



Security Devices Inc.

omnilock

WWW.OMNIOLOCK.COM



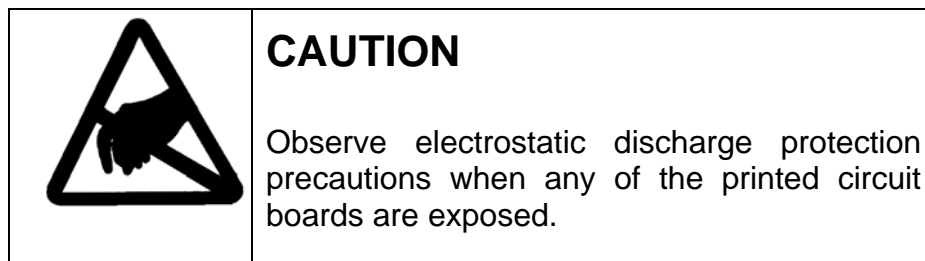
**2000 SERIES
ACCESS CONTROL SYSTEMS
ADMINISTRATOR'S GUIDE**

The information contained in this document is subject to change without notice.

OSI Security Devices makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

OSI Security Devices shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The programs that control **OMNILOCK**[®] products (“Firmware”) are copyrighted and all rights are reserved. Reproduction, adaptation, or translation of those programs is strictly prohibited.



OSI SECURITY DEVICES, INC

1580 Jayken Way
Chula Vista, Ca. 91911-4644
Phone: (619) 628-1000
Fax: (619) 628-1001
E-mail: sales@omnilock.com
Website: <http://www.omnilock.com/>

Copyright ©2004 OSI Security Devices, Inc. All rights reserved.
OMNILOCK is a Registered Trademark of OSI Security Devices, Inc.
SCHLAGE is a Registered Trademark of Ingersoll-Rand Corporation.
ARROW is a Registered Trademark of Assa-Abloy.
FALCON is a trademark of FALCON LOCK CO.
Microsoft, Windows, Windows NT, Windows CE, Windows Pocket PC, ActiveSync, Windows Media and/or other Microsoft products referenced herein are either trademarks or registered trademarks of Microsoft Corporation.
Pentium is a Registered Trademark of Intel Corporation.
All other Trademarks used or referenced in this document are the property of their respective owners.

Table of Contents

- Table of Contents..... i**
- .: Chapter 1 :. Introduction 1**
 - Welcome!..... 1
 - Lock Package Contents..... 1
 - Administrator’s Kit Contents 1
 - Software System Requirements 1
 - Hardware Requirements..... 1
 - Optional Accessories 1
 - Lock Installation and Testing 2
 - Software Installation 2
- .: Chapter 2 :. Overview 3**
 - The Basics..... 3
 - The Lock: OM2000 vs. OP2000 3
 - Daylight Savings Time (DST) 4
 - Passwords and Microsoft Access Compatibility..... 4
 - Facilities, Locations, and Locks 4
 - User IDs and PINs..... 5
 - User Types 6
 - Programmer..... 6
 - Manager 7
 - General Users..... 7
 - Service Users 7
 - Access Levels and PIN Required 7
 - PIN Required 8
 - Unlocked..... 8
 - Unlock with ID..... 8
 - Enrolled ID Required (most common) 8
 - Facility Card Required (Magnetic Cards ONLY)..... 8
 - Lockout..... 9
 - Shutdown..... 9
 - User Groups and Group Access..... 9
 - Home Groups and Associate Groups..... 9
 - Group PIN Re-coding 10
 - Time Schedules and Holidays 10
 - Overview..... 10
 - Master Access Level Schedule..... 10
 - Group Access Level Schedule..... 11
 - Holidays..... 12
 - Credentials 12
 - Codes 12
 - Magnetic Card Features 13
 - Proximity Card Features 14
- .: Chapter 3 :. Programming..... 17**
 - Overview..... 17
 - Installing ActiveSync..... 17
 - Installing the Omnilock Facility Manager and OmniLink 18
 - Setting Up a Facility..... 18
 - Setting Up Groups 19

Table of Contents

Setting Up Users	20
Adding Users	20
Removing Users	21
Changing User Information or Credentials	21
Setting Up Time Schedules	22
Master Schedules	22
Group Schedules	23
Holidays	24
Lock Enrollment	25
Schedule Names	25
Deleting, Modifying, and Using a Schedule as a Template	25
Enrolling the Pocket PC	26
Enrolling Locks in the System	26
Adding Locations	26
Adding Locks	27
The Data Exchange Process	28
Doing a Data Exchange	29
OmniLink	29
Programming the Lock	30
Closing the Omnilock Link Program – A Word About Synchronization	32
Updating Your Facility	32
.: Chapter 4 :. Lock Operation.....	33
Introduction	33
Anti-Tamper	33
Normal Operation	33
Setting Access Levels and Group Access	33
Programmers	33
Managers	35
PIN Required Operation	37
Additional Lock Features	37
Remote Switch Operation	37
Key Detection (Option 1)	37
Chapter 5 :. Reports	39
Reporting Features	39
Audit Reports	39
Introduction	39
Audit Report Criteria	39
Running an Audit Report	40
Lock Reports	40
Introduction	40
Lock Report Criteria	41
Running a Lock Report	41
Users Reports	42
Introduction	42
User Report Criteria	42
Running a User Report	43
.: Chapter 6 :. Tutorial.....	45
Overview	45
Setting Up a Sample Facility	45
First Step, Setting Global Facility Parameters	45
Second Step, Setting Up Groups	46
Third Step, Adding Lock Users to the Database	46

Table of Contents

Notes:

.: Chapter 1 .:

Introduction

Welcome!

Thank you for choosing the OMNILOCK 2000 Series Access Control System for your building access control needs. The OMNILOCK is a sophisticated building access device that is fully self-contained (requiring no wiring), battery-operated, and capable of managing entrance security needs for small and large buildings, facilities, and even the largest LAN and WAN-based facilities. With its rugged housing, robust electronics, and patented low-power motorized locking mechanism, this Access Control System can provide years of maintenance-free service with infrequent battery replacement.

Please check the contents of all packages to ensure that all items are accounted for.

Lock Package Contents

- Keyboard/Electronics Housing (Additional electronics housing with WX units.)
- Lockset (not included with the Wall-Mount System or Quick Adapters)
- Installation Hardware
- Hardware Installation Instructions
- Installation Template
- Warranty/Registration Card

Administrator's Kit Contents

- OMNILOCK Facility Manager **Software Installation Disk**
- 10 Manager programming instruction cards
- Default Programmers ID Cards
- Product Registration Form

Software System Requirements

- Windows 98SE/ME/2000/NT/XP
- Microsoft ActiveSync (Provided with Pocket PC)
- Pentium II (or equivalent)
- 32 MB RAM*
- 24 MB Disk Space*
- Mouse (or other pointing device) and keyboard
- 16-bit color display

* Requirements based on initial installation, and may vary according to database size.

Hardware Requirements

- OSI Approved Windows Pocket PC
- OM/OP2000 Series Lockset

Optional Accessories

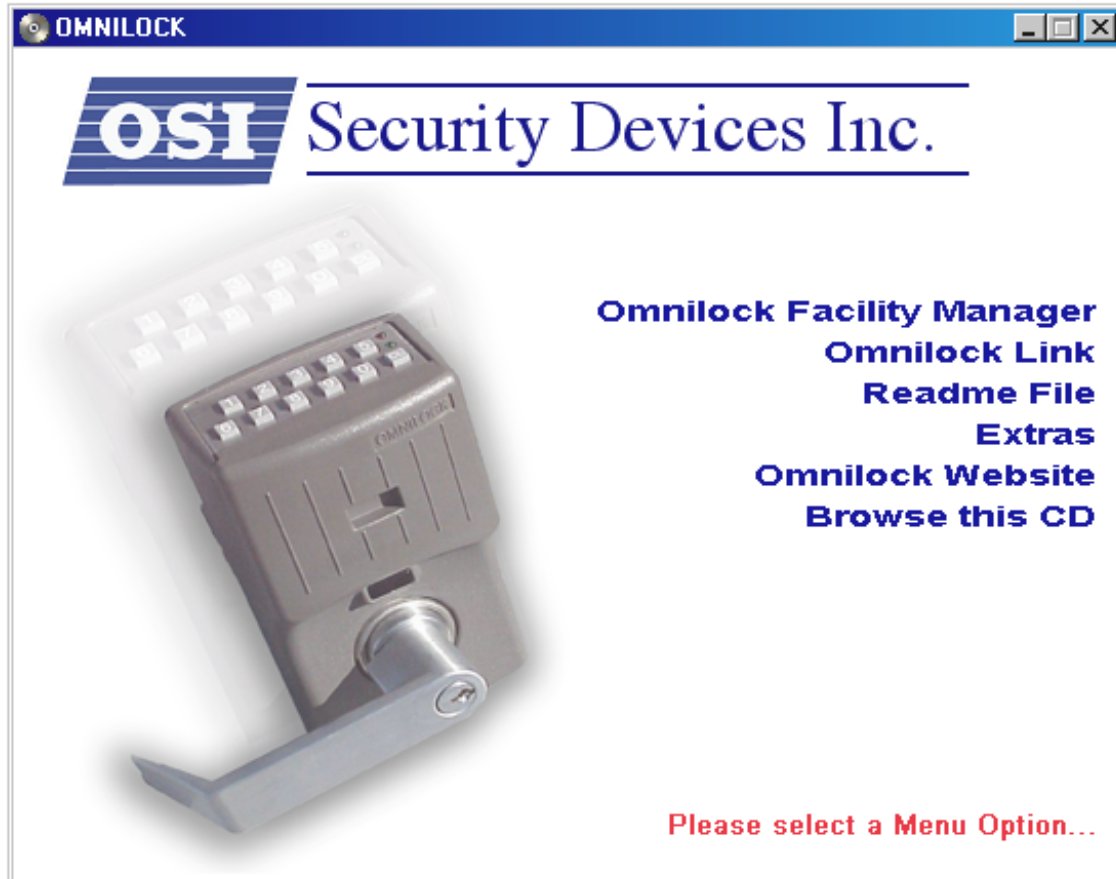
- Track 2 or Track 3 Magnetic Cards (ISO 7810 and 7811)
- Magnetic Card Reader (Requires PS/2 or USB Port)
- HID Compatible Proximity Credentials
- Proximity Enrollment Reader (Requires USB Port)

Lock Installation and Testing

Please refer to the hardware installation instructions included with your OMNILOCK 2000 Series lockset or visit the Technical Support page at <http://www.omnilock.com/>. If you are unable to locate the instructions, feel free to call the support center at (619) 628-1000.

Software Installation

Software installation instructions are included in the packaging of the CD-ROM as well on the CD itself. If the Menu does not automatically start upon CD insertion, simply run Main.exe from the CD-ROM directory. The menu should appear as below:



Please read and follow all software installation instructions included with CD. If you see the menu above, simply select the option you wish to install. If you have trouble installing the software, please contact your IT or IS administrator for assistance.

.: Chapter 2 .: Overview

The Basics

The accompanying OMNIOLOCK Facility Manager (OFM) software allows you to easily configure one or more facilities, each with up to 65,000 locks and 65,000 users. The software allows for each user to use either keypad or identification card for access. It also allows the administrator to design a multitude of access time control plans, define up to 2,000 users per lock, as well as generate reports for each lock and monitor battery condition. Once a facility is set up in the software, all the user information is downloaded to a Pocket PC. It is then transferred to each lock via the infrared port (IR) on your Pocket PC. Each lock keeps a log of all lock activity. This activity includes any entries that are made by users; including the date and time of their entry. It also includes all time schedule events, anti-tampers, and can even keep record of any key bypasses. This log is automatically retrieved every time updates are made to the lock.

The Lock: OM2000 vs. OP2000

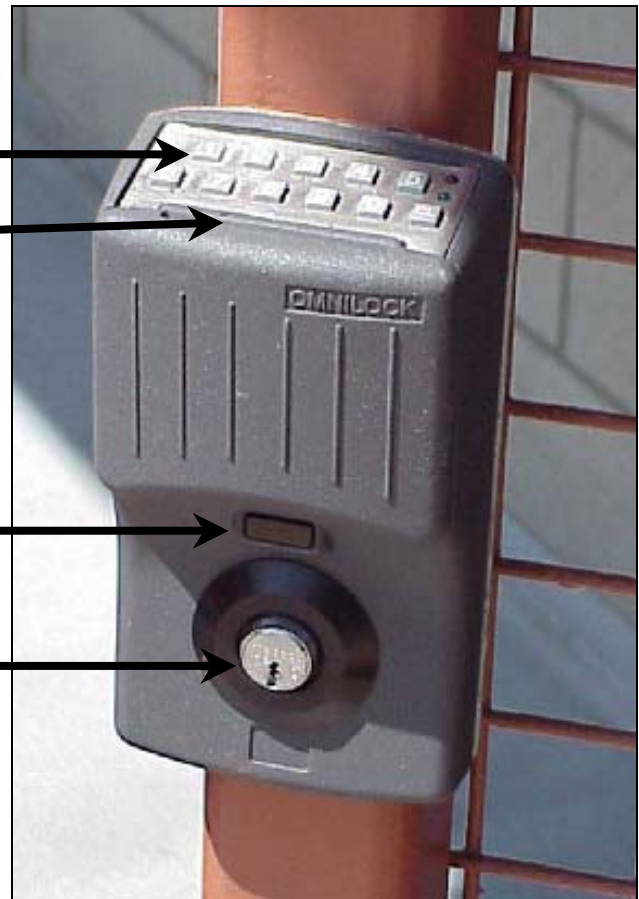
Let's take a look at the lock. OSI currently has two variations of the 2000 Series: Magnetic Card and Proximity. Although, you can order the 2000 without any sort of card reader, most of the time it will be one of the two variations mentioned above. Aside from the basic credential advantages, all variations of the 2000 Series have the exact same feature sets in regards to operation, management and flexibility.

