: You should update your locks to reflect modified door groups by programming the M-Unit and uploading the information to the locks. For more information, refer to **M-Unit Handheld** in Chapter 5, **Programming and Auditing Locks**.

Managing Doors

In the Enterprise software, doors are literally the physical doors at your site where the applicable E-Plex locks are installed. You can define new doors, edit parameters of doors and delete existing doors from the database.

[Start]

For Wireless: Your facility may have either a **mix of** both non-wireless (standalone) and **wireless** E-Plex locks, or **all wireless** locks. For wireless enabled locks, additionally, you will have to select all wireless related parameters so as to enable these locks to “join” your E-Plex ZigBee wireless network – this was (i) either already configured using your E-Plex Gateway under the *Systems Settings* menu earlier, or (ii) you will need to configure joining the network using your E-Plex Gateway, anytime later on under the *Systems Settings* menu.

[End]

The software allows you to manage doors through the **Manage Doors** menu.

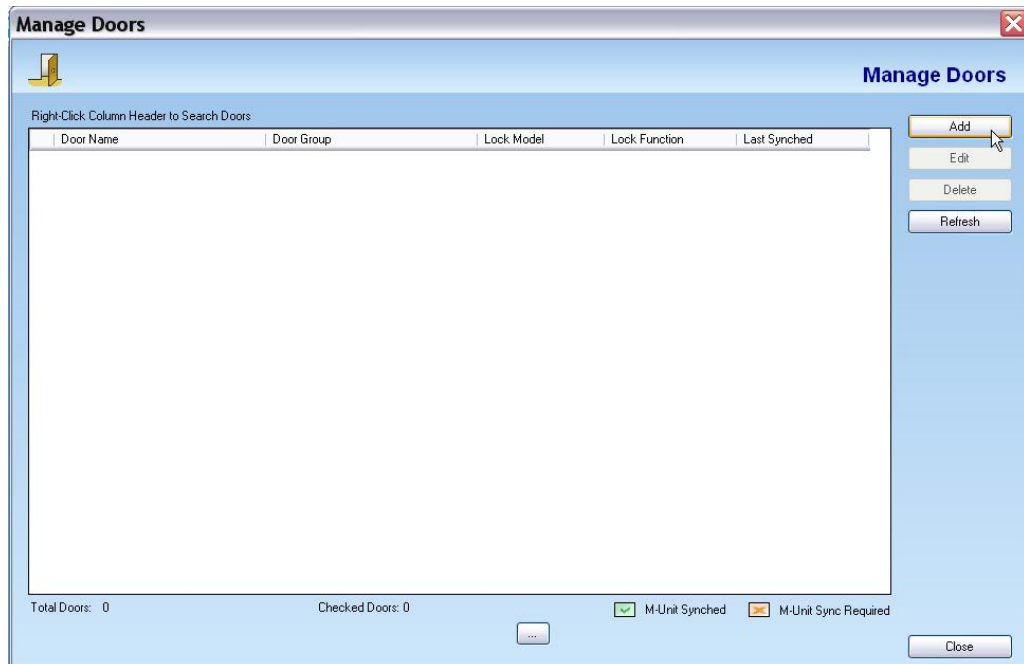
Note: You can define unlimited number of doors in the database.

To manage doors, select **Manage Doors** from the **Door** menu, or click the **Manage Doors** button.



Note: The system will alert you if there is no Door Group already created in the system, in which case you must create one.

Click **OK**. The software displays the **Manage Doors** window.



Adding a Door [Standalone / Non-wireless]

Complete the following steps to add a door:

- From the **Manage Doors** window, click **Add**. The software displays the **Add Door** window.

- Select a **Door Group** from the drop-down list.

Note: Depending on the door group name you selected here, all the default lock parameter values of this door will be exactly the same values as those in this door group since they are derived from this door group. However, you can change any or all lock parameter values for this door, if preferred.

- In the **Door Name** field, type the door name.

Note: A door name can be a maximum of 20 alphanumeric characters and no spaces and special characters are allowed, except for the “-“ character.

- Click **Access Schedules** to select the schedules that were previously created under the Manage Schedules menu. Assign schedules to this door so that during this time the lock will grant access to valid users. The software displays the **Assign Door Access Schedules** window.
- Select an **Available Schedules** from the drop-down list at the bottom of the window. The software displays the schedules in the **Door Access Schedules** pane.

Note: Once a schedule is highlighted, the **Available Schedules** area becomes grayed out.

Manage Access Schedules ✕

Assign Door Access Schedules

Door Information

Door Group: DG-Technical
 Door Name: Physics Lab-1
 Lock Model: E-Plex 5700
 Lock Function: Entry Lock

Door Access Schedules

Schedule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start	End	Credential	Passage Mode
Always	✓	✓	✓	✓	✓	✓	✓	12:00 AM	12:00 AM	Card	Manual

Available Schedules

Select Schedule: End

- Select Schedule
- 7AM-6PM,M-F
- Always
- EveningShift

Required Credential:

Required Passage Mode:

Refresh Assign Unassign OK Cancel

- Select the **Required Credential** – PIN access, or Card access or PIN & Card access during this selected schedule from the drop-down list.
- Select one of the four **Required Passage Mode** options from the drop down list, either (i) None – ie., the lock never grants free passage, (ii) Automatic – ie., the lock automatically enters free passage at the start of this schedule and locks back at the end of the schedule automatically, (iii) First Authorized Passage – ie., the lock goes into free passage, only after a valid “privileged” user opens it with her/his credential at or after the start of this schedule, or (iv) Manual – ie., only the Master or the Manager users can manually set/reset the free passage at the lock keypad between the start and end times of this schedule for the Manual Passage mode duration set in the software.

Door Access Schedules

Schedule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start	End	Credential	Passage Mode
Always	✓	✓	✓	✓	✓	✓	✓	12:00 AM	12:00 AM	Card	Manual

Available Schedules

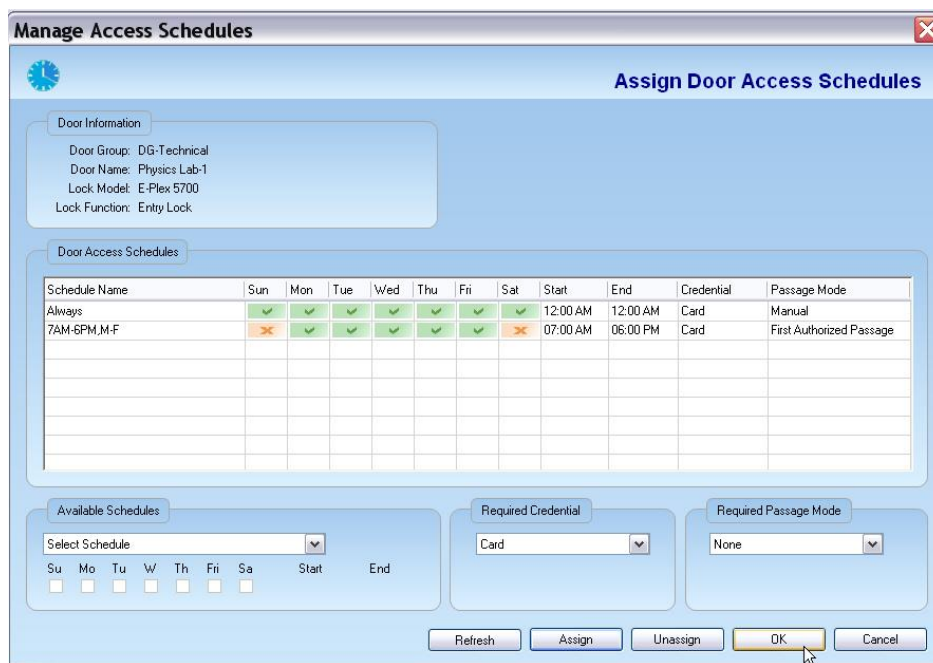
7AM-6PM,M-F

Required Credential:
 Card
 PIN & Card
 PIN

Required Passage Mode:

Refresh Assign Unassign OK Cancel

- Click **Assign**. The software displays the assigned schedule in the **Door Access Schedules** pane.



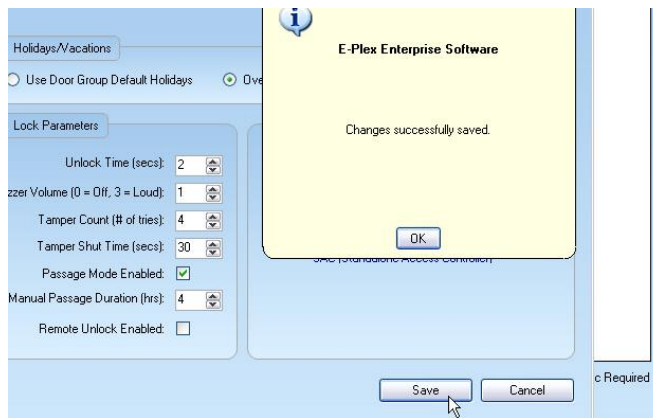
Note: After a schedule is assigned to the door, the drop-down lists return to their default settings.

- Click **OK**. The system displays the **Edit Door** window.
- Select the appropriate **Holidays/Vacations** settings:
 - **Use Door Group Default Holidays**, if you are happy with the holiday setting previously set under the Manage Door Groups menu where this lock belongs.
 - **Override Holidays for this door**, if you want to change the previously setup holiday settings under the Manage Door Group menu.

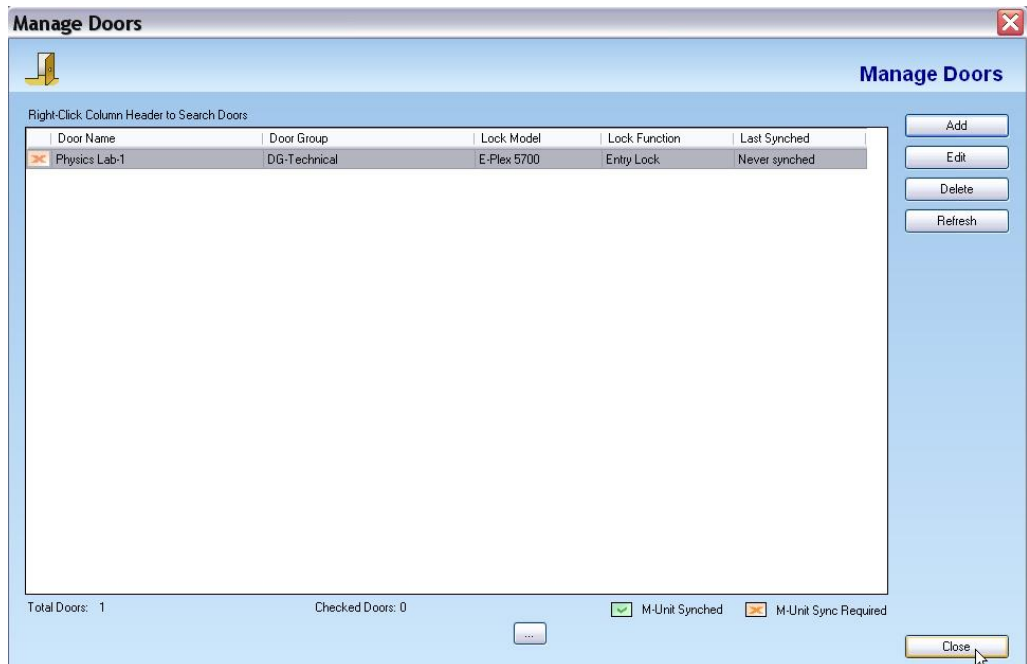
Note: When **Use Door Group Default Holidays** is selected, the **Holidays/Vacations** button is grayed out.

Note: Refer to the separate “E-Plex 5X00 and 3x00 Lock Function Setup Guide” for instructions on setting up the desired BHMA lock function at the lock itself.

- Click **Save**. The system saves the changes and displays a confirmation message.



- Click **OK**. The software displays the updated **Manage Doors** window.



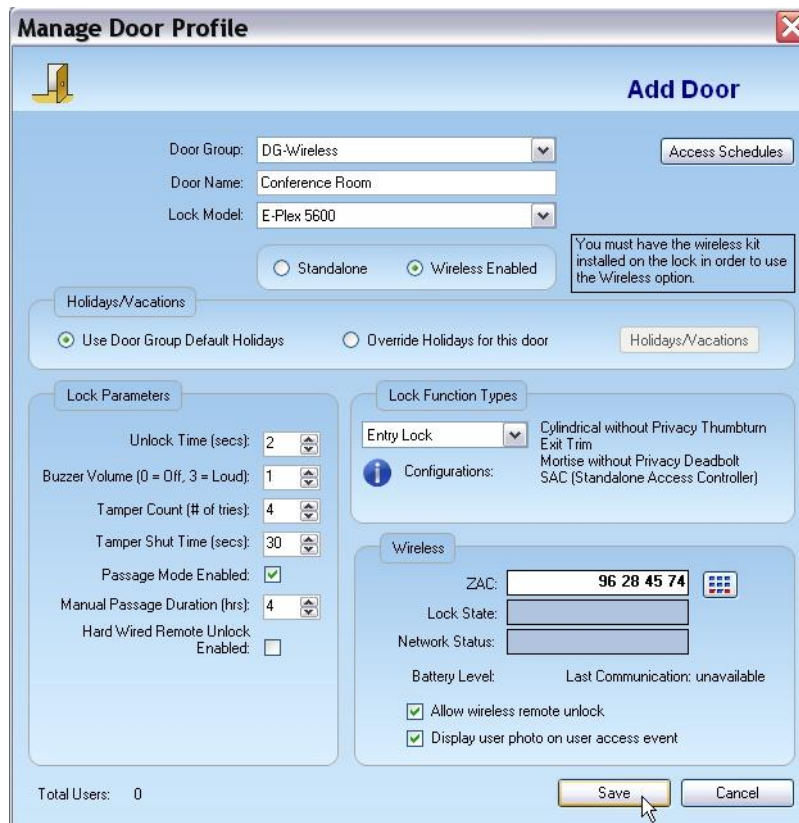
Note: You will see an orange color “X” symbol against the Door Name in the very first column indicating that this door configuration data needs to be synchronized with (transferred to) the M-Unit PDA before programming this door. Once sync’d with the PDA, the orange “X” will be replaced with a green “check” symbol for this door.


You can add additional doors at any time.

[Start]

Adding a Door [Wireless]

The following section will highlight only the wireless lock related menu parameters that need to be entered and completed, since all of the non-wireless parameters are the same as that for the standalone lock parameters as described earlier. The following few screen shots show adding a wireless door called “Conference Room”: **Note:** The “Wireless Enabled” option for a lock will be available only after you setup and configure your wireless E-Plex Gateway under the *System Settings* menu.



ZAC (ZigBee Access Code): This is an 8-digit number, generated automatically by the system as a unique random number for the wireless lock. A different random ZAC number can also be generated anytime by clicking on the small “keypad template” square box () shown on the right of the ZAC field. The ZAC number must be saved in the Software before it can be used wirelessly to ‘Join On’ a lock.

When Adding or Editing a door where the Lock Type is Narrow Stile (E3200/3600/3700 series), the type of locking device used will determine if Emergency Commands (Emergency Open and Emergency Lockdown) will be allowed.

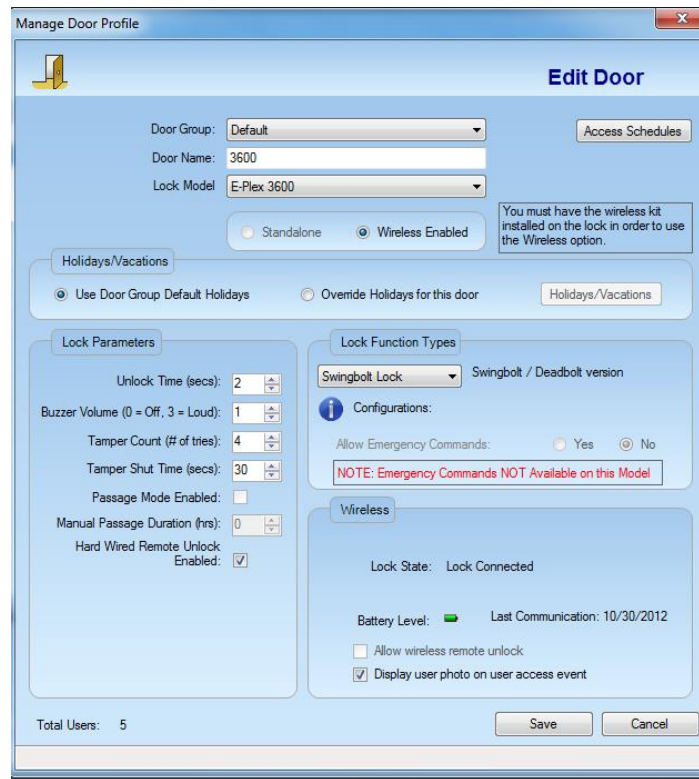
Per below, when choosing a Deadlatch Lock (E3x65 series), you may select 'yes' under emergency commands only if the Adams Rite locking device will not be manually set to Latch Holdback (commonly known as dogging the latch).

The screenshot shows the 'Manage Door Profile' window with the 'Edit Door' tab selected. The 'Lock Function Types' section has 'Deadlatch Lock' chosen from the dropdown menu. Below it, the 'Allow Emergency Commands' radio buttons are set to 'Yes'. A red text box contains the note: 'NOTE: Manual Latch Holdback at Keypad NOT Allowed'. Other settings include 'Door Group: Default', 'Door Name: 3600', 'Lock Model: E-Plex 3600', and 'Wireless Enabled' selected. The 'Lock Parameters' section shows 'Unlock Time (secs): 2', 'Buzzer Volume: 1', 'Tamper Count: 4', 'Tamper Shut Time: 30', 'Passage Mode Enabled: []', 'Manual Passage Duration: 0', and 'Hard Wired Remote Unlock Enabled: [x]'. The 'Wireless' section shows 'Lock State: Lock Connected', 'Battery Level: []', 'Last Communication: 10/30/2012', and 'Allow wireless remote unlock' and 'Display user photo on user access event' both checked. The 'Total Users' is 5. 'Save' and 'Cancel' buttons are at the bottom right.

If Emergency commands are set at 'no', the latch holdback function may be used electronically at the keypad or manually at the Adams Rite deadlatch locking device.

This screenshot is identical to the one above, but with the 'Allow Emergency Commands' radio buttons set to 'No'. The red text box now contains the note: 'NOTE: Manual Latch Holdback at Keypad Allowed'. All other settings remain the same.

If the Swingbolt or Deadbolt version (E3x66 series) is selected, the Emergency Commands option is **not available** (will be greyed out) since the state of the Adams Rite Deadbolt locking device being locked or unlocked is always unknown in the software so Emergency Commands can't be verified.



Important: Kaba is not responsible or liable when emergency commands are used with these locks if they are incorrectly identified or entered into the software.

You may also optionally select a couple of parameters as shown below, (i) to be able to remotely unlock this door via a wireless command from the Host PC, and (ii) for the system to display the photo of the user (assumes the photo has already been added in the software) every time this person opens this door with her/his valid credential.



When you are ready to “join” a new wireless lock on a door to your E-Plex (ZigBee) wireless network, you must initiate the wireless network “join on” process from the software first. After sending the “Join On” command, somebody else (your colleague, for example) must be physically present at this door location and enter the ZAC on the lock keypad. This action will make the lock join your E-Plex wireless network and at the same time will wirelessly program the lock with user access rights, credentials etc data; you do not need to program the lock with a portable PC M-Unit anymore.

Important: It is recommended that you “ZAC” all your wireless locks at a later time after all your wireless locks are configured with schedules etc and added in the system, your users and credentials are created in the system and assigned to their wireless locks/doors for access etc. Please refer to Chapter 5, “Programming and Auditing Locks” on how to ZAC and program the locks.



Ensure that your E-Plex Gateway has also been configured properly and ready to wirelessly communicate to your locks in the network.



Click **Save** to save this lock's door profile in the database. After you save this door profile, the previous "Manage Doors" menu will open up as shown below, and display the status of this newly added wireless door lock as "Not in Service", ie., it is a wireless lock but has not joined the E-Plex wireless network yet.

The screenshot shows the 'Manage Doors' interface. At the top right, it says 'Manage Doors'. Below that is a table with columns: Door Name, Door Group, Lock Model, Lock Function, Lock State, Last Synched, and Network Status. The table contains four rows of data. To the right of the table are buttons for 'Add', 'Edit', 'Delete', and 'Refresh'. At the bottom of the interface is a control panel with sections for 'Updates' (Sync'd, Sync Required), 'Wireless' (Normal, Low, Dead), and 'Send Wireless Command' (Access, Maintenance, Discover Locks, Put Out of Service). A 'Close' button is also present.

Door Name	Door Group	Lock Model	Lock Function	Lock State	Last Synched	Network Status
Canteen	DG-Manufacturing	E-Plex 5700	Entry Lock	N/A		N/A
Conference Room	DG-Wireless	E-Plex 5600	Entry Lock	Unknown		Not in Service
Office-Corridor	DG-Accounting	E-Plex 5700	Entry Lock	N/A		N/A
Physics Lab-1	DG-Technical	E-Plex 5700	Entry Lock	N/A		N/A

Total Doors: 4

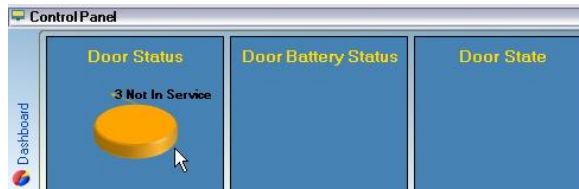
The "Updates" status on the bottom part of the screen above is represented by a semi-circle arrow: if it is Green (), it means that the lock and its users' access data have been transferred (Sync'd) from the Host PC to the lock and programmed for normal use; if it is Red (), it means that the lock needs to be updated (Sync Required) before it can be used.

The "Wireless" signal strength status above is represented in a Green staircase pattern of 5 steps (); a good wireless signal strength range (RSSI = Radio Signal Strength Indicator) should be between -20dB and -80dB. A strong RF signal is represented by the display of 3 to 5 little Green "staircase steps" for proper lock-to-Gateway wireless communication. If there is no RF signal (yet), it will be shown as a Red "staircase steps" pattern ().

You can add as many wireless enabled locks in the database as you have in your facility by repeating the above "Manage Doors / Add" menu dialog sequence. Here is an example where three wireless locks have been added which are not yet "joined" to the E-Plex wireless network..

The screenshot shows the 'Manage Doors' interface with three wireless locks listed in the table. The 'Network Status' for all three is 'Not in Service'.

Door Name	Door Group	Lock Model	Lock Function	Lock State	Last Synched	Network Status
Conference Room	DG-Wireless	E-Plex 5600	Entry Lock	Unknown		Not in Service
Marketing-Docs-R...	DG-Wireless	E-Plex 5700	Entry Lock	Unknown		Not in Service
Supplies-Area	DG-Wireless	E-Plex 5600	Entry Lock	Unknown		Not in Service



“Join” a Wireless Lock to the Network, ZAC & Program:

Assuming that you had finished creating all your wireless enabled locks/doors and assigned all your users who should have access to these doors with proper access schedules, credential usage requirement (PIN, Card or PIN & Card) etc, you are now ready to “Join On”, ZAC and program the locks on doors wirelessly.

Please refer to implementing this actual process which is described in detail in *Chapter 5*, under **“Programming and Auditing Locks”**, towards the end of that chapter.

[End]

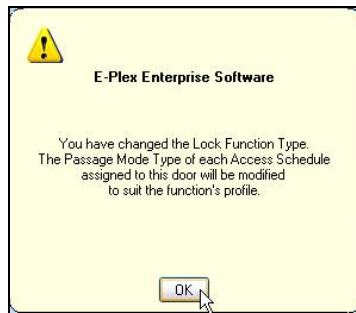
Editing a Door

Complete the following steps to edit a standalone door; **the procedure is very similar for a wireless door also which contains more fields to edit:**

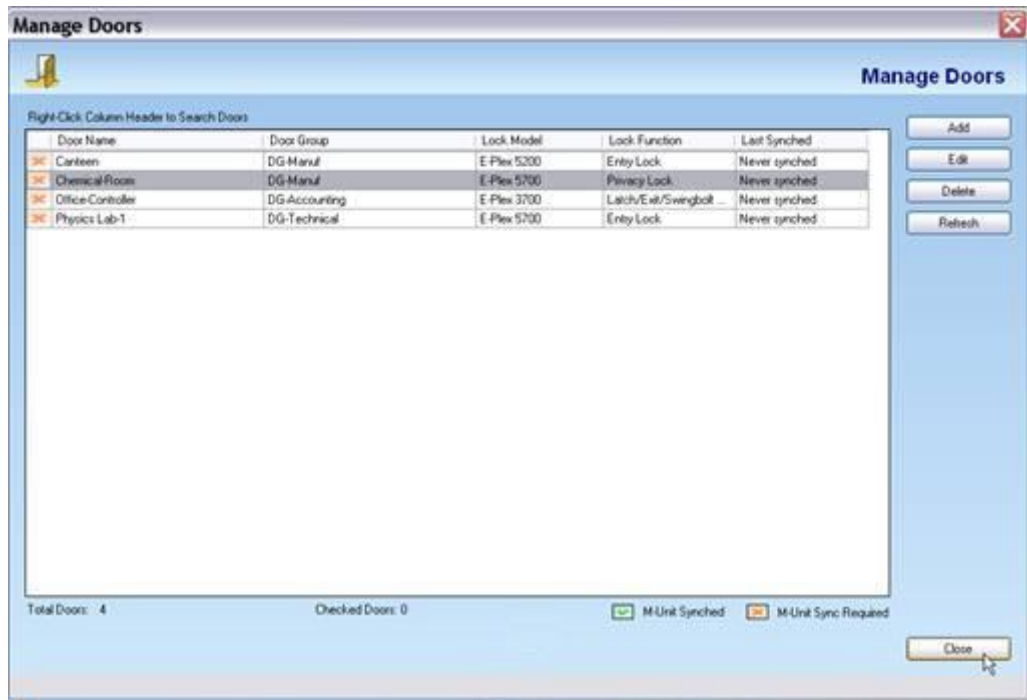
- From the **Manage Doors** window, select a door to edit.
- Click **Edit**. The software displays the **Edit Door** window.



- Select a different **Lock Function Type** from the drop-down list, if appropriate.
- Edit any or all required fields that you want changed.
The software notifies you about the change.



- Click **OK**.
- Click **Save**. The system saves the changes and displays a confirmation message.
- Click **OK** and then **Save**. The software displays the updated **Manage Doors** window.



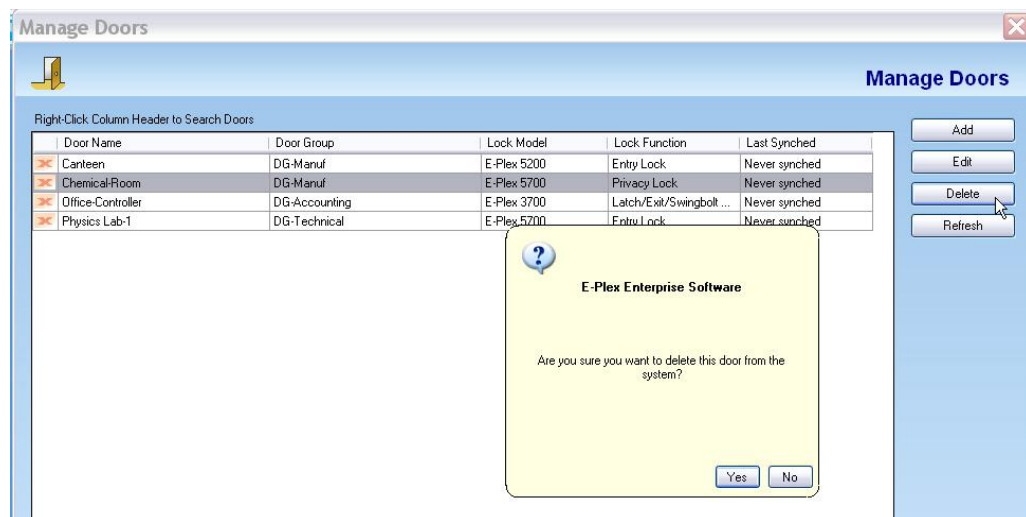
Note: You should update your locks to reflect modified doors by programming the M-Unit and uploading the information to the locks. For more information, refer to **Portable PC M-Unit** section in **Chapter 5, Programming and Auditing Locks**.

Deleting a Door

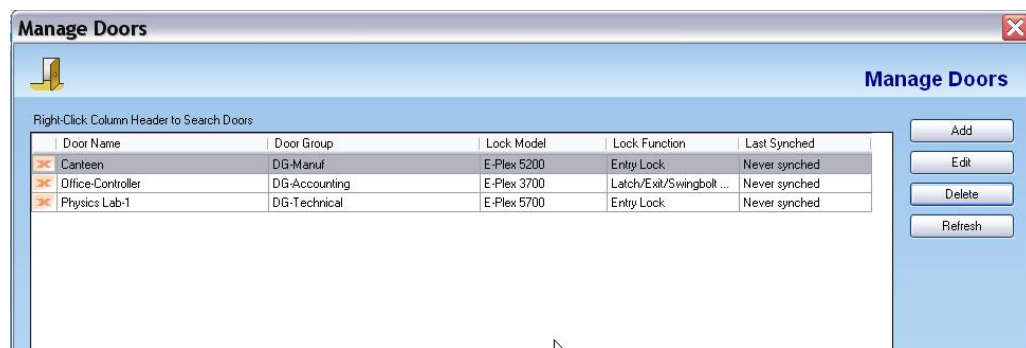
Complete the following steps to delete a door; **the procedure is the same for a wireless door also:**

- From the **Manage Doors** window, select a door to delete.
- Click **Delete**. The system prompts you for confirmation.

► Using the E-Plex Enterprise Software



- Click **Yes**. The door is deleted and the software displays the updated **Manage Doors** window.



- Click **Close** to exit the **Manage Doors** window and return to the Main Menu.

Note: You should update your locks to reflect modified doors by programming the M-Unit and uploading the information to the locks. For more information, refer to **Portable M-Unit in Chapter 5, Programming and Auditing Locks**.

Managing Access Groups

In the Enterprise software, you can group a bunch of doors with their own schedules and credential access types (ie, PIN only, Card only or PIN & Card) etc in an Access Group. This makes it extremely efficient when you need to add a new employee/user in the system, as shown in one of the following chapters under “*Managing Users*” dialog menu – ie., with one selection in the *Managing User* menu dialog, you can assign access rights to this new user in all those various doors contained under one Access Group. **The “Managing Access Groups” procedure is the same for both standalone and wireless doors.**

Adding an Access Group

Note: You can assign any number of access groups in the database.

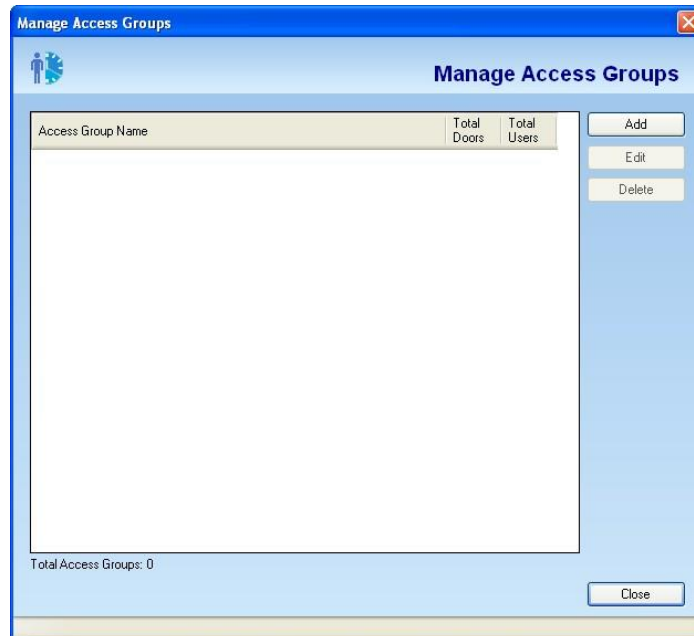
To manage access groups, select **Manage Access Groups** from the **Access Groups** menu or click the **Manage Access Groups** button.