Keypad: Used for entering Code IDs or PINs. Also can be used by Managers to manually set the access level at the lock without the Pocket PC.

Magnetic Card Reader: This small opening is the entry for all Magnetic Cards enrolled in the system. It can be set to read track 2 or Track 3; however, this setting **MUST** be set prior to installation.

Infrared Transceiver: This is portion that the lock uses to communicate with the Pocket PC. You must align the Pocket PC 6-8" from this portion of the lock during programming. Alignment is critical!!

Key Bypass: All of OSI's locks have a key bypass feature in case of lock failure. This particular system uses a key cylinder to cover all wiring. Once removed, the end user can manually connect the wiring for the access point to gain entry.

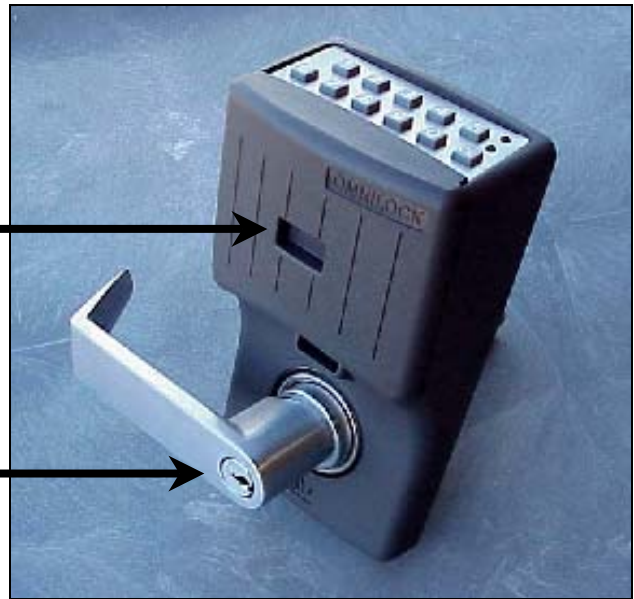


Chapter 2: Overview

The OP2000 is exactly the same as above except for the card reader portion. There is no opening for the Magnetic Card, but rather an indent for the proximity card.

Proximity Card Reader: This small indentation is the center point of the Proximity Antenna assembly built into the lock. It's main purpose is a insert point for Key Fobs, but also acts as a general reference point as to where you should hold your proximity cards when using them.

Key Bypass: In this Cylindrical Lock system, the key cylinder will mechanically open the door, completely bypassing the electronics altogether.



Daylight Savings Time (DST)

Changes in daylight savings time can be configured in the lock so that they occur automatically in accordance with Northern American, Southern hemisphere, or European standards. If these don't meet your needs, you may enter the desired changeover times or have NO time changes take place. Setup or changes to the DST settings can be accomplished on the Facility Properties page.

Passwords and Microsoft Access Compatibility

If you want to secure the database so that only authorized persons can view or modify it, you should set up a password. The use of a password is strongly recommended, particularly if the database is on any computer accessible from a network. Select Facility and then select Password from the menu. A dialog box will appear allowing you to type in a password. Passwords may contain numeric, alpha (case sensitive), or special characters (@, #, \$, etc.) and must be between 6 and 14 characters long.

The OFM utilizes a Microsoft Access database for storing all facility information. This allows for easier portability and usability outside of the OFM application. If changes are made to the database using Microsoft Access, the database could become unusable by the OFM! Nevertheless, Microsoft Access may be useful for advanced users who wish to access and modify the database through external scripting. In general, though, it is not recommended to make ANY changes to the database through Access or other programs without first making a backup of the database. If it is decided that you wish to open the database in Microsoft Access, you may be asked to "convert" or "open" the database. Never select convert, **select only the "open" option.**

CONVERTING THE DATABASE FROM ITS NATIVE FORMAT WITH ACCESS WILL CAUSE IT TO BECOME UNUSABLE BY THE OFM APPLICATION

The Access Compatibility box in the password dialog determines whether you can use the same password for Access as you would for the OFM. Leaving it unchecked will require a different password for Access, thus locking out all novice users from making any modifications to the database through Access.

Facilities, Locations, and Locks

When you first create your facility, the OFM creates a database file in the following location on your hard drive:

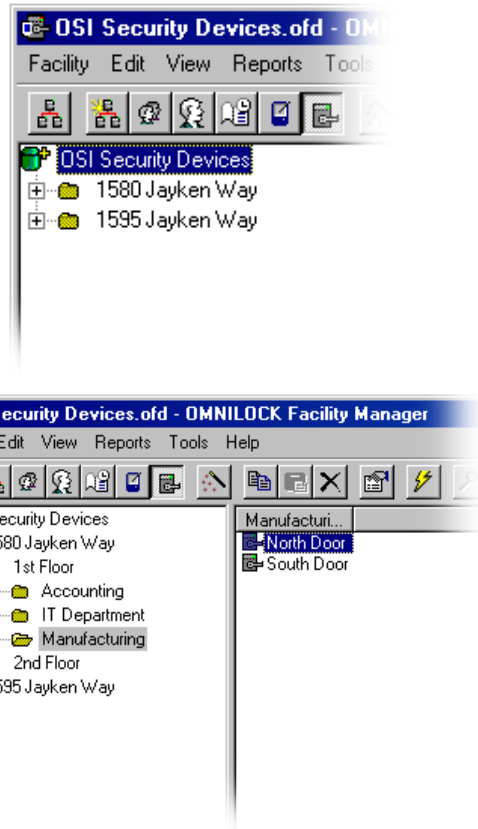
C:\Program Files\OSI Security Devices\OMNILOCK Facility Manager\Facilities

The database will end with file extension of “.ofd.” For example, a facility with a name of “OSI Security Devices” would have a file named “OSI Security Devices.ofd” in the above location. That file is the entire database. It is recommended that you make regular backups of this file in the event of a system crash. There will be no other way to recover your facility without this file.

A Facility can be defined quite liberally, usually somewhere from a single building to a large, contiguous campus of buildings; but in some cases the Facility may be an expansive LAN or WAN-based interstate system. While you are setting up your access control plan, define the Facility in a manner that makes the most sense to you.

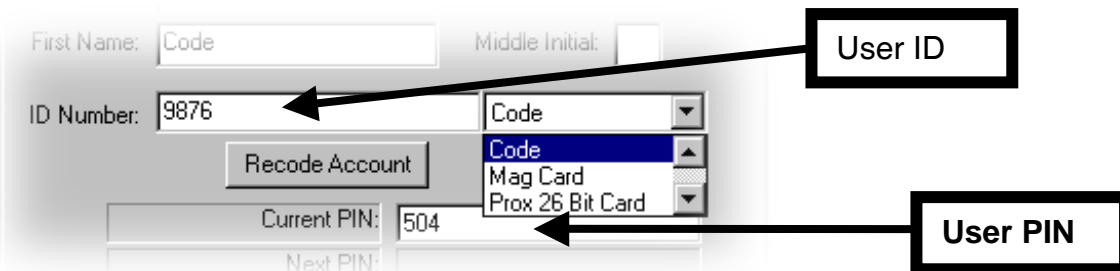
Within a Facility are Locations and Locks. Locations are the segments into which you divide a Facility. Depending on the physical layout of your Facility. Locations can be defined to be anything from a room, a wing, to an entire building. The example to the right displays the building addresses as the Locations.

Locks are just what they appear to be. A lock depicted in the OFM software represents an actual lock that is installed at the Location within the Facility. The left is a lock in the Manufacturing section of 1580 Jayken Way.



User IDs and PINs

A User ID uniquely identifies every system user. No two users will ever have the same User ID. The ID can simply be a code, which is entered into the keypad. Or it can be a magnetic card (i.e. student ID.) The ID can also be an HID compatible proximity credential. Throughout this manual, you will see the words “User ID” mentioned a lot. It is important that you understand the difference between an ID and a PIN.



As an additional security feature, a PIN (Personal Identification Number) can be assigned in addition to each user’s ID. The PIN feature is generally useful in applications where a greater level of security is desired. If cards are used for the ID, the PIN provides an additional level of verification. **Remember, PINs are in ADDITION TO the ID. It is not a substitute credential in place of a card.**

In cases where you would prefer the option to use a card or a code, you must be enrolled twice into the facility: once with a code as an ID, and once with a card as an ID.

User Types

The system supports four different types of users: Programmers, Managers, General Users and Service users. As you know, you can have up to 65,000 individual users in system and they can be of any sort of User Type. More than likely, over 90% of the users enrolled in your database will be General Users. You may not even use Managers or Service IDs. It is almost guaranteed that the majority will be General Users. Each user type is described below:

Programmer

The Programmer ID is the only User type that can program changes into the lock. The Programmer ID is the only type of ID that will initiate the communication between the Pocket PC and the lockset; therefore, each lock must have at least one programmer enrolled in the lockset. We'll get into enrollment and programming much later. Just remember, you must have at least one programmer. One of the nice features about a Programmer is that just because they can program the lock, it doesn't mean they can get through the door. Programmers have certain Restrictions that must be assigned to them during the enrollment process. This allows the administrator to delegate the tasks of walking through the building to someone else without having to compromise the building security.

Programmers have four different restrictions that can be assigned to them:

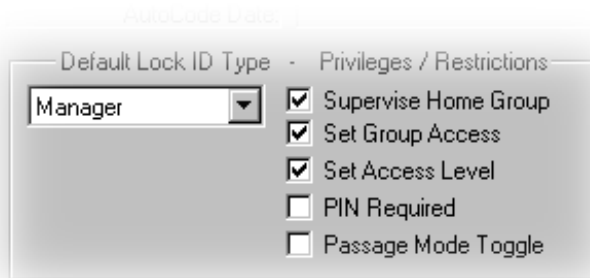
- Entry** – This privilege allows the programmer entry through the lock. Without it, the lock will not unlock.
- Run Diagnostics** – This privilege allows the user to run computer diagnostics at the lock. *This privilege requires that Entry privilege also be assigned.*

- Set Access Level** – This privilege allows the user to set various access levels at the lock by using the Pocket PC as an interface. *This privilege requires Entry and Run Diagnostics privilege also be assigned.*
- PIN Required** – This is an optional restriction to enable extra security. Although rarely used, this feature is beneficial to programmers with cards. In the event the card is lost or stolen, it cannot be used to access the lock since the additional PIN would have to be known as well.

Manager

Managers are one of the most useful types of IDs. Managers may be given the unique capability of changing the access level of the lock with a few simple key presses. It should be noted, however, that any changes that a manager makes to the access level can and will be overridden by the time schedule or another manager or programmer. Another benefit of the Manager is that managers are always allowed access to a lock. For those facilities that require an individual to have access at all hours of the day without giving any extra privileges, Managers can fill that need.

Manager privileges are described in the illustration below.



- Supervise Home Group** – This allows managers to enable or disable only their home group.
- Set Group Access** – This allows managers to enable or disable any of the other 8 groups in the system. *This privilege requires Supervise Home Group to be assigned.*

- Set Access Level** – This allows managers to change to/from any access level, EXCEPT shutdown. *This privilege requires Supervise Home Group and Set Group Access to be assigned.*
- PIN Required** – This is an optional restriction to enable extra security. Although rarely used, this feature is beneficial to programmers with cards.
- Passage Mode Toggle** – This setting restricts the manager so that can only set the access level to Unlocked (commonly referred to as free passage) or ID Required. All other access levels are then denied to the Manager.

General Users

In most applications, the vast majority of system users are General Users. The General Users are only allowed entry when the access level is set to Enrolled ID Required or Facility Card. General Users never have access when the lock is Lockout or Shutdown. There are no privileges or other rights to be granted to General Users. They are the most basic and most common of user types.

Service Users

Service type users have the exact same entry privileges that General Users have EXCEPT service users are always required a PIN for entry. Administrators who want to create general users that require a PIN can use Service ID in place of general users. Another use is for contractors. Often a building or facility will require maintenance work that requires access by contractors who need entry rights on a temporary basis. This PIN can be set to change on a daily, weekly or monthly basis through their group enrollment. We'll get to Groups in just a second. Just remember that a PIN is always required for a Service User.

Access Levels and PIN Required

So, by now perhaps one of the biggest questions is "What is an Access Level?" This concept may take a little while to grasp, so don't be afraid to go over this section again.

A lock is always in one of six possible levels of access. The lock's access level can only be changed in one of three ways:

- Time Schedule Events
- Managers with Access Level Privileges through use of the keypad.
- Programmers through use of the Pocket PC

Chapter 2: Overview

Generally, if the User's ID that is entered meets the requirements of the current access level, the lock will disengage the locking mechanism, enabling entry access for a specified period of time (usually 3-5 seconds). The lock will then re-engage the locking mechanism and remain locked until the next valid ID is entered.

Access levels do not define "who" can enter, but rather "what" can enter. Group access settings define "Who" can get in. Access levels define the **type** of users that can gain access through the door. For example, if the lock is in Shutdown, only Programmer IDs can gain entry, therefore the "what" would be Programmer IDs. If a lock were placed in "Lockout", then the "what" would be only Manager and Programmer IDs.

PIN Required

Some of the access levels have a feature called "PIN Required." When this feature is enabled, it requires that all General Users enter their respective ID and PIN to be validated in the system. PIN Required is not a separate access level. It is simply an added feature to existing levels. This is most useful where card accountability is a problem. With this feature, any General User with a card must also enter a valid PIN corresponding to that card to be given access to the door. This feature does not affect Programmers or Managers because each one is individually set up in the OFM.