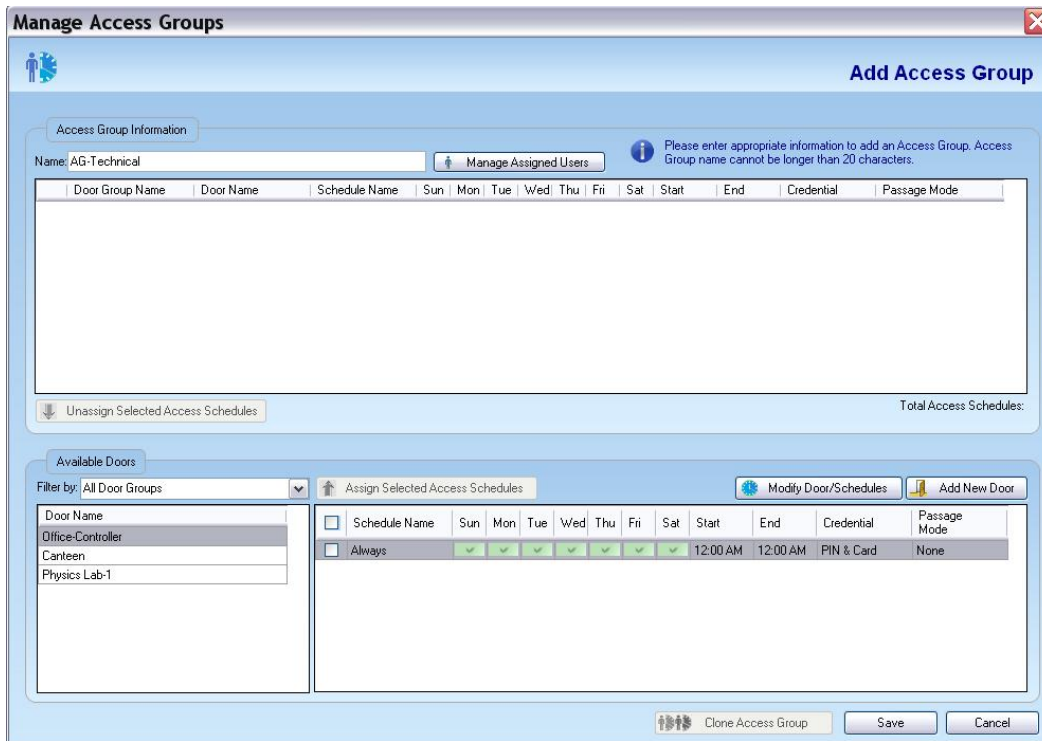
The software displays the **Manage Access Groups** window.

Complete the following steps to add an access group:

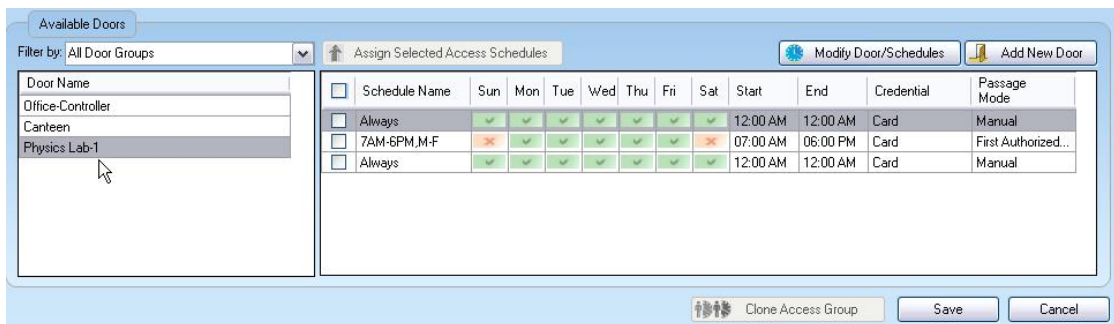
- From the **Manage Access Groups** window, click **Add**.



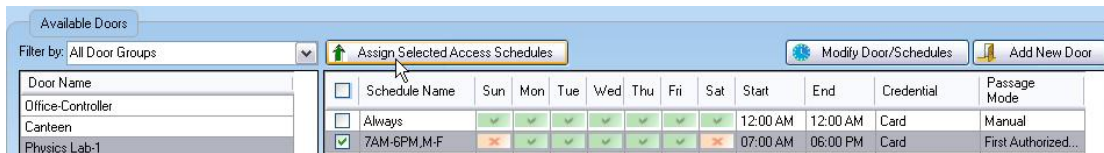
- The software displays the **Add Access Group** window.
- At the top left panel of the screen, enter the name of this new access group (of doors with access schedules and credential types) you are going to create; E.g.: AG-TechStaff.
- The bottom half panel of the screen shows all available doors that can be assigned to this new access group.



- Select one door at a time; for the selected door on the right side, you will see the access schedules and credential types that have been already assigned to this door, earlier.



- Select the required access schedule(s) for this door by checking the box(s) against it/them and click on **Assign Selected Access Schedules** tab.



- You will see that this selected door (Physics Lab-1, in this example) with all its parameters is assigned to this access group, as shown at the top left panel.
- Repeat the process by selecting other doors, one at a time to assign them in this access group. If a door has more than one access schedule assigned to it, you can select this door again and select a different schedule(s) for this door and assign it again to the access group.

Add Access Group

Access Group Information

Name: AG-Technical Manage Assigned Users Please enter appropriate information to add an Access Group. Access Group name cannot be longer than 20 characters.

Door Group Name	Door Name	Schedule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start	End	Credential	Passage Mode
<input type="checkbox"/>	DG-Technical	Physics Lab-1	7AM-6PM,M-F	✗	✓	✓	✓	✓	✗	07:00 AM	06:00 PM	Card	First Authorized Pass...

Unassign Selected Access Schedules Total Access Schedules: 1

Available Doors

Filter by: All Door Groups Assign Selected Access Schedules Modify Door/Schedules Add New Door

Door Name	Schedule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start	End	Credential	Passage Mode
<input type="checkbox"/>	Office-Controller								12:00 AM	12:00 AM	Card	Manual
<input type="checkbox"/>	Canteen								12:00 AM	12:00 AM	Card	Manual
<input type="checkbox"/>	Physics Lab-1								12:00 AM	12:00 AM	Card	Manual

- If you want to un-assign a previously assigned door or doors from this access group, simply check against that box or boxes and click on **Unassign selected Access Schedules**; now these doors will be removed from this access group.

Access Group Information

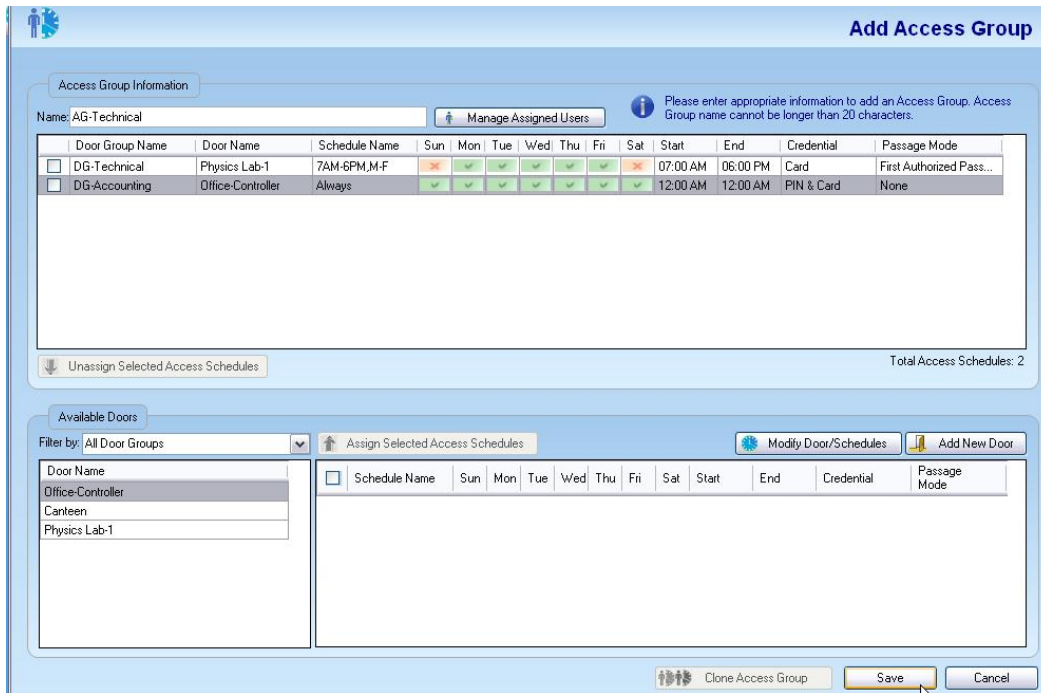
Name: AG-Technical Manage Assigned Users Please enter appropriate information to add an Access Group. Access Group name cannot be longer than 20 characters.

Door Group Name	Door Name	Schedule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start	End	Credential	Passage Mode
<input type="checkbox"/>	DG-Technical	Physics Lab-1	7AM-6PM,M-F	✗	✓	✓	✓	✓	✗	07:00 AM	06:00 PM	Card	First Authorized Pass...
<input checked="" type="checkbox"/>	DG-Accounting	Office-Controller	Always	✓	✓	✓	✓	✓	✓	12:00 AM	12:00 AM	PIN & Card	None

Unassign Selected Access Schedules Total Access Schedules: 2

Available Doors

- Finally click **Save** and all the doors with their access schedules and credential types assigned to this access group will be saved in the database.

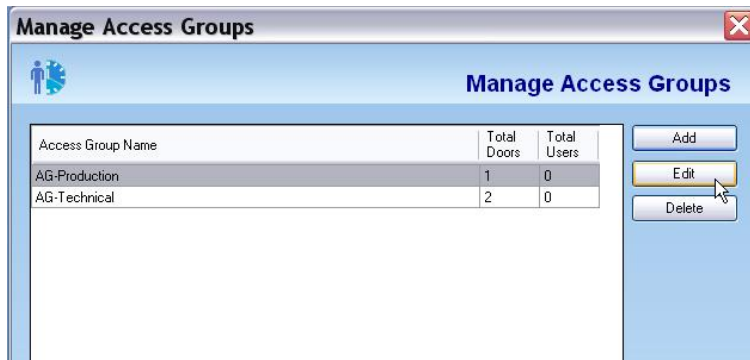


- Click **OK** to finish adding an access group.

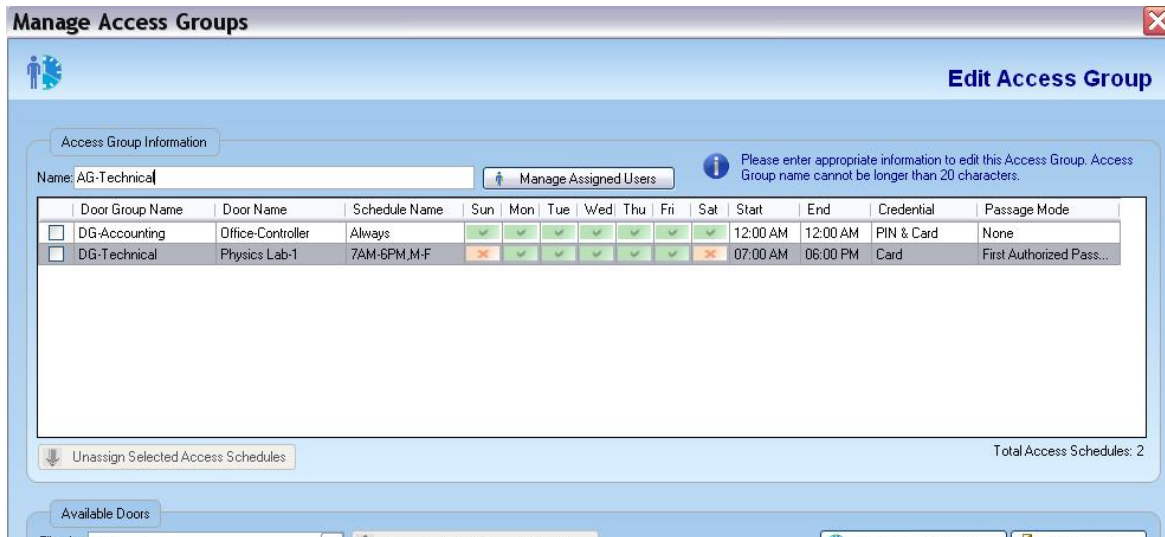
Editing an Access Group

Complete the following steps to edit an access group:

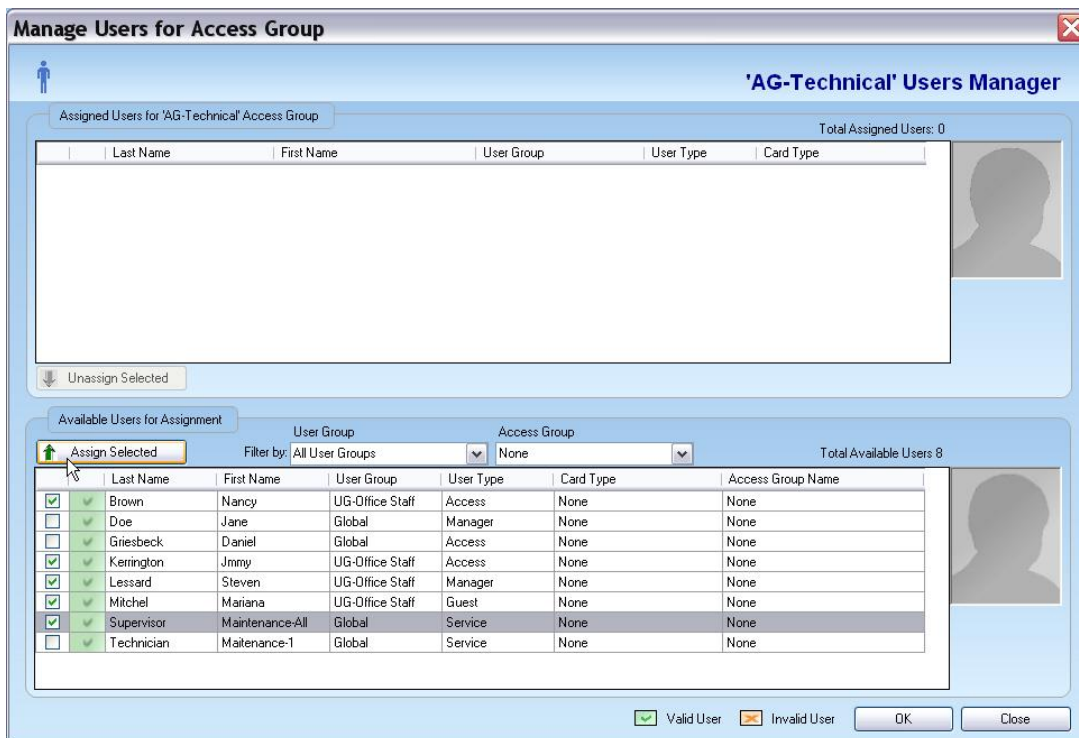
- From the **Manage Access Groups** window, select an access group to edit.
- Click **Edit**. The software displays the **Edit Access Groups** window.



- In addition to editing (adding or removing doors to access group), you can also assign users in the selected access group in this dialog menu. A typical case would be that you had already imported hundreds, if not thousands of users into the database. If that is the case, you can assign any or all of these users to your required Access Group(s) here.
- Click on **Manage Assigned Users** tab on top part of the screen panel.

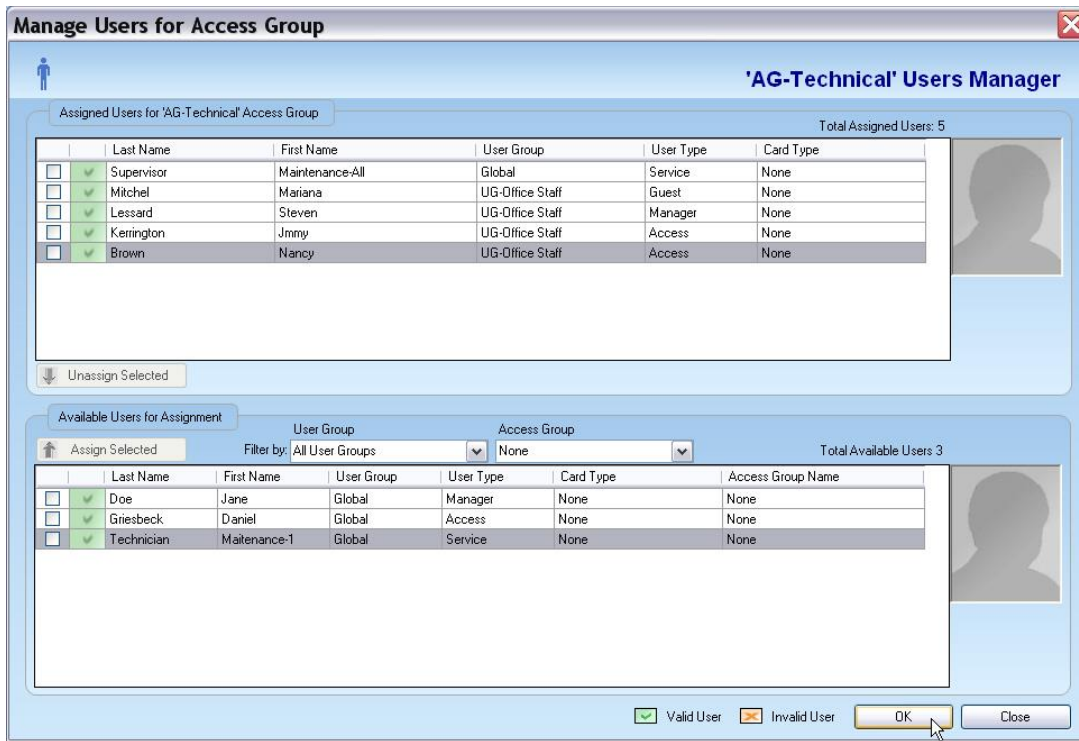


- The following window will open up showing the available users in the system that can be selected and assigned to this access group as shown below.

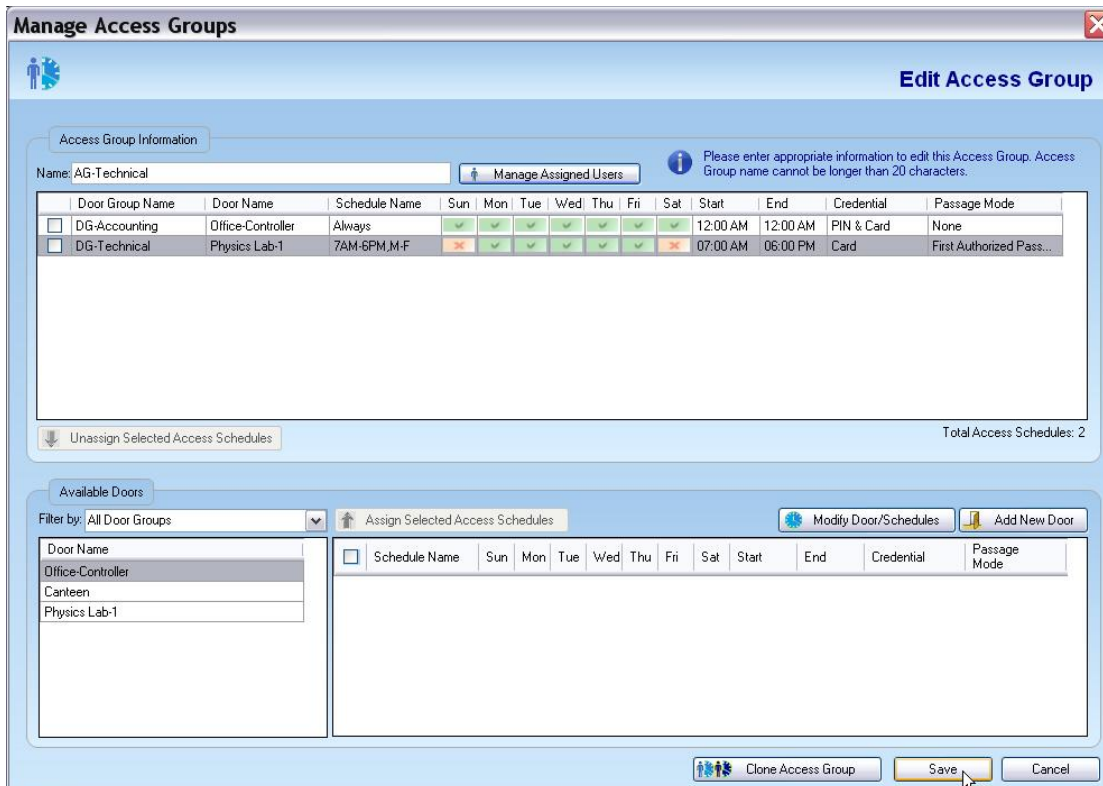


- Select required users by checking the boxes against them and click on **Assign Selected** tab on the left side of the bottom panel. Now all the selected users will be assigned to this access group as shown on the top panel.

► Using the E-Plex Enterprise Software



- Click **OK** and then **Save**.



- You may also “clone” an existing access group and give it a different name. After cloning, you can easily add or remove doors and/or users in the cloned access group to suit your need.
- Click on **Clone Access Group**.

Manage Access Groups **Edit Access Group**

Access Group Information

Name: AG-Technical Manage Assigned Users

Please enter appropriate information to edit this Access Group. Access Group name cannot be longer than 20 characters.

Door Group Name	Door Name	Schedule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start	End	Credential	Passage Mode
<input type="checkbox"/> DG-Accounting	Office-Controller	Always	✓	✓	✓	✓	✓	✓	✓	12:00 AM	12:00 AM	PIN & Card	None
<input type="checkbox"/> DG-Technical	Physics Lab-1	7AM-6PM,M-F	✗	✓	✓	✓	✓	✓	✗	07:00 AM	06:00 PM	Card	First Authorized Pass...

Unassign Selected Access Schedules Total Access Schedules: 2

Available Doors

Filter by: All Door Groups Assign Selected Access Schedules Modify Door/Schedules Add New Door

Door Name	Schedule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start	End	Credential	Passage Mode
Office-Controller												
Canteen												
Physics Lab-1												

Clone Access Group Save Cancel

- By default, the system will automatically name this cloned access group as “Clone of xxxxx” where xxxxx is the original name of the access group that was cloned from. You can rename this cloned access group to whatever name you want.
- Click **Save** to save this cloned access group in the database.

Manage Access Groups **Edit Access Group**

Access Group Information

Name: Clone of AG-Technica Manage Assigned Users

Please enter appropriate information to edit this Access Group. Access Group name cannot be longer than 20 characters.

Door Group Name	Door Name	Schedule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start	End	Credential	Passage Mode
<input type="checkbox"/> DG-Accounting	Office-Controller	Always	✓	✓	✓	✓	✓	✓	✓	12:00 AM	12:00 AM	PIN & Card	None
<input type="checkbox"/> DG-Technical	Physics Lab-1	7AM-6PM,M-F	✗	✓	✓	✓	✓	✓	✗	07:00 AM	06:00 PM	Card	First Authorized Pass...

Unassign Selected Access Schedules Total Access Schedules: 2

Available Doors

Filter by: All Door Groups Assign Selected Access Schedules Modify Door/Schedules Add New Door

Door Name	Schedule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start	End	Credential	Passage Mode
Office-Controller												
Canteen												
Physics Lab-1												

E-Plex Enterprise Software

The name of the Cloned Access Group is 'Clone of AG-Technica'.

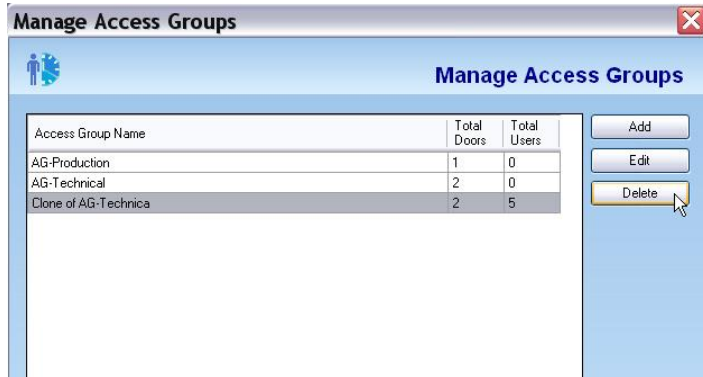
OK

Clone Access Group Save Cancel

Deleting an Access Group

Complete the following steps to delete an access group:

- From the **Manage Access Groups** window, select an access group to delete.
- Click **Delete**.

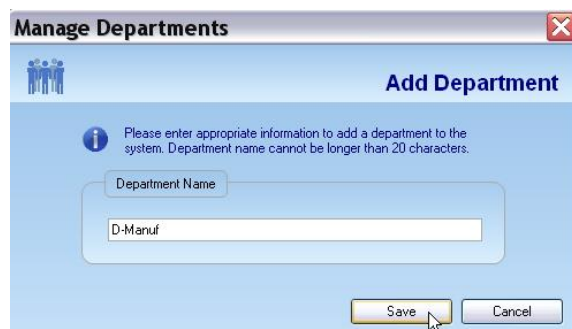


- The system displays the following screen with a message to caution you what will happen when you delete this access group. Click **Yes** if you really intended to delete this access group.

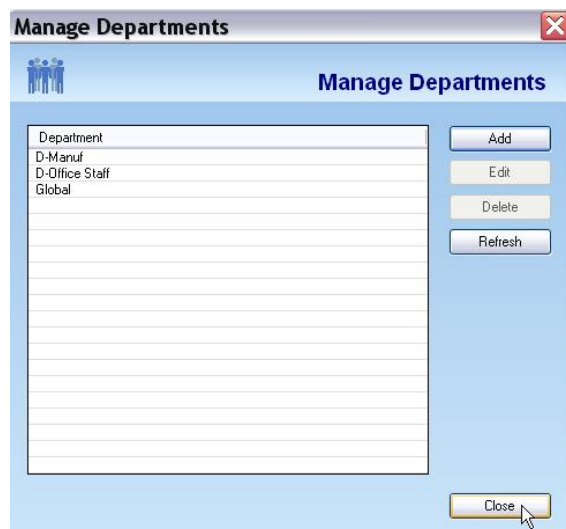


- In the **Department Name** field, type the name of the user group you are adding.

Note: The **Department Name** can be a maximum of 20 alphanumeric characters and no spaces and special characters are allowed, except for the “-“ character.



- Click **Save**. The system saves the changes and displays a confirmation message.
- Click **OK**. The software displays the new Department (user group) in the **Manage Department** window. Click **Close**.

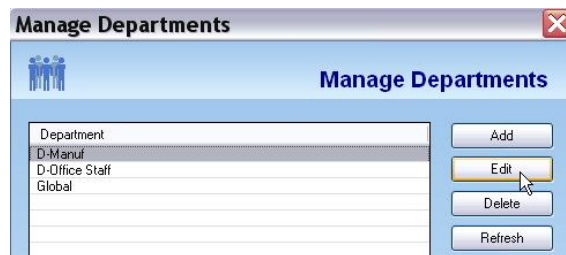


Note: You can add additional Departments at any time.

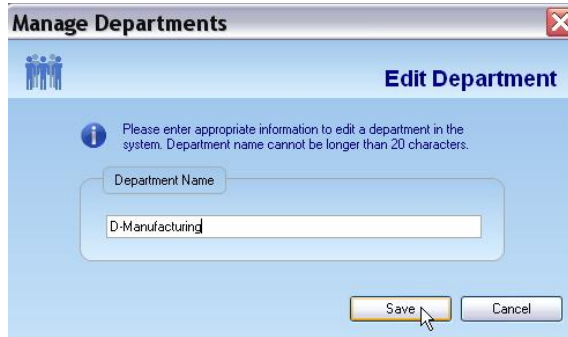
Editing a Department

Complete the following steps to edit a user group.

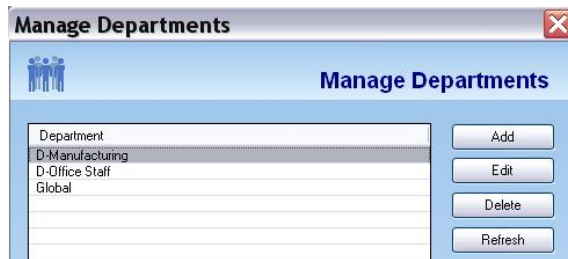
- From the **Manage Department** window, click a user group to edit.
- Click **Edit**. The software displays the **Edit Department** window.



- In the **Department Name** field, change the name of the user group.



- Click **Save**. The system saves the changes and displays a confirmation message.
- Click **OK**. The software displays the updated **Manage Department** window.



- Click **Close** to exit the **Manage Department** window.

Deleting a Department

Complete the following steps to delete a Department.

- From the **Manage Department** window, select and click a Department to delete. If a Department contains any users in it, you must first delete all these users before able to delete this Department.



- Click **Delete**. The software prompts you for confirmation.



► *Using the E-Plex Enterprise Software*

- Click **Yes**. The system displays the updated **Manage Department** window. Click **Close**.



Managing Users

In the Enterprise software, you can add and maintain users and assign their associated PIN. In addition to the PIN, you can also assign a Prox card and/or a smartcard such as iClass, Mifare or DESFire to the user, if this user will be accessing any Prox and/or smartcard based E-Plex locks in the facility. If you will be using smartcards as ID credentials, you must select only one type of smartcard (iClass, or Mifare or DESFire) that you will be using in your facility. That is, each user can be assigned dual card credentials – one is always a Prox but the second one can be only the same type of a smartcard.

Also in this menu, you may assign an *Access Group* to each user, change or delete user information etc.

The Enterprise software allows you to manage users from the **Manage Users** menu.

Note: You can add up to 10,000 users in the database whether all the users are configured to have 4, 5, 6, 7 or 8 digit length PINs. However, you can put a maximum of only 3,000 users in the lock.

- Select a **Credential Type** that the Master user must use to program and/or audit locks from the drop-down list. By default it is **PIN** only credential, meaning that the Master user needs to enter only her/his 8-digit PIN when programming or auditing the locks. If you choose **PIN & Card** credential for higher security, then the Master will be required to use dual credential (PIN and card), every time s/he accesses the lock for programming or auditing.
- In this example, let us assume that each user of this facility carries two types of ID card credentials -> one of them is a legacy Prox card (works in E3700 & E5700 series locks) and the other one is a smartcard (works in E3600 & E5600 lock series); the smartcard used here is an iClass card.

Note: The one and only Master user and one Door Group Manager user are pre-assigned in the system as default users, both belonging to the Global Department. The Master user who is also automatically the very first Level-1 Operator cannot be deleted from the system.

To manage users, select **Manage Users** from the **Users** menu or click the **Manage Users** button.



- From the **Manage Users** window, click **Add**. The software displays the **Add User** window.

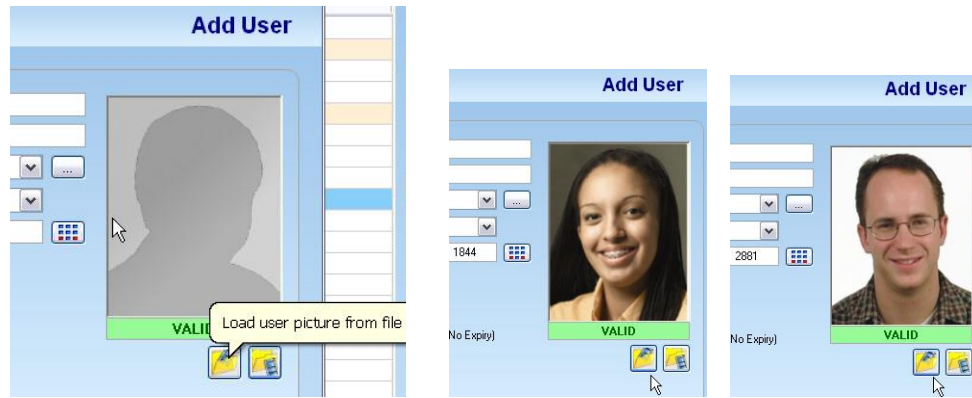
- In the **Last Name** field, type the last name of the user.
- In the **First Name** field, type the first name of the user.
- From the **Department** drop-down list, select a department.
- From the **Access Group** drop-down list, select an access group that was already created under the *Managing Access Group* menu earlier, or leave it as default “None”.
- From the **User Type** drop-down list, select a user type.

Note: The **User Type** field defaults to Access User. The Service user type is PIN only and so does not require any card enrollment.

- In the **User PIN** field, the user PIN for this user will be automatically generated by the software. The first 4 digits of automatically generated PINs are always unique for security reasons. You can override the PIN by entering a new 4-digit PIN (5, 6, 7 or 8 digit PINs, if user PIN is configured as such in Systems Setup), but making sure that the first 4 digits are unique for each user. You can also re-generate a unique PIN automatically by clicking the auto (other) PIN Generator button.

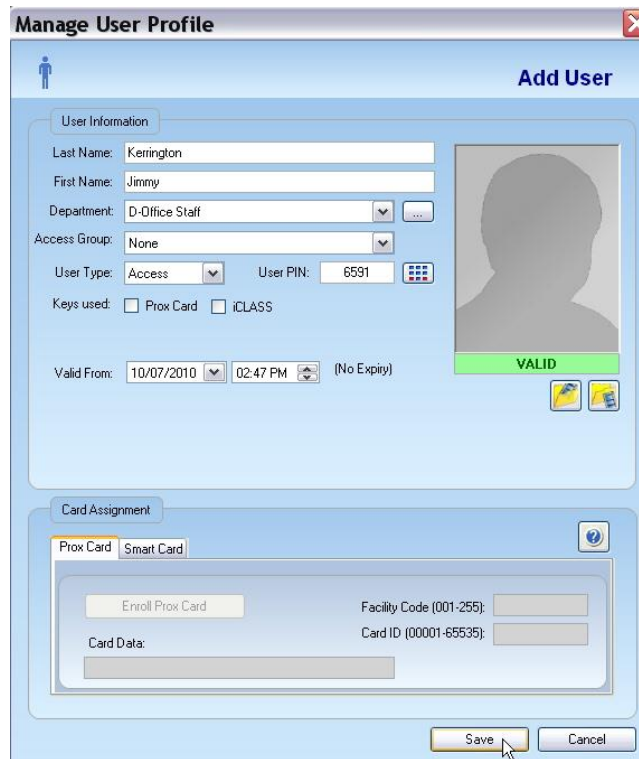


- You also have an option of importing (attaching) a JPG image of the user's photo (and detaching it, if you do not like it). The recommended JPG image resolution is ~400 x 500 pixels.



- In the **Keys Used** (ie., Card Type Assigned) field, check both “Prox Card” and “iClass” fields. If you leave the *Keys Used* fields unchecked, then this user can access only the PIN based E-Plex locks such as E3200 and/or E5200.

Important: If you are going to be enrolling any non standard 27 to 84 bit format Prox tokens (Standard format = 26-bits), you must use the card enroller(s) to enroll cards. The following example shows user creation without any card enrollment.

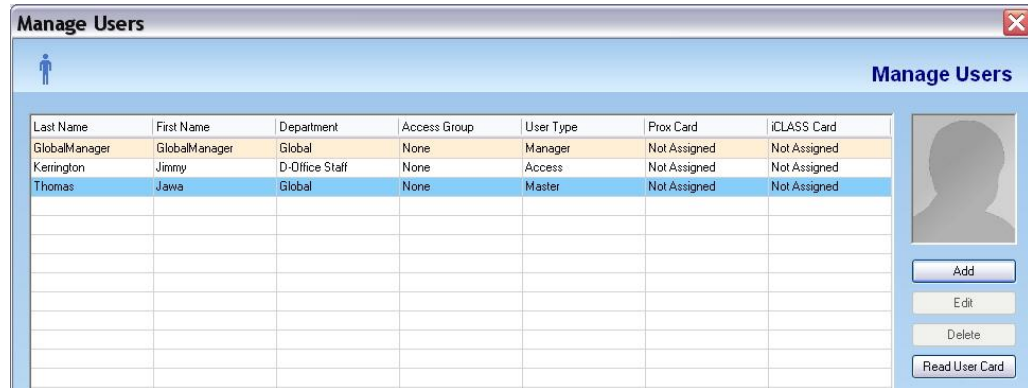


Note: By default, there is no expiry for Access and Manager type users. Optionally, you can enter the “Valid From” date to be sometime in the future by few days/weeks etc.

- Click **Save**. The system saves the changes and displays a confirmation message.

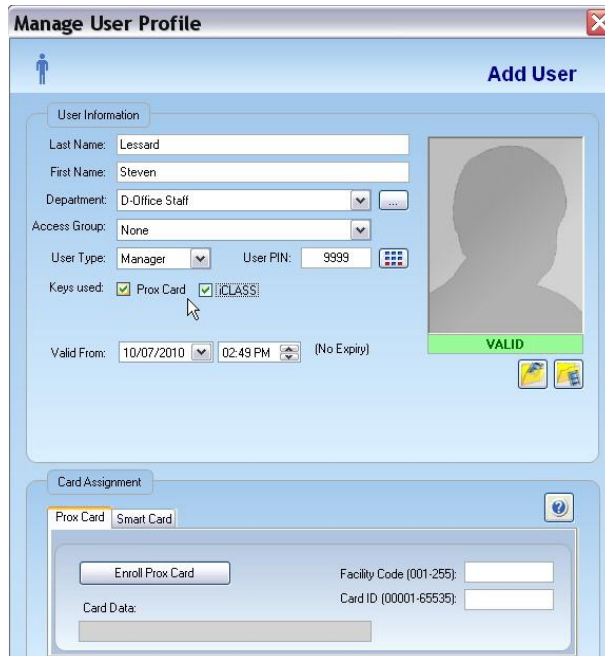


- Click **OK**. The software displays the updated **Manage Users** window.



Example showing both Prox and Smartcard Enrollment

Ensure that the “Keys Used” (Card Type Assigned) fields are checked for both Prox and iClass,

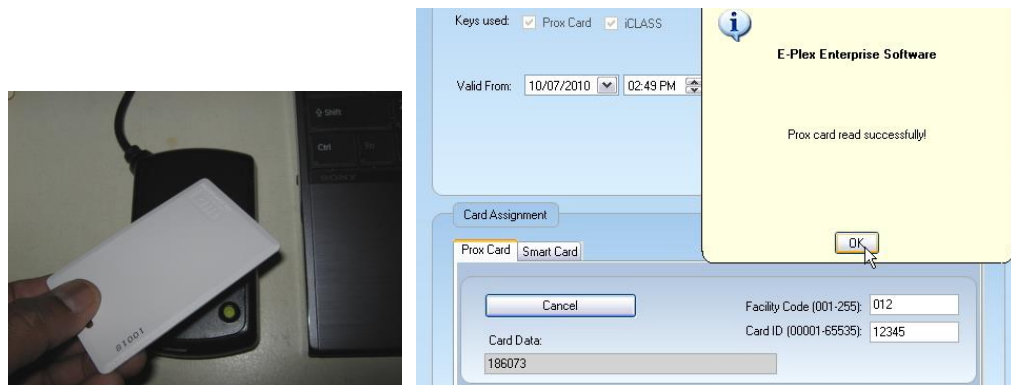


- **Prox Card Assignment** -> There are two different methods available to enroll a user's Prox token as described below.

Method 1 - with the Prox Enroller: Click **Enroll Prox Card** and then present this user's

► Using the E-Plex Enterprise Software

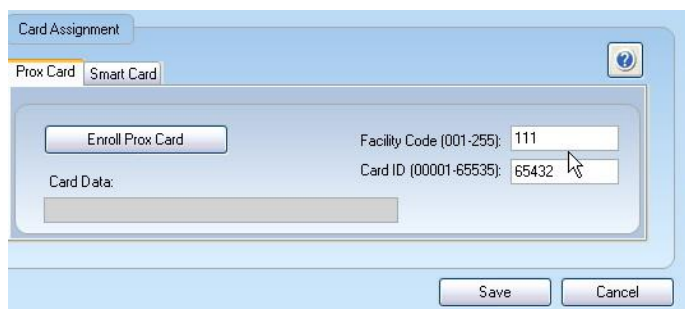
Prox card momentarily on top of the enroller, wait for the red light to turn green and flash once to indicate that the card ID has been read and stored in the database correctly.



Or,

Method 2 – by entering **Facility Code** (001 – 255) & **Card ID** (00001 – 65535) values directly in these two fields, but only if you know them:

Important: This Method 2 can be used only for the standard 26-bit format HID Prox cards and you must know what values to enter.



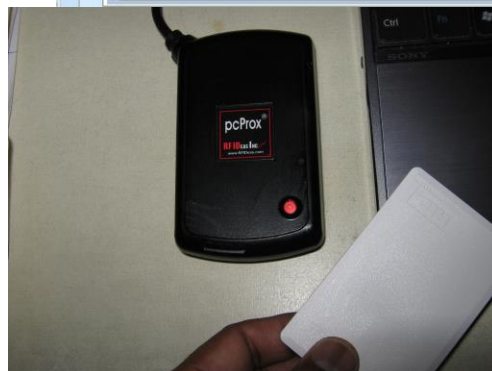
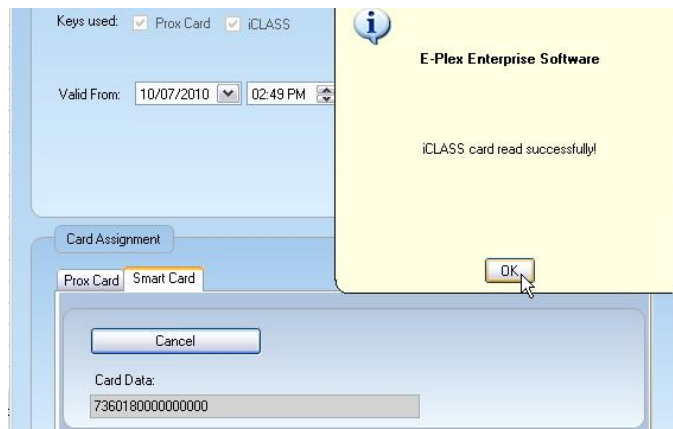
Click **Save** to save this user profile (if you are done and will not be enrolling a smartcard).



- **Smartcard (iClass) Card Assignment** -> For IClass only, again like Prox, there are two different methods available to enroll a user's token, assuming of course that the iClass card ID data conforms to the Standard 26 bit format. **Note:** For Mifare and DESFire, the card data format does not conform to the Standard 26 bits and so you must use the smartcard enroller.

In this example, the iClass cards being used are non-standard (27 to 84 bits) format and so we will use the smartcard enroller.

Click **Enroll iClass Card** and then present this user's card momentarily on top of the smartcard enroller, wait for the red light to turn green and flash once, followed by a beep to indicate that the card ID has been read and stored in the database correctly.



Click **OK** and then **Save**. The software returns to the **Manage Users** window with this user's profile updated.

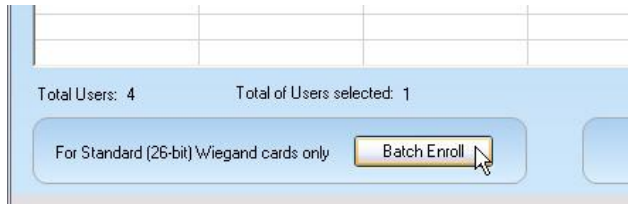
Note: The newly created user is now shown as created in the system database with both card types assigned to this user.

Last Name	First Name	Department	Access Group	User Type	Prox Card	iCLASS Card
GlobalManager	GlobalManager	Global	None	Manager	Not Assigned	Not Assigned
Kerrington	Jimmy	D-Office Staff	None	Access	Not Assigned	Not Assigned
Lessard	Steven	D-Office Staff	None	Manager	012-12345	7360180000000000...
Thomas	Jawa	Global	None	Master	Not Assigned	Not Assigned

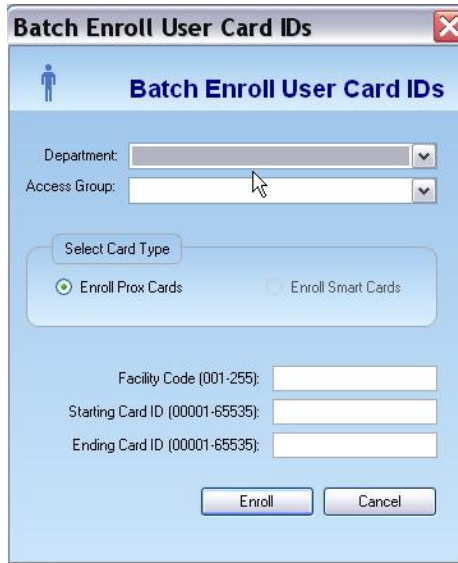
Batch Enrollment (without an Enroller)

Important: This method can be used only for the Standard 26-bit format HID Prox and/or iClass cards only, and you must know what values to enter. In this example we will ‘batch’ enroll a few Standard format Prox cards.

- From the **Manage Users** window, click **Batch Enroll** at the bottom left corner of the screen.



- The following screen is displayed for you to enroll “en masse” tens, or hundreds, or even thousands of Prox credentials, provided all these cards have the same 3-digit Facility code (001 through 255) and that the 5-digit card numbers being enrolled (00001 through 65535) all have sequential card numbers.

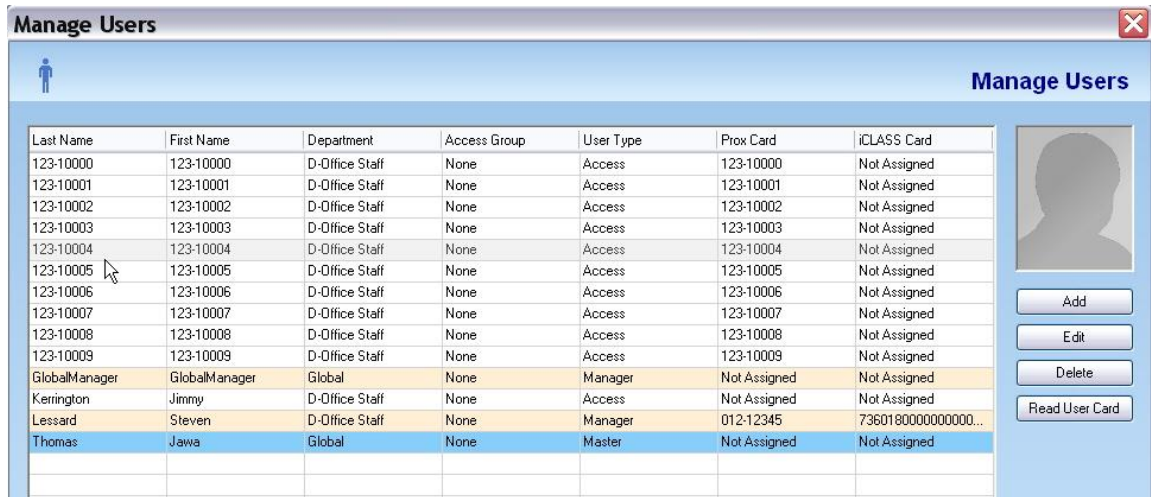


- The following batch enrollment example shows where the Facility code = 123, and the starting Card number is 10000, the ending card number is 10009 to batch enroll 10 cards.
- Click **Enroll** and then **Yes** when asked for confirmation..



- The message “User card IDs enrolled successfully” is displayed and click **OK**.

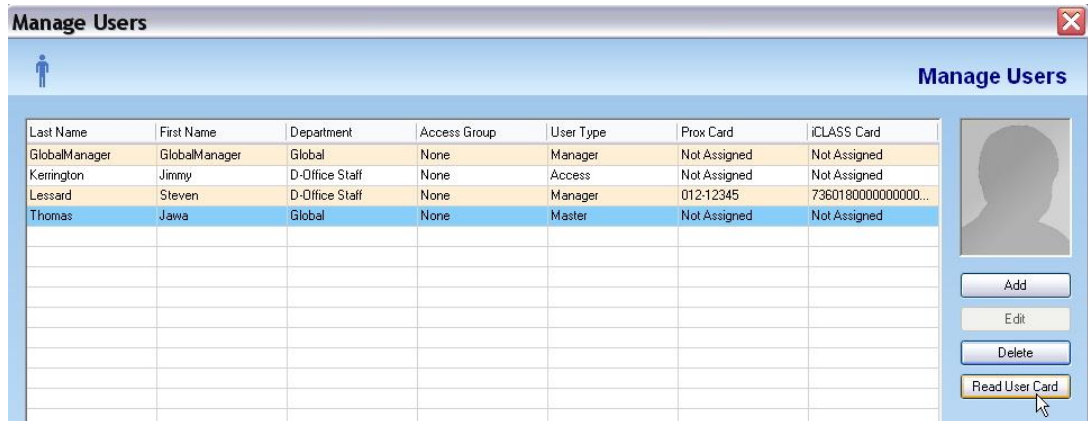
- The screen displays the ten batch enrolled users. Each batch enrolled user's Last name and First name contain the Card ID (123-10000, 123-10001... etc). You can edit their names with real Last and First names, if desired.



- Click **Close**.

Reading a User's Card

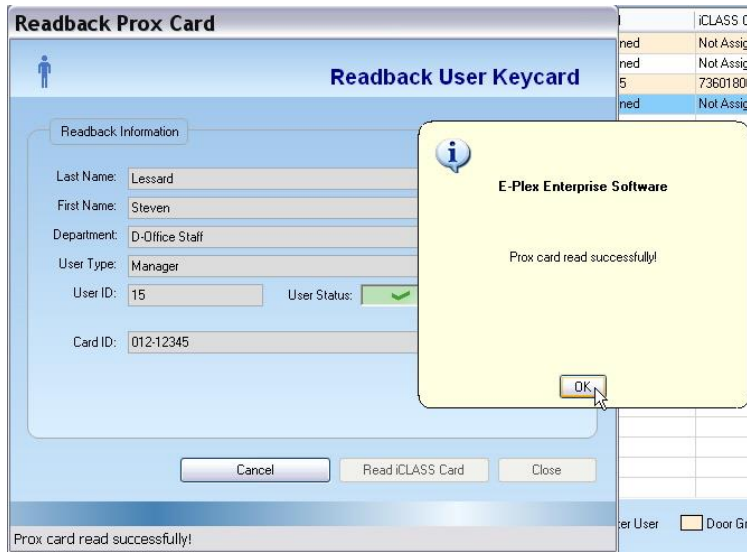
- With an enroller, you can also read the complete Card number (Facility code + Card ID) of a "lost and found" card – Prox or Smartcard by using the applicable enroller. If the card is already enrolled in the system, it will show the complete card number and the user's profile of the card read. If the card is not enrolled in the system, it will only show the card number but not the user's profile info.
- This example shows reading back of a previously enrolled Prox user's card, From the **Manage Users** menu, click **Read User Card**.



- Read the card in the enroller. If the card read is already enrolled in the system database, the message will display as such including whose card it is; else, it will just display the card ID of the card read.



[Card read user is in the system]:



[Card read user is not in the system]:



- Click **Close** to exit from this sub-menu.

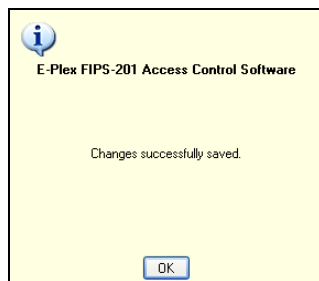
Editing a User

Complete the following steps to edit a user:

- From the **Manage Users** window, click the user name you want to edit.
- Click **Edit**. The software displays the **Edit User** window.

The screenshot shows the 'Manage User Profile' window with the 'Edit User' tab selected. The 'User Information' section contains the following fields: Last Name (Smith), First Name (Jane), Department (D-Manufacturing), Access Group (None), User Type (Access), User PIN (9163), and Valid From (10/08/2010 01:50 PM). There are checkboxes for 'Prox Card' and 'ICLASS'. A 'VALID' status bar is present. The 'Card Assignment' section has tabs for 'Prox Card' and 'Smart Card', with an 'Enroll Prox Card' button and fields for Facility Code (001-255) and Card ID (00001-65535).

- Edit any required fields (e.g., PIN) where changes need to be made, including assigning/un-assigning Prox and/or smartcard or not.
- Click **Save**. The system saves the changes and displays a confirmation message.



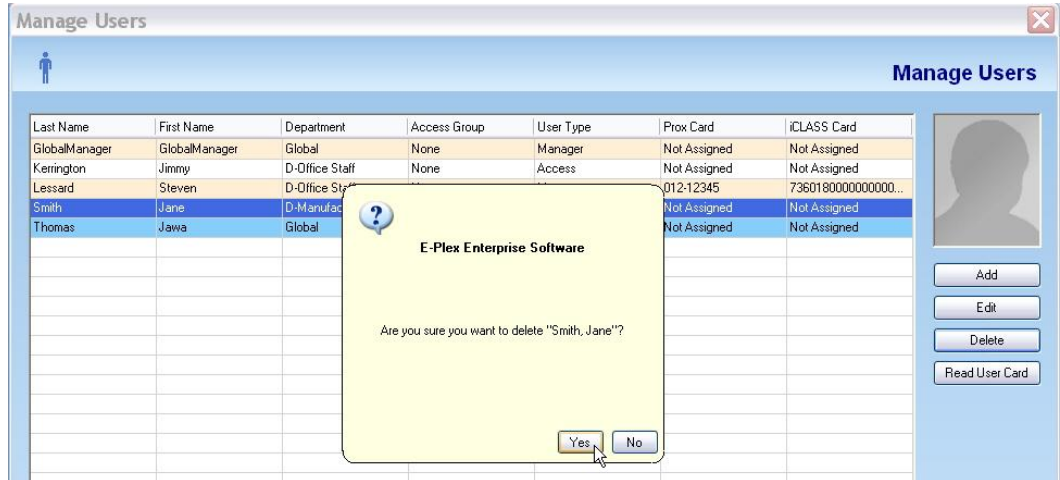
- Click **OK** to exit this menu.

Note: You should update your locks to reflect modified user profile by transferring the changed info to the M-Unit and uploading/programming the information to the locks. For more information, refer to **Portable PC M-Unit** section in **Chapter 5, Programming and Auditing Locks**.

Deleting a User

Complete the following steps to delete a user:

- From the **Manage Users** window, select the user to delete.
- Click **Delete**. The software prompts you for confirmation.



- Click **Yes**. The software displays the updated **Manage Users** window with the deleted user gone from the list.

Note: You should update your locks to reflect any unassigned and deleted users by transferring the deleted user(s) info to the M-Unit and uploading/programming this information to the locks. For more information, refer to **Portable PC M-Unit** section in **Chapter 5, Programming and Auditing Locks**.

Managing Access Assignment

The “specific” access assignment function allows you to assign each door, one at a time—its access granting schedules to users and their privileges, if any. The “Managing Access Assignment” procedure is the same for both standalone and **wireless** doors.

You can just use this menu function, instead of the “Manage Access Groups” function to perform the same thing. That is, if you have only a handful of locks/doors (say, fewer than 10) and say, fewer than 50 users to assign to these doors, you can do so in this menu dialog. This is because for a small facility, doing this way may be more convenient than performing the same functions under the “Manage Users/Access Groups” menu dialog.

Important: If you had already assigned all your users to all your doors for access under the Manage Users menu via the Access Group option earlier, you can skip this Access Assignment menu. However, if you want to give any of your users one or more of the three Privileges, you can do it only under this Access Assignment menu.

From this menu, you must select a door and assign the users who should have access to this door. Then, for each user you must select and assign one or more available schedules that were already assigned to this door earlier. Finally, for each user you can also optionally assign any one or more of the following three privileges:

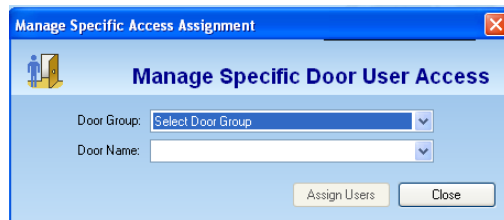
- Override holidays/vacations
- Override deadbolt/privacy
- First user passage entry

After this process, the lock configuration data with its users are set up and prepared to be synchronized with the M-Unit for later uploading to the door/lock.

To manage door access assignment, select **Manage Specific Access Assignment** from the **Access Assignment** menu, or click the **Manage Specific Access Assignment** button.



The software displays the **Manage Specific Door User Access** window.



From this window, you can manage door access assignment, including the following:

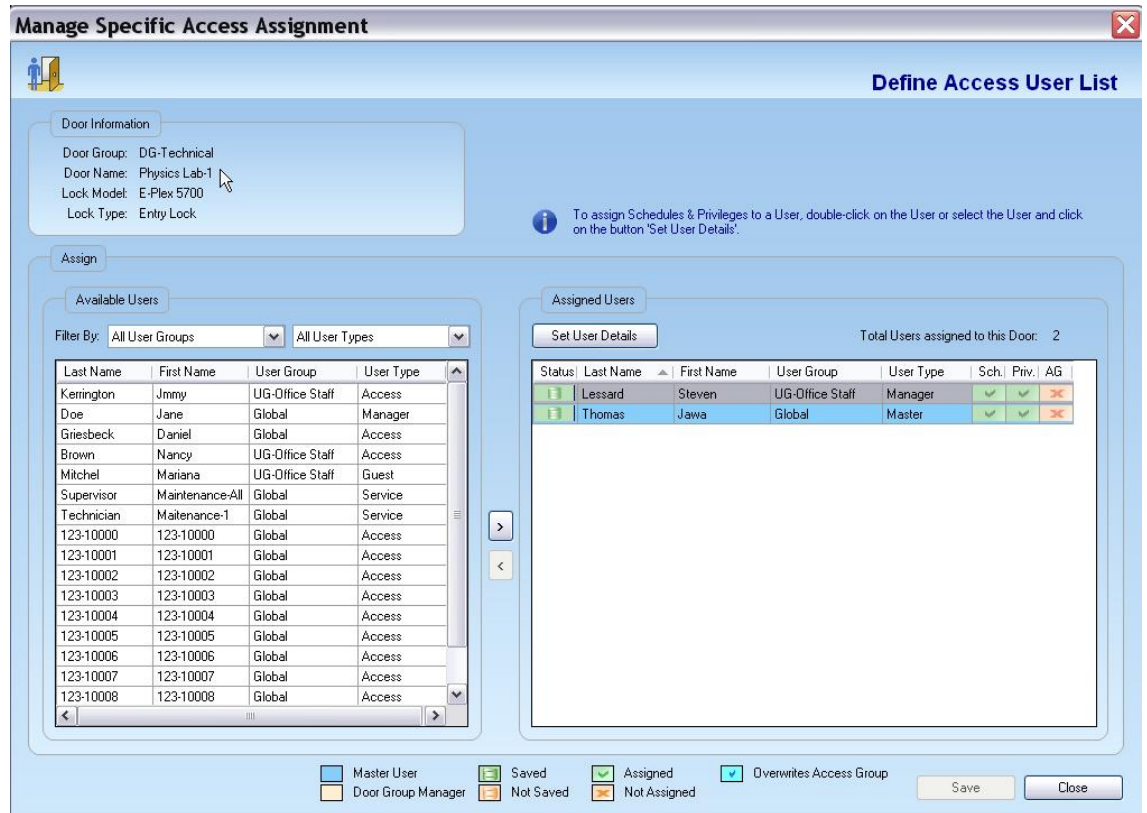
- Assigning access schedules to the door
- Assigning access schedules to each user
- Optionally assigning privileges to each selected user.

Assigning Users to Lock with Privileges

Complete the following steps to manage door access assignment:

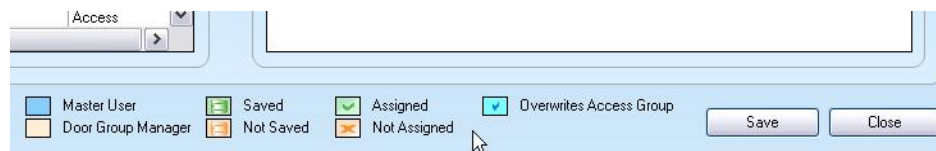
- Select a **Door Group** from the drop-down list.
- Select a **Door Name** from the drop-down list.


- Click **Assign Users**. The software displays the **Define Access User List** window.

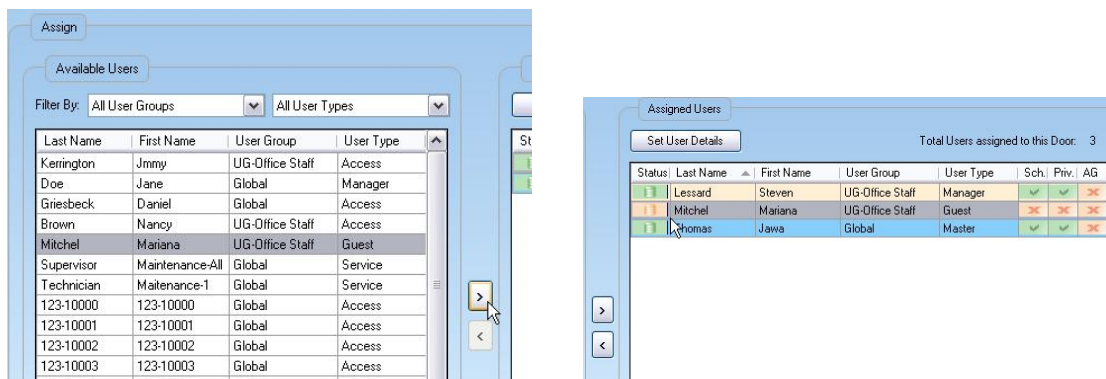


Note: Once you select the door group and the door name, the software displays the **Lock Model** and **Lock Type** for that door.

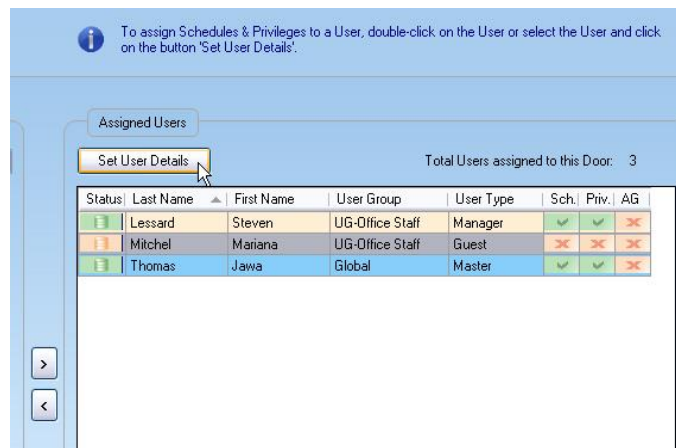
- The left side of the screen shows the **Assign** (users to doors) area. Select your users from the **All Departments** and **All User Types** drop-down lists – either all of them or only the “filtered” users as you desire.
- Each icon/pictogram at the bottom of the screen dialog explains what each one means.



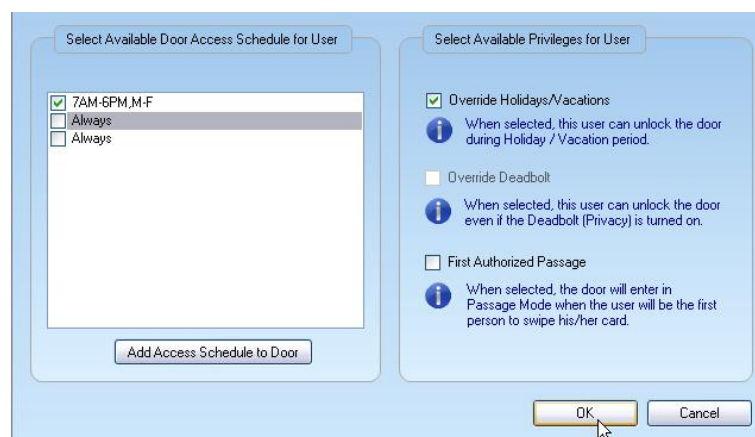
- Click the appropriate user name in the list to select and highlight it.
- Click the **right arrow**  to move the selected user from the database to the door. The moved user is now shown on the right side of the screen under **Assigned Users**.



- You must now assign one or more of the available (door) Access Schedules to this user by checking the box(e). **Note:** The “Always” schedule cannot be combined with any other available schedules for assignment since it overlaps with all other schedules. Optionally, you can also assign one or more of the “privileges” to this user.
- Select/highlight this user and either double click or click **Set User Details**.



- The software displays the **Assign Access Schedules and Privileges to User** window. This screen display is for either an “Access” user or a “Guest” user assignment. **Note:** The Guest user’s maximum expiry is only one year.
- Check the required Access Schedule(s) on the left pane of the screen and any optional Privilege(s) on the right pane of the screen for this user.