Unlocked

When the lock is in the Unlocked state, the locking mechanism is not engaged, enabling passage by anyone. The Unlocked Access Level is commonly used, for example, on a main entrance door that is intended to be unlocked during business hours.

Unlock with ID

This access level is frequently referred to as "First Person In". It is essentially a modified version of the Unlock Access Level in that it is set to go into the Unlocked state, however, it will only do so after the first valid ID (code or card) is entered. For example, you may want a lock to be Unlocked from 8 a.m. to 5 p.m. on weekdays, but only after the first person with a valid Enrolled ID (code or card) has entered. If no one comes in until 9 a.m. then the lock will not unlock until 9 a.m. This access has the additional feature of being able to require a PIN in addition to the ID, thus making it Unlock with ID + PIN.

Enrolled ID Required (most common)

This is the most common of access levels and is usually the main reason people access control systems. In the Enrolled ID Required state, a valid ID must be given to the lock for entry access to be granted. This is certainly the most frequently used access level. As with Unlock with ID, this access lock can be configured to require an ID plus an additional PIN. Once a valid ID + PIN has been entered, entry is granted.

Facility Card Required (Magnetic Cards ONLY)

This access level is specifically designed for magnetic cards. Locks at this level will allow access for any valid card ID within the entire facility. The individual user need not be enrolled in the lock for access. For example, an outside door might be set to this level to allow any employee to enter the main building, but interior doors could be set to Enrolled ID Required to allow individual access to secure work areas. This level requires that the system be specifically set up to use it and also requires that cards have the Facility ID in addition to the User ID programmed on each card. This access level used in more advanced programming. Entry gained under this access level is not recorded in the Audit Log. However, an event will be recorded in the audit log if the user is enrolled in the lock.

Lockout

In the Lockout state, the lock will give entry access only to a user with a Programmer or a Manager ID. This access level is convenient, for example, for locks that manage access to areas that are required to be inaccessible to the general user community during specific hours, but will remain still accessible to company management.

Shutdown

In Shutdown, the lock will give entry access **only** to a user with a Programmer ID. Likewise, Shutdown can only be set by the Programmer or by the lock itself in case of failure. This level cannot be set or changed by a manager or by a time schedule. Once in shutdown, a Programmer must manually take it out of Shutdown with the Pocket PC. A Shutdown level may be exhibited in the lock if there is imminent battery or motor drive failure. However, it can be set by a Programmer to deny access when no one is supposed to be in an area. For example, a hazardous condition might exist in the area controlled by a lock that a Programmer might elect to set to Shutdown.

User Groups and Group Access

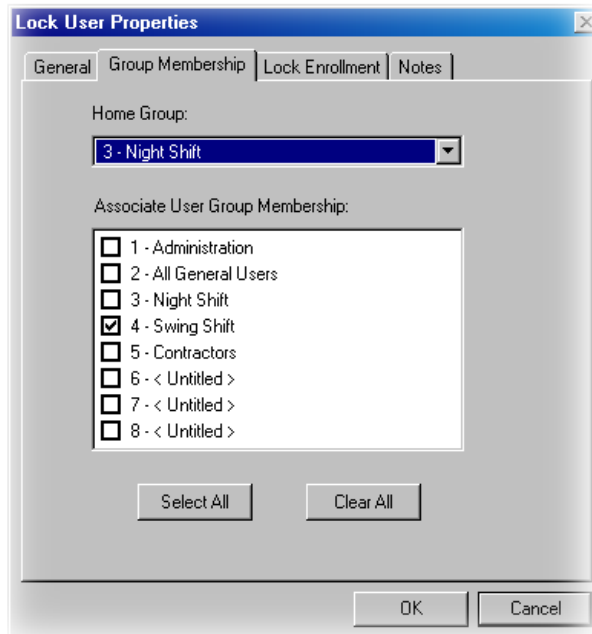
The system allows you to set up user groups to accommodate time-dependent access requirements for different people. For example, a day shift and a night shift could be assigned to their own specific groups and then set up to have access only during their period of duty. Each Facility can have up to eight different User Groups. Every user belongs to at least one of these groups.

At any given time a user's assigned group is either enabled or disabled. When a Group is enabled, all members of that Group have access when the lock is in the Enrolled ID Required state. Multiple groups may be enabled at any given time, but only members of enabled groups will have the right to gain entry.

Home Groups and Associate Groups

All users belong to a home group, but may also have an associate membership in another group or groups. This allows an administrator to combine access privileges of other groups for a single user. For example, someone may need to have access during the night shift and swing shift. Instead of creating another group that has privileges throughout, the administrator can assign the user's home group to Night Shift and associate the user with Swing shift. Now when either shift is enabled, that user will have access.

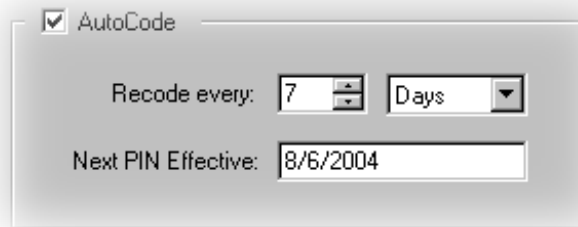
For general users, it doesn't matter which group is the Home Group and which is an Associate Group. The distinction between home and associate groups is important only for Managers that have the Supervise Home Group privilege.



Chapter 2: Overview

Group PIN Re-coding

PINs (Personal Identification Numbers) may be set manually or may be set to change automatically on a periodic basis by home group as desired. In addition to providing a higher level of security for selected groups, it is very useful when using contractors for maintenance work.



The screenshot shows a dialog box titled "AutoCode" with a checked checkbox. Below the checkbox, there are two fields: "Recode every:" with a numeric input field containing "7" and a dropdown menu set to "Days"; and "Next PIN Effective:" with a date input field containing "8/6/2004".

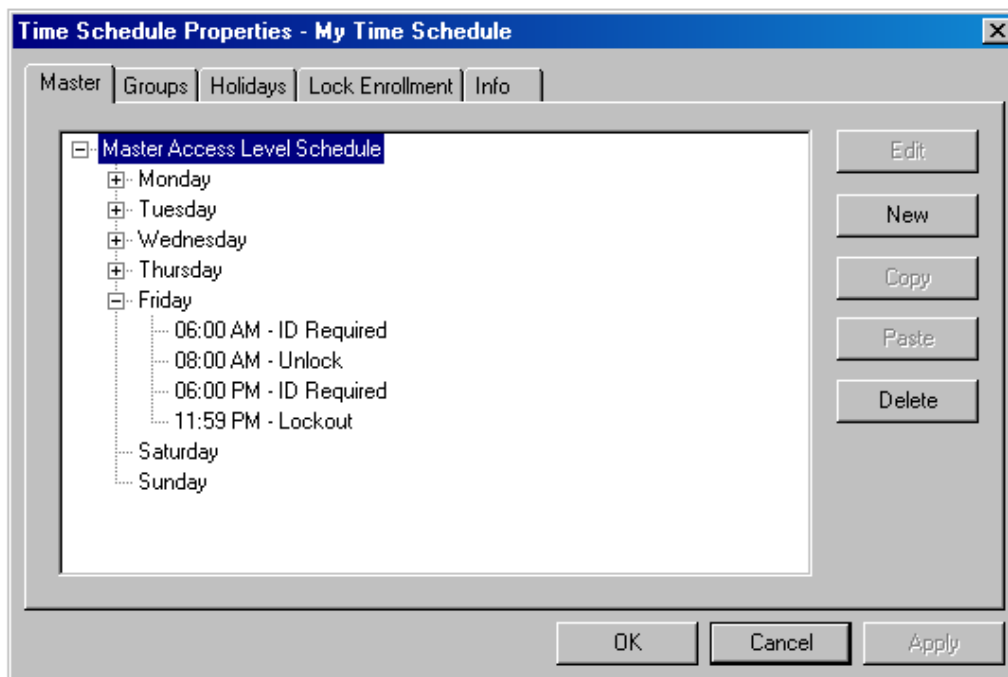
Time Schedules and Holidays

Overview

It is this feature that brings the most versatility and flexibility to the 2000 Series Access Control System. Although Time Schedules are not by any means a necessary portion of the lock, they become a very handy tool when managing various groups who have different working hours. Time Schedules allow the System Administrator to configure the lock so that it changes the Access Level or Group Access settings automatically. For example, the lock can automatically unlock at 8 AM and relock at 5 PM. Up to 255 Time Schedules can be created within each Facility. Each schedule can hold up to 255 events in total. Furthermore, observation of up to 32 holiday periods annually can be preset into the system and changed when necessary. Each of the schedules is broken up into 3 main portions: Master Access Level Schedule, Group Access Level Schedule, and Holiday schedules.

Master Access Level Schedule

The Master Schedule controls the overall Access Level of the lock. It does not control Group Access. In the example below, there is an existing Schedule that has been copied from Monday all the way through Friday. The schedule sets the lock into Enrolled ID Required at 6 AM and then automatically unlocks at 8 AM.

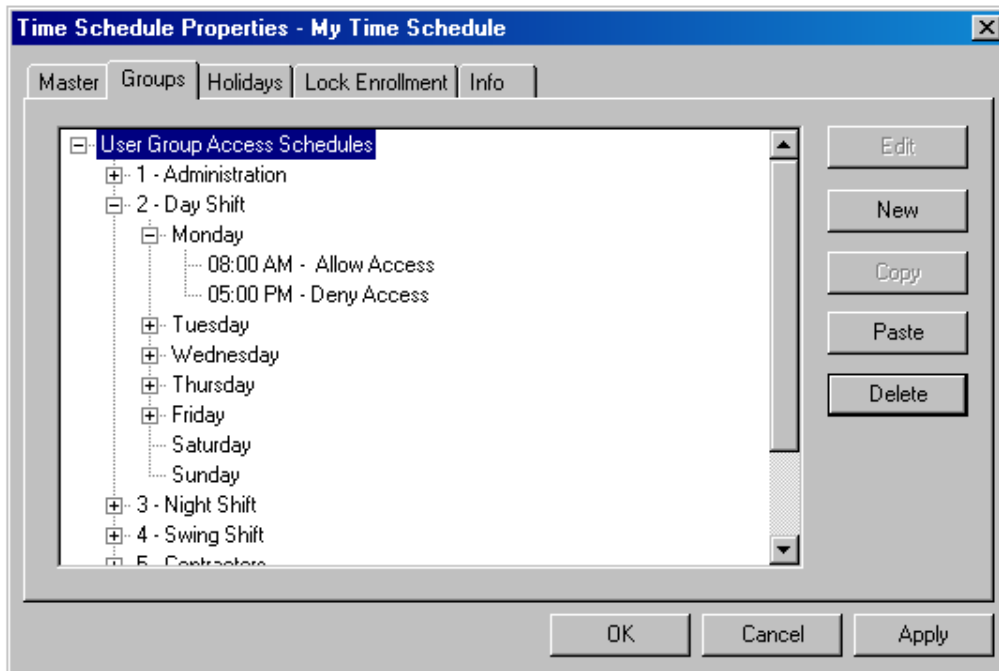


The screenshot shows a dialog box titled "Time Schedule Properties - My Time Schedule" with a close button (X) in the top right corner. The dialog has several tabs: "Master", "Groups", "Holidays", "Lock Enrollment", and "Info". The "Master" tab is selected. The main area contains a tree view with the following items: "Master Access Level Schedule" (expanded), "Monday", "Tuesday", "Wednesday", "Thursday", "Friday" (expanded), "Saturday", and "Sunday". Under "Friday", there are four time-based events: "06:00 AM - ID Required", "08:00 AM - Unlock", "06:00 PM - ID Required", and "11:59 PM - Lockout". To the right of the tree view are five buttons: "Edit", "New", "Copy", "Paste", and "Delete". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

Any day that does not have a specific schedule programmed will remain in whatever Access Level it was in the day before. In the example above, Friday's last event was Lockout at 11:59 PM. The lock will therefore remain in the Lockout state until Monday morning, at which time it will go into ID Required at 6 AM.

Group Access Level Schedule

Group Access is the portion of the schedule that enables or disables specific groups in your facility. For example, you may have a day shift and night shift that work separate hours and you don't want them to be able to come in outside of those hours. If you place the members of those shifts into their own groups (a Day shift Group and a Night Shift Group) you can set the schedule so that those groups only have access during those specific hours. Likewise, you can set a schedule to restrict students from coming outside of school hours. Below is an example of the schedule previously described with different shifts working.



You can see that Group 2 – Day Shift does not have access before or after 5 PM.

Chapter 2: Overview

Holidays

As previously mentioned, the OM2000 Series can hold up to 32 individual holidays. Holidays can be configured to match either an existing schedule, or be set to a specific level the entire period. Holidays can stretch over a period of a few hours up to an entire year. More commonly, Holidays are used on major national holidays such as Memorial Day or Labor Day. However, there can be instances during a convention or business meeting where you may want the locks to be unlocked for free passage. You can see an example of the holiday page to the right.

Holiday Period

Holiday Name: 4th of July

Start Date: 07/01 End Date: 07/06

Start Time: 06:00 AM End Time: 06:00 AM

Set Access Level

Access Level: ID Required

Restrictions: Unlock, Unlock with ID, ID Required, Facility Card, Lockout

PIN Required

User Groups: 1 - Administration, 2 - Day Shift, 3 - Night Shift, 4 - Swing Shift, 5 - Contractors, 6 - < Untitled >, 7 - < Untitled >, 8 - < Untitled >

Use Daily Schedule

Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday

<< Select All Groups

<< Clear All Groups

Holidays are set by the date, so you have to remember that on holidays like Labor day where the date changes every year, you have to go back and update the holiday list.

Credentials

The OM2000 Series system currently accepts 3 types of credentials for access control: Codes, Magnetic Cards, and Proximity Cards. These credentials can be mixed and matched through a single facility or can be uniformed to a single type.