Important: The “Always” door access schedule cannot be assigned to the door and user(s) along with any other schedules because it overlaps with all other schedules

- The following are the three optional privileges:
 - **Override Holidays/Vacations** – The user can unlock the door during holiday/vacation period.
 - **Override Deadbolt** – The user can unlock the door even if the deadbolt (privacy) is thrown from inside (projected) for privacy.
 - **First Authorized Passage** – The door will enter Passage Mode when this user with this privilege will be the first person to open the door with her/his credential.
- Click **OK** when done.
- Note: Optionally, you can also add more Access Schedules and Credential usage within this menu dialog for this door and user(s).
- You will see that now this user's schedule and privilege status boxes are shown as checked in green, meaning that this user has been assigned access to the door.

Status	Last Name	First Name	User Group	User Type	Sch.	Priv.	AG
	Lessard	Steven	UG-Office Staff	Manager	✓	✓	✗
	Mitchel	Mariana	UG-Office Staff	Guest	✓	✓	✗
	Thomas	Jawa	Global	Master	✓	✓	✗

- The following is an example of the window **Assign Access Schedules and Privileges to User** when a “Service” user is selected for access assignment. The Service user's maximum expiry can be either once (one shot), or from 1 through 96 hours or no expiry. **Note:** The Service user is not restricted to any access schedules but will always have 24/7 access.

User & Door Information

User Group: Global
 User Name: Supervisor, Maintenance-All
 User Type: Service
 Access Grip: None

Door Group: DG-Technical
 Door Name: Physics Lab-1
 Lock Model: E-Plex 5700
 Lock Type: Entry Lock

Select Available Door Access Credential for User

A Service User cannot be assigned to an Access Schedule.

Select Available Privileges for User

Override Holidays/Vacations
 When selected, this user can unlock the door during Holiday / Vacation period.

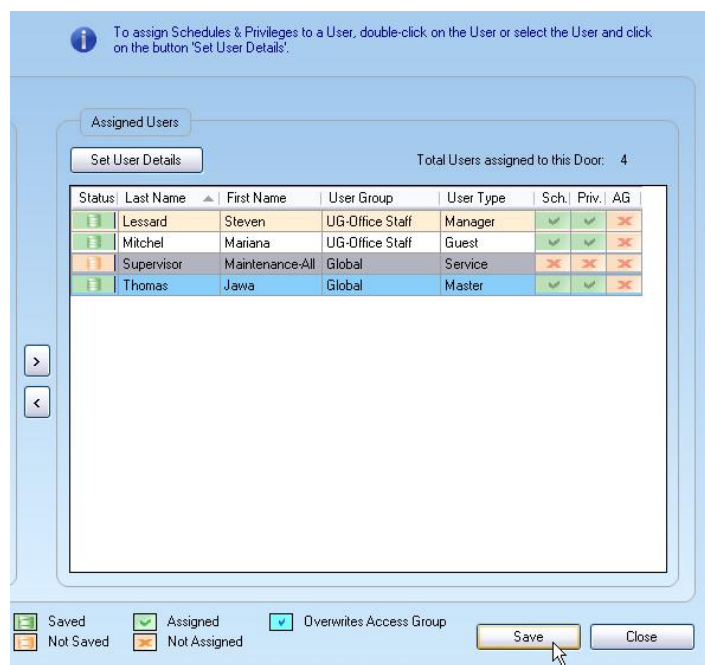
Override Deadbolt
 When selected, this user can unlock the door even if the Deadbolt (Privacy) is turned on.

First Authorized Passage
 When selected, the door will enter in Passage Mode when the user will be the first person to swipe his/her card.

OK Cancel

- Click **OK, Save** and then **Close**.

► Using the E-Plex Enterprise Software



The software returns to the **Manage Specific Door User Access** window.

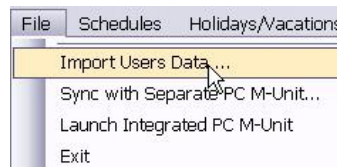
Note: You should synchronize all updated doors/locks with these newly assigned users with the M-Unit PDA and then program these doors with the M-Unit by uploading the information to the locks. For more information, refer to **Portable PC M-Unit** section in **Chapter 5, Programming and Auditing Locks**.

Importing Users

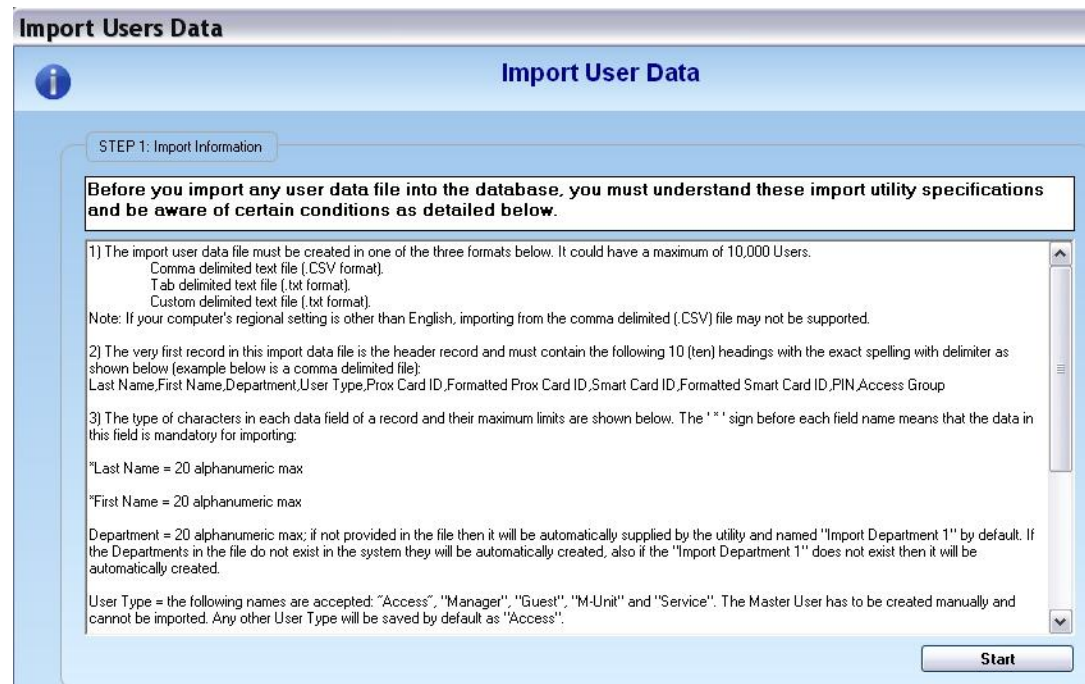
The software allows you to also import up to 20,000 user profile records from an external source. Each user record must contain the Last name and the First name of the user; the PIN and the Prox card ID, if available are optional and so does not have to be included in each user record that needs to be imported into the Enterprise database.

The complete info, import data rules and specifications will be displayed on the screen when you click on **File** first, then on **Import Users Data...** menu. You will need to simply follow the of the screen prompts when you are ready to import a user profile data file. The **Format** of the file to be imported must be either in a TAB delimited (*.txt) or a "Comma" delimited (*.csv) text format file, and optionally your own custom format with your specified delimiter character.

- To import a user profile data file, select **File** from the main menu or and then click the **Import Users Data...** button.



- The software displays the **Import User Data** window. Please scroll down and read all required info before starting the import process.



- Click **Start** to begin the process of importing users into the Enterprise database from an external .txt or .csv text file.
- The following window opens. Select the file **Format** as described earlier of your import file.
- Under **User PIN**, select either "Automatically Select User PIN" which will automatically generate and assign an 8-digit PIN to each imported user, or select "Import PIN" which will import the end user supplied PIN number for each user from the import file.

Note: The length of the imported users' PINs must be of the same length (e.g. = 4) as what is already configured in the software database under *System Settings*.

- Click **Browse** to locate your input import file from which the users' info will be imported.

Important: The very first line/row of the import file should contain the following 10 headers, exactly in this following sequence from left to right with the correct spelling of each header name as shown below:

Last Name First Name Department User Type Prox Card ID
Formatted Prox Card ID Smart Card ID Formatted Smart Card ID PIN Access Group

STEP 2: Select source file

Format
The format of the data file to be imported.

Tab Delimited
 CSV Delimited
 Custom Delimited

System Settings

Prox Card: Prox Card: Standard 26-bit
Smart Card: Smart Card: Non 26-bit
PIN Length: 4

Import File Location
Choose the data file by clicking the browse button.

File Path: C:\Documents and Settings\thomas\My Documents

User PIN

Automatically generate User PIN
Import PIN

- In the next displayed window, select and click **Open** the actual import file. In this example, the import file contains 10 user records, with not all fields containing data.

Important: As a minimum, the import file must contain data in the first two fields -> *Last Name* and *First name*. Additionally, the *PIN* field will be always populated with 8-digit PINs for each imported user, if the “Automatically provide User PIN” option was selected.

- Click **Next** to start importing the users' info from this file. The next window shows all 10 fields of the imported users' records. You can also navigate horizontally through various tab headers on top to view the status of each header.

STEP 3: Verify and Manipulate Data

New Identified Users (10) Duplicate Users (0) Users already in the Database (0) Users with Data Errors (0)

Save in the Database	Last Name	First Name	Department	User Type	ProxCARDID	Formatted ProxCARDID	SmartCARDID
<input checked="" type="checkbox"/>	HARRISON	DHIREN		Manager	0c244a03	165-04614	
<input checked="" type="checkbox"/>	COSTA	MICHEL		Access	2d934a03	165-18838	
<input checked="" type="checkbox"/>	KENNEDY	JIM		Access	1eb54a01	165-23183	
<input checked="" type="checkbox"/>	MINGO	DIANE		Access	89124d03	166-35140	
<input checked="" type="checkbox"/>	DEMONTE	JAMIE		Access	98584b01	165-44108	
<input checked="" type="checkbox"/>	THOMPSON	JOHN		Access	3fcb4d03	166-58783	
<input checked="" type="checkbox"/>	BERNARD	MARIANA		Access	43454a03	165-08865	
<input checked="" type="checkbox"/>	GEORGE	STEVEN		Manager	9ab3f702	123-55757	
<input checked="" type="checkbox"/>	GEORGE	SUSAN		Access	611e1800	012-03888	073590a0000000
<input checked="" type="checkbox"/>	ST.JULES	JULIAN		Access	77fc1d02	014-65083	070c9030000000

with Data Errors (0)

Formatted SmartCARDID	PIN	Access Group
	1314	
	4045	
	1058	
	1507	
	4718	
	5178	
	5788	
	4668	
3000	4107	
3000	3085	

Previous Next

- Click **Next** and the next window displays a complete status of all user records imported under various headers including error messages, if any.
- Verify to ensure that there are no errors and then click **Save data in the Database** to save the imported user info in the database.

Import User Data

STEP 4: Save Users data in the Database


Please Note: only rows that are selected will be saved in the database.

Total New Users:	10	Total to be saved:	10
Total Duplicate Users:	0		
Total Existing Users:	0	Total to be Overwritten :	0
Total new Departments to be added:	0		
Total new Access Groups to be added:	0		
Total Erroneous Users, that cannot be saved:	0		

► Using the E-Plex Enterprise Software

- Click **OK** in “Changes successfully Changed” popup message box and then click **Close** to exit from the import users dialog menu and get back to the main menu.
- From the main menu click **Manage Users** and verify for the presence of these imported users. You will see them under the Department named “*Import Department 1*”, if no Department name was provided in the original import input file.

Manage Users						
Last Name	First Name	Department	Access Group	User Type	Prox Card	iCLASS Card
BERNARD	MARIANA	Import Department 1	None	Access	165-08865	Not Assigned
COSTA	MICHEL	Import Department 1	None	Access	165-18838	Not Assigned
DEMONTE	JAMIE	Import Department 1	None	Access	165-44108	Not Assigned
GEORGE	SUSAN	Import Department 1	None	Access	012-03888	73590a0000000000...
GEORGE	STEVEN	Import Department 1	None	Manager	123-55757	Not Assigned
HARRISON	DHIREN	Import Department 1	None	Manager	165-04614	Not Assigned
KENNEDY	JIM	Import Department 1	None	Access	165-23183	Not Assigned
MINGO	DIANE	Import Department 1	None	Access	166-35140	Not Assigned
ST.JULES	JULIAN	Import Department 1	None	Access	014-65083	70c9030000000000...
THOMPSON	JOHN	Import Department 1	None	Access	166-58783	Not Assigned
GlobalManager	GlobalManager	Global	None	Manager	Not Assigned	700c902000000000...
Thomas	Jawa	Global	None	Master	Not Assigned	Not Assigned
Kerrington	Jimmy	D-Office Staff	None	Access	Not Assigned	Not Assigned
Lessard	Steven	D-Office Staff	None	Manager	012-12345	7360180000000000...



Add

Edit

Delete

Read User Card

Viewing/Printing/Exporting Reports

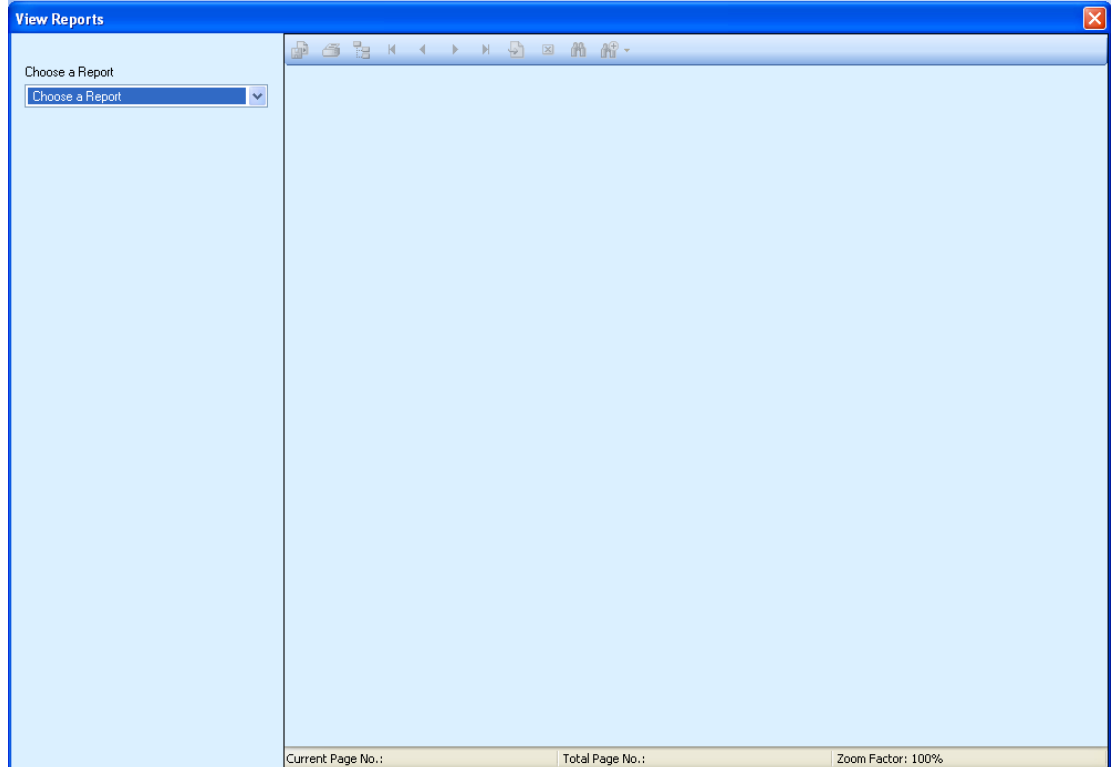
The **Reports** option can be used to view and report on the data that you have defined in the E-Plex Enterprise software and locks. It can also report on the data that you have uploaded to locks defined in the software and also the lock audits downloaded from locks. Once data have been synchronized from the lock to the PC, you can view and report on data from the lock. The software allows you to generate reports from the **Reports** menu.

Note: Once a report is open for viewing, you will have the option to either print this report or export it in a specific file format type like PDF, Excel, Word etc and save it in any folder of your choice either in your local drive or in any external storage drive.

To access reports, select **Reports** from the **Reports** menu or click the **Reports** button.



The software displays the **View Reports** window.



From this window, you can select a report to view, print, or export.

Viewing Reports

Complete the following steps to view reports:

- Select a report from the **Choose a Report** drop-down list in the **View Reports** window.

Note: The available *Filter By* and *Sort By* options change based on the type of report you choose.

► Using the E-Plex Enterprise Software

Select from the **Filter By** options if you want to filter out particular data item(s) to view.

Select from the **Sort By** options to view the data item(s) in a particular sorting order.

Click **Generate**. The software displays the selected report in the **Main Report** pane.

The screenshot shows the 'View Reports' window. On the left, there are controls for 'Choose a Report' (System Activity Log), 'Filter By' (Operator: All Operators, Activity Start Date: Wednesday, June 17, 2009, Activity End Date: Thursday, June 18, 2009), and 'Sort By' (Activity Date, Descending (From Z to A)). A 'Generate' button is highlighted. Below it are 'PDF' and 'Export' buttons. The main report area displays the 'System Activity Log Report' for Thursday, June 18, 2009, 09:11 AM, with a total of 13 logs. The report includes the KABA logo and a table of activities.

Activity Date	Event	Description	Operator	Login Level
6/18/2009 09:10 AM	Users Operations	View Report	1	lco
6/18/2009 09:05 AM	Operator Login/Logout	Operator Login	1	lco
6/17/2009 05:04 PM	Operator Login/Logout	Operator Logout	1	lco
6/17/2009 05:04 PM	Database Management	Backup Database	1	lco
6/17/2009 05:00 PM	Site Configuration	Modify User Specific Access	1	lco
6/17/2009 04:31 PM	Users Operations	Add Keycard	1	lco
6/17/2009 04:31 PM	Users Operations	Modify User	1	lco
6/17/2009 04:21 PM	Users Operations	Add Keycard	1	lco
6/17/2009 04:21 PM	Users Operations	Modify User	1	lco
6/17/2009 04:21 PM	Users Operations	Add User	1	lco
6/17/2009 04:20 PM	Site Configuration	Add User Specific Access	1	lco
6/17/2009 10:00 AM	Users Operations	Add User	1	lco
6/17/2009 09:52 AM	Operator Login/Logout	Operator Login	1	lco

If you want to view more Reports, select another report from “Choose a Report” field in the upper left corner of this **View Report** window.

When you are finished viewing the reports, click the red X in the upper right corner to exit the **View Report** window and return to the Main Menu.

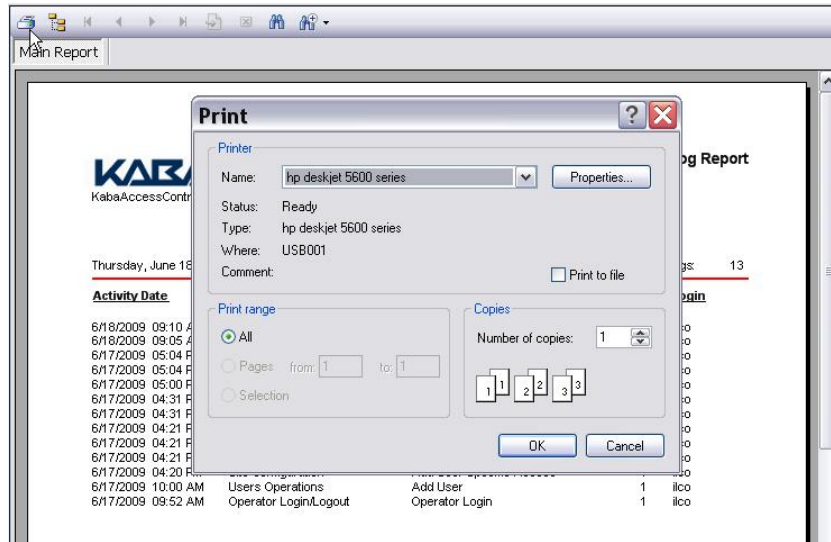
Printing Reports

Complete the following steps to print a report by first generating it to view:

- Click the **Print Report** icon in the **Main Report** pane.

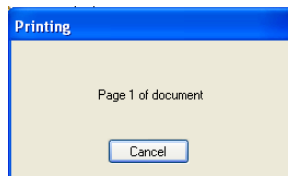


- The system displays the **Print** window.



Select your printer and any additional print options.


Click **OK**. The report is sent to the printer for printing.



Note: On some printers, the printed column alignment of a report may not be correct. If this happens, save the file as a text file (the default folder to save reports is **C:\Program Files\Kaba\E-Plex Enterprise MainClient\Reports Module\Reports**). Later, you can retrieve the saved report through Windows Explorer, and then print it to get a properly aligned report.

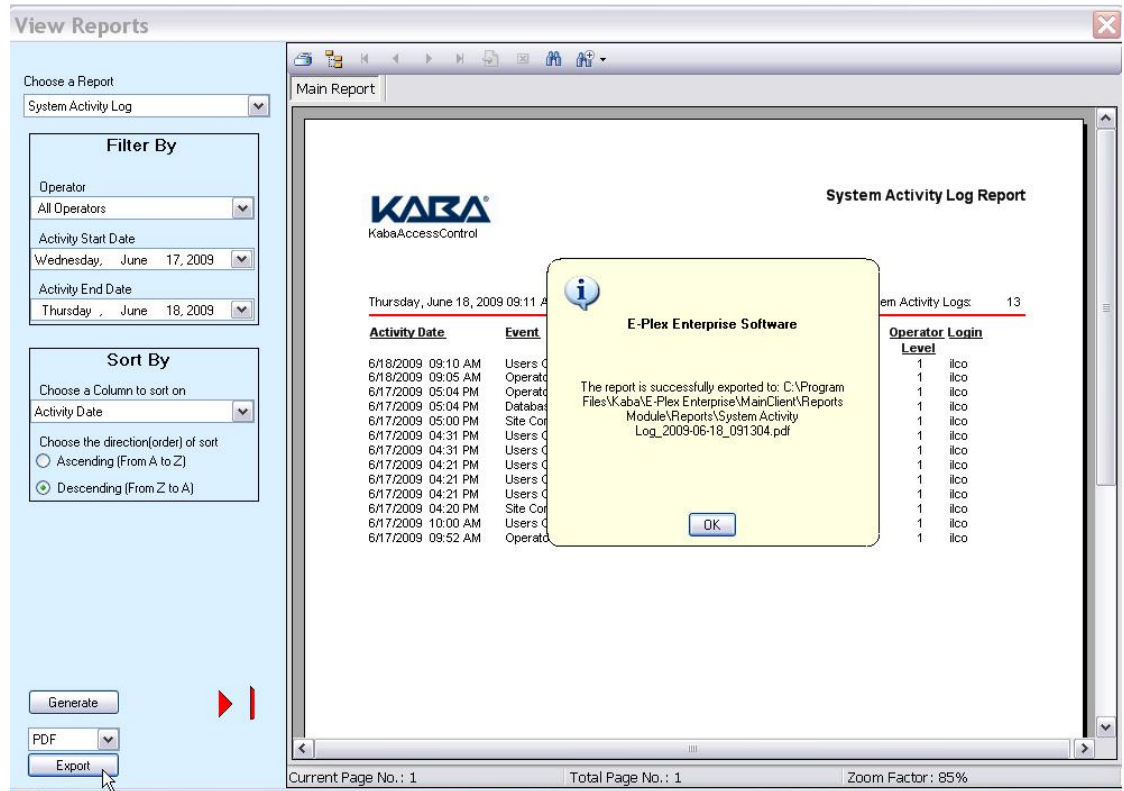
Exporting a Report

Complete the following steps to export (and save) a report in a specific file format by first generating it to view:

- From the drop down menu, select the specific file format you want the report file to be exported and saved. The available file formats are **PDF, Word, Excel, Rich Text** and **HTML**.
- Click the **Export Report** icon. 
- It will export and save to the specified Reports folder and a “successful” message will be displayed. If no Reports export/save folder path is specified in the **System Setup/Systems Settings** menu, the screen will display the **Export Report** window with

► Using the E-Plex Enterprise Software

options for you to export and save, either in a folder on your local drive, or any external or network drive.



Click **OK**. The software returns to the Reports window.

Access Schedules Report

The Access Schedules report displays all schedules that have been defined in the E-Plex Enterprise software.

The screenshot shows the 'Schedules Report' window in the KABA AccessControl software. The left sidebar contains the following controls:

- Choose a Report:** Schedules
- Filter By:**
 - Access on Sunday
 - Access on Monday
 - Access on Tuesday
 - Access on Wednesday
 - Access on Thursday
 - Access on Friday
 - Access on Saturday
- Sort By:**
 - Choose a Column to sort on: Schedule Name
 - Choose the direction(order) of sort:
 - Ascending (From A to Z)
 - Descending (From Z to A)
- Buttons:** Generate, PDF, Export

The main report area displays the following information:

KABA
KabaAccessControl

Thursday, June 18, 2009 10:06 AM Total Schedules: 3

Schedule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start	End
7 AM-6PM,M-F		✓	✓	✓	✓	✓		07:00 AM	06:00 PM
Always	✓	✓	✓	✓	✓	✓	✓	12:00 AM	12:00 AM
EveningShift		✓	✓	✓	✓	✓		03:00 AM	11:30 PM

At the bottom of the window, the status bar shows: Current Page No.: 1, Total Page No.: 1, Zoom Factor: 85%

From this window, you can print and export/save the Access Schedules report.

Holidays/Vacations Report

The Holidays/Vacations report displays all holiday/vacation periods that have been defined in the Enterprise software.

The screenshot shows a software window titled "View Reports" with a sidebar on the left and a main report area on the right. The sidebar contains a "Choose a Report" dropdown set to "Holidays/Vacations", a "Sort By" section with a "Choose a Column to sort on" dropdown set to "Holiday/Vacation Name" and two radio buttons for "Ascending (From A to Z)" (selected) and "Descending (From Z to A)", and a "Generate" button at the bottom. The main report area displays the "KABA ProEdit" logo and the title "Holidays and Vacations Report". It shows the date and time "Tuesday, January 22, 2008 04:24 PM" and "Total Holidays/Vacations: 3". Below this is a table with three columns: "Holiday/Vacation Name", "Start Date Time", and "End Date Time".

<u>Holiday/Vacation Name</u>	<u>Start Date Time</u>	<u>End Date Time</u>
Campus Fall Break	10/11/2008 12:00 AM	10/19/2008 11:59 PM
Christmas Holiday	12/24/2008 12:00 AM	12/25/2008 11:59 PM
Independence Day	7/4/2008 12:00 AM	7/5/2008 11:59 PM

At the bottom of the window, it shows "Current Page No.: 1", "Total Page No.: 1", and "Zoom Factor: 85%".

From this window, you can print and export/save the Holidays/Vacations report.

Audits from Downloaded Doors

Each Enterprise software driven E-Plex lock stores up to 30,000 audit events. The audit file is “circular” in that the oldest audited record is overwritten by the most recent one. A hard reset of the lock does not clear the audit trail for security reasons.

The *Audits from Downloaded Doors* report displays all door audits that have been downloaded from a door or doors to the PC system through the M-Unit. The software displays a list of “download” data files, indicating the name of each door/lock from which a data file has been received.

View Reports

Choose a Report
Audits from Downloaded Doors

Filter By

Door Groups
Staff Offices

Doors
Office 1

Audit Dates
Choose an Audit Date

User Groups
Choose a User Group

Users
Choose a User

Generate

Main Report

KABA
Pro Edit

Audits from Doors Report

Thursday, January 24, 2008 03:24 PM

Door Group:	Staff Offices	Audit Date:	1/24/2008 3:21:13 PM	Total Events:	100
Door Name:	Office 1	Firmware Version:	1.0	Number of Opens:	0
Lock Function:	Entry Lock	Lock Model:	E-Plex 6800	Operator:	daniel

Date/Time	Last Name	First Name	User Type	Card Seq	Transaction
1/24/2008 02:10 PM	Griesbeck	Daniel	Master	1	Access denied - Invalid Credentials
1/24/2008 02:10 PM	Griesbeck	Daniel	Master	1	Access denied
1/24/2008 02:10 PM	Griesbeck	Daniel	Master	1	Access denied - Invalid Credentials
1/24/2008 02:10 PM	Griesbeck	Daniel	Master	1	Access denied
1/24/2008 02:10 PM	Griesbeck	Daniel	Master	1	Access denied - Invalid Credentials
1/24/2008 02:10 PM	Griesbeck	Daniel	Master	1	Access denied
1/24/2008 02:10 PM	Pickens	LaToya	Access	2	Lockunlock/lock. Due to an access granted, the lock unlocked and after the programmed opening duration, relocked.
1/24/2008 02:11 PM				1	Access denied - The user is not found in the lock database
1/24/2008 02:11 PM				1	Access denied - The user is not found in the lock database
1/24/2008 02:11 PM	Pickens	LaToya	Access	5	DESFire command card 'reactivate FIPS' succeed
1/24/2008 02:11 PM	Pickens	LaToya	Access	5	DESFire command card 'reactivate FIPS' succeed
1/24/2008 02:16 PM	Griesbeck	Daniel	Master	1	Access denied - Invalid Credentials
1/24/2008 02:16 PM	Davis	Tiffany	Manager	2	Lockunlock/lock. Due to an access granted, the lock unlocked and after the programmed opening duration, relocked.
1/24/2008 02:18 PM				0	Access denied
1/24/2008 02:19 PM	Pickens	LaToya	Access	2	Lockunlock/lock. Due to an access granted, the lock unlocked and after the programmed opening duration, relocked.
1/24/2008 02:20 PM	Griesbeck	Daniel	Master	1	Access denied - Invalid Credentials
1/24/2008 02:20 PM	Griesbeck	Daniel	Master	1	Access denied
1/24/2008 02:20 PM	Pickens	LaToya	Access	5	DESFire command card 'reactivate FIPS' succeed
1/24/2008 02:20 PM	Pickens	LaToya	Access	5	DESFire command card 'reactivate FIPS' succeed
1/24/2008 02:22 PM				0	Access denied

Page 1 of 5

Current Page No.: 1 Total Page No.: 5 Zoom Factor: Page Width

From this window, you can print and export/save the Audits from Downloaded Doors report.

Cards Status Report

The Cards Status report displays card creation (enrollment) date and card ID info of all card/token users in the system.

The screenshot shows the KABA Cards Status Report interface. On the left, there is a sidebar with the following controls:

- Choose a Report: Cards Status
- Sort By: Choose a Column to sort on: Last Name
- Choose the direction(order) of sort:
 - Ascending (From A to Z)
 - Descending (From Z to A)
- Buttons: Generate, PDF, Export

The main report area displays the KABA logo and the title "Cards Status Report". Below the logo, it shows the date and time: "Thursday, June 18, 2009 10:17 AM" and the total number of cards: "Total Cards: 9".

Last Name	First Name	Creation Date	Formatted Card ID
123-10000	123-10000	6/15/2009 02:17 PM	123-10000
123-10001	123-10001	6/15/2009 02:17 PM	123-10001
123-10002	123-10002	6/15/2009 02:17 PM	123-10002
123-10003	123-10003	6/15/2009 02:17 PM	123-10003
123-10004	123-10004	6/15/2009 02:17 PM	123-10004
Brown	Nancy	6/15/2009 03:21 PM	014-16836
Griesbeck	Daniel	6/15/2009 03:26 PM	004-22184
Lessard	Steven	6/15/2009 03:10 PM	012-12345
User-Guest	Christin	6/17/2009 04:31 PM	012-60844

At the bottom of the interface, there is a footer with the following information:

- Current Page No.: 1
- Total Page No.: 1
- Zoom Factor: 85%

From this window, you can print and export/save the Cards Status report.

Door Groups Report

The Door Groups report displays all door groups that have been defined in the Enterprise software.

The screenshot shows the 'Door Groups Report' interface. On the left, there is a control panel with the following elements:

- Choose a Report:** A dropdown menu set to 'Door Groups'.
- Sort By:** A section with two options:
 - Choose a Column to sort on:** A dropdown menu set to 'Door Group Name'.
 - Choose the direction(order) of sort:** Two radio buttons: 'Ascending (From A to Z)' (selected) and 'Descending (From Z to A)'.
- Buttons:** 'Generate', 'PDF', and 'Export'.

The main report window, titled 'Main Report', displays the following content:

KABA®
KabaAccessControl

Thursday, June 18, 2009 10:23 AM Total Door Group(s): 3

<u>Door Group Name</u>	<u>Manager</u>	
DG-Accounting	Jane	Doe
DG-Manuf	Steven	Lessard
DG-Technical	Steven	Lessard

At the bottom of the window, the status bar shows: Current Page No.: 1 | Total Page No.: 1 | Zoom Factor: 85%

From this window, you can print and export/save the Door Groups report.

Doors Report

The Doors report displays all doors, up to 100,000 that have been defined in the Enterprise software.

Choose a Report
Doors

Filter By

M-Unit Sync Required

Lock Function Type
Choose a Lock Function Type

Sort By

Choose a Column to sort on
Door Name

Choose the direction(order) of sort
 Ascending (From A to Z)
 Descending (From Z to A)

Generate

PDF

Export

Main Report

KABA
KabaAccessControl

Thursday, June 18, 2009 10:24 AM

DOOR GROUP NAME: **DG-Accounting** Total Doors: 1

Door Name	Assurance Level	Lock Function	Remote Unlock	Tamper Count	Passage Mode Enabled	Tamper Time (Sec.)	Buzzer Volume	Unlock Time (Sec.)
Office-Controller	High	Latch/Exit/Swingbr	<input type="checkbox"/>	4	<input type="checkbox"/>	30	1	2

DOOR GROUP NAME: **DG-Manuf** Total Doors: 1

Door Name	Assurance Level	Lock Function	Remote Unlock	Tamper Count	Passage Mode Enabled	Tamper Time (Sec.)	Buzzer Volume	Unlock Time (Sec.)
Canteen	High	Entry Lock	<input type="checkbox"/>	4	<input checked="" type="checkbox"/>	30	1	2

DOOR GROUP NAME: **DG-Technical** Total Doors: 1

Door Name	Assurance Level	Lock Function	Remote Unlock	Tamper Count	Passage Mode Enabled	Tamper Time (Sec.)	Buzzer Volume	Unlock Time (Sec.)
Physics Lab-1	High	Entry Lock	<input type="checkbox"/>	4	<input checked="" type="checkbox"/>	30	1	2

Current Page No.: 1 | Total Page No.: 1 | Zoom Factor: 85%

From this window, you can print and export/save the Doors report.

Doors for a User Report

The Doors for a User report allows you to view all doors that a particular user has been assigned to, as well as the access schedules associated with each door, in the Enterprise software.

The screenshot displays the 'Doors for a User Report' window. On the left, there is a sidebar with a 'Filter By' section containing three dropdown menus: 'User Groups' (set to 'Doors for a User'), 'Users' (set to 'Choose a User Group'), and 'Choose a User' (set to 'Choose a User'). Below these are buttons for 'Generate', 'PDF', and 'Export'. The main report area features the KABA logo and the title 'Doors for a User Report'. It shows the date and time: 'Thursday, June 18, 2009 10:28 AM'. The report is organized into sections for different users. The first section is for 'Thomas Jawa' (User PIN: 87654321, User Type: Master, User Group: Global). It lists three doors: 'Office-Controller', 'Canteen', and 'Physics Lab-1'. The second section is for 'Steven Lessard' (User PIN: 9999, User Type: Manager, User Group: UG-Office Staff). It lists two doors: 'Canteen' and 'Physics Lab-1'. At the bottom, it indicates 'Current Page No.: 1', 'Total Page No.: 2', and 'Zoom Factor: 85%'.

Last Name	First Name	User PIN	User Type	Revoked	User Group
Thomas	Jawa	87654321	Master		Global
1	Door(s) assigned from 'DG-Accounting' Door Group				
Door ID	Door Name				
2	Office-Controller				
1	Door(s) assigned from 'DG-Manuf' Door Group				
Door ID	Door Name				
3	Canteen				
1	Door(s) assigned from 'DG-Technical' Door Group				
Door ID	Door Name				
1	Physics Lab-1				
			Jawa Thomas has access to 3 Distinct Door(s)		
Last Name	First Name	User PIN	User Type	Revoked	User Group
Lessard	Steven	9999	Manager		UG-Office Staff
1	Door(s) assigned from 'DG-Manuf' Door Group				
Door ID	Door Name				
3	Canteen				
1	Door(s) assigned from 'DG-Technical' Door Group				
Door ID	Door Name				
1	Physics Lab-1				
			Steven Lessard has access to 2 Distinct Door(s)		

From this window, you can print and export/save the Doors for a User report.

Access Groups with Doors Info Report

The Access Groups with Doors Info report allows you to view all doors assigned to a particular access group in the Enterprise software.

Choose a Report: Access Groups with Doors info

Filter By: Door Groups, Choose a Door Group

Sort By: Choose a Column to sort on: Door Name, Ascending (From A to Z)

Generate PDF

Main Report: Access Groups with Doors info Report

Thursday, June 18, 2009 10:37 AM Total Access Groups: 2

Access Group	Total Doors: 1											
Door Name	Credential	Schedule Name	Passage Mode	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start	End
Canteen	PIN	Always	Manual	✓	✓	✓	✓	✓	✓	✓	12:00 AM	12:00 AM

Access Group	Total Doors: 2											
Door Name	Credential	Schedule Name	Passage Mode	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start	End
Office-Contr	PIN & Card	Always	None	✓	✓	✓	✓	✓	✓	✓	12:00 AM	12:00 AM
Physics Lab-1	Card	7AM-6PM,M-F	First Authorized Passage		✓	✓	✓	✓	✓		07:00 AM	06:00 PM

From this window, you can print and export/save the Access Groups with Doors Info report.

Access Groups with Users Info Report

The Access Groups with Users Info report allows you to view all users assigned to a particular access group in the Enterprise software.

Choose a Report: Access Groups with Users info

Filter By: User Groups, Choose a User Group

Sort By: Choose a Column to sort on: Last Name, Ascending (From A to Z)

Generate PDF Export

Main Report: Access Groups with Users info Report

Thursday, June 18, 2009 10:38 AM Total Access Groups: 3

Access Group	Total Users: 0				
User Group	Last Name	First Name	Card ID	User PIN	
AG-Production					

Access Group	Total Users: 0				
User Group	Last Name	First Name	Card ID	User PIN	
AG-Technical					

Access Group	Total Users: 15				
User Group	Last Name	First Name	Card ID	User PIN	
Global	123-10000	123-10000	123-10000	7536	
Global	123-10001	123-10001	123-10001	8355	
Global	123-10002	123-10002	123-10002	7912	
Global	123-10003	123-10003	123-10003	6023	
Global	123-10004	123-10004	123-10004	2854	
UG-Office Staff	Brown	Nancy	014-16836	1835	
Global	Griesbeck	Daniel	004-22184	6377	
UG-Office Staff	Kerrington	Jimmy		6591	
UG-Office Staff	Lessard	Steven	012-12345	9999	

Current Page No.: 1 Total Page No.: 1 Zoom Factor: 85%

From this window, you can print and export/save the Access Groups with Users Info report.

Operators Report

The Operators report displays all three levels of Operators that have been defined in the Enterprise software.

The screenshot shows the 'Operators Report' window in the KABA AccessControl software. The left sidebar contains a 'Choose a Report' dropdown set to 'Operators', a 'Sort By' section with 'Last Name' selected, and radio buttons for 'Ascending (From A to Z)' and 'Descending (From Z to A)'. Below these are 'Generate', 'PDF', and 'Export' buttons. The main report area displays the KABA logo, the title 'Operators Report', and the date/time 'Thursday, June 18, 2009 10:40 AM'. It also shows 'Total Operators: 2'. A table lists the operators:

<u>Last Name</u>	<u>First Name</u>	<u>Login Name</u>	<u>Operator Level</u>
Doe	Jane	kabakaba	2
Thomas	Jawa	lco	1

At the bottom of the window, it shows 'Current Page No.: 1', 'Total Page No.: 1', and 'Zoom Factor: 85%'.

From this window, you can print and export/save the Operators report.

Systems Activity Log Report

The Systems Activity Log Report displays all Operator activity in the E-Plex Enterprise PC system software.

Choose a Report
System Activity Log

Filter By

Operator
All Operators

Activity Start Date
Monday, June 08, 2009

Activity End Date
Wednesday, June 17, 2009

Sort By

Choose a Column to sort on
Activity Date

Choose the direction(order) of sort
 Ascending (From A to Z)
 Descending (From Z to A)

Generate

PDF

Export

Main Report

KABA
KabaAccessControl

System Activity Log Report

Thursday, June 18, 2009 10:43 AM Total System Activity Logs: 91

Activity Date	Event	Description	Operator Login Level
6/17/2009 05:04 PM	Operator Login/Logout	Operator Logout	1 ilco
6/17/2009 05:04 PM	Database Management	Backup Database	1 ilco
6/17/2009 05:00 PM	Site Configuration	Modify User Specific Access	1 ilco
6/17/2009 04:31 PM	Users Operations	Add Keycard	1 ilco
6/17/2009 04:31 PM	Users Operations	Modify User	1 ilco
6/17/2009 04:21 PM	Users Operations	Add Keycard	1 ilco
6/17/2009 04:21 PM	Users Operations	Modify User	1 ilco
6/17/2009 04:21 PM	Users Operations	Add User	1 ilco
6/17/2009 04:20 PM	Site Configuration	Add User Specific Access	1 ilco
6/17/2009 10:00 AM	Users Operations	Add User	1 ilco
6/17/2009 09:52 AM	Operator Login/Logout	Operator Login	1 ilco
6/16/2009 04:11 PM	Operator Login/Logout	Operator Logout	1 ilco
6/16/2009 04:11 PM	Database Management	Backup Database	1 ilco
6/16/2009 04:09 PM	Operator Login/Logout	Operator Login	1 ilco
6/16/2009 08:21 AM	Operator Login/Logout	Operator Login	1 ilco
6/15/2009 05:26 PM	Operator Login/Logout	Operator Logout	1 ilco
6/15/2009 05:26 PM	Database Management	Backup Database	1 ilco
6/15/2009 03:29 PM	Users Operations	Delete User	1 ilco
6/15/2009 03:26 PM	Users Operations	Add Keycard	1 ilco
6/15/2009 03:26 PM	Users Operations	Modify User	1 ilco
6/15/2009 03:26 PM	Users Operations	Modify User	1 ilco
6/15/2009 03:22 PM	Users Operations	Add User	1 ilco
6/15/2009 03:21 PM	Users Operations	Add Keycard	1 ilco
6/15/2009 03:21 PM	Users Operations	Modify User	1 ilco
6/15/2009 03:21 PM	Users Operations	Modify User	1 ilco
6/15/2009 03:10 PM	Users Operations	Add Keycard	1 ilco

Current Page No.: 1 Total Page No.: 2 Zoom Factor: 85%

From this window, you can print and export/save the Systems Activity Log Report.

Departments Report

The Departments report displays all Departments defined in the Enterprise software.

From this window, you can print and export/save the Departments report.

Users Report

The Users report displays all the users defined in the Enterprise software.

Global						
Group Name	Last Name	First Name	User Type	Card ID	Valid From	Valid To
Global	123-10000	123-10000	Access	123-10000	6/15/09 2:17 pm	6/15/10 2:17 pm
	123-10001	123-10001	Access	123-10001	6/15/09 2:17 pm	6/15/10 2:17 pm
	123-10002	123-10002	Access	123-10002	6/15/09 2:17 pm	6/15/10 2:17 pm
	123-10003	123-10003	Access	123-10003	6/15/09 2:17 pm	6/15/10 2:17 pm
	123-10004	123-10004	Access	123-10004	6/15/09 2:17 pm	6/15/10 2:17 pm
	Griesbeck	Daniel	Access	004-22184	6/15/09 3:26 pm	6/15/10 3:26 pm
	Supervisor	Maintenance-All	Service		1/1/00 12:00 am	1/1/00 12:00 am
	Technician	Maintenance-1	Service		1/1/00 12:00 am	1/1/00 12:00 am
	Thomas	Jawa	Master		4/27/09 4:06 pm	4/27/09 4:06 pm
	User-MUnit	Peter	M-Unit		6/17/09 10:00 am	6/17/10 10:00 am
UG-Office Staff						
Group Name	Last Name	First Name	User Type	Card ID	Valid From	Valid To
UG-Office Staff	Brown	Nancy	Access	014-16836	6/15/09 3:21 pm	6/15/10 3:21 pm
	Kerrington	Jimmy	Access		5/6/09 4:32 pm	5/6/10 4:32 pm
	Lessard	Steven	Manager	012-12345	6/15/09 3:01 pm	6/15/10 3:01 pm
	Mitchel	Mariana	Guest		5/19/09 2:54 pm	4/30/10 12:00 am
	User-Guest	Christin	Guest	012-60844	6/17/09 4:21 pm	9/15/09 4:21 pm

From this window, you can print and export/save the Users report.

Users for a Door Report

The Users for a Door report allows you view all users assigned to a particular door in the Enterprise software.

The screenshot shows the 'Users for a Door' report interface. On the left, there are controls for 'Filter By' (Door Groups, Doors) and 'Sort By' (Last Name, Ascending/Descending). The main report area displays the KABA logo and a table of users for three doors: Physics Lab-1, Office-Controller, and Canteen. The table columns are Door Name, Door Group, Lock Function, Passage Mode, and Assurance. Below each door name, there is a summary of total users and a list of individual users with their details.

Door Name	Door Group	Lock Function	Passage Mode	Assurance	
Physics Lab-1	DG-Technical	Entry Lock	Enabled	High	
Total Users: 4					
Last Name	First Name	Card ID	User PIN	User Type	Use
Lessard	Steven	012-12345	9999	Manager	UG-4
Mitchel	Mariana		3292	Guest	UG-4
Supervisor	Maintenance-All		7874	Service	Glob
Thomas	Jawa		87654321	Master	Glob
Office-Controller	DG-Accounting	Latch/Exit/Swingbolt Lock	Disabled	High	
Total Users: 1					
Last Name	First Name	Card ID	User PIN	User Type	Use
Thomas	Jawa		87654321	Master	Glob
Canteen	DG-Manuf	Entry Lock	Enabled	High	
Total Users: 2					
Last Name	First Name	Card ID	User PIN	User Type	Use
Lessard	Steven	012-12345	9999	Manager	UG-4
Thomas	Jawa		87654321	Master	Glob

From this window, you can print and export/save the Users for a Door report.

Users Without an Active Card Report

The Users Without an Active Card report displays all users that have been defined in the E-Plex Enterprise software but have not been assigned a card/token yet.

The screenshot shows the 'Users Without an Active Card' report in the KABA software. The interface is divided into a sidebar on the left and a main report area on the right.

Sidebar:

- Choose a Report: Users Without an Active Card
- Sort By:
 - Choose a Column to sort on: Last Name
 - Choose the direction(order) of sort:
 - Ascending (From A to Z)
 - Descending (From Z to A)
- Buttons: Generate, PDF, Export

Main Report:

KABA
KabaAccessControl

Thursday, June 18, 2009 10:52 AM Total Users:

Group Name: Global Total Users: 5

Last Name	First Name	User Type	Valid From	Valid To	User PIN
Doe	Jane	Manager	6/11/09 1:58 pm	6/11/10 1:58 pm	5420
Supervisor	Maintenance-All	Service	1/1/00 12:00 am	1/1/00 12:00 am	7874
Technician	Maintenance-1	Service	1/1/00 12:00 am	1/1/00 12:00 am	2013
Thomas	Jawa	Master	4/27/09 4:06 pm	4/27/09 4:06 pm	8765
User-MUnit	Peter	M-Unit	6/17/09 10:00 am	6/17/10 10:00 am	7777

Group Name: UG-Office Staff Total Users: 2

Last Name	First Name	User Type	Valid From	Valid To	User PIN
Kerrington	Jimmy	Access	5/6/09 4:32 pm	5/6/10 4:32 pm	6591
Mitchel	Mariana	Guest	5/19/09 2:54 pm	4/30/10 12:00 am	3292

Current Page No.: 1 Total Page No.: 1 Zoom Factor: 85%

From this window, you can print and export/save the Users Without a Card report.

(Wireless) Lock Status Report

The (wireless) Lock Status report displays the current status of each wireless enabled lock that is either online or offline in the E-Plex Enterprise wireless configuration enabled system.

The screenshot shows the 'Lock Status Report' window. On the left, there are controls for 'Filter By' (Doors: Choose a Door) and 'Sort By' (Choose a Column to sort on: Door Name, with options for Ascending and Descending). At the bottom left, there are buttons for 'Generate', 'PDF', and 'Export'. The main report area displays the following data:

Conference Room		Battery Status	Normal	Unlocked Passage Mode
Door Name	Conference Room	Battery Level	5.68V	Access Schedule
MAC Address	FD938A00006F0D00	Thumb Turn	False	False
Lock Function		Emer. Lockdown	False	False
Lock Model	E5600	Emer. Passage	False	False
Odometer	18456142	Lockout State	False	False
Last Key	1	Remote Unlock	False	
Openings	303			
Clock Reset	False			

Marketing-Doc-Room		Battery Status		Unlocked Passage Mode
Door Name	Marketing-Doc-Room	Battery Level		Access Schedule
MAC Address		Thumb Turn		Manual
Lock Function		Emer. Lockdown		Deadbolt Unlock
Lock Model		Emer. Passage		Lock Open
Odometer		Lockout State		
Last Key		Remote Unlock		
Openings				
Clock Reset				

Supplies-Area		Battery Status		Unlocked Passage Mode
Door Name	Supplies-Area	Battery Level		Access Schedule
MAC Address		Thumb Turn		Manual
Lock Function		Emer. Lockdown		Deadbolt Unlock
Lock Model		Emer. Passage		Lock Open
Odometer		Lockout State		
Last Key		Remote Unlock		
Openings				
Clock Reset				

From this window, you can print and export/save the Lock Status report.

Offline Wireless Locks Report

The Offline Wireless Locks report displays all wireless enabled locks that are defined in the E-Plex Enterprise software but are currently offline.

The screenshot shows the 'Offline Wireless Locks' window. On the left, there are controls for 'Filter By' (Door Groups: Choose a Door Group) and 'Sort By' (Choose a Column to sort on: Door Name, with options for Ascending and Descending). At the bottom left, there are buttons for 'Generate', 'PDF', and 'Export'. The main report area displays the following data:

DG-Wireless		Total Doors in Door Group:	
Door Name	Marketing-Doc-Room	Lock Function	Entry Lock
	Supplies-Area	Lock Type	E-Plex 5600
			E-Plex 5600
		ZAC	88 91 43 30
			99 96 15 16

From this window, you can print and export/save the Offline Wireless Locks report.

Wireless Network Map Report

The Wireless Network Map report displays the E-Plex ZigBee wireless network map of your installation in your facility, configured in the E-Plex Enterprise software.

The screenshot shows the 'Main Report' window for the 'Wireless Network Map'. On the left sidebar, there are sections for 'Filter By' (Gateways) and 'Sort By' (Gateway Name, Ascending). At the bottom of the sidebar are 'Generate', 'PDF', and 'Export' buttons. The main report area displays the KABA logo and a table of gateway information.

Wireless Network Map

Monday, April 18, 2011 11:27 AM

Gateway	Company	Gateway	Controller	2.52	Controller Build Date	20/02/2011	1:18:28PM	Lock Count	0	USBTue
MAC Address	00:0E:2A:00:1A:2A	AVR	2.0		Last Communication	18/04/2011	9:18:50AM	Join Count	1	
IP Address	From DHCP	AVR	Boot 0.4		Status	Online		Unjoin Count	0	
NodeID	0	Ember	4.2.53		Sub Net Mask	From server		Total Lock Count	1	

Door	MAC	Parent Node ID	Node ID	Last Communication	Status	RSSI		Firmware Version				
						From	To	Lock	Lock Boot	AVR	AVR Boot	Em
Conference Room	FD938A000008F0D00	0	04777	18/04/2011 9:17:45AM	Online	-37	-38	99.52.1	1.2	2.0	0.4	4.2

Page 1 of 1

From this window, you can print and export/save the Wireless Network Map report.

4 Operating the E-Plex Lock at its Keypad

All E-Plex Wireless Locks & System related info are highlighted in this turquoise color background for easy reference.

This section describes how to operate the Enterprise software driven E-Plex lock at the lock keypad, including the following topics:

- Overview of the Lock
- Configuring the Lock Functions
- Initial Programming of the Lock
- Initializing (ZAC'ing) a Wireless Lock to Join the Network ;[**Wireless lock only**]
- Performing Emergency Commands at Wireless Lock's Keypad ;[**Wireless lock only**]

Overview of the Lock

The E-Plex lock series that can be operated by the E-Plex Enterprise software system are:

- | | |
|-------------------------------------------|---------------------------------|
| E5200, E5600 and E5700 | – “Standard” locks |
| E5200 SAC, E5600 SAC and E5700 SAC | – Standalone Access Controllers |
| E3200, E3600 and E3700 | – Narrow stile locks |

Please refer to the “*E-Plex 3xxx/5xxx Lock Series Operations Manual*” for detailed lock keypad commands and operations of each of these models.

This section will provide an overview of only the “standard” E5xxx lock series which includes the following topics:

- States of the Lock
- Battery Life and Replacement
- Sequence of Operations
- Default Values of the E-Plex Lock Programmable Parameters

[Start]

- **For Wireless:** Additionally, you can perform a few other operations such as “joining” and ZAC’ing (ZigBee Access Code) the lock to your E-Plex wireless network and remotely programming the lock without a portable M-Unit device.
- Also, during and emergency situation, you can also activate the Emergency Lockdown and Emergency Passage (evacuation) operations of wireless locks right at that one lock’s keypad, instead of performing this emergency operation from the Host PC.
- Please refer to these wireless specific lock keypad functions which are explained in detail at the end of this Chapter.

[End]

States of the Lock

There are four states of the E-Plex lock: 1- (default) Factory Mode, 2- Access Mode by “LearnLok, 3- Access Mode by Software and, 4- Pushbutton Programming Mode.

Factory Mode

The default Factory Mode is one of four primary states of the lock. The main characteristics of this state include the following:

The E-Plex lock opens only when the 8-digit factory default Master user PIN -> 1-2-3-4-5-6-7-8 is entered at the lock keypad.

The visual indication for “access granted” is the green LED flashing once. A high-pitched tone is also generated while the green LED is on.

The Master User must change this factory default Master PIN to be able to exit permanently from the Factory Mode and switch to the normal Access Mode (by LearnLok or by software) and its Pushbutton Programming Mode of operations.

Access Mode by “LearnLok”

This mode refers to the lock that is operational for user access after the factory default Master PIN of 12345678 is changed to something else. When the lock enters the Access Mode in LearnLok mode, the Master (and Manager users) can add or delete regular users in the lock simply by entering relevant command codes at the lock keypad. Please refer to the “**E-Plex 3xxx/5xxx Lock Series Operations Manual**” for details.

Access Mode by Software

This mode refers to a lock that is operational for user access after it is programmed by the M-Unit with its lock/user configuration data downloaded from the E-Plex Enterprise system software. When the lock enters the Access Mode, the method of lock access is either by, (i) PIN only, or by (ii) Card only, or by (iii) PIN followed by the associated Card -> Prox or Smart (Mifare, DESFire or iClass).

Note: The Service users can have PIN only access (ie., no tokens).

Access Mode refers to a lock that is fully operational for user access and not in Factory Mode. You will operate the lock in conjunction with the E-Plex Enterprise software and the portable PC M-Unit by programming the lock with valid user access credentials etc.

Pushbutton Programming Mode

The E-Plex lock enters the Pushbutton Programming Mode when the Master user or one of the Manager users enters the **# key first** on the lock keypad, followed by presenting the credential (PIN, Card or PIN followed by Card) to put the lock in programming mode. Once the lock is in the Pushbutton Programming Mode, the Master/Manager can enter one or more command sequences. Each command sequence **ends with a # key** that acts like an <Enter> button on a PC keyboard. At the very end of all sequences of programming commands, enter **one more # key** to remove the lock from the Pushbutton Programming Mode and return to the normal Access Mode.

Battery Life and Replacement

The E-Plex locks use four “AA” alkaline batteries. A variety of factors will determine how long your lock operates on a set of batteries, including the following:

- Shelf life of the batteries
- Number of openings per day
- Environmental conditions
- Battery brand
- Access credential settings (PIN only, Card only or both PIN & Card)
- Lock parameter settings

In most cases, you can expect between 50,000 openings (wireless) and 90,000 openings (non-wireless) per set of 4, AA alkaline batteries, and about two and a half times this range if you use the optional 4, C alkaline battery pack kit.

A flash of both red and green LEDs identifies a low battery condition when a valid credential is presented, and the lock will still open. Though under ideal conditions the lock will keep operating for another thousand or so openings, the batteries as a complete set should be replaced as soon as possible when you observe a low battery condition,

Battery Pack Replacement

Always replace all four batteries in the pack with good quality, AA (or, the optional four C, if used) alkaline batteries. If you replace the batteries within two to three minutes, the lock will continue working as before, granting and denying access to users based on their access schedules.

If the battery replacement time is longer than two to three minutes, you will lose the current date and time of the lock from its memory, even though all users and locks configuration parameter information will not be lost. When the lock loses its date/time, all of your access schedule times will be out of sync, thus denying access to valid users. In this case, you must update the lock's date/time with the current date/time.

To update the current date & time you can either use the lock keypad command sequences 001# and 002# along with the current date and current time parameters, or simply re-program this lock with its proper lock ID using the portable M-Unit. This is described in detail in ***E-Plex PC M-Unit User Guide***.

Important: Please ensure that your M-Unit's current date and time are set correctly before synchronizing with the lock. If you forget to update the date/time, the lock will keep flashing the red LED every 10 seconds or so as a reminder until the lock's date/time is updated.

Note: In rare instances, when you reconnect the lock with new batteries, the lock may not re-initialize properly; a typical symptom is that the lock does not recognize any pushbutton input. If this happens, disconnect the battery pack, press any one of the pushbuttons for a minimum of 2 seconds to discharge the built-in circuit capacitance, and then re-connect the battery pack. Wait a couple of seconds until you see the green LED flash once, followed by the sound of the motor crunching and a high pitched beep indicating that the lock has re-initialized properly.

Sequence of Operations

This section describes the sequence of operations for accessing and programming the E-Plex lock.

- With the lock still in Factory Mode, do the following:
- Program the "Lock Function" of the lock if you want it to be anything other than the factory default "Entry" lock function.

Configuring the Lock Functions

Before putting the lock in service, you must first program the lock function when still in Factory Mode. The default lock function for any lock from the factory is "Entry" lock function, which is the same as a Cylindrical lock without a privacy thumbturn, or a Mortise lock without a deadbolt, or an Exit Trim lock. The command codes involved here are 011# and 013#.

Note: Refer to the separate "***E-Plex 5X00 Lock Function Setup Guide***" for instructions on changing to the desired BHMA lock function.

- Change the Factory Master user PIN to your own Master PIN (always eight digits) to place the lock in Access Mode.

The lock is now "activated" and can be programmed using the portable PC M-Unit. For more details on using the PC M-Unit, please refer to the manual, the *E-Plex P M-Unit User Guide*.

Default Values of the E-Plex Lock Programmable Parameters

Parameters	Factory Default Values
Date (MM/DD/YY)	01/01/00
Time (HH:MM)	00:00
Lock state	Un-programmed
BHMA Lock function	Entry
Manual Passage Mode open time limit	4 hours
Passage Mode	Disabled
Lockout Mode	Disabled
Unlock time	2 seconds
Buzzer volume control	Low (=1)
Tamper shutdown time	30 seconds
Tamper attempt count	4 attempts
Access PIN length	4 digits
Master PIN	12345678 (Eight digits)
Privacy privilege	Disabled
Remote unlock	Disabled

Initial Programming of the Lock

Once the required lock function is set, the lock must be programmed by the Master or the Manager(s) for everyday use. This section provides information about the initial programming of the lock, including the following:

- Entering Pushbutton Programming Mode
- Modifying the Master User PIN
- Additional Pushbutton Keypad Commands
- Resetting the Lock
- Summary of Pushbutton Programming Commands
- Visual Feedback Message Definitions

Entering Pushbutton Programming Mode

This section describes the sequence of tasks to program the lock at its keypad in Pushbutton Programming Mode.

- Put the lock in Pushbutton Programming Mode by pressing **# Master or Manager Credential** (PIN, or Card, or PIN followed by Card) **#**.
- Use the Error! Reference source not found. table found later in this Chapter to enter the 3-digit command sequence (command type + function code), followed by **#**.
- Enter the appropriate command codes as required.
- Press **#** to end Pushbutton Programming Mode.

► Operating the E-Plex Lock at its Keypad

- Once the lock is in Pushbutton Programming Mode, multiple command sequences can be entered (chaining of command codes) without having to repeat the **# Credential #** every time. However, if there is no activity for 5 seconds at the keypad, the lock will automatically exit from Pushbutton Programming Mode and return to its normal Access mode.

Example:

If the Master or Manager User, or any user of the system with a valid credential presents her/his credential the lock will open (lock is normally in Access mode) .

If the Master or Manager(s) enters **#Credential#**, the lock will enter the Pushbutton Programming mode and will wait for the next part of the command code(s) sequence.

When s/he enters one more **#** at the end of the command code sequence, the lock will exit the Pushbutton Programming mode and revert back to its normal Access mode.

Note 1: The # (pound sign) acts like the Enter key on a keyboard in your communications with the lock. The # tells the lock that one part of the entry is finished. The # serves another purpose—to distinguish a programming type command from a simple access code to open the door. A Master or Manager User can use the same Credential to open the door or to put the lock in Pushbutton Programming Mode, the only difference being that s/he uses the # sign in front to signal that s/he is about to enter a programming command.

Note 2: Correct errors during a command sequence. If an invalid entry occurs, recover from the mistake by entering the (*) key, which will clear all entries made from the beginning of the current command sequence and will reset the 5-second time limit for entering the command code again. In this case, you still have 15 seconds from the first number entered to enter the whole command code sequence.

Modifying the Master User PIN

Required User Level: Master

To change the factory Master PIN or current Master PIN, follow these steps:

- Put lock into Pushbutton Programming Mode by pressing the **#** key.
- Use the command, **000**, for Master, and then enter the new Master PIN number.
- You must use eight digits between 00000001 and 99999999 as follows: **000# MMMMMMMM#**; for example, **000# 87654321#**.
- Enter the Master PIN again: **87654321#** for confirmation.
Example of complete entry: **000# 87654321# 87654321#**.
- Key in another **#** to indicate the end of Pushbutton Programming Mode.
- After you are finished, you will always have to use this new Master PIN as part of your access credential, depending on if the Master is configured in the software to user either PIN only or PIN followed by card for programming/auditing the lock, and also for normal door access.
- **Important:** Please write down the PIN and keep store it in a safe place. You should enter this same 8-digit Master PIN in the E-Plex Enterprise initial software configuration screen (for the Master PIN) also, to be consistent. The factory Master PIN of 12345678 is no longer valid from this point.

Additional Pushbutton Keypad Commands

The following operations (except for setting up date & time which are also done through the software via the portable M-Unit) can only be performed at the lock's keypad. All other functions must be set up and sent from the E-Plex Enterprise software via the M-Unit:

- Setting date and time (commands 001# and 002#)
- Activating/de-activating Passage Mode (command 399#)
- Increasing/decreasing programmed Passage Mode duration (command 005#)
- Activating/de-activating global Lockout Mode (command 499#)
- Performing manual diagnostics (command 500#)
- Identifying an E-Plex lock model (command 501#)
- Start M-Unit communication session with the lock (command 900#)

Setting Date and Time (Commands 001# and 002#)

The following two commands are performed one after the other in sequence to set up the lock with current date and time. The factory default is 01/01/2000 00:00 when you first connect the battery pack and so must be changed to reflect the actual/current date & time.

Required User Level: Master

- Put the lock into Pushbutton Programming Mode.
- Enter command **001#** followed by MMDDYY# and again MMDDYY#, where MM=01 to 12 (Month), DD=01 to 31 (Day) and YY=08 to 99 (Year).
- 3. Enter command **002#** followed by HHMM# and again HHMM#, where HH=00 to 23 (Hour) and MM=00 to 59 (Minute).
- 4. Enter another **#** to indicate the end of programming.

Note: *The date and time can also be set by the M-Unit. Whenever you program the lock with the M-Unit, the M-Unit automatically sends the current date, time and the DST setting from its settings to the lock and so they should have been set correctly.*

Activating/De-activating Passage Mode (Command 399#)

You have already set up in the software a duration for a lock to remain in manual Passage Mode (default is 4 hours, though in the lock in its "LearnLok" mode, the default is 9 hours) and enabled it. When you activate manual Passage Mode at the lock keypad, it becomes active for the duration you have set in the software.