Codes

When you first create your facility, you must set the Code length. Codes can be set to 4-10 digits. However, the greater the length: the higher the security. Codes are designed around a uniform basis, meaning that if you want one user to have a 5-digit code, then EVERYONE must have a 5-digit code. This allows the system to effectively monitor and register keyboard tampering on the lock itself.

Magnetic Card Features

More than 95% of users will use Track 2 cards and will not need to set up any type of advanced card parameters. If you are not informed of your card specifications, a lot of this information may not be understood and can be skipped.

OSI Security Devices currently stocks and provides Track 2 or Track 3 magnetic cards. These cards conform to ISO standards and can be ordered pre-encoded or blank. The system can be used with either Track 2 or 3 cards, however you cannot use both types within the same facility.

The system is flexible and may accept coding from existing Track 2 or Track 3 cards as long as they do not exceed the maximum number of characters for that track. These characters include any digits and field separators, however exclude the starting and ending sentinels. The maximum number of characters that the system can read on Track 2 is twenty-five (25) characters, however Track 3 will read up to thirty-one (31) characters.

Card Parameters

Card Data on: Track 2

User ID Starts at: Character 1

ID Issue Number at: Not Used 1

Facility Code:

Facility Code Starts at: Not Used 1

Expiration Date Starts at: Not Used 1

Expiration Date Format: DDMMYY

Card Valid Thru Expiration Date

User Defined Note Fields

Contact 1: Contact1 Reference: Reference

Contact 2: Contact2

If your existing card access system currently has a Facility Code, Issue number, or Expiration date encoded on each card, the Omnilock system can read and interpret that information by setting up the card parameters under the facility properties. This is usually set up when you first create the facility, however can be entered at a later period.

Card Issue ID

If a replacement card is required, the Card Issue ID may be used in lieu of issuing a new User ID. The Card Issue ID consists of one digit from 0 through 9. After using the card with an incremented (higher number) Card Issue ID in a lock, that lock will no longer accept cards with the same User ID that have a lower Card Issue ID. To ensure facility security, it is recommended that the administrator download the new card information to all affected locks.

Card Expiration Date

A Card Expiration Date may be encoded on the card to cause the card to be invalid once the expiration date is reached. The location of the expiration date on the magnetic stripe of the card must be identified on the Facility Properties page. The expiration may be specified as "to" or "through" the date and the date may be specified in a variety of formats:

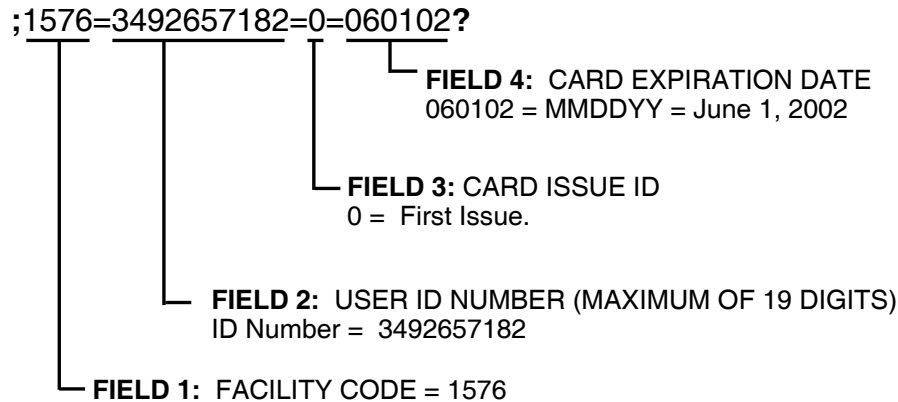
DDMMYY, DDMMYYYY, MMDDYY, MMDDYYYY, MMY, MMYYYY, YY, YYDDMM, YYMM, YYMMDD, YYYY, YYYYDDMM, YYYYMM OR YYYYMMDD.

Chapter 2: Overview

Using Fields

The ANSI standard includes a Field Separator (FS) character, generally represented as an “=” sign. When this is encoded on a card, it is understood to separate two independent data fields. Thus a card using the method might have the owner’s individual ID encoded at the beginning of the stripe followed by the FS character then the global facility ID. The fields can be in either order, or there can be more than two fields, which could be required for compatibility with pre-existing systems, and any one of them can be set up as User ID, Facility ID, Card Issue ID, or Expiration Date. The total character count cannot exceed 25 (Digits plus Field Separators). To use the Field Separator, select Field in the card section of the Facility property sheet, and then select the field number; “1” is at the beginning of the magnetic data stripe.

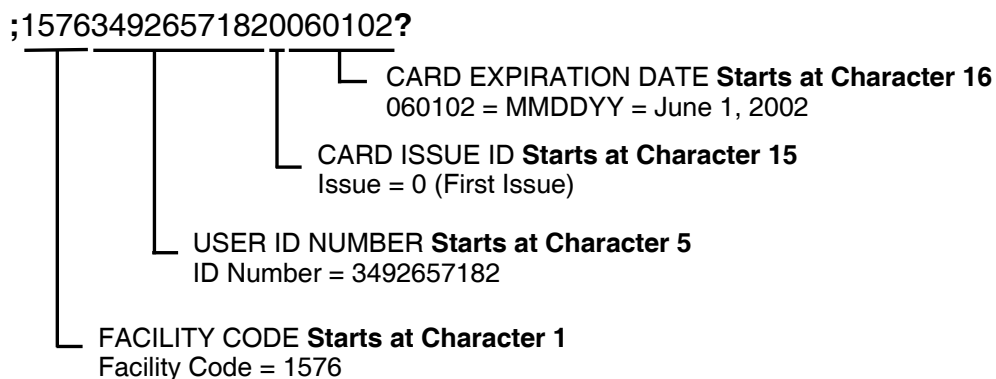
Example of encoded data using fields on Track 2:



Using Digit Count

Instead of using a FS to separate the IDs, you can set up a fixed digit count for the beginning of each ID. To use this method, select Character in the card section of the Facility property sheet. For example, the Facility ID could start at the beginning of the data stripe, digit count of 1. If the Facility ID has eight digits, the User ID would be set to start at digit count of 9. This method requires that all data groups with exception of the last one have a fixed number of digits and that the total number of digits not exceed 25.

Example of encoded data using character count on Track 2:



Proximity Card Features

OSI Security Devices now incorporates RFID Proximity access cards, Key Fobs, and Eprox tags from HID Corporation into the 2000 Series Access Control Systems. Virtually any HID formatted HID credential can operate in the system, from 26-bit to 35-bit Corporate 1000.

Existing HID proximity cards, Key Fobs, or eProx tags using one or all of these bit formats may be enrolled into your Facility using the optional RF Ideas proximity card reader (P/N: 11507-002) available from OSI. Various types of HID compatible Prox II cards, Key Fobs, and Eprox tags may be purchased separately from OSI Security Devices.

If you are using proximity cards in your facility, the Card ID Parameters (Card Data, Facility Code, Issue Number) on the Global Facility Property Page are bypassed and will not have an effect on the Proximity Card ID's enrolled in the Facility. If you have Magnetic Cards and Proximity Cards enrolled in the Facility simultaneously, these Card ID parameters will only affect the Magnetic cards enrolled.

.: Chapter 3 .: Programming

Overview

There are six steps in setting up your facility for the first time.

1. Install Microsoft ActiveSync and establish your partnership with your Pocket PC.
2. Install the Omnilock Facility Manager Software.
3. Install the OmniLink application for the Pocket PC.
4. Set up your facility by enrolling your users, locks, schedules and your Pocket PC.
5. Program your locks.
6. Update your facility after programming.

Before you begin setting up your facility, you should ask yourself a few questions. It may be helpful for you to write the answers to these questions down so you can properly set up your facility.

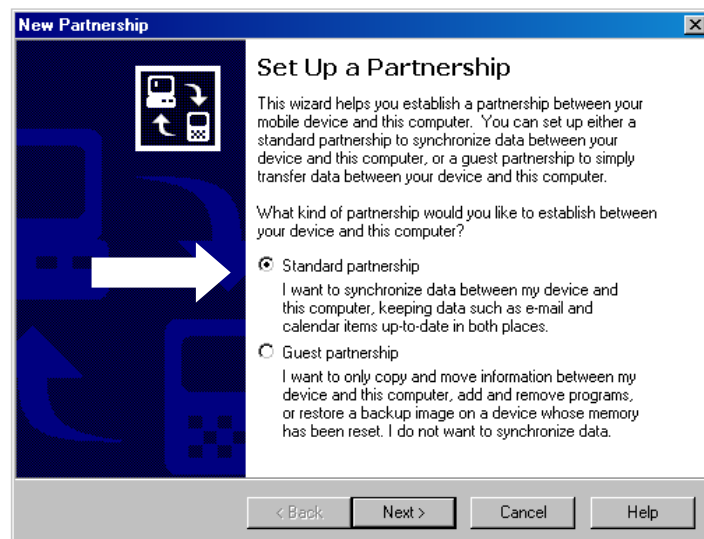
1. Will I be using codes in my facility? If so, what code length do I want those codes to be? Be sure to pick the number high enough so that you don't run the risk of running out of codes. (i.e. a 4-digit code can only support up to 10,000 users with codes.
2. Will I also be using cards in my facility? And, if so, will I want my Users to use a PIN in addition to those cards for extra security? And if so, what length should I set the PIN to?
3. What kind of cards will I be using? Proximity or Magnetic Cards?
4. If I'm using Magnetic Cards, will I be using Issue Codes, Expiration Dates or the Facility Code? If so, you will need to get the all the card settings for your card access system.
5. Will I want a schedule on the lock?

Installing ActiveSync

ActiveSync must be installed prior to installation of any OSI software. When setting up your device, you are free to select the options that would suit you, however, OSI requires that you choose a STANDARD partnership.

DO NOT CHOOSE GUEST OR HIT CANCEL!

OSI does not require that you select any of the boxes at the end of the partnership setup for synchronization. Doing so without having Outlook setup will cause errors while synchronizing.

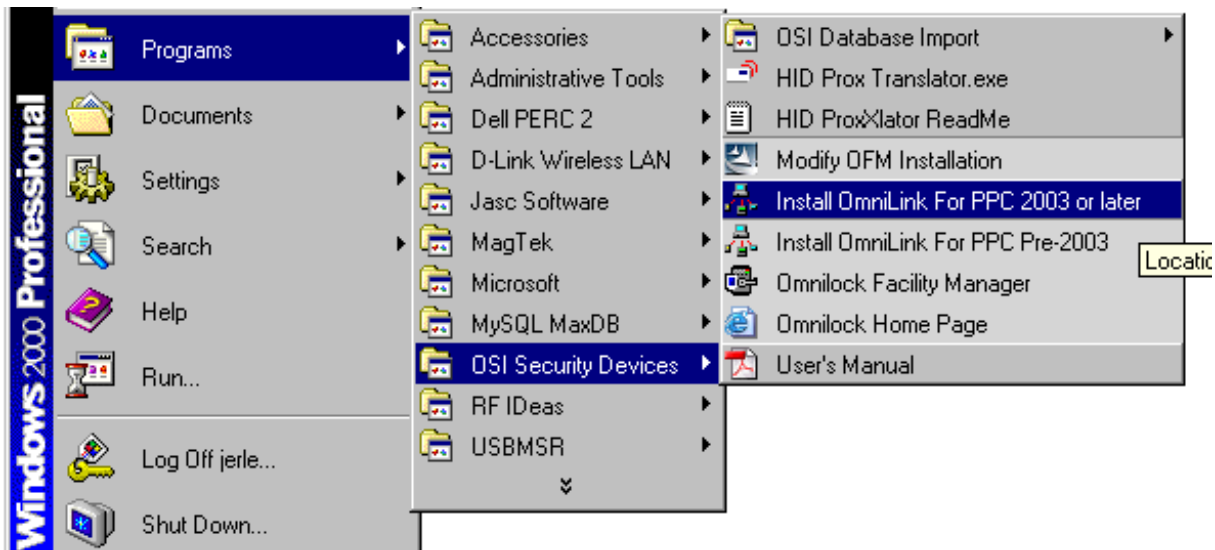


Installing the Omnilock Facility Manager and OmniLink

All necessary applications for running and administering the Omnilock Software are located on the installation CD. Simply insert the CD into your CD-ROM drive and choose follow the instructions on your screen and that come with the packaging. If nothing comes up after inserting the CD, run Menu.exe from the CD directory.

Alternately, if the Omnilock Facility Manager has already been installed and you only need to install the OmniLink application, you can click on:

Start > Programs > OSI Security Devices > Install OmniLink for (appropriate selection here)

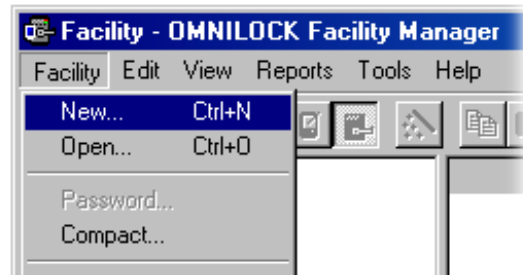


Setting Up a Facility

To begin setting up your facility, follow the steps below:

1. **First, make sure your Pocket PC has been connected and you have established a partnership.** Follow the instructions provided with your Pocket PC to properly establish a partnership. If you have problems with the Pocket PC, please contact the MANUFACTURER of the Pocket PC.

2. Double click the Omnilock Facility Manager Icon that is on your desktop.



3. From the **Facility Menu**, click **New...** You should see the General page come up for the facility settings.

4. Name your facility.
5. Set your code and PIN lengths.
6. Set your magnetic card settings. These can be skipped if you will not be using magnetic cards or if you don't know the parameters for the cards. Also, if you plan on using a mixture of cards (i.e. driver's license) then you should skip this portion as well.
7. Click **Next**.