If your duration is setup as six hours, and you manually activate Passage Mode, say at 10:00 a.m., it will automatically re-lock at 4:00 p.m. Even if the lock was taken in and out of Passage Mode multiple times during this six-hour period, it will still re-lock after six hours from the original starting period. This ensures that a lock will never remain in Passage Mode beyond the programmed time period.

Note: *This manual Passage Mode function is different from the automatic access schedule-based Passage Mode setup in the software.*

Required User Level: Master, Manager

1. Put the lock into Pushbutton Programming Mode.
2. Enter command **399#** to activate/de-activate Passage Mode.
 - Enter the code where **1** = activate Passage Mode and **0** = de-activate Passage Mode.
An example of complete entry to activate Passage Mode is **399#1#** and to de-activate Passage Mode, it is **399#0#**.
 - Enter another **#** to indicate the end of Pushbutton Programming Mode.

Increasing/Decreasing Passage Mode Duration Temporarily (Command 005#)

As in the above example, say your manual passage mode duration is programmed for duration of six hours. So if you manually activated Passage Mode at 10:00 a.m., it will automatically re-lock at 4:00 p.m. However, there may be times when you may want to either shorten or prolong this remaining passage mode duration temporarily on that day (only) by a few hours. You can do this but you must enter this command sequence before the expiry of the current passage mode end time. Keep in mind that the next day onwards, the manual passage mode duration that was set originally will take effect again.

Required User Level: Master, Manager

1. Put the lock into Pushbutton Programming Mode.
2. Enter command **005# HH#** where HH=01 to 24 hours.

Let us take the same example as before -> activate manual passage at 10 a.m. so that it will automatically end at 4 p.m. after 6 hours. But if you want to temporarily shorten the current duration by say, 1 hour to end at 3 p.m., then you must enter HH=01 at around 2:00 p.m.

Similarly, if you want to temporarily extend the current duration by say, 2 more hours to end at 6 p.m., then you must enter HH=02 just before around 4:00 p.m.
3. Enter another **#** to indicate the end of Pushbutton Programming Mode.

Activating/De-activating Lockout Mode (Command 499#)

You may need to use the global Lockout Mode, for example, during a fire or an emergency evacuation when you do not want anyone to return to his or her office. This procedure will de-activate all regular user access credentials that are active, including Manager credentials, but excluding the Master credential.

Important: Use extreme care in using this command because if you (the Master) forget to de-activate the lockout mode after activating it, nobody in the facility will have access to the door anymore.

Required User Level: Master

- Put the lock into Pushbutton Programming Mode.
- Enter command **499#** for Lockout Mode (all except Master).
- Enter **1#** to activate Lockout Mode and **0#** to de-activate it.
Example of complete entry: **499#1#** or **499#0#**.
- Enter another **#** to indicate the end of programming.
- You have now activated or de-activated Lockout Mode.

Performing Manual Diagnostics (Command 500#)

Use the diagnostics code to perform manual diagnostics of the lock, green LED, red LED, buzzer, and the 12 pushbuttons—0 through 9, *, and #.

Required User Level: Master, Manager

- Put the lock into Pushbutton Programming Mode.
- Enter command **500#** for diagnostics. You will see a green LED and hear a high beep followed by a red LED and a low beep.
- Press **123456789*0#**, in that exact order, to test each pushbutton. If every pushbutton is working correctly, you will see a green LED and hear a normal beep for each pushbutton that is pressed.

Example of a complete entry: **500#123456789*0#**.

- Enter another **#** to indicate the end of programming.
- If you see a red LED at any time when pressing a pushbutton indicates a possible problem with the pushbuttons electronics.
- Enter another **#** to indicate the end of programming.
- If the above sequence did not pass even after two or three tries, please contact Kaba's technical support line to resolve the issue.

Identifying a Lock Model (Command 501#)

Use the Lock Model Identification code to identify if the lock model series is an E32xx/52xx, or an E36xx/56xx, or an E37xx/57xx.

Required User Level: Master, Manager

- Put the lock into Pushbutton Programming Mode.
- Enter command **501#** for Lock Model Identification.
- E32xx/52xx: The lock will flash the red and green LEDs two times with accompanying two high-pitched tones.
- E36xx/56xx: The lock will flash the red and green LEDs six times with accompanying six high-pitched tones.
- E37xx/57xx: The lock will flash the red and green LEDs seven times with accompanying seven high-pitched tones.
- Enter another **#** to indicate end of programming.

Resetting the Lock

You must know the last master code that was assigned to the lock to perform a quick reset to the default Master PIN below. As a security measure, if you do not know the last Master PIN that was assigned to the lock, you will have a 15 minute wait at the lock after the reset button is pushed and then the factory Master PIN 12345678 can be entered to complete the reset process. You can return to factory default parameters by performing a Hard Reset. This returns the lock to Factory Mode, including deleting all credentials, putting the lock back to factory default values (four-digit access PIN length), and making the Master PIN **12345678**. Also, the lock function will revert to the default "Entry" lock function. A hard reset is performed as follows (example for E-Plex 5xxx locks only):

- Insert the mechanical override key, turn to retract latch, and hold in (lock) open position.

► *Operating the E-Plex Lock at its Keypad*

- Within five seconds, press # and then release the key (latch extends back to relock).
- While the red/green lights flash alternately, press **12345678#** on keypad.
- The lock will reset. You will see two flashes of the green light with a corresponding high pitch tone, followed by the sound of the lock motor “crunch,” indicating that the reset was successful.
- The lock is now reset to the Factory Mode and the Master PIN is now 12345678.

Note: *The hard reset operation does NOT delete any audited events stored in the lock, for security reasons.*

[Start]-----

For Wireless:

- **Performing ZAC (ZigBee Access Code) Operation on Lock**

- For the ZAC operation to be successful the wireless lock must be in the default Factory Mode with its Master PIN set as **12345678**; the 3-digit ZAC command code is “**088**”.
- Before entering the 8-digit unique ZAC number of this lock on its keypad, this wireless lock is assumed to be already put in a “join on” network mode, initiated from the E-Plex Enterprise s/w from the Host PC; it will then automatically program the lock remotely.
- Let us assume that in this example the ZAC number for this lock is 11 22 33 44 and so enter the following sequence to “ZAC” the wireless lock:

12345678# 088# 11223344

The lock will start flashing the Green & Red LEDs simultaneously every three seconds for a few seconds to show that it is transferring required wireless data from the Host PC via the Gateway to the lock. On successful joining of the wireless network and of automatically getting programmed remotely, the lock will flash one last Green light (only) and will emit a high pitched tone. The lock/door is now ready for normal wireless use.

- **Activate / Deactivate Emergency Lockdown**

Note: For a Level-2 Manager or a Level-3 Access Operator/Access user, s/he must have been already programmed in this lock to perform the Emergency commands.

The Credential here refers to the user’s valid PIN only, Card only or PIN & Card.

[Master, Manager or authorized Access user’s Credential]# 911#

Important: During the Emergency lockdown state, only the mechanical override key will open the lock. None of the valid user credentials including the Master’s will open the door.

- **Activate Emergency Passage**

[Master, Manager or authorized Access user’s Credential]# 811#

The ‘Return to Normal’ command can only be entered by a Level 1 or 2 Access Operator using the software at the client or host PC.

[End]

Summary of Pushbutton Programming Commands

Name	Command	Description	Authorization
Configuration	000 # MMMMMMMM# MMMMMMMM#	Modify Master User PIN (always eight digits)	Master
Set Date	001# MMDDYY# MMDDYY#	Setup current Date MM = 01 or 12; DD = 01 to 31; YY = 08 to 99	Master
Set Time	002# HHMM# HHMM#	Setup current t Time HH = 00 or 23; MM = 00 to 59	Master
Set Temporary Passage Mode Duration	005# HH#	Setup Temporary Passage mode Duration HH = 00 or 24	Master, Manager
Manual Passage Mode	399# P#	Activate/de-activate Passage Mode P = 0 or 1; 0 = disable Passage Mode; 1 = enable Passage Mode	Master, Manager
Global Lockout Mode	499# L#	Activate/de-activate Lockout Mode (Master User is not affected by global Lockout Mode) L = 0 or 1; 0 = disable Lockout Mode; 1 = enable Lockout Mode	Master
Diagnostics	500# 123456789*0#	Manual diagnostics	Master, Manager
Lock Model Identification	501#	Identify if the lock is an E-Plex 32xx/52xx, or 36xx/56xx, or 37xx/57xx: 2 sets of green and red LEDs flash for E32xx/5200; 6 sets of same flash sequence for E36xx/56xx; and 7 sets of same flash sequence for E37xx/57xx.	Master, Manager
Communication Startup	900#	IrDa Communication startup between the lock and M-Unit PDA	Master, Manager
For Wireless Only	-----	-----	-----
ZAC (ZigBee Access Code)	088#	Initialize a wireless lock (lock must be in factory defaults)	Master, all Users
Emergency Lockdown	911#	Put wireless lock(s) in emergency shutdown (lockdown) state	Master, Manager, authorized Users
Emergency Passage	811#	Put wireless lock(s) in emergency evacuation (passage) state	Master, Manager, authorized Users
Return to Normal from Emergency	111#	Put wireless lock(s) back to the Normal state from emergency state	Master, Manager

Visual Feedback Message Definitions

Condition	Parameters			
	Green LED	Red LED	Duration	Rate
Valid pushbutton pressed	ON	OFF	1/10 sec	Once
Timeout expired	OFF	ON	1 sec	Once
Valid access credential entered/presented	ON	OFF	1/10 sec	Once
Access granted	ON	OFF	1/10 sec	1 sec
Access granted (battery low condition)	ON	ON	1/10 sec	1 sec
Access denied	OFF	ON	1 sec	Once
Valid programming entry	ON	OFF	1 sec	Once
Invalid programming entry (including duplicate access credential)	OFF	ON	1 sec	Once
Tamper shutdown beginning	OFF	ON	2 sec	Once
Tamper shutdown state	OFF	ON	1 sec	10 sec
Tamper shutdown ending	ON	OFF	2 sec	Once
*Communication starting	ON	OFF	1 sec	Once
*Communication ending	ON	OFF	1 sec	Once
*Communication aborted	OFF	ON	1 sec	Once
*Communication in progress	ON (Alternate)	ON (Alternate)	1/10 sec	1 sec
Deadbolt/Thumbturn Privacy Activated	OFF	ON	1 sec	Once
Deadbolt/Thumbturn Privacy De-activated	ON	OFF	1 sec	Once
Hard Reset sequence progress	ON (Alternate)	ON (Alternate)	½ sec	Continuously
Hard reset sequence ended successfully	ON	OFF	2 sec	Once
Hard Reset sequence failed	OFF	ON	2 sec	Once
Hard Reset sequence progress	ON (Alternate)	ON (Alternate)	½ sec	Continuously
Hard reset sequence ended successfully	ON	OFF	2 sec	Once
Hard reset sequence ended successfully	OFF	ON	2 sec	Once
For Wireless Lock only:	-----	-----	-----	-----
Invalid ZAC entry	OFF	ON	1 sec	Once
ZAC sequence in progress	ON	ON	½ sec	1 sec
ZAC sequence successful	ON	OFF	1 sec	Once
ZAC sequence failed	OFF	ON	1 sec	Once

5 Programming and Auditing Locks

All E-Plex Wireless Locks & System related info are highlighted in this turquoise color background for easy reference.

A PC based Maintenance Unit called the “M-Unit” - either the same laptop PC where the Enterprise & PC M-Unit software is installed, or a separate independent mini laptop / Netbook PC is used as a portable device, The main two functions of the portable M-Unit are:

- to send (upload) data to for the purpose of programming a lock, and
- to receive (download) data from the lock for the purpose of auditing the lock’s events.

The data transfer between the portable M-Unit and the E-Plex lock is via the industry standard IrDa interface, working in conjunction with **Kaba’s E-Plex PC M-Unit Communications Kit**.

M-Unit User Definition

- In addition to the global Master user, specific Door Group Managers and the other Manager users, there can be M-Unit user types who can also program and audit the E-Plex Enterprise software based locks using the M-Unit. This M-Unit user’s credential is used only to program and/or audit the lock as a maintenance function only, ie. the M-Unit credential will NOT open the lock. When an M-Unit User presents her/his M-Unit credential, the lock enters the Communications Mode with the M-Unit handheld immediately (equivalent to entering the command sequence: # Master credential #, or # Manager’s credential #, followed by 900#), indicated by alternate green and red flashing LEDs. Now the M-Unit User can program or audit the lock.

Important: *Ensure that the current date and time on your system PC and your portable M-Unit are accurate, including the Daylight Saving Time setup. If the date and time are not correct, your users will not be able to access the lock even if they have the right credentials.*

[Start]-----

For Wireless:

- to wirelessly “join” E-Plex (ZigBee) wireless network and perform a ZAC (ZigBee Access Code) operation, which also automatically programs the lock wirelessly, and
- to perform general lock Maintenance functions wirelessly such as (re)program, audit, set date/time, page a lock, remote unlock, remote passage, Emergency Lockdown, Emergency Passage (evacuation), take a lock off the wireless network (put out of service) etc.

Note 1: If you have only the E-Plex wireless locks in your facility, you do not need to use the portable PC M-Unit at the lock to program/audit or perform a diagnostics of the lock(s). All these functions can be easily executed by remote wireless commands from the Host PC itself. However, if the wireless communications between the lock and the Gateway and Host PC is lost for some reason for a long period, you can do these functions using the PC M-Unit.

Note 2: Please skip the next few PC M-Unit related pages and jump directly to the end of this Chapter on how to ZAC a wireless lock and then wirelessly program, audit, perform Emergency remote operations etc on the lock.

[End]-----

Portable PC M-Unit with Kaba's IrDA Kit

The "M-Unit" is Kaba Access Control system's term for a PC based portable unit that communicates with the locks through industry standard infrared (IrDa) interface by making use of *Kaba' PC M-Unit Communications Kit*. The kit contains the following items in the package: **Note:** This kit is not required for E-Plex wireless enabled locks and system].



IrDa Adapter



USB Extension Cable



USB Flash Drive



Netbook PC (as portable M-Unit)

1. An industry standard **IrDA** (*Infrared Data Access*) **adapter** with a **USB** interface to connect to the M-Unit PC,
2. A **USB extension cable** to connect the above IrDA adapter to the M-Unit, if need be, and
3. A **USB flash drive**, preloaded with the *E-Plex PC M-Unit software* application along with its *User Guide* in electronic format,
4. A 2-page "Getting Started" sheet in color as a quick reference guide.

One end of the IrDA adapter plugs in to one of the M-Unit's USB ports and the other end of the IrDa transmit/receive infrared data window will be pointed at the E-Plex lock's IrDa window to transfer required data between the M-Unit and the lock.

The USB memory drive will be used (after installing the PC M-Unit software on the separate Netbook PC) to store and transfer the lock configuration data and the audited events data between the M-Unit and the Host PC where the main E-Plex Enterprise applications its locks/user access configuration database reside. The USB flash drive will be used as a portable transport medium between the two non-networked PCs – i.e., between the Host PC and the portable M-Unit.

Optionally, if your Host PC operates under a networked environment, either by **wired LAN** (Local Area Network) or by **wireless LAN**, you will not need the USB drive to transfer data between the Host and the M-Unit. You can simply make use of the **Host PC's IP address** to transfer data between the two PCs over the network.

Important: Please consult with your local IT personnel on how to setup your Host PC's network IP addressing and related schemes.

Note: If on the other hand, you use the same laptop which contains the main Enterprise applications and the M-Unit applications (built-in), you will not need the flash drive to transfer data; this is because this data transfer and syncing occur within the same laptop's hard-drive.

PC M-Unit Software Installation

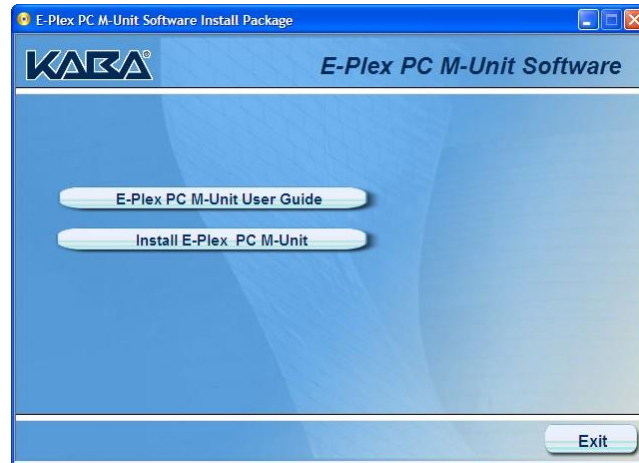
This procedure is for installing the PC M-Unit part of the software on the separate portable Netbook or mini laptop; the Enterprise applications software should have been already installed and running on the Host PC.

Important: If you are using one/same (“integrated”) portable PC where the *E-Plex Enterprise* software was installed, you can skip the next few pages and go directly to the Section on **Page 5-9** -> **Automatic PC/M-Unit Sync**. This is because the *E-Plex PC M-Unit* part of the software already resides within the main Enterprise software and so no separate PC M-Unit installation is required.

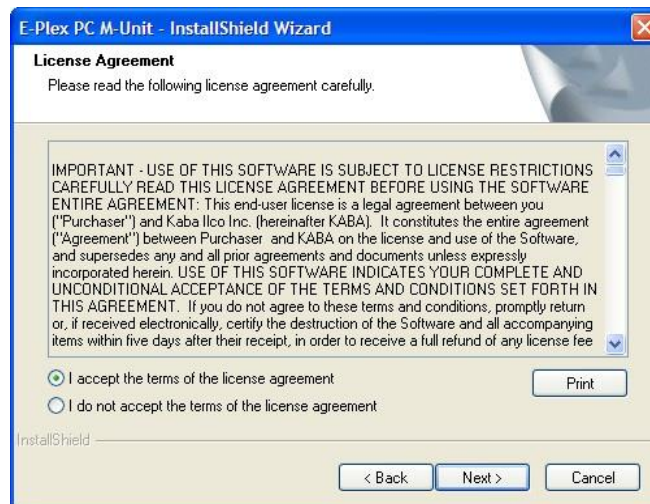
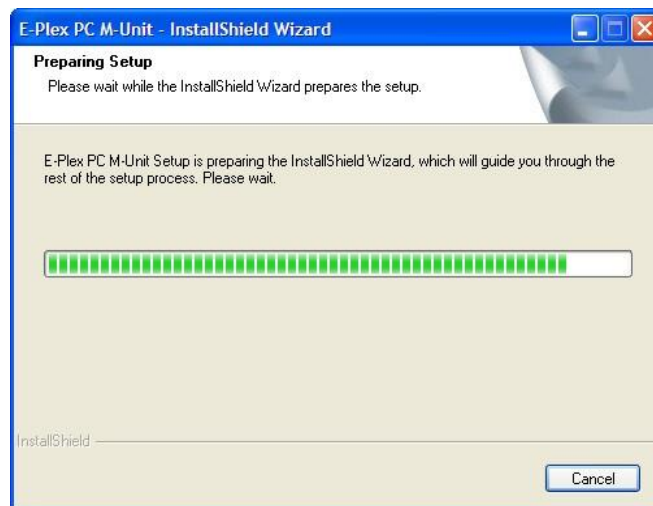
Note: This same PC M-Unit installation procedure can also be found in the **PC M-Unit User Guide**. It is shown here again in this document for convenience. Please also refer to the 2-page color, **E-Plex PC M-Unit Getting Started** sheet as a quick reference guide.

- The *E-Plex PC M-Unit Software* and the *PC M-Unit User Guide* are located on the USB flash drive that comes with *Kaba’s PC M-Unit Communications Kit*.
- Plug in this USB drive into one of the USB ports of your dedicated M-Unit (Laptop or Netbook PC).
- In a few seconds, you will see the following screen on your M-Unit portable unit. Ensure that “*Show Kaba’s E-Plex PC M-Unit Software ...*” is highlighted. Click *OK* to continue which will open the next window, giving you an option to either view/print the *PC M-Unit User Guide* or install this software.

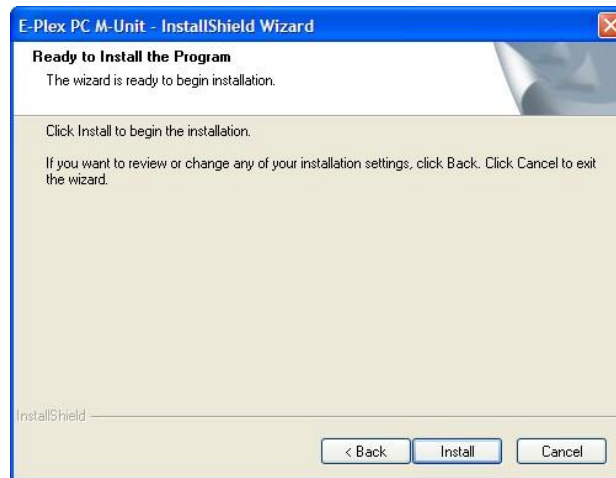
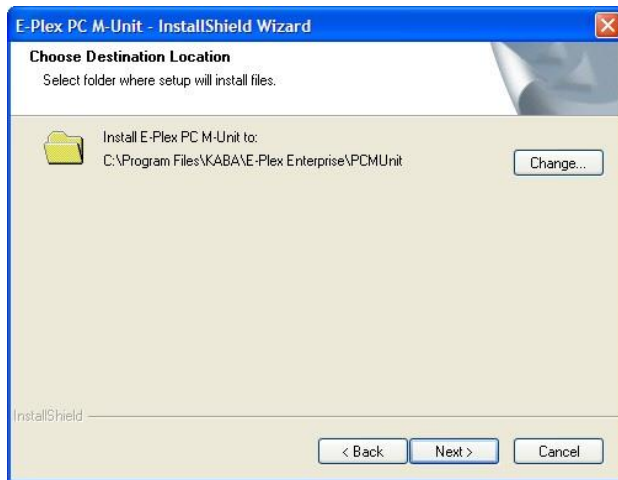
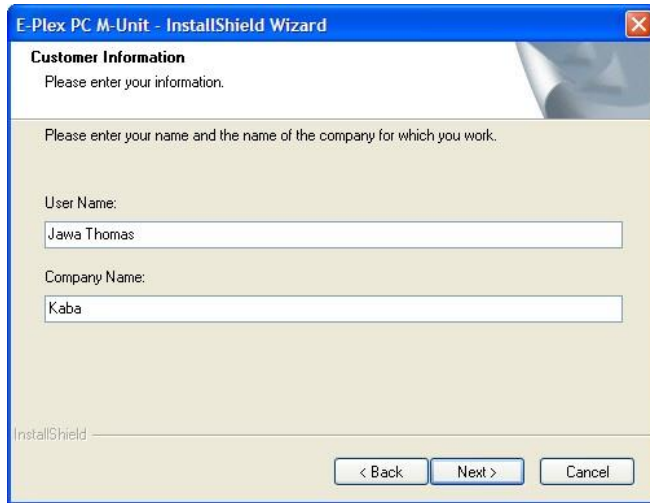


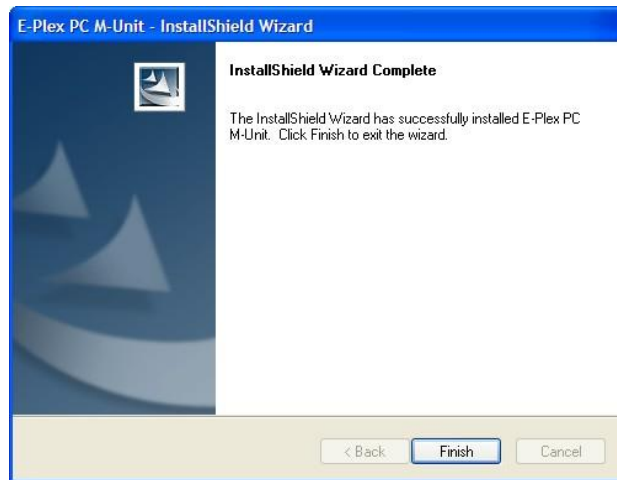


- When you click “*Install E-Plex PC M-Unit*” tab, the software installation process will begin and you need to just follow the instructions on the screen. The following are a few screen shots taken during the install process. Click *Finish* when done.



► Programming and Auditing Locks





- The E-Plex PC M-Unit software is now installed on your separate M-Unit portable unit and the program's icon will be displayed on your PC M-Unit's Desktop as shown below. Whenever you want to run this program, double click on this icon.



- For the very first time of PC M-Unit login, the default login User name is “kaba” and the default Password is also “kaba”. Please refer to the “*E-Plex PC M-Unit User Guide*” for detailed operational use of this program.
- The main operations involving the M-Unit are the following:
 - Downloading doors/users access configuration data to the M-Unit from the Host PC
 - Programming the doors (locks) using the M-Unit via IrDA
 - Auditing the doors (locks) using the M-Unit via IrDA
 - Uploading doors' configuration info and audits to the Host PC from the M-Unit
 - Performing lock maintenance/diagnostics via IrDA

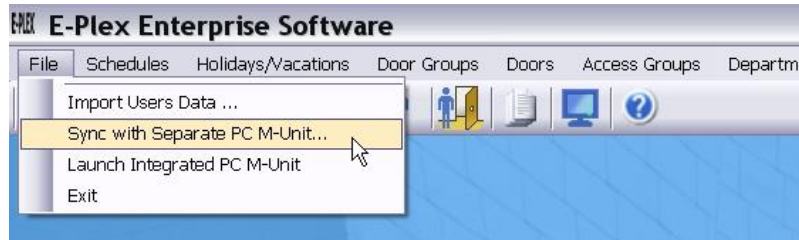
Note: The functionality and features of the E-Plex PC M-Unit software is generic, so it will work with most of Kaba's E-Plex lock models and their related SACs (Stand-Alone Access Controllers) such as:

E3200, E3600, E3700, E5200, E5600, E5700 Series – with E-Plex Enterprise software (this software)
E5800 Series – with E-Plex FIPS (General & High A.) software
E2000, P2000, E3000, E5000 Series – with E-Plex Standard software

Manual PC/M-Unit Sync (Data Transfer with “Separate” PC M-Unit via a USB flash drive)

You must perform the manual data transfer, both from the E-Plex Enterprise Host PC’s side and from the separate portable PC M-Unit’s side as described below. Ensure that both the E-Plex Enterprise and the E-Plex PC M-Unit programs are running on both PCs (Host and M-Unit).

From the main menu of E-Plex Enterprise software, click **File** and then **Sync with Separate PC M-Unit...**



From this point on, please refer to the ***E-Plex PC M-Unit User Guide*** on how to perform the data transfer manually between the two devices via a USB flash drive. The E-Plex PC M-Unit user guide is included as an electronic document on the USB flash drive of the ***E-Plex PC M-Unit kit***.

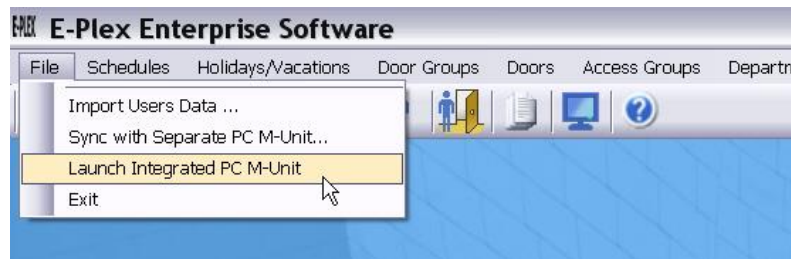
Data Transfer via IP Addressing: The M-Unit data transfer between the Host PC and the PC M-Unit can also be performed via the Host PC’s IP address without having to use the USB flash memory drive. In this case, the data transfer is initiated only from the PC M-Unit side as “Download Doors” (to M-Unit) or as “Upload Audits” (to Host PC). The transferred data will be automatically stored, both in the Host PC’s and the M-Unit’s respective databases; no “initiate data transfer” action is necessary from the Host PC’s side. Please refer to the E-Plex *PC M-Unit User Guide* for more details on how to transfer data between the Host PC and the M-Unit via the IP Addressing scheme. You must have either wired or wireless network connection for the Enterprise Host PC and the M-Unit for this IP address based data transfer to function.

Note: If on the other hand you use one/same standalone laptop PC as one “integrated” PC to run both the E-Plex Enterprise application and the PC M-Unit application, go to the next section -> ***Automatic PC/M-Unit Sync***.

Automatic PC/M-Unit Sync (Data Transfer within the same “Integrated” Laptop PC which acts as both Host PC & PC M-Unit)

If you use one/same standalone laptop PC to run both the E-Plex Enterprise software as a Host PC and the PC M-Unit software (as a portable PC M-Unit), the system automatically does the data sync transfer without you having to specify and use a common folder location on the hard drive, or on the USB flash drive like you do with “Manual” data sync transfer on a separate Netbook PC; also, no network connection is required. You will still need to connect and use the IrDA interface adapter with this laptop PC when programming and/or auditing an E-Plex lock. In this case, this same “integrated” laptop PC functions both as the Host PC running the E-Plex Enterprise software and as the portable PC M-Unit running the PC M-Unit software within.

From the main menu of *E-Plex Enterprise software*, click **File** and then **Launch Integrated PC M-Unit** to open the main *PC M-Unit software* screen.

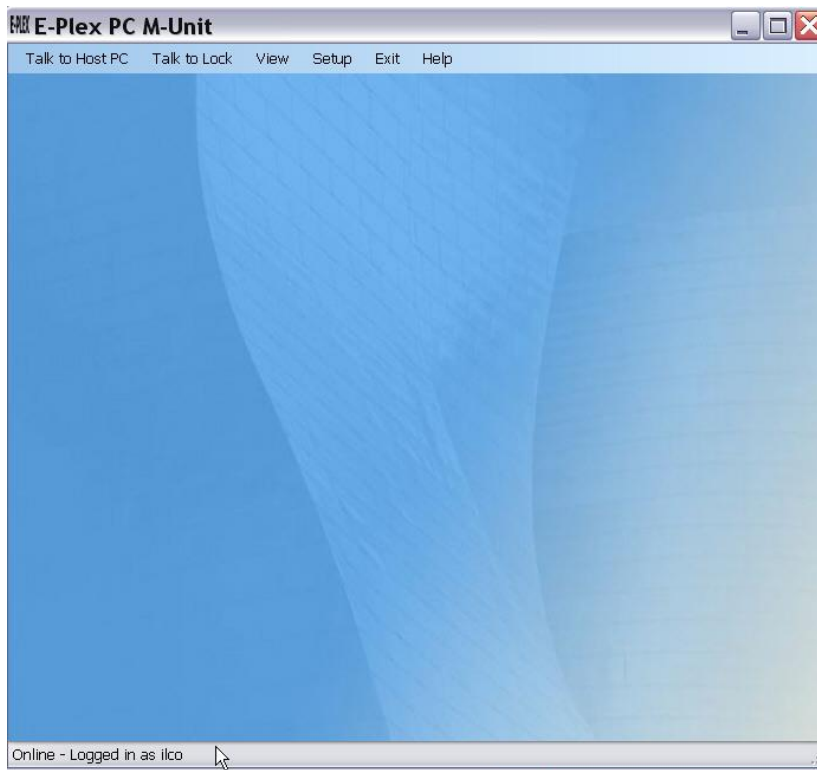


From this PC M-Unit menu you can,

- (i) download users <-> locks access configuration data for each selected E-Plex lock from the Host PC,
- (ii) so as to program these locks,
- (iii) audit each lock for event transactions,
- (iv) then upload the audited info back to the Host PC to view/print them under the Enterprise Reports menu, and/or
- (v) perform lock diagnostics.

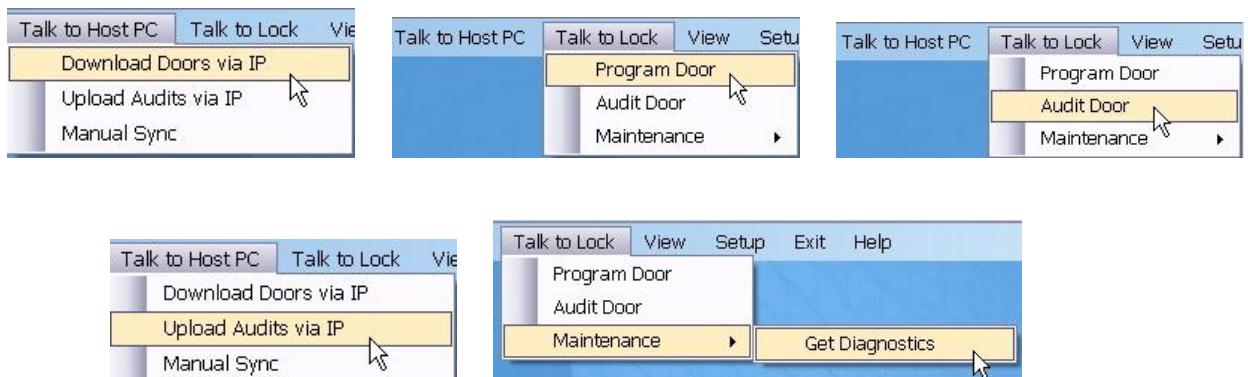
Note: Whenever you need to “talk” (communicate) to the E-Plex lock, you must use Kaba’s IrDA communications (PC M-Unit) kit -> the IrDA dongle and its cable.

► *Programming and Auditing Locks*



From this point on, please refer to the ***E-Plex PC M-Unit User Guide*** on how to perform the data transfer to perform the above tasks in more details. The E-Plex PC M-Unit user guide is included as an electronic document on the USB flash drive of the ***E-Plex PC M-Unit kit***.

The following are a few sample screens showing the PC M-Unit sub-menus from where you will launch the above five -> (i) through (v) tasks.



Wireless Data Transfer between Host PC & Locks via Gateway (&Routers)

[Start]

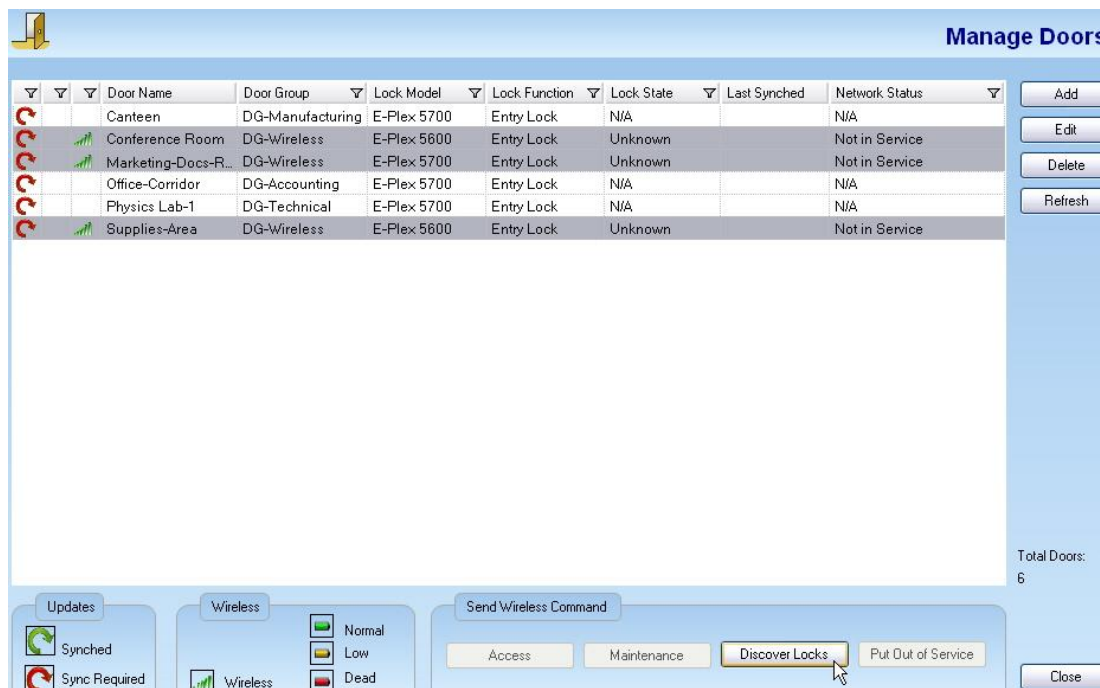
1. Commissioning of a Wireless Lock:

The process of commissioning a new wireless enabled lock for operation is done by following a 2-step process which includes the following sequence:

- join the lock wirelessly to the E-Plex Gateway via the ZigBee wireless network,
- physically go to the lock and ZAC it by entering its unique 8-digit ZAC number at its keypad, and
- program the lock wirelessly.

Once this process is completed, the wireless lock becomes fully functional and can be controlled remotely by the Enterprise software system operator from the Host PC. :

From the *Manage Doors* menu, first highlight and select your wireless lock(s) and then click *Discover & ZAC* tab button at the bottom of the menu screen.



Step 1: As shown in “Step 1” of the *Discovery Mode* screen menu, highlight and select your wireless Gateway (“Company-Gateway”, in this example) and click “*Send Join On Command...*” tab button to initiate the network “join on” of this E-Plex Gateway to any of your selected wireless lock(s); you will select your wireless locks to be joined in *Step 2*. This process may take between a few seconds to a few minutes to complete, depending on your environment. On successful completion of the “join on” process, the system will automatically send a “join off” command to the Gateway. You may also select the timeout duration for the “join off” command to take effect -> 10 minutes through 2 hours so that the Gateway does not unnecessary stay in a long “join on” mode if the lock(s) did not join the network for any reason.

Note: Optionally, you may also perform this same “join on” command from the *Network Map* menu screen by highlighting and selecting this Gateway, right clicking on it and then clicking “Send Join On”. In either case of initiating the “join on” command, the Gateway icon should turn green (from blue) as shown below to indicate that it is ready to communicate.

► *Programming and Auditing Locks*

Discovery Mode

Info
Select the gateway that you want to put in Discovery Mode [Put the Gateways and all the routers in its Network in Join On mode]. Once in Discovery mode you will be able to go at each door location and enter its associated ZAC number.
Please perform Step 1 from the software and Step 2 from the lock.

Step 1: Put a Gateway in Join On mode.

The following list shows the available Gateways in the system. You can have **ONLY ONE Gateway** at a time in the **discovery mode (Join On Mode)**. Choose the gateway that is physically closest to the selected door(s) in the Door list below.

Gateway Name	Status	Network Status
Company-Gateway	Online	Network Down R...

Exit Zigbee Network after all doors are in service (are part of the Gateway's Network).
 If not all Doors Joined then automatically send the Join Off command after...

10 minutes (Default)
 20 minutes
 1 hour
 2 hours

Send Join On Command to the Selected Gateway

Step 2: Enter the ZAC in the Door

Door Name	Zigbee Access Code
Conference Room	96 28 45 74
Marketing-Docs-Room	53 73 07 68
Supplies-Area	03 48 28 19

The following list shows the **ZAC numbers** that must be entered for each selected doors once the **Send Join On** command is sent.

To enter ZAC in the Door:
088 # [ZAC]

Note: the lock must be in factory default with new master user already set.

Network Map

Gateways
Company-Gateway

Step 2: Then as shown in “Step 2” of the *Discovery Mode* screen, highlight and select your wireless lock or locks (“Conference Room”, in this example) that will join the wireless network after a ZAC command is performed at its lock keypad..

Step 2: Enter the ZAC in the Door

Door Name	Zigbee Access Code
Conference Room	96 28 45 74
Marketing-Docs-Room	53 73 07 68
Supplies-Area	03 48 28 19

The following list shows the **ZAC numbers** that must be entered for each selected doors once the **Send Join On** command is sent.

To enter ZAC in the Door:
088 # [ZAC]

Note: the lock must be in factory default with new master user already set.

Wireless

ZAC: 96 28 45 74

Lock State: []

Network Status: []

Battery Level: [] Last Communication: unavailable

Allow wireless remote unlock.

The lock must be at factory default state with default factory Master PIN set as 12345678 for the ZAC command to work.

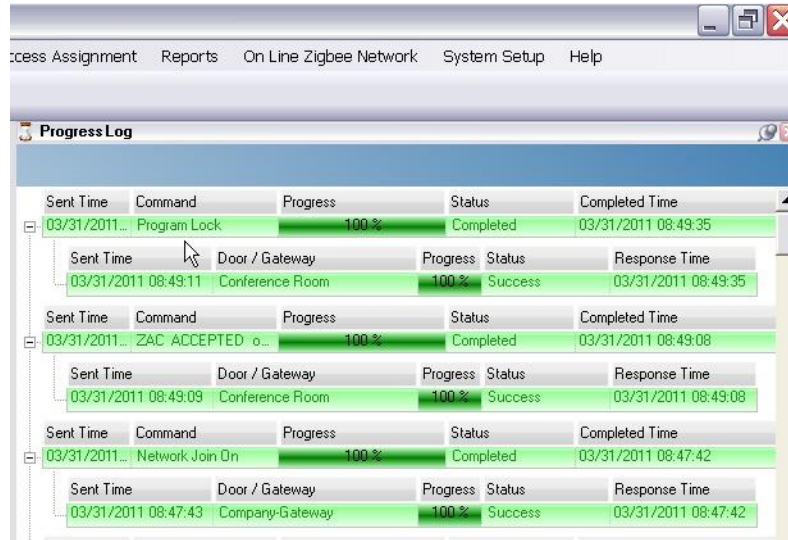
The lock keypad command sequence to “ZAC” a wireless lock at its keypad is:

088# [enter the 8-digit ZAC for this lock]
 For the above example, enter: ## 088 # 96 28 45 74 #

To ZAC a lock, somebody else (your colleague) must be physically present at this door location and enter the above ZAC command sequence at the lock. The lock will flash both the Red and the Green LEDs simultaneously every second for a few seconds. It will end with one last flash of the Green only LED with high pitched tone of its internal buzzer, indicating that it has successfully joined the E-Plex (ZigBee) wireless network. (It will end with Red light / low pitched buzzer tone, if ZAC'ing was unsuccessful).

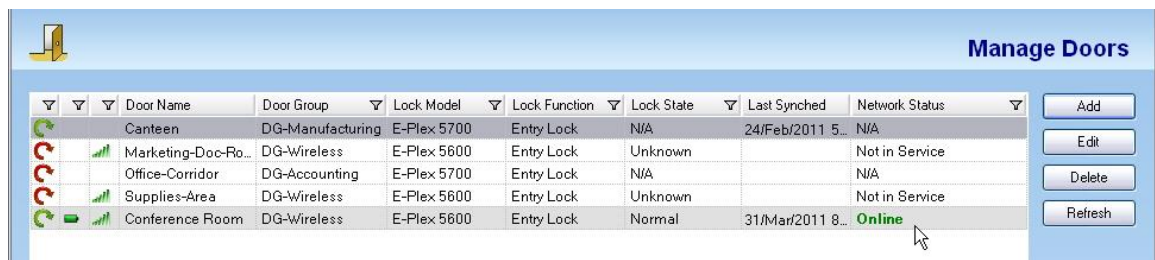
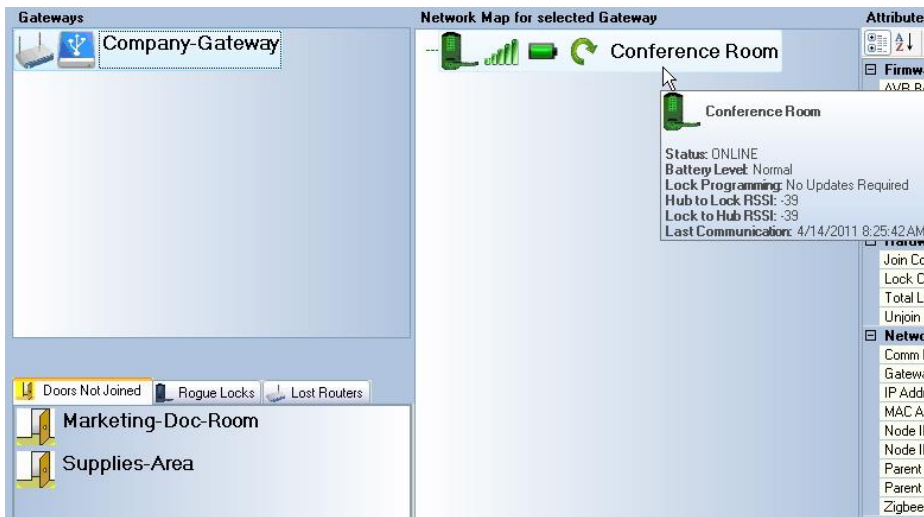
Right after this, the Host PC will wirelessly (remotely) program this lock by downloading to this lock the lock <-> users access rights data. **Note:** This last process may take from a few seconds to a couple of minutes and so you must wait till it is done before the lock is ready for normal use. It will grant access to users with valid credentials, plus the Enterprise system operator from the Host PC or any Client (if networked) PCs can control the lock wirelessly such as re-programming, auditing, temporarily unlocking, activating/deactivating passage, sending Emergency lockdown or Emergency passage commands etc.

- The following screen shows the successful completion of the above sequence under the *Progress Log* part of the screen -> network join, ZAC and programming of the lock wirelessly.

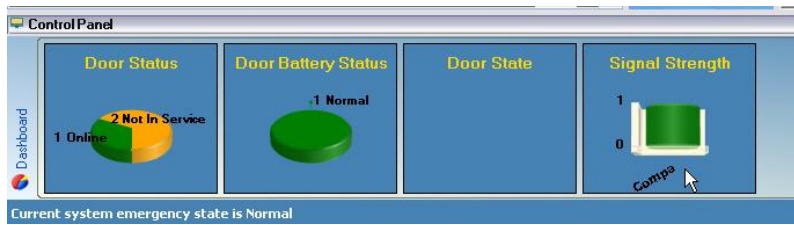


The following are a few example screen shots showing various commands that can be given wirelessly from the Host PC station to the lock, and the consequent status info from the lock, back to the Host PC. All this ZigBee wireless communication is via the E-Plex Gateway (and the Routers, if installed):

- The “Conference Room” lock belonging to the E-Plex Gateway called the “Company Gateway” is wirelessly online now with very good RF signal strength (between -20dB and -80dB). It also shows the other two wireless locks in the system, but are not yet joined online (not in service yet):

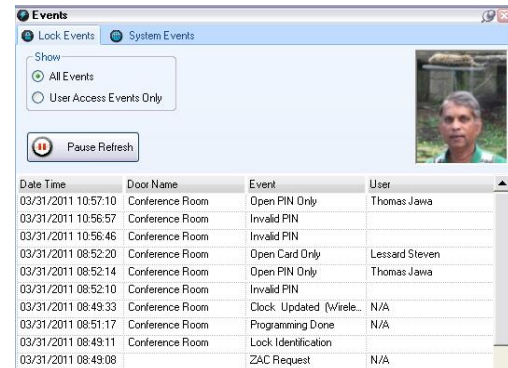


► *Programming and Auditing Locks*

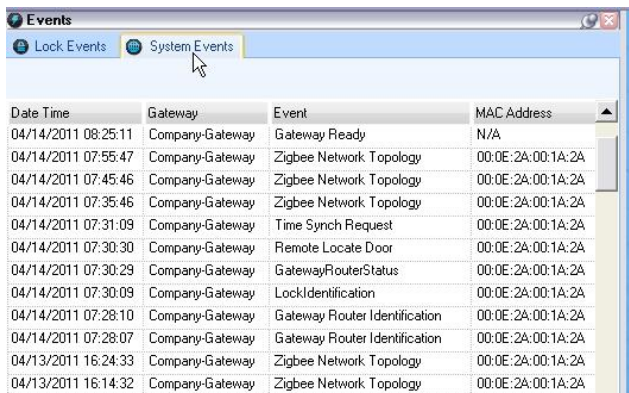


2. Remote Control & Maintenance of a Wireless Lock:

- The “Lock Events” of *Events* part of the screen shows the audited events that occurred at the lock such as user access, passage, remote unlock etc which are shown in real time:



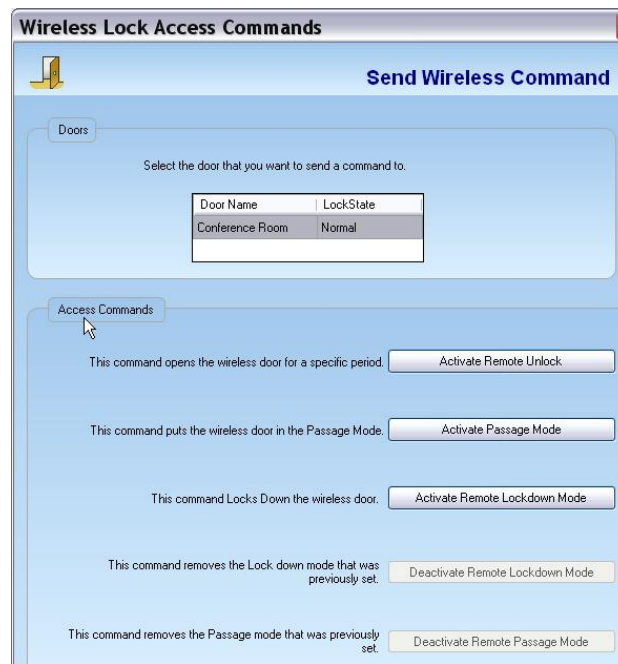
- The “System Events” of the *Events* part of the screen shows the Gateway, Router, network etc related system level events.



- This screen shows the (wireless Commands sent & the received Status) *Progress Log* info:

Sent Time	Command	Progress	Status	Completed Time										
03/31/2011...	Get Lock Status	100 %	Completed	03/31/2011 11:32:42										
<table border="1"> <thead> <tr> <th>Sent Time</th> <th>Door / Gateway</th> <th>Progress</th> <th>Status</th> <th>Response Time</th> </tr> </thead> <tbody> <tr> <td>03/31/2011 11:32:41</td> <td>Conference Room</td> <td>100 %</td> <td>Success</td> <td>03/31/2011 11:32:42</td> </tr> </tbody> </table>					Sent Time	Door / Gateway	Progress	Status	Response Time	03/31/2011 11:32:41	Conference Room	100 %	Success	03/31/2011 11:32:42
Sent Time	Door / Gateway	Progress	Status	Response Time										
03/31/2011 11:32:41	Conference Room	100 %	Success	03/31/2011 11:32:42										
03/31/2011...	Audit Lock	100 %	Completed	03/31/2011 11:30:29										
<table border="1"> <thead> <tr> <th>Sent Time</th> <th>Door / Gateway</th> <th>Progress</th> <th>Status</th> <th>Response Time</th> </tr> </thead> <tbody> <tr> <td>03/31/2011 11:30:09</td> <td>Conference Room</td> <td>0 %</td> <td>Success</td> <td>03/31/2011 11:30:29</td> </tr> </tbody> </table>					Sent Time	Door / Gateway	Progress	Status	Response Time	03/31/2011 11:30:09	Conference Room	0 %	Success	03/31/2011 11:30:29
Sent Time	Door / Gateway	Progress	Status	Response Time										
03/31/2011 11:30:09	Conference Room	0 %	Success	03/31/2011 11:30:29										
03/31/2011...	Remote Cancel Passage...	100 %	Completed	03/31/2011 11:27:28										
<table border="1"> <thead> <tr> <th>Sent Time</th> <th>Door / Gateway</th> <th>Progress</th> <th>Status</th> <th>Response Time</th> </tr> </thead> <tbody> <tr> <td>03/31/2011 11:27:29</td> <td>Conference Room</td> <td>100 %</td> <td>Success</td> <td>03/31/2011 11:27:28</td> </tr> </tbody> </table>					Sent Time	Door / Gateway	Progress	Status	Response Time	03/31/2011 11:27:29	Conference Room	100 %	Success	03/31/2011 11:27:28
Sent Time	Door / Gateway	Progress	Status	Response Time										
03/31/2011 11:27:29	Conference Room	100 %	Success	03/31/2011 11:27:28										
03/31/2011...	Remote Passage Door	100 %	Completed	03/31/2011 11:22:35										
<table border="1"> <thead> <tr> <th>Sent Time</th> <th>Door / Gateway</th> <th>Progress</th> <th>Status</th> <th>Response Time</th> </tr> </thead> <tbody> <tr> <td>03/31/2011 11:22:33</td> <td>Conference Room</td> <td>100 %</td> <td>Success</td> <td>03/31/2011 11:22:35</td> </tr> </tbody> </table>					Sent Time	Door / Gateway	Progress	Status	Response Time	03/31/2011 11:22:33	Conference Room	100 %	Success	03/31/2011 11:22:35
Sent Time	Door / Gateway	Progress	Status	Response Time										
03/31/2011 11:22:33	Conference Room	100 %	Success	03/31/2011 11:22:35										
03/31/2011...	Remote Door Unlock	100 %	Completed	03/31/2011 11:21:23										

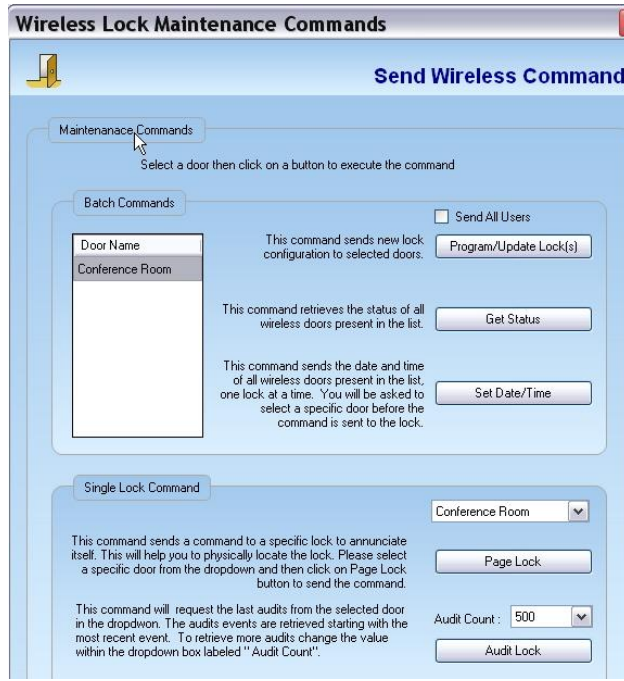
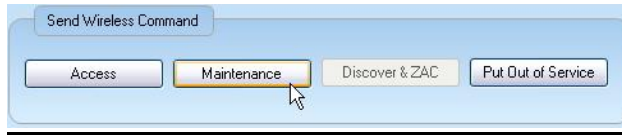
- From *Manage Doors* menu, select your lock and click Access tab to perform various wireless remote access functions on this lock such as -> Remotely Unlock (for temporary access only for each unlock activation), or Activate/Deactivate Passage mode, or Activate lockdown:



- From *Manage Doors* menu, select your lock and click Maintenance tab to perform various wireless remote maintenance functions on this lock such as -> Program lock, or Get Status from lock, Set Date&Time in lock, Page a lock, or download Audit (saves it in Reports automatically):
Note: When you program the lock the first time with a large number of users who should have access to the door, it will send all these users to the lock. If you reprogram the lock with only a few

► *Programming and Auditing Locks*

user access changes (additions and/or deletions), the system will send only this changed info to the lock (“delta”), instead of updating all users again, thus considerably saving the reprogramming time period.



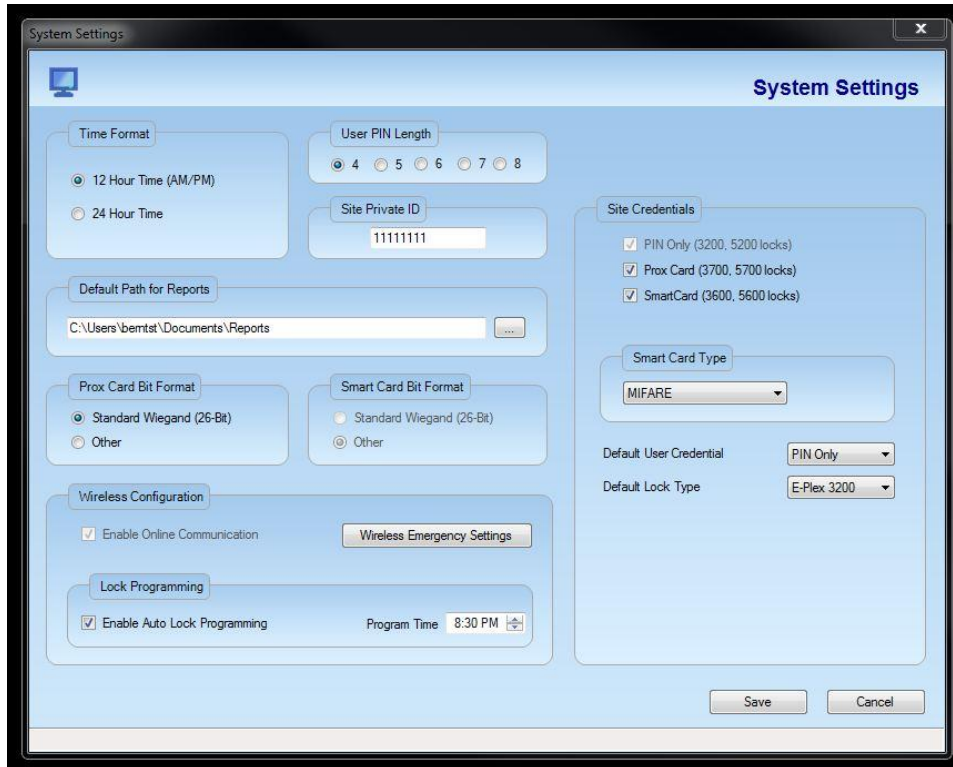
- From *Manage Doors* menu, select your lock and click Put Out of Service tab to take an existing wireless lock from its online to offline wireless status. The only time you will need to do this to a wireless lock or locks is, if there is any service to be performed on this lock(s) or its parent Gateway (and/or Routers).

Important: Once the applicable device is serviced and ready, you must “join on” and re-ZAC the lock to your wireless network so as to put it back in service for normal operations.



3. Scheduled Auto Programming of Wireless Locks:

- After changes have been made to doors in the software, they will need to be wirelessly reprogrammed. To avoid having to program locks manually and the disruption during the day this may cause, a feature that allows you to schedule or defer the programming to another or later time is available under 'System Settings' per below. Under 'Lock Programming', you can 'Enable Auto Lock Programming' and select a more convenient or off-time where the system will automatically reprogram the locks.



4a. Emergency Lockdown & Emergency Passage of Wireless Lock(s):

- The E-Plex Enterprise wireless system supports two major emergency situations on your site where the E-Plex wireless locks are installed ->
 - a system wide global, or by a pre-configured Door Groups based Emergency Lockdown (shut down) of the wireless door locks, and
 - same as above to perform an Emergency Passage (evacuation) mode.

Important: In *System Settings*, you must select and check ahead of time what Door Groups where the locks belong must respond accordingly to the above Emergency commands. You also have an option of checking the "Global" setting box in which case all your wireless door locks on your site will be affected by the Emergency commands.

- From the time you send one of these two Emergency commands from the Enterprise software Dashboard menu tabs to the time the locks go into these emergency states is very quick and is typically under 10 seconds.
- You can do only one of the two Emergency commands (Lockdown or Passage /Evacuation) at a time. After sending an Emergency command, you must always send a

“Normal” mode command for the locks to get back to their previous non-emergency state. Only after getting back to the “normal state” will you be able to send the other Emergency command to the locks.

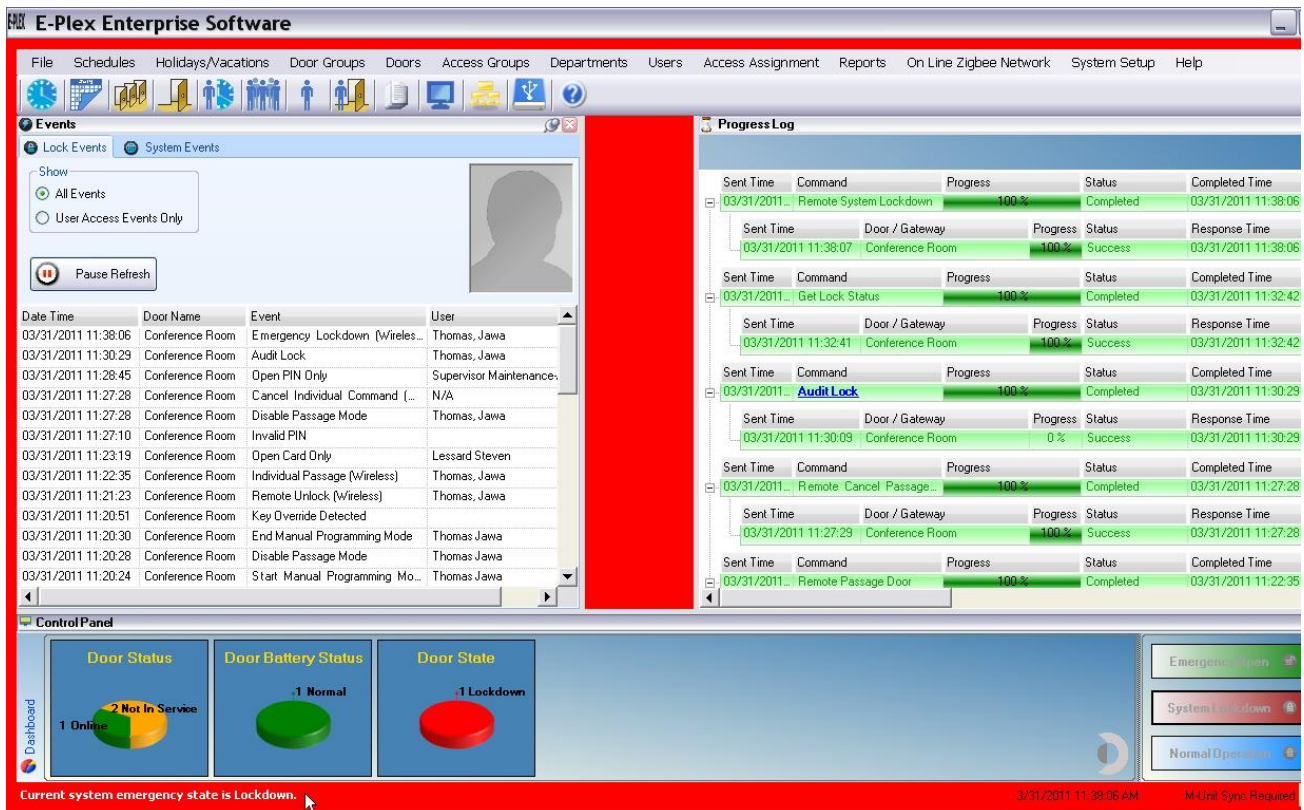
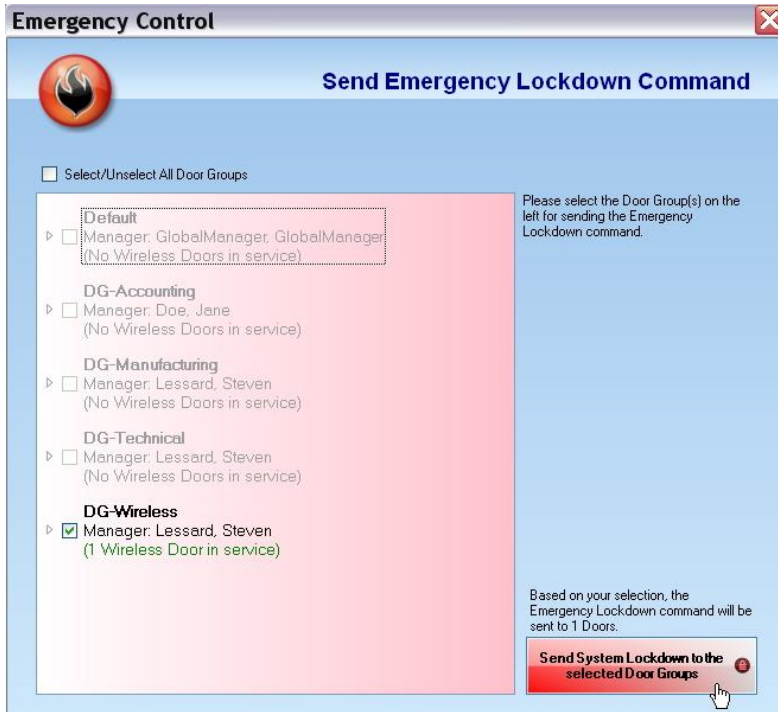
Warning: During an Emergency lockdown/shutdown state, only those users selected under the system settings screen will open the door(s), except for the mechanical override key.

- The following few screens show the operational effects the Emergency commands and are self explanatory:

Send an Emergency Lockdown command to a selected Door Group(s), view the affected door(s) to enter this shutdown state (Red color main menu), send the Normal state command (Blue color main menu), and repeat the above for an Emergency Passage (Green color main menu).



[Emergency Lockdown...]



► Programming and Auditing Locks

[Normal state command...]