8. If you will be using a USB Proximity Enrollment Reader, set this to Auto-Detect. Otherwise, you must select the appropriate COM Port for your device.

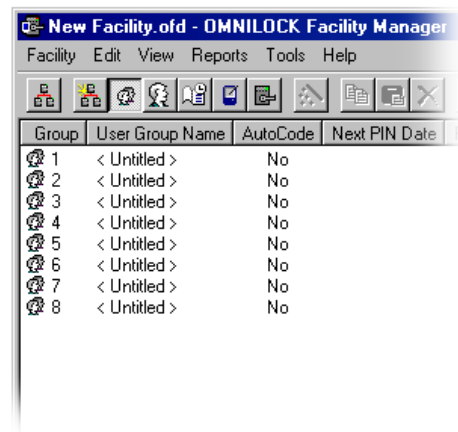
9. Select your Daylight Savings option. If you do not have one, simply choose "None" or if you follow a different Daylight Savings standard, simply choose Other and customize your settings to your needs.
10. Click **Finish**.
11. You will be prompted to set a password. This is optional, however, *if you lose the password, you will never be able to open your database again.*

Setting Up Groups

To set up your groups, follow the instructions below:

Chapter 3: Programming

1. Click on the View User Groups button from the toolbar. You will see the groups listed on your screen with the words "<UNTITLED>". 
2. Simply double-click the User Group you want to rename.
3. If desired, enable the Auto-Code feature. This allows the PINs to automatically change according the interval you specify. This feature only changes the PINs. It does not change the ID.




Setting Up Users

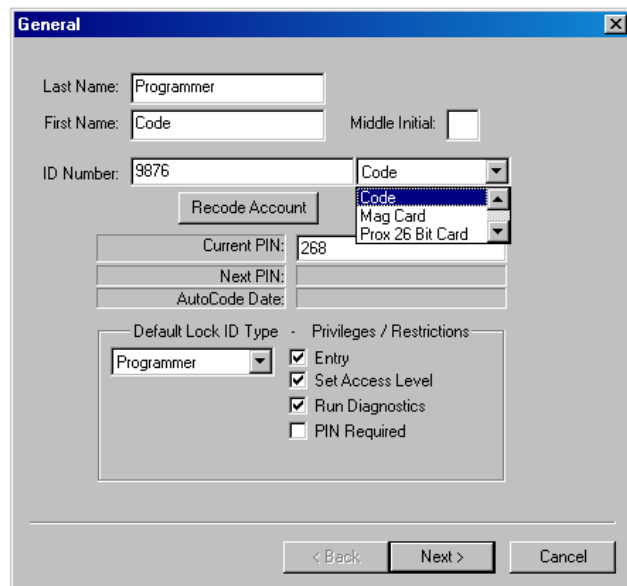
The following instructions describe the procedures for adding, removing, and changing user properties for the OFM.

Adding Users

Note: You cannot set up any Locks until you have established at least one *Programmer* to assign to that lock. Therefore, it is recommended that the first User you add is the Programmer.

To begin adding Users follow the steps below: 

1. Click on the View Lock Users button, then click the Magic Wand button to create a new user.
2. Fill in all appropriate name fields.
3. To the right of the ID field, select the appropriate credential setting.
 - a. If you using magnetic cards, select Mag Card first, then swipe your card with your Enrollment reader.
 - b. If you are using prox, be sure to verify that the Proximity Reader is detected when you select your format.
 - c. For Codes, simply type in the code you wish to use.
4. Press Next.
5. In the Group Membership screen, select the User's Home Group from the drop down menu on the top of the display. The associate User Group Memberships are optional and none have to be selected.
6. Click Next.

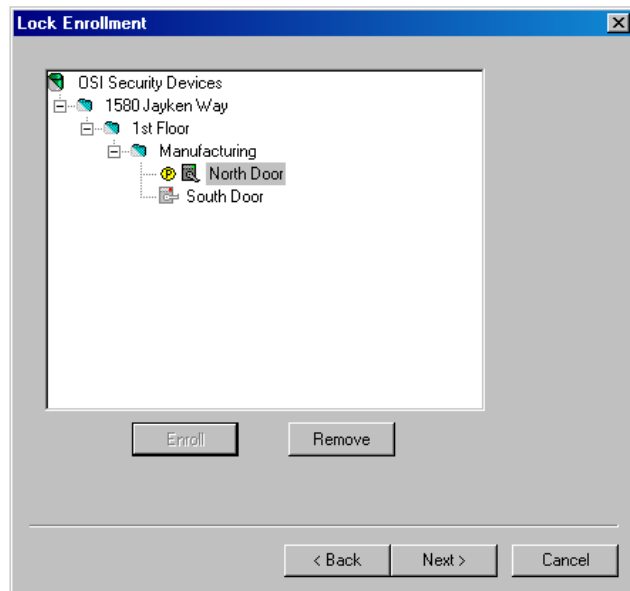


The screenshot shows the 'General' dialog box for user configuration. It contains the following fields and options:

- Last Name: Programmer
- First Name: Code
- Middle Initial: (empty)
- ID Number: 9876
- Recode Account button
- Current PIN: 268
- Next PIN: (empty)
- AutoCode Date: (empty)
- Default Lock ID Type: Programmer
- Privileges / Restrictions:
 - Entry
 - Set Access Level
 - Run Diagnostics
 - PIN Required

At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'.

7. On the Lock Enrollment screen, click on the locks you want the User to have access to and press the Enroll button. You can enroll the user into as many locks as you wish. (If this is your first user or if you don't want to enroll them at this time, you can simply click Next to skip this step.)
8. Click Next.
9. The final Notes fields are optional and are for your reference only.
10. Click Finish



Removing Users

Note: To remove a user you must FIRST remove them from any locks in which they are enrolled prior to deleting them from the facility.

To begin removing users, follow the directions below:



1. Click on the View Lock Users button.
2. Double-click the User you want to remove from the system.
3. Click on the Lock Enrollment Tab.
4. Click the Remove Button.
5. Click Apply and Ok.
6. Complete the Data Exchange Process to update your locks.
7. Synchronize the information with your database after the Data Exchange.
8. Right-click and select Delete on the User you wish to Remove.

Changing User Information or Credentials

If a user wants a new code or a new card, it is not necessary to recreate the user. You can simply change the existing information.

To change a User's profile, follow the instructions below:



1. Click on the View Lock Users button.
2. Double-click the User's name.
3. The property page for that user will appear. Simply change any information to the desired state or value. (For new Magnetic Cards, you must delete the old Card number from the ID field before swiping the new card.)

Chapter 3: Programming

4. Click Apply and OK.
5. Complete the Data Exchange Process to update your locks.

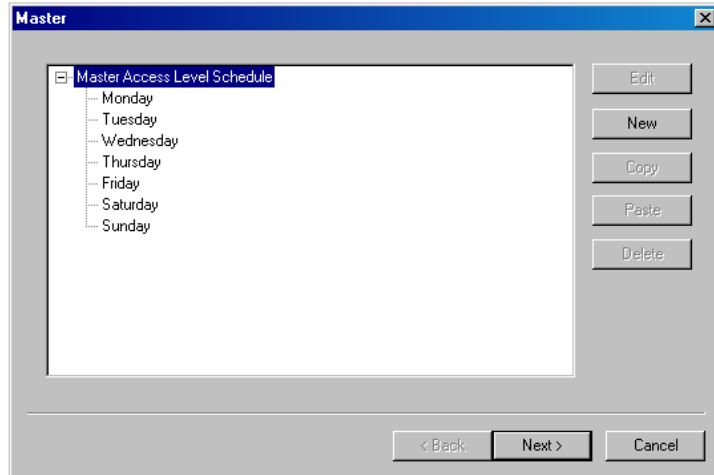
Setting Up Time Schedules

To create an optional time schedule, follow the instructions below:



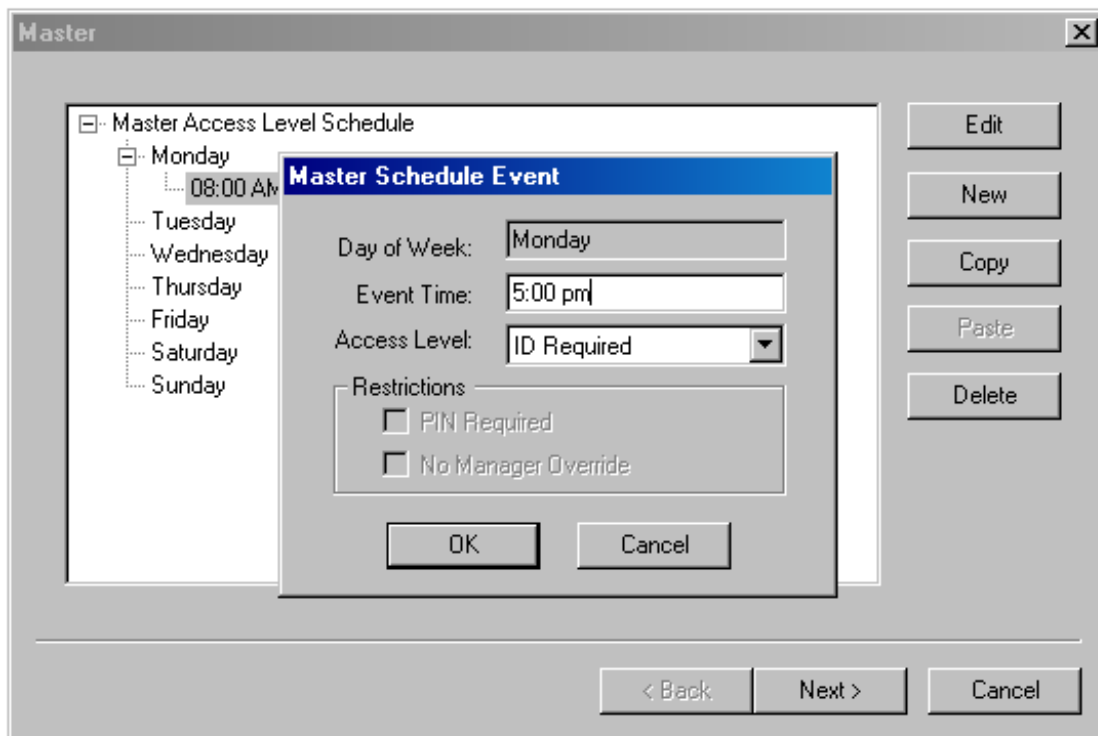
Click on the View Time Schedules Button, then click on the Magic Wand button. You should be presented with the New Time Schedule Dialog below:

If you do not want to add a Master schedule, simply select “Next” until you reach the next section that applies to you. Remember, Master and Group Schedules are vastly different. Please Review the Overview section of this manual for more information.



Master Schedules

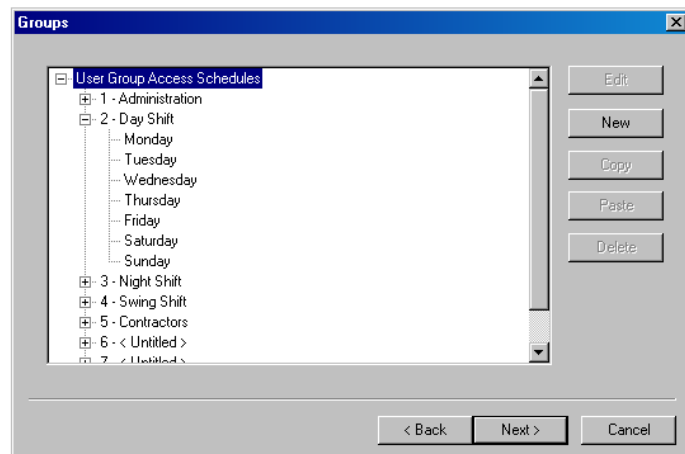
1. To add a schedule to a specific day, select the day you wish to add a schedule to and click the button that says “New.”
2. Enter the time you wish to the Access Level event to occur and then select the access level you wish the lock to be set at.



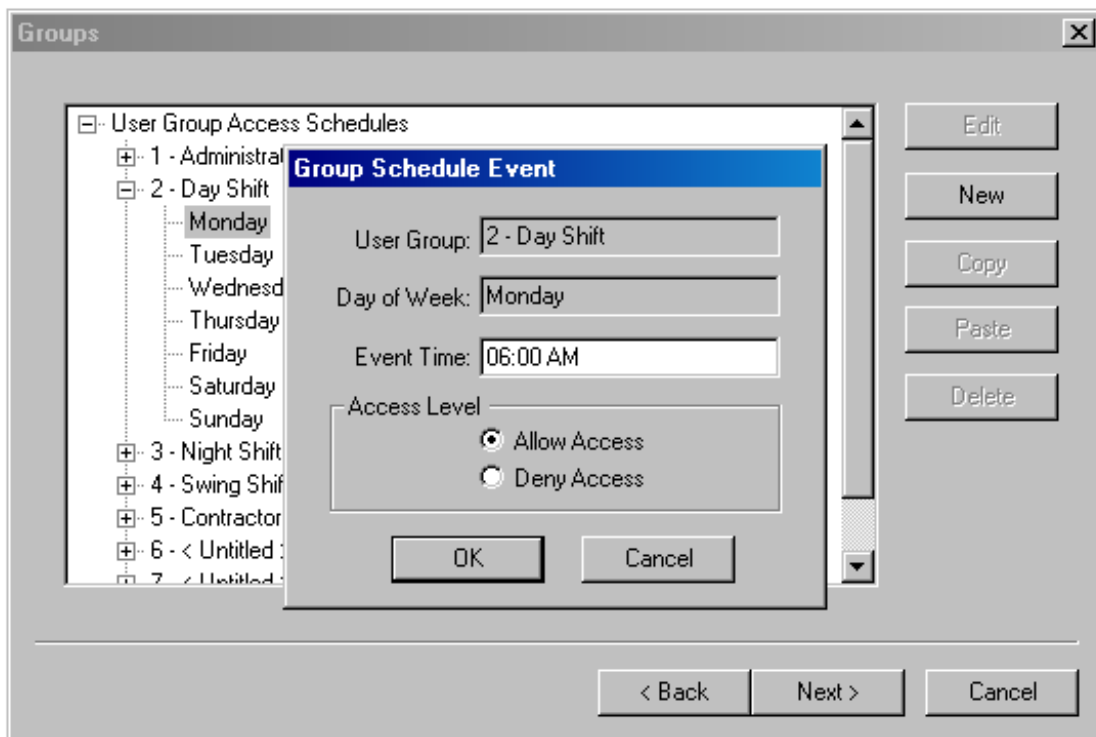
3. When you have finished, press OK.
4. You may continue to add up to 255 events to each day, however, it is more common that there are only 2-3 events per day.
5. When you have added all the schedules to the days you wish, press "Next." If you will not be adding Group Schedules at this time, you may continue to press "Next" until you reach the next appropriate section of the New Schedules Dialog.