Sent Time	Command	Progress	Status	Completed Time
03/31/2011 11:41:25	Remote System Normal	100%	Completed	03/31/2011 11:41:25

[Emergency Passage...]

Emergency Control

Send Emergency Passage Command

Select/Unselect All Door Groups

- Default**
 - Manager: GlobalManager, GlobalManager (No Wireless Doors in service)
- DG-Accounting**
 - Manager: Doe, Jane (No Wireless Doors in service)
- DG-Manufacturing**
 - Manager: Lessard, Steven (No Wireless Doors in service)
- DG-Technical**
 - Manager: Lessard, Steven (No Wireless Doors in service)
- DG-Wireless**
 - Manager: Lessard, Steven (1 Wireless Door in service)

Please select the Door Group(s) on the left for sending the Emergency Passage command.

Based on your selection, the Emergency Passage command will be sent to 1 Doors.

Send Emergency Open to the Selected Door Groups

E-Plex Enterprise Software

File Schedules Holidays/Vacations Door Groups Doors Access Groups Departments Users Access Assignment Reports On Line Zigbee Network System Setup Help

Events

Lock Events System Events

Show: All Events User Access Events Only

Date Time	Door Name	Event	User
03/31/2011 11:45:49	Conference Room	Emergency Passage (Wireless)	Thomas, Jawa
03/31/2011 11:41:25	Conference Room	Cancel Emergency (Wireless)	Thomas, Jawa
03/31/2011 11:39:38	Conference Room	Key Override Detected	
03/31/2011 11:38:06	Conference Room	Emergency Lockdown (Wireless)	Thomas, Jawa
03/31/2011 11:30:29	Conference Room	Audit Lock	Thomas, Jawa
03/31/2011 11:28:45	Conference Room	Open PIN Only	Supervisor Maintenance
03/31/2011 11:27:28	Conference Room	Cancel Individual Command (...)	N/A
03/31/2011 11:27:28	Conference Room	Disable Passage Mode	Thomas, Jawa
03/31/2011 11:27:10	Conference Room	Invalid PIN	
03/31/2011 11:23:19	Conference Room	Open Card Only	Lessard Steven
03/31/2011 11:22:35	Conference Room	Individual Passage (Wireless)	Thomas, Jawa
03/31/2011 11:21:23	Conference Room	Remote Unlock (Wireless)	Thomas, Jawa
03/31/2011 11:20:51	Conference Room	Key Override Detected	

Progress Log

Sent Time	Command	Progress	Status	Completed Time
03/31/2011 11:45:49	Remote System Passage	100%	Completed	03/31/2011 11:45:49
03/31/2011 11:45:50	Door / Gateway Conference Room	100%	Success	03/31/2011 11:45:49
03/31/2011 11:41:25	Remote System Normal	100%	Completed	03/31/2011 11:41:25
03/31/2011 11:41:21	Door / Gateway Conference Room	100%	Success	03/31/2011 11:41:25
03/31/2011 11:38:07	Remote System Lockdown	100%	Completed	03/31/2011 11:38:06
03/31/2011 11:38:07	Door / Gateway Conference Room	100%	Success	03/31/2011 11:38:06
03/31/2011 11:32:42	Get Lock Status	100%	Completed	03/31/2011 11:32:42
03/31/2011 11:32:41	Door / Gateway Conference Room	100%	Success	03/31/2011 11:32:42
03/31/2011 11:30:29	Audit Lock	100%	Completed	03/31/2011 11:30:29

Control Panel

Door Status: 2 Not In Service, 1 Online

Door Battery Status: 1 Normal

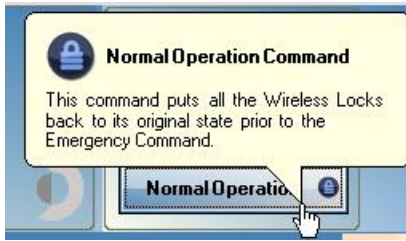
Door State: 1 Passage

Emergency Open System Lockdown Normal Operation

Current system emergency state is Global Passage.

3/31/2011 11:45:49 AM M-Unit Sync Required

[Back to Normal state ...]



4b. Initiating Emergency Commands via a Wireless Lock's Keypad:

- The same Emergency commands above can also be executed directly at a wireless lock's keypad.

Note 1: The emergency commands can be performed by the Master or any other authorized Manager or Access user at any one wireless lock that was already pre-configured in the software to switch to emergency state. This action at one lock's keypad will automatically put all pre-configured wireless locks to switch to emergency state immediately within 10 seconds.

Note 2: The authorized user credential (Manager or Access User) that can perform this Emergency operation at the lock's keypad must have been already programmed into this lock as a valid user.

- The emergency command executions at the wireless lock's keypad are as follows:
 - # authorized Credential # **911** # for **Lockdown**,
 - # authorized Credential # **811** # for **Passage/Evacuation**

Important: During the Emergency lockdown state, only the user levels selected under system settings will open the locks that are in emergency state. In default mode, none of the valid user credentials including the Master's credential will open the door.

Warning: All Emergency Commands can only be set to 'Return to Normal' by a Level 1 or 2 Operator using the Enterprise Software at the Host or Client PC. These commands cannot be 'Returned to Normal' at any lock keypad.

Please refer to Chapter 4, "*Operating the E-Plex Lock at its Keypad*" for more details.

[End]

6

Appendix

Appendix: Software Installation

The Enterprise Version 3.1 Software supports Kaba's E-Plex Wireless system Locks

This section describes the complete software installation process including the software registration and activation process.

Note 1: The software installation procedure described here is for a “**Standalone**” **Express** installation with minimal user interaction. All software modules will be installed on a Standalone single PC where it will automatically install the Server and the Client components of the software and also the PC M-Unit software.

You may also select the “**Network**” **Custom** Install option if you are installing software on separate Server and Client PCs in a networked environment. In this case, you must follow the correct order/sequence of installation which is described in the (Software) “**Installation Procedure**” document shown on the software CD main menu.

Note 2: During the *Standalone / Express* install option, the installation software will also install the *PC M-Unit* program on the same PC. At the end of installation you will have the Server, Client and M-Unit software components, all installed on one PC for convenience.

If you prefer, you can install the PC M-Unit software only, on a separate Windows OS (Home Edition or higher) compliant portable **mini Laptop or Netbook PC**. In any case, when you want to program and/or audit the locks, you must use Kaba's IrDA Communications adapter kit that comes with the *E-Plex PC M-Unit kit*.

Note 3: If your facility contains only the E-Plex wireless enabled lock models, you do not need to use the PC M-Unit for programming and auditing the locks since these functions are done wirelessly from the Host PC software remotely. However, if your E-Plex wireless network is down and you need to program and/or audit the wireless locks, you can use the PC M-Unit to do carry out these functions.

Software Registration and Licensing

Kaba Access Control's E-Plex Enterprise software requires you to register your individually licensed copy of the software with Kaba Access Control in order to use the software. Registering the software will help secure your system database and the locks on your site and will also aid Kaba Access Control in making you aware of any new software upgrades, patches, etc. when required.

On the CD envelope of the E-Plex Enterprise software CD, you will see a sticker with a unique 6-digit *Serial Number* for the software which is part of your unique 10-digit *Site License Number*. Additionally, the second line of the label on the CD jewel case will be titled "*Site Private ID*" with a blank space against it. For easy reference, you can write down this 8-digit software security key (number) that you will be asked to enter when you login to the software system the very first time. This key is used in the system as part of a unique encryption key for your facility and can also be accessed from the "System Setup" menu.

The 10-digit unique Site License number contains your:

- (i) **Serial number** (6 digits, always unique),
- (ii) **Software Type** (1 digit: "1"= Full Featured version, ie., Not a Trial version),
- (iii) **Number of Seats** (2 digits: "25"= Unlimited). and
- (iv) **Software Product** (1 digit: "1" = E-Plex Enterprise).

You will be required to enter the above digits of your Site License number which is printed on the sticker of the software CD envelope. (*Note:* The very last digit "1" for "Software Product" is not required to be entered),

The following are a few examples of End Users' Site License number that you must enter to register the software. Note that only your 6-digit Serial number is unique; you must enter the "Software Type" as always "1" and the "Number of Seats" as always "25", as shown on the software CD envelope sticker.

112233 – 1 – 25

223344 – 1 – 25

334455 – 1 – 25

The registration process is quite simple, and you can register the software in one of two ways:

Register online at Kaba Access Control's software registration website, anytime of the day or night (24/7), or

Register by calling our Technical Support line at 800-849-8324 or 336-735-1331, Monday through Friday between 8:00 AM and 5:00 PM Eastern Standard Time.

Important: *You will not be able to install the software if you do not complete the registration process with Kaba Access Control.*

Software Registration

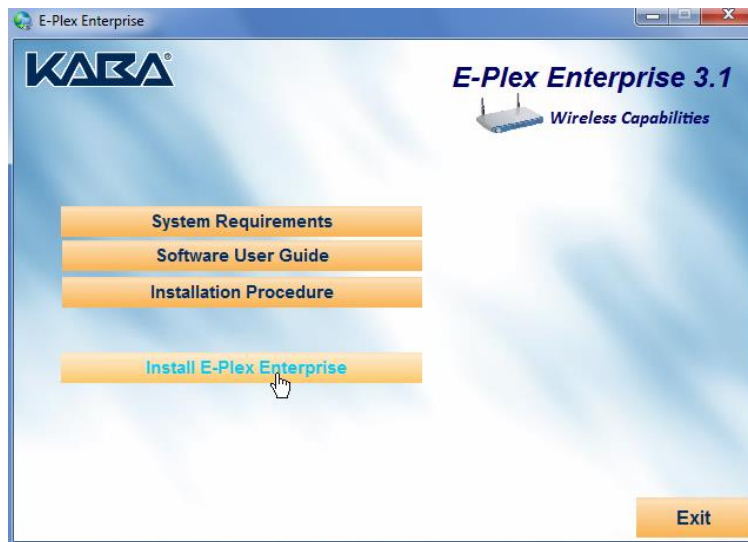
Complete the following steps to register the software:

- Insert the E-Plex Enterprise Installation CD into the appropriate drive of the PC.
- The E-Plex Enterprise Software Installation Browser loads and displays the **E-Plex Enterprise Software** browser menu.

- The **System Requirements, Software User Guide** and the **Installation Procedure** documents are provided on the install CD for your reference. There are two software installation options available: (i) For most cases where everything will be run from one PC, select the **“E-Plex Enterprise for Standalone” (Express) install** option. (ii) If you are going to be using separate Server PC and many different Client PCs in a networked environment, select the **“E-Plex Enterprise for Network” (Custom) install** option.

- ***Important:*** If you selected Network / Custom install option, you must follow the exact sequence of Server and Client parts of the software modules installation in Custom / Network install environment as described in the (Software) **Installation Procedure** document included on the software install CD.
Please consult with your IT department personnel for Network install authorization rules, SQL related info, firewall restrictions etc that apply to your situation. All this must be sorted out before installing the E-Plex Enterprise software for a successful Network install environment.

Note: The software registration process occurs at the very beginning of the installation, both for the Standalone Express install and for the Network Custom install; when doing a Network install, the software registration will be done only on the Server software install phase (and not during Client(s) part of the software install) .



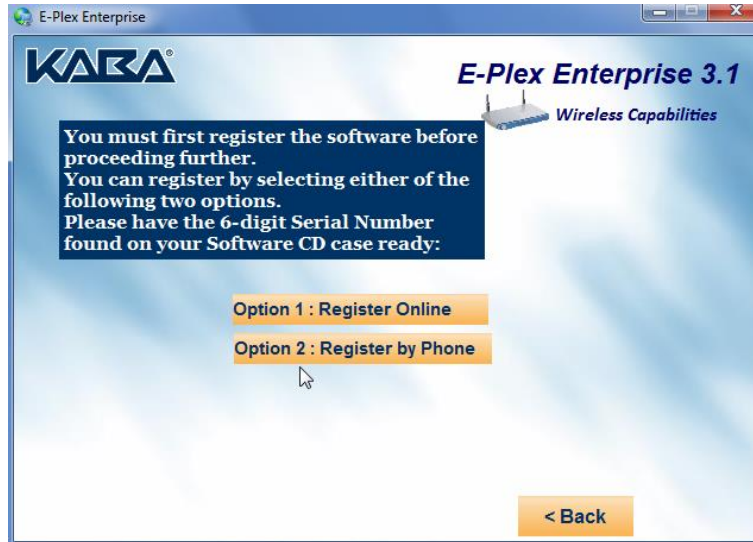
Option 1: Standalone / Express Installation:

- **The software install section here is for the Standalone Express install option, starting with the software registration process.**



Note: You may also have a third option for “Upgrade”. That is, if you already have a previous Enterprise software Version 1.2 or higher installed on your PC, you simply click on the “Upgrade” option. Your current Version software will be automatically upgraded to the new Version 3.1 software which also contains the wireless capability, maintaining your existing database. For further info on upgrading your current software version to the newer software version, please contact Kaba’s Technical Support team.

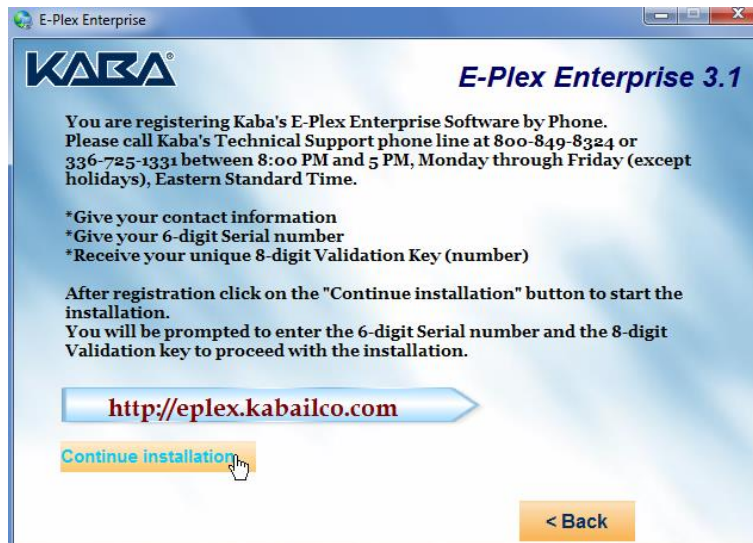
- The system displays the following screen, which prompts you to choose one of the two options to register your software – (i) either through Kaba Access Control's dedicated website, or (ii) by calling Kaba Access Control's Technical Support phone line, as shown below:



If you click **Option1: Register Online**, proceed to the next step. If you click **Option 2: Register by Phone**, proceed to *Page 6-9 “Option 2. Registering by Phone...”*.

(Registration) Option 1: Registering Through Kaba Access Control's Website

- This action assumes that your PC can connect to the Internet. When you select this option, the system displays the following screen directing you to Kaba Access Control's software registration website:



- Click the **Kaba Software Registration Website** link first. The system opens your default Web browser to the **Kaba Access Control Software Registration** page.



- Select the **E-Plex Enterprise** Software Registration option. The system opens the **E-Plex Enterprise Software Registration** page.



Click on **Registering my product for the First time** option.

Note: If you had already registered in the past and want to just retrieve your original registration/activation key from Kaba Access Control, proceed to *Page 6-9*, “**Lost Registration/Activation Key**”.

Registering for the First Time:

- If you are registering your software for the first time, select the first (Green) option. The system displays the **E-Plex Enterprise Software Registration** page.

E-Plex Enterprise Software Registration

Thank you for purchasing our product. To activate your lock, please fill out this form to receive your registration key.

Please note that any information you submit to us will be kept strictly confidential and will not be shared with any other company.

* required fields

CONTACT INFORMATION

Tuesday, June 23, 2009

First Name* <input type="text"/>	Last Name* <input type="text"/>
Company/Organization* <input type="text"/>	Title/Position: <input type="text"/>
Address:* <input type="text"/>	
City:* <input type="text"/>	State/Province:* Select State / Province ▼
Zip/Postal Code: <input type="text"/>	Country:* Select Country ▼
Phone Number:* <input type="text"/>	Fax Number: <input type="text"/>
Email address:* <input type="text"/>	Email address again to confirm:* <input type="text"/>

- Complete the fields of the **Contact Information** area. Fields followed by an asterisk (*) are required.
- Complete the fields of the **Software Registration** area. Your Serial Number, Software Type and the Number of Seats info are located on the sticker on your software CD jewel case. Also, select the E-Plex lock model(s) you will be using this software version.

Purchased from which dealer? <input type="text"/>	Date registered: (mm/dd/yyyy)* select 04/19/2011
-------------------------------------------------------------	------------------------------------------------------------

SOFTWARE REGISTRATION

Select the lock model(s) that will be used with this software:* **Software version:**
 E-Plex Enterprise

EXX00W = E-Plex Wireless Enabled Lock

E5700 E5600 E5200 E3700 E3600 E3200
 E5700W E5600W E5200W E3700W E3600W E3200W

Please enter your 6-digit Serial No. from the Site License No. as printed on your CD/jewel case:

[Site License No. = Serial Number - Type - Seats]

Serial Number:* (6 Digits) 235462	Type: 1 (Full Featured) ▼	Seats: 25 Seats ▼
------------------------------------------------	-------------------------------------	-----------------------------

SITE INFORMATION

How did you first hear about this Kaba product?

- Complete the fields of the **Site Information** area if you choose to provide additional information to Kaba Access Control. A sample of some of the fields is shown below.

SITE INFORMATION

How did you first hear about this Kaba product?

Advertisement
 Web Search
 Kaba Sales Representative
 Security Consultant
 Access Control Dealer
 Door Company/Distributor
 Locksmith Wholesaler
 Locksmith
 Other / specify:

**What type of installation will be utilizing the software?
(check all that apply)**

Commercial Building
 College / University
 School / Educational
 Airport / Port Authority
 Industrial / Manufacturing
 Government / Military
 Hospital / Healthcare
 Other / specify:

Note: Information submitted is kept private and used only by Kaba Access Control for informational purposes.

- When you have completed the registration, click **Submit**.

▶ SUBMIT
▶ CLEAR

Click on "SUBMIT" only once and wait. It may take up to 30 seconds for the system to process and validate your request.

Copyright ©2009 Kaba Ilco Corp.

The system will automatically generate your unique 8-digit **Registration/Activation Key** based on your input:

Your Registration Key: 37200992

Please write down your registration key number and close this page. Follow the software install screen prompts to finalize your installation.

- Complete the registration process by clicking on the tab **Continue Installation** as displayed on the registration screen earlier, shown on *Page 6-6*.

After registration click on the "Continue installation."
You will be prompted to enter the 6-d
Validation key to proceed with the in:

<http://eplex.kabailco.com>

Continue installation

- You will be asked to enter your Serial number again along with your Registration /Activation key you just received to complete the registration and activation of the

software. Proceed to **Continue with Registration** on Page 6-11.

Lost Registration/Activation Key:

- If you had lost your registration key and need it for re-installation of the previously registered software, select the second (Red border) option. The system displays the **Registration/Activation Key Retrieval** screen.



- Type your **Email Address** in the field and click **Send Registration/Activation Key**. You will receive a separate e-mail from Kaba Access Control with your Registration Key.



E-Plex Enterprise Software Registration
Registration / Activation Key Retrieval - CONFIDENTIAL

This is an automated message. Do not reply.

Your Registration / Activation Key: 18057364

- Write your Registration key down and close the window. This number will be used to re-activate your software. On the **Install E-Plex Enterprise Access Control Software** screen, click **Continue Installation** tab on the screen to complete the software registration process.

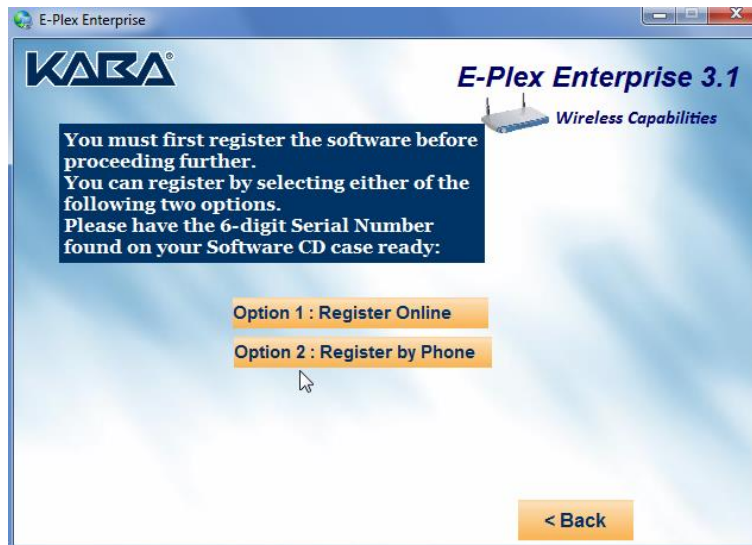


You will be asked to enter your Serial number again along with the Registration / Activation key you received to complete the installation.

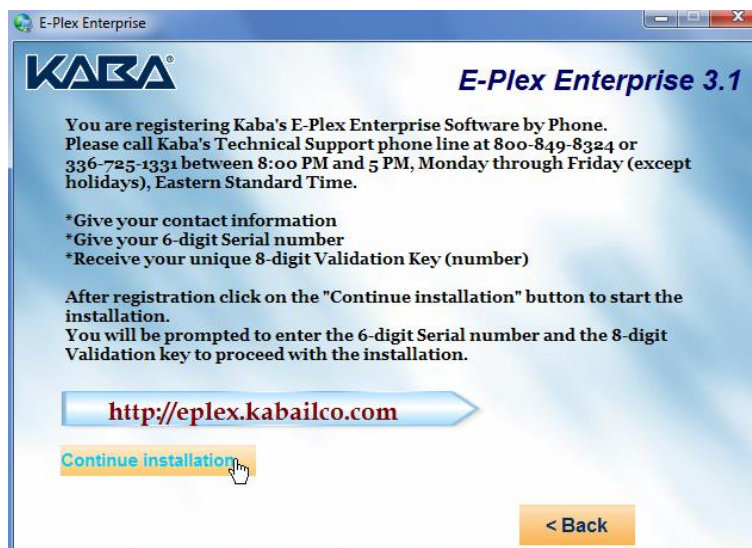
Proceed to **Continue with Registration** on Page 6-11 in this chapter.

(Registration) Option 2: Registering by Phoning Kaba Access Control's Technical Support

- Click to select this option.



- The system displays the following screen.



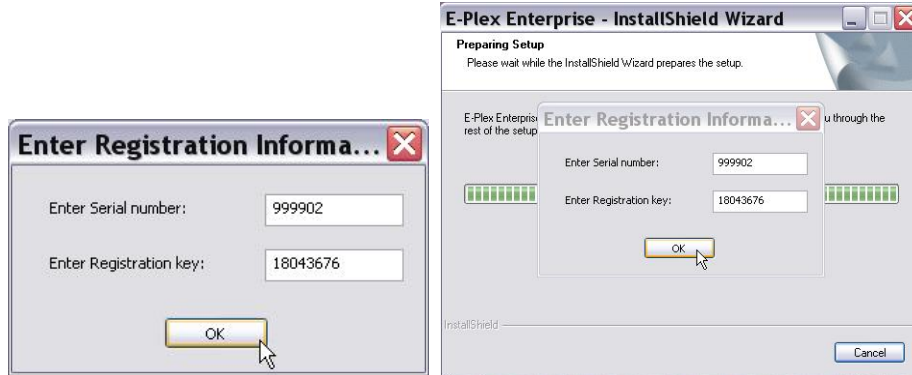
- Follow the instructions on the screen to register by calling Kaba Access Control's Technical Support line.
- Kaba Access Control's Technical Support personnel will first register your contact info, Serial Number, Type of Software info and the Number of Seats info for your software (from your software CD jewel case sticker), and will then give you a unique 8-digit **Registration/Activation Key** for your software over the phone.
- Write your Registration key down and click **Continue Installation** tab at the bottom left of the screen to complete the software registration process.

You will be asked to enter your Serial number again along with your Registration /Activation key you just received to complete the registration and activation of the software. Proceed to *Error! Reference source not found.* below.

Continue with Registration

Complete the following steps to finish registering the E-Plex Enterprise Software.

- Click Continue Installation on the Install E-Plex Enterprise Access Control Software screen.
- The system displays the **Enter Registration Information** screen.



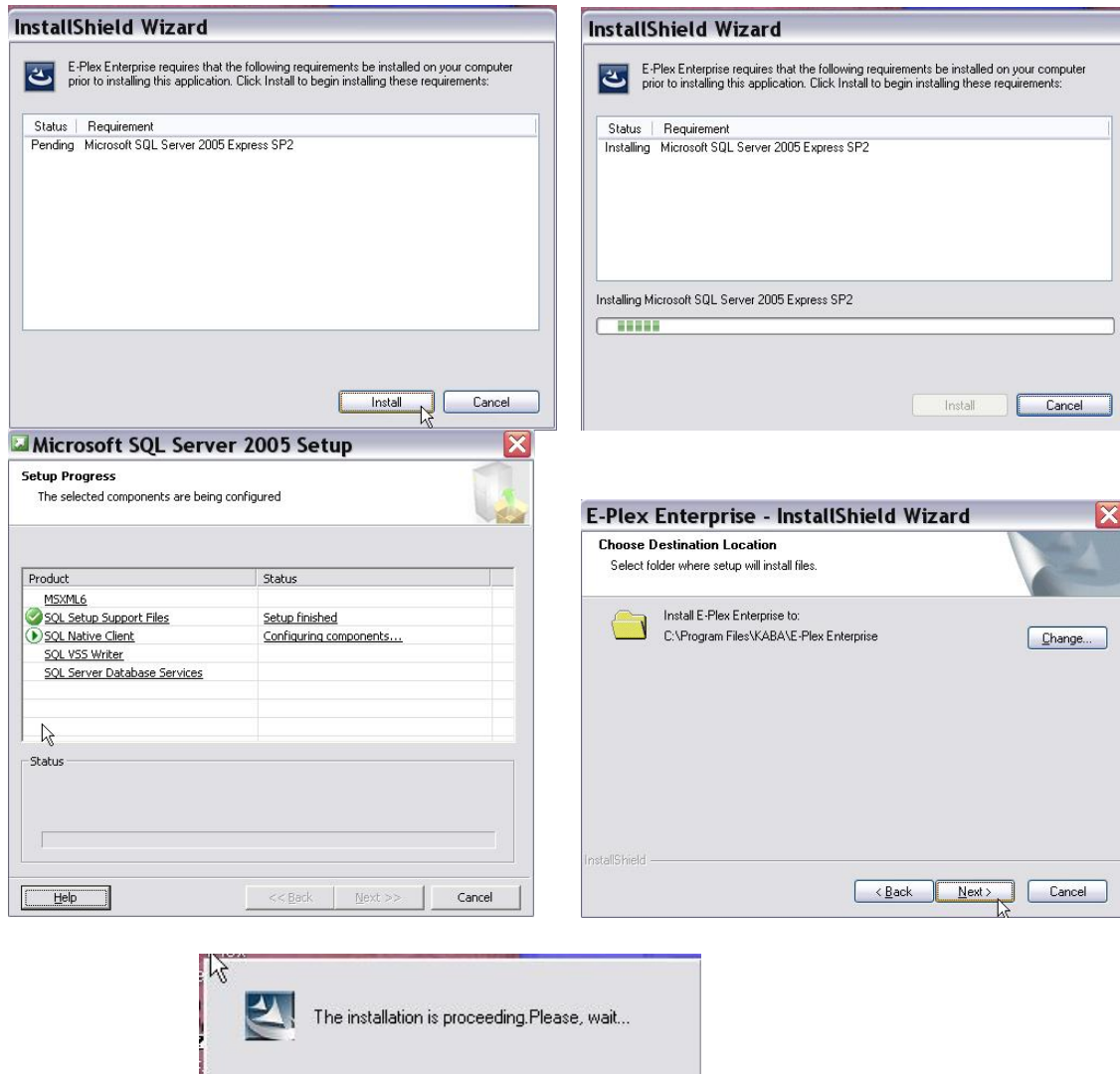
- Complete the **Enter Serial number** and **Enter Registration key** fields.
- Click **OK**. The system congratulates you for successful registration with Kaba.



- Click **OK** and proceed to the rest of the installation of the E-Plex Enterprise software which will be the actual installation of the E-Plex Enterprise Server, Client and PC M-Unit software modules.

(Rest of the) Software Installation

- After the registration of the software, the (Standalone/Express) installation will continue automatically until done. It will install the Server and the Client modules first, followed by the M-Unit software on this same standalone PC.
- The following are a few sample screens of the rest of the software installation:





- You must restart your computer to activate all the installation to take effect.

Option 2: Server/Client Networked Installation:

Important: Please consult with your IT personnel for network installation of the E-Plex Enterprise software involving a dedicated Server PC and other multiple Client PCs.

- Click *E-Plex Enterprise for Network* from the E-Plex Enterprise software CD install screen



2-1: Install Server PC part of Software

- Click *Enterprise Server Software* and follow the screen prompts. **Important:** Consult with your IT personnel for any network server related tweaking that affects your environment.

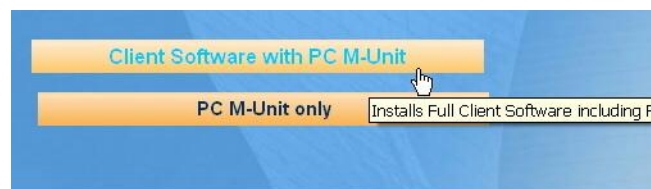


2-2: Install Client PC(s) & M-Unit parts of Software

- After the Server part of the software is installed on the server, you must install the Client part of the software (only) on each one of your Client PCs, one at a time.
- Click *Enterprise Client Software*.



- Click *Client Software with PC M-Unit* and follow the screen prompts.



- Assuming that you installed the Client part of the software in the default path of the Client PC which is, "**C:\Program Files\Kaba\E-Plex Enterprise\Main Client**", go to this directory and open the configuration file "**ACSNetEplex.exe.config**" with the Notepad.
- By default, each E-Plex Enterprise Client PC's configuration file IP address will point to "127.0.0.1" as the remote Host's (Server PC's) IP address. You must edit this text file using a text editor such as "Notepad" and replace this default IP address with the actual Server PC's IP address.
- Replace the default IP address value "127.0.0.1" of "RemoteHostUri" with the actual IP

address value, such as “10.106.15.44” (example IP address only). Save the file and close. Repeat this for each Client PC in your facility.

- The following screen shot shows exactly this IP address value should be replaced in the Client configuration file of each Client PC.

```

<configuration>
  <configSections>
  </configSections>
  <connectionStrings>
  </connectionStrings>
  <system.runtime.remoting>
    <application>
      <lifetime
leaseTime="0"
sponsorshipTimeout="1M"
renewOnCallTime="1M"
leaseManagerPollTime="1M"/>
      <channels>
        <channel type="Belikov.GenuineChannels.GenuineTcp.Genui
MaxQueuedItems="100"
          MaxTimeSpanToReconnect="5000"
          MaxContentSize="50000000"
          MaxTotalSize="50000000"
        />
      </channels>
    </application>
  </system.runtime.remoting>
  <appSettings>
    <add key="RemoteHostUri" value="gtcp://127.0.0.1:8740"/>
    <add key="FIPSReaderName" value="OMNIKEY CardMan 5x21 0"/>
    <!-- OMNIKEY CardMan 5x21 0 OMNIKEY AG Smart Card Reader USB 0-->
  </appSettings>
</configuration>

```

- All parts of the software installation are now complete – whether your software installation was on an Express install on one Standalone PC, or was a Network install on a Server PC and one or more Client PCs.
- You must restart your PCs and after that you should be ready to launch and use the E-Plex Enterprise software by clicking the ***E-Plex Enterprise Client*** icon from your Host PC (Client) desktop.



- Please go back to the Chapter, “2. Getting Started”.
- In this Chapter, resume from the Section, “Quick Start Tips” on Page 2-16.



BEYOND SECURITY

Kaba ADS Americas
2941 Indiana Avenue
Winston-Salem, NC 27105 USA
Tel: (800) 849-8324 (336) 725-1331
Fax: (800) 346-9640 (336) 725-3269

www.kabaaccess.com
www.e-plexlock.com

PKG3288 0313

Disclaimer: While reasonable efforts were made to ensure the accuracy of this document at the time of printing, Kaba assumes no liability for any errors or omissions. This information is subject to be revised without notice, and changes may be incorporated in future releases.