Group Schedules

1. To add a Group Schedule to restrict User access by their groups, you must first expand the Group that you wish to restrict by clicking the Plus sign to the left of the Group Name.
2. Select the day of the week you wish to restrict the group by clicking on that day.
3. Press "New."



4. You will be shown the Group Schedule Even dialog. You will notice that the group has already been filled in for you as well as the day of the week.
5. Simply enter the time of day you wish to Allow or Deny the Group access.
6. Select the Allow or Deny Option and click Ok.

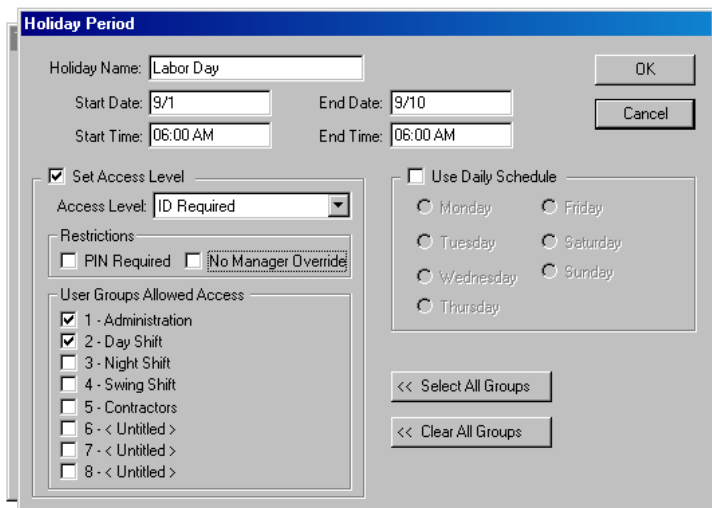


7. You can continue to add events to other groups or if you have finished simply click “Next.”

Holidays

This section is strictly for holiday periods. You can predefine all the holidays or you can wait until the holiday is close to address this section.

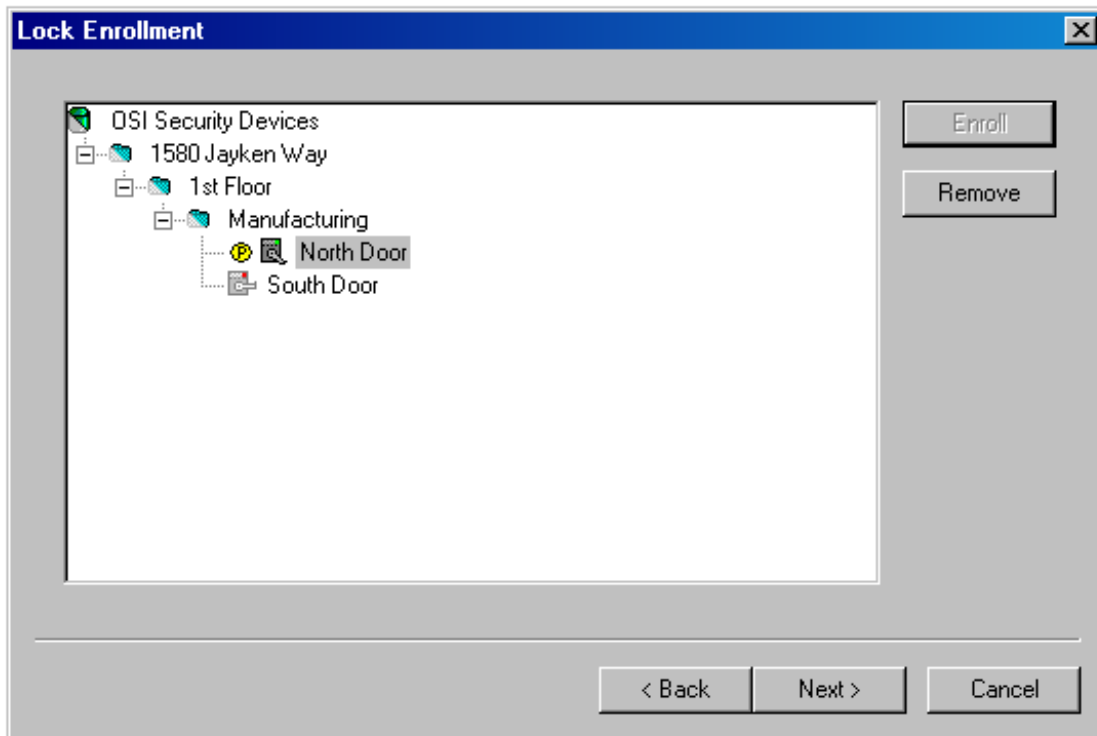
1. To add a holiday, click the “New” button.
2. Enter the Holiday period Name.
3. Enter the Start day you wish the holiday schedule to go into effect.
4. Enter the End Date. (The holiday period will span the entire time between these dates. You cannot have different changes throughout the period.)



5. Select the Access Level you wish the lock to remain during this time period, or you can select normal daily schedule for the lock to follow. For example, if it's a weekend and you want normal working hours for the weekend during this period.
6. Click Ok when finished.
7. Click “Next” when finished.

Lock Enrollment

A tree view of the Locks in the facility allows you to select the Locks you wish this schedule to apply to (or enroll in). Highlight each lock for enrollment and click Enroll. If a lock has been selected in error, highlight it and select Remove. When lock enrollment has been completed, click “Next.”



Schedule Names

If there are to be multiple schedules used throughout the facility, the name generally bears a logical relationship to the Locks to which it will be applied. Names such as First Floor, Manufacturing Area, Physics Labs, or Passenger Boarding Gates are typical. After assigning the name, click Finish to add the new schedule to the list. Remember: you may have up to 256 Time schedules per facility!

Deleting, Modifying, and Using a Schedule as a Template

Once a schedule is on the list, it can be modified, deleted in its entirety, or used as a predefined starting point for a new schedule. Right click on the desired schedule to allow a selection of these choices. To delete, simply select the Delete button; you will be asked if you really want to delete before the schedule will be irretrievably lost.

To modify the schedule, select double-clicking the desired schedule to bring up the Properties page. The properties of the schedule will be shown on a tabulated table. Select the tab for the property you need to modify and simply double-click any existing event to change it.

You can also Copy an existing schedule by right clicking the schedule to copy selecting Copy. This action begins a “New Schedule” dialog with everything preset as a template. From here on the process is just like creating a new schedule, but all of the events in the template have already been entered (or copied) for you.

The schedule-creating wizard shows up and you can modify any event by clicking the edit button, or add new ones using the Copy, Paste, New and Delete buttons. The final window shows “New Time Schedule”; at this point a suitable name should be typed in and Finish selected to save the schedule under the new name (i.e. Perimeter Doors, Classroom Schedule).

Enrolling the Pocket PC

Recall that you installed Microsoft ActiveSync (it comes on a CD provided with your Mobile Device or may be downloaded free from Microsoft) and established a Partnership prior to installing the OFM. If you have done this and you currently have an established and synchronized connection, then the enrollment of a Mobile Device into your Facility is a snap.

1. Simply click on the blue Mobile Device icon and then click the “New” (Wand) button.
2. Once the Mobile Device appears on the Mobile Device page you may double click on it to open its property page. On the property page you may optionally fill in the Assigned to text box.
3. Click OK and then “Yes” to update the device directory.

Note: For questions regarding Microsoft ActiveSync installation, synchronization, partnerships or troubleshooting please refer to the Microsoft Website.

Enrolling Locks in the System

We have finally reached the point where we can add locks to the system. This can be a single step or two-step process depending on your needs. Remember, while there are usually Locks and Locations within a single facility, Locations are completely optional. If you feel you will not need to organize your facility by locations, simply go to the Adding Locks section of this

Adding Locations

To add a new Location, follow the instructions below:

1. Right-click on the area you want the new location to appear. If this is your first location, then right-click on the facility name.
2. Select New.
3. Select Location. A folder will appear beneath the location you selected. Simply type the new name of the location and press enter.
4. You may add up to 256 Locations PER Location, however, it is very unlikely you will have to reach that number.



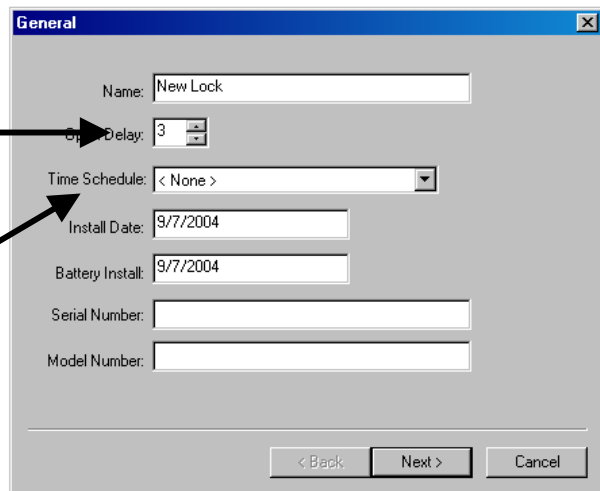
Adding Locks

To add a new lock to a location, follow the instructions below:

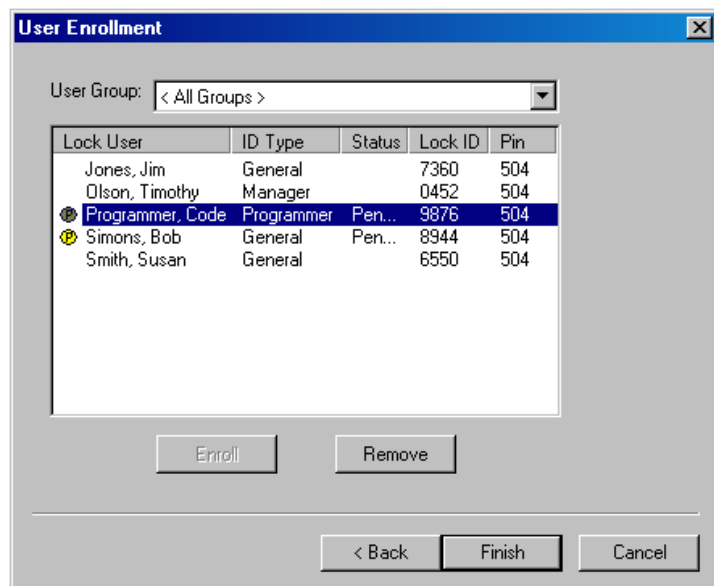
1. Right-click on the location you wish to add the lock to.
2. Select New.
3. Select Lock...
4. A new lock wizard will appear.



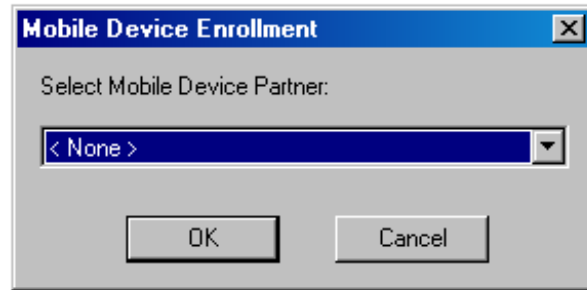
5. Type the new name of the lock you wish to create. Usually this is a Room No.
6. Set the open delay timing. This is the amount of time the lock will remain unlocked after a valid code or card is presented.
7. Select the time Schedule you wish to enroll into this particular lock. You can only assign one schedule to a lock, however this can be changed at any time.
8. The rest of the fields are **optional**, however are recommended. Should you require technical support, OSI will need to know the model number and perhaps the serial number for the lockset in discussion.



9. Click Next.
10. On the User Enrollment Section, you can select the individuals you want to have access through that lock. If you do not enroll the individual into the lock, they will be denied access at all times. **YOU MUST ENROLL AT LEAST ONE PROGRAMMER.**
11. Click the name of individuals you want to enroll and click "Enroll."
12. Click Finish when done.



13. A message will appear asking you to enroll your Pocket PC. This is a commonly skipped step. You must select a Pocket PC to enroll into your locks. Otherwise, you will not be able to download the information to your Pocket PC.
14. After selecting your Pocket PC, click Ok.

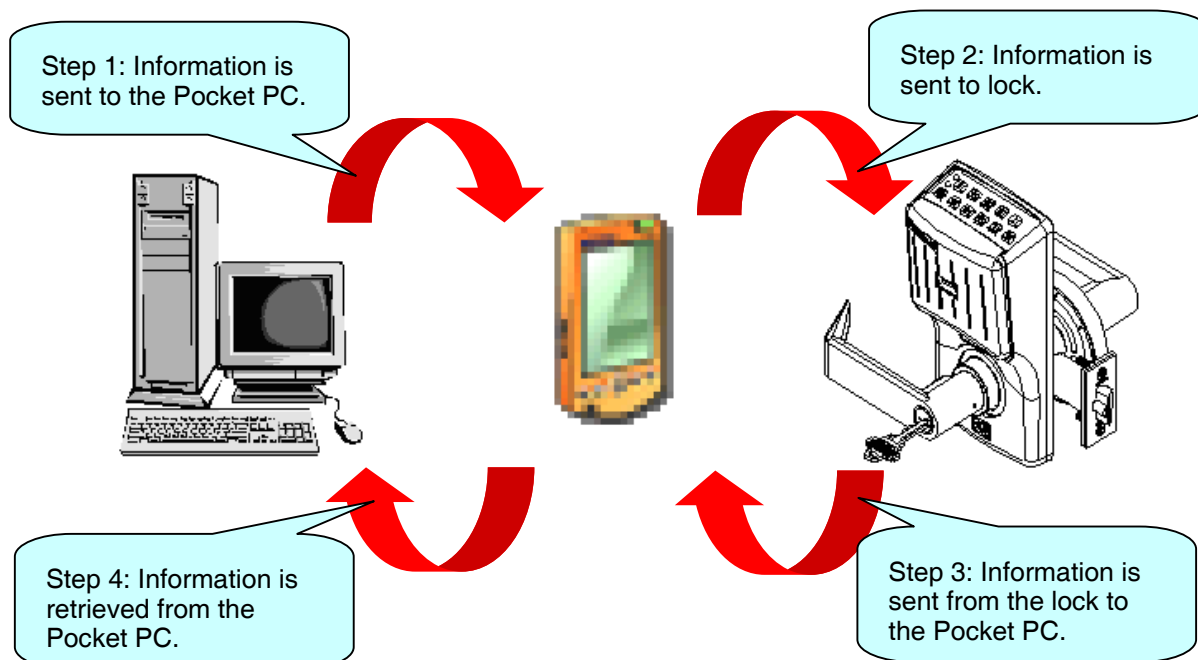


The Data Exchange Process

The Data Exchange process is the most important aspect of the system. It is through this process that we are able to update and program the locks. It also provides the means for retrieving valuable audit data and lock status information, such as the battery level. Each part of the system (the lock and Pocket PC) has its own part of the main database. When changes to the main database are made, those changes must be transferred and updated throughout the other parts of the system.

There are 4 major events that occur when performing the data exchange process.

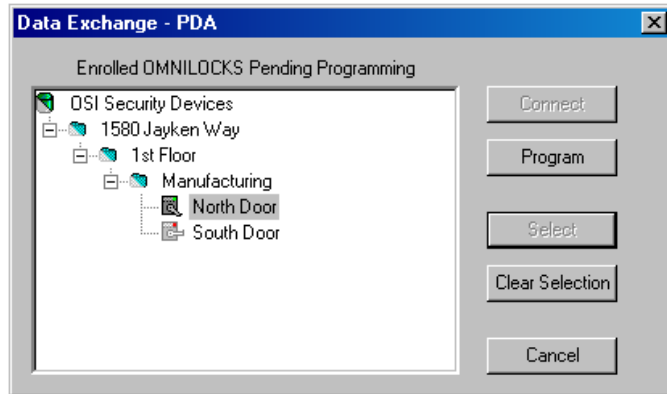
1. First event: When you hit the Data Exchange button, data is sent from the OFM to the mobile device database.
2. You must now download that information to the lock so the lock will be up to date.
3. At the same time you update the lock, the lock sends all the valued information back to the Pocket PC so that you can store it in the main facility. This step requires no intervention from you. It happens simultaneously with Step 2.
4. At this point, you must return to your desktop and hit the lightning bolt again to transfer the recently retrieved information back to your database. In actuality, once your database has been established, Steps 1 and 4 will also occur simultaneously.



Doing a Data Exchange

Once you have finished setting up any users or doing any changes you feel are necessary, the last step in the process is to program the locks. This begins the Data Exchange Process.

1. To begin the Data Exchange, click the Lightning Bolt button. You will see some progress bars that relate to connecting to the remote database.
2. You will then see the Data Exchange dialog. This dialog will only show locks that need to be programmed. It does not show all the locks in your facility, but rather those that you have recently made changes to or that you have just created.
3. You must now choose which locks you wish to go program by clicking on the lock and pressing the Select Button. You may select as many locks as you wish. If you select a location, it will automatically select any locks within that location.
4. Press the Program button to commit that information and send it to the Pocket PC.



5. After the Data Exchange is complete, only the locks you did **not** select will remain. You must now visit the actual lock in your building to update it. In the example above, only the North Door was selected, so only the North Door will be available to program.

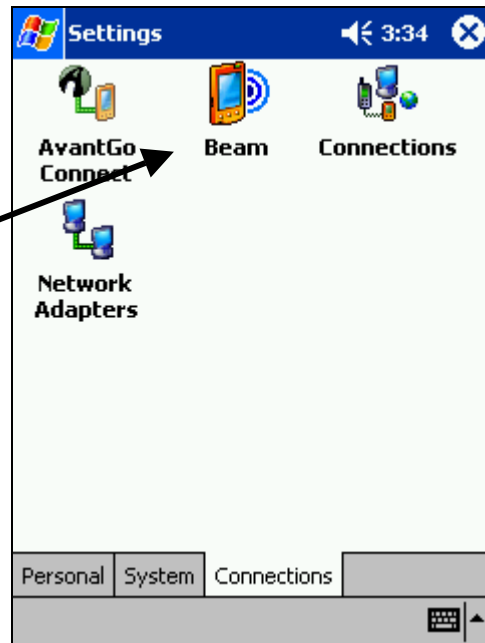
You are now ready to use the OmniLink application.

OmniLink

Before using the OmniLink program, you must first configure your Pocket PC to work with the software.

Follow the instructions below to set up your Pocket PC to work with the OmniLink application:

1. Tap on Start.
2. Tap on Settings
3. On the bottom, Tap on Connections.
4. Select Beam from the options.
5. **Uncheck** the Box that says Receive all incoming Beams.
6. Tap on "OK" in the top right corner.
7. Close out of all windows with the X in the upper right corner.



Chapter 3: Programming

Your Pocket PC should now be configured to work with the OmniLink application. When you start the program, you should see something very similar to the image on the right.

To start the program, simply tap on Start > Programs> Omnilock Link. Sometimes, Omnilock Link will be right under the start Menu.

You should see any and all locks that are pending programming listed as well as a current count of those locks.



Programming and Updating the Lock

To start programming the lock, follow the instructions below:

1. Start the OmniLink program.
2. Align the infrared port on the Pocket PC with the infrared port on the lockset. If you are unsure about the whereabouts of the IR on your Pocket PC, please consult your User's Manual.
3. Maintain a 6-8 inch distance from the lock when programming. Failure to do so may result in erroneous programming of the lock.

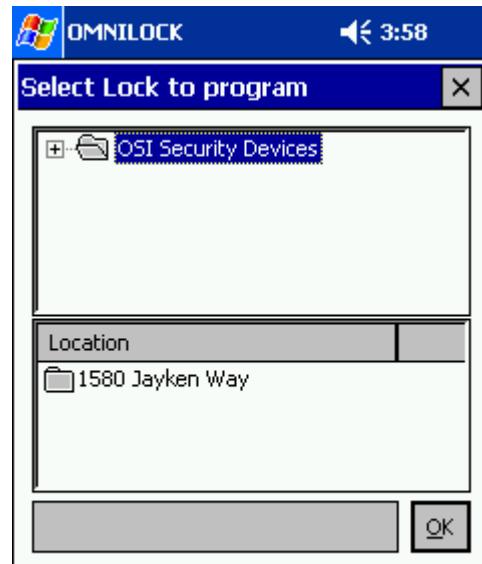


4. Enter the current Programmer Code or Card into the lock. If it is in factory default, the current code is 1-2-3-4. If you have already programmed the lock once and have not reset it since, use the Programmer Code or Card that you defined in your setup.

***** DO NOT MOVE THE POCKET PC *****

5. If your lock is no longer in the factory settings and has already been set to your new Master Code or Card, skip to step 9.

6. Your Pocket PC should present you with a dialog similar to the one on the right. At this point, you must navigate through any locations until you see the lock you wish to program on the bottom of the screen.

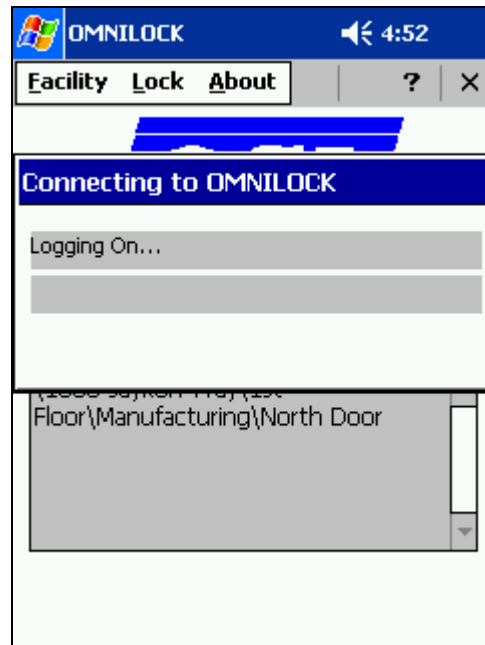


7. Tap on the lock on the bottom until it is highlighted.
8. Click "OK."



Chapter 3: Programming

9. The Pocket PC should begin logging on and programming.
10. When you see the message "Data Exchange Complete," tap OK and close the OmniLink application.
11. You may now move the Pocket PC away from the lock.
12. Return the Pocket PC to its cradle or sync cable and hit the lightning bolt one final time. The Data Exchange Dialog on the OFM should be empty at this point.



Closing the Omnilock Link Program – A Word About Synchronization

Before you return the Pocket PC to its dock at the PC, **you must click the X at the upper right hand corner** of its display to terminate the OmniLink program. Failure to do this will make it difficult to connect to the PC or if it does connect, the OFM will be unable to access files on the Mobile Device. If you forget to close the OmniLink program and plug it in anyway, simply unplug the device, close down the OmniLink program, and reconnect it to the PC.

If you have problems syncing even after you have closed the OmniLink program, try disconnecting and reconnecting the Pocket PC from the computer. Simply removing it from the cradle or unplugging it from the sync cable will accomplish this.

Updating Your Facility

OSI expects that there will be changes throughout your facility. Employees may leave and you may hire new employees. This will all have to be updated in your database. The steps are exactly the same as described above, however, you must realize that any time you make a change to your database, you must make sure you update all your locks. Because this is a standalone system, the locks are not connected to your PC by any means, which requires that you visit each lock that you have made changes to.

.: Chapter 4 .: Lock Operation

Introduction

Once the lock is programmed, you can begin taking advantage of all of the features in which you have invested. In most instances, using the lock simply means typing your code or entering presenting your card to gain entry. However, there are certain circumstances and access levels where it may not be that simple and recognizing the difference will be important.

Anti-Tamper

When an invalid credential is presented to the lock, the lock will flash 1 Red light. If this happens 3 times in a row, the lock will enter what is called Anti-Tamper. Anti-Tamper essentially kills the lock for 10 seconds. It will not recognize or even acknowledge any codes or cards presented to the lock until the 10-second period has ended. At this point, **the next card or code presented to the lock MUST be valid**, otherwise, it will kill the lock for another 10 seconds. This mode will otherwise continue until such time.

This mode of operation is automatic and is used to prevent someone from entering the lock by means of "brute force." Brute force is a tactic used where all possible combinations (i.e. 0001, 0002, 0003, etc.) are entered into a system until a valid combination is found. With Anti-Tamper, Brute Force becomes very limited as every invalid code that is entered after the first 3 must wait an additional 10 seconds.

An example:

- You have the code length set to minimum of 4 digits, and the only valid code is 3456.
- The brute-force attacker starts his process at 0001.
- It would take the attacker a MINIMUM of 9 hours and 36 minutes before he reaches the valid code with Anti-Tamper. Without Anti-Tamper and providing the attacker can type at least one code per second, the code will be cracked in less than an hour.

Normal Operation

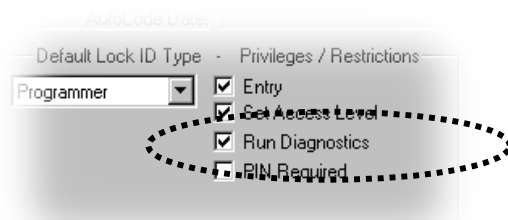
In most cases, the lock will be in ID Required and everyone will need some sort of valid card or code to get through the door. In the majority of these instances, the lock will simply flash one Green light and the door will open. The only exception to that is Programmers. ALL Programmers will get a total of 6 Green lights when their card or code is presented.

Setting Access Levels and Group Access

There may be times when you may need to stray from the standard Access Level of ID Required. You may need the door completely unlocked at all times letting anyone through, or you may want to restrict everyone below a Manager level from gaining access to an entry. This is where it becomes important to know how and where to set the various access levels outside of using the schedules.

Programmers

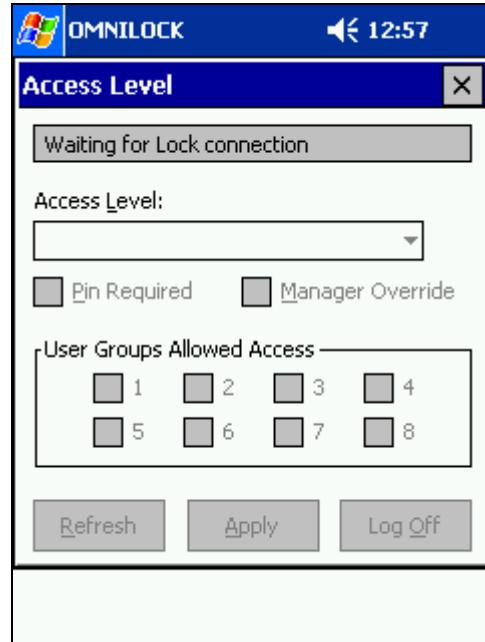
In order for a Programmer to set the access level, the Programmer ID MUST have had the Set Access Level privilege assigned to it during the setup. The Programmer can then use the Pocket PC to check or change the Access Level and Group Access settings.



Chapter 4: Lock Operation

To set the Access Levels and Group Access, follow the instructions on the below.

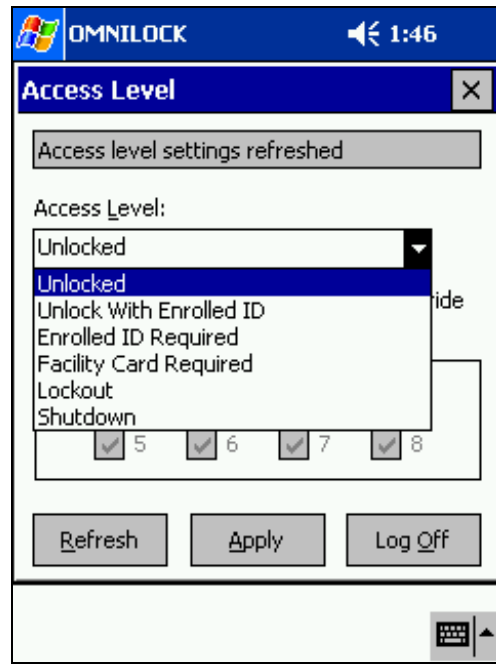
1. Start the OmniLink Program on the Pocket PC.
2. Tap on Lock and then Access Level. The Access Level Screen to the right should appear on your Pocket PC.



3. Align the Pocket PC with the IR on the lock.
4. Enter the Programmer Code or Card along with any necessary PIN. The lock should begin communicating with the Pocket PC. You will notice the words "Retrieving Access Level Settings..." appear on the top of the screen.
5. The Pocket PC should then read "Access Level Settings Refreshed." At this point, you will be able to see the current Access Level of the lock. The example on the right shows the Factory default access level.



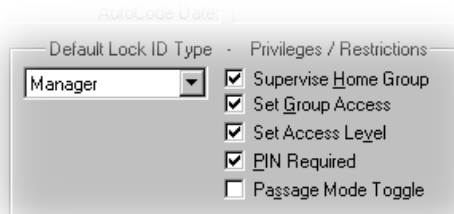
6. To change the Access Level, select the new access level from the Access Level menu.
7. Check or Uncheck the group number of the group you wish to enable or disable.
8. Check or Uncheck PIN Required if desired.
9. Check or Uncheck Manager Override if desired.
10. Tap “Apply.”
11. The message “Access Level Set” will be displayed on the top of the screen.
12. Tap “Log Off.”



Managers

As with Programmers, Managers also have certain rights assigned to them. The lock will respond in accordance with those assigned rights. If you recall, the rights that Managers can be assigned are as follows:

- Supervise Home Group
- Set Group Access
- Set Access Level
- PIN Required
- Passage Mode Toggle



In order for a Manager to set the Access Level, the Manager must have been assigned the Set Access Level privilege.

To change the current access level:

1. Enter the Manager Code or Card.
2. Press the key for the corresponding Access Level from the table on the right.
3. Press and hold the CL key until the Green light flashes.

Access Level	Key Number
Unlocked	2
Unlocked following first valid ID entered	3
Unlocked following first valid ID + PIN entered	4
Enrolled ID Required	5
Enrolled ID + PIN Required	6
Facility Card	7
Lockout	8

Chapter 4: Lock Operation

Group Access

If a Manager is given full Group Access privileges, then the Manager can enable or disable Groups within the facility that are not his own. To take advantage of this privilege, first ensure that the Manager has been given Group Access privileges. It is important to remember that Group Access settings are appended to any previous settings that were already in effect. This means, if you enable Group 2 and you know that Group 3 is already enabled, then Group 2 and Group 3 are now both enabled. If you only want Group 2 enabled, then you will have to disable Group 3 when you enable Group 2.

To enable a Group, follow the instructions below:

1. Enter the Manager Code or Card.
2. **Press 1.**
3. Press the corresponding button for the Group you wish to **enable** (i.e. 3 for Group 3).
4. Press and Hold the CL button.

To disable a Group, follow the instructions below:

1. Enter the Manager Code or Card.
2. **Press 0.**
3. Press the corresponding button for the Group you wish to **disable** (i.e. 3 for Group 3).
4. Press and Hold the CL button.

To enable or disable ALL Groups at once, follow these instructions.

1. Enter the Manager Code or Card.
2. **Press 0 to disable or 1 to enable.**
3. Press and Hold the CL button.

Home Group Supervision

Some managers may not be given full Group Access Level, but rather just Home Group Supervision. This allows Managers to enable or disable their own HOME Group. If only this privilege is given, then the Manager can only enable or disable their own Home Group, and not manage any other groups in the facility. This feature works in a toggle function, meaning that if the group is enabled, then using this feature will disable the Group; however, if the Group is disabled, this feature will enable it.

You can check current Group status by doing the following:

1. Enter the Manager Code or Card.
2. **Briefly** press the CL key. The Green light will flash once, then another light will flash.
 - a. If the second light is Green, then the Home Group is enabled.
 - b. If the second light is Red, then the Home Group is disabled.

You can now determine if whether you need to disable or enable the Home Group. To accomplish this, follow the instructions below:

1. Enter the Manager Code or Card.

2. Press and **Hold** the CL key until the Green light flashes 3 times. The Home Group will now be in the opposite state it was in previously.

Toggle Managers

If a Manager is assigned as a Toggle Manager, they work the same as a Manager with Set Access Level privileges; however, they are essentially given only two commands: 2 and 5. This allows them to only set the lock to Unlocked or ID Required.

PIN Required Operation

When the lock is placed into a state where a PIN is required, any valid Codes or Cards that are presented will flash 2 Green lights. You must enter the corresponding PIN for that ID after the two Green flashes.

There are two ID types that may not require a PIN regardless of the Access Level: Managers and Programmers. The reason for this is that those ID types have individual settings for PIN. The lock does not govern them. For Managers and Programmers to be required a PIN, they must be specifically set up that way in their User Properties in the OFM by checking the "PIN Required" check box.

Additional Lock Features

Remote Switch Operation

The lock may be unlocked remotely by pressing a normally open switch that has been connected to the terminal block provided in the lock. The lock will remain unlocked as long as the switch is closed. When the switch is opened the lock will remain unlocked for the duration of the Open Delay Time. This event is recorded in the Audit Log as a Remote Entry. This Remote Switch terminal block may also be connected to a wireless transmitter-receiver system or a Fire/Life Safety circuit

Key Detection (Option 1)

This optional feature detects when the lock has been unlocked with a standard key and makes an entry in the Audit Log with time only. This option is available on the Schlage locks and the Arrow locks; but not on the Falcon Mortise lock. The minimum elapsed time between recorded key entries is one minute..:

.: Chapter 5 .:

Reports

Reporting Features

The 2000 Series is equipped with embedded Crystal Reports. This allows the OFM to generate 3 user reports used for managing and monitoring lock activity. The three reports are as follows:

- Audit Reports: allows you to view all activity occurring in the lock
- Lock Reports: allows you to bring up a list of who is enrolled in that lock and other useful information about the lock in question
- User Reports: displays a list of all users in the facility

Each report has its own set of features and options. If already have a full version of Crystal Reports 8.5 or previous installed on your PC, you can take advantage of the exporting features of Crystal Reports.

Audit Reports

Introduction

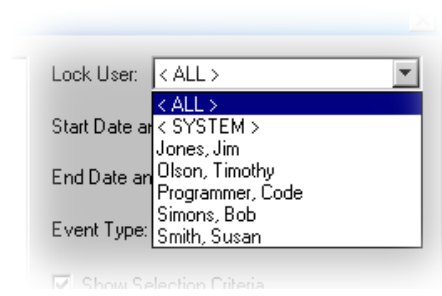
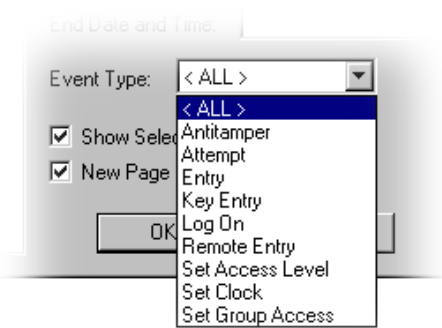
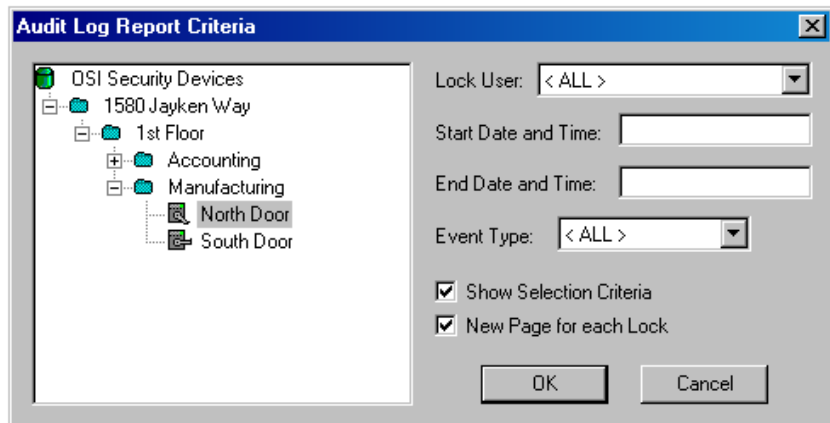
The Locks keep a record of nine significant types of access control events. These events include:

- | | |
|---|--|
| <input type="checkbox"/> User Entries | <input type="checkbox"/> Programmer Logons |
| <input type="checkbox"/> Access Level Changes | <input type="checkbox"/> Anti-Tampers |
| <input type="checkbox"/> Group Access Changes | <input type="checkbox"/> Key Entries |
| <input type="checkbox"/> Entry Attempts by Unauthorized Users | <input type="checkbox"/> Remote Entries |
| <input type="checkbox"/> Time Changes (i.e. Daylight Savings) | |

Audit Report Criteria

The Audit Report Criteria Dialog displays a short form of the Facility Explorer. You can see it on the left. On the right side of the dialog are various filter options. You can either select specific types of events or you can narrow it down to a particular person.

If you have a lot of audit data, you can narrow your search down to just a short period of time. This can reduce the number of pages by a great deal.



Chapter 5: Reports

Running an Audit Report

Audit reports can be run in one of two ways:

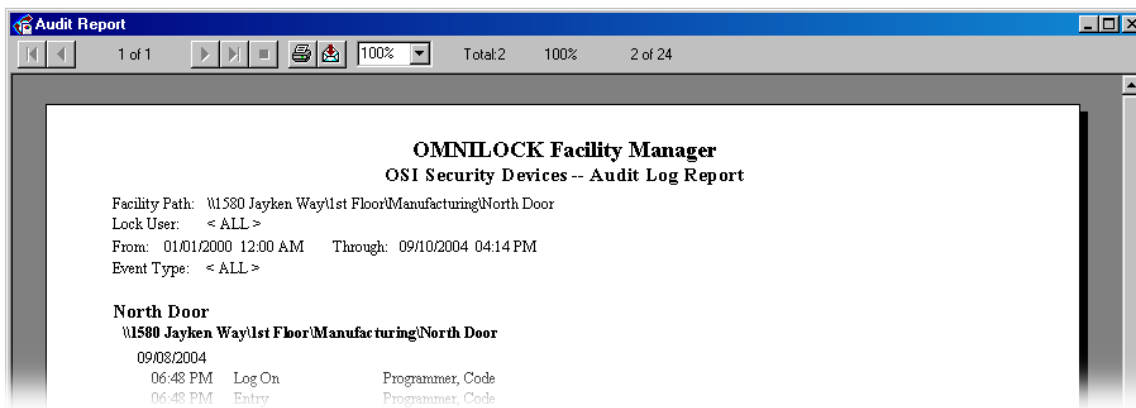
1. Clicking on the Report Menu and select Audit Report.

OR

2. Right-clicking on the lock you wish to run a report on and selecting Audit Report.

Both methods will bring up the same Audit Report Dialog, so we'll start from there.

1. If you have not already done so, you must collect Audit from the lock prior to running an Audit for the latest Audit information. To collect Audit, simply do a Data Exchange with the lock and your Pocket PC. You do not need to send any information to the lock or make any changes to the lock to collect the audit.
2. From the Audit Report Criteria dialog, select the Lock User you wish to query, if necessary.
3. Select the event type you query if necessary.
4. Optionally, you can enter a date and time range that you wish to view for the report. The OFM supports numerous formats, however the standard is "Month DD, YYYY and then HH:MM AM/PM."
5. Select any other options you would like to use.
6. Click "Ok."
7. The report should appear similar to report below. The small envelope on top of the toolbar can only be used if you currently have a full version of Crystal Reports installed on your PC.



Lock Reports

Introduction

Lock reports can provide the administrator with two pieces of information:

1. The most current available lock status
2. A list of users that are enrolled into the lock

The latter can be optionally declined, however the main purpose of the report is to allow the administrator to view a list of all the locks in the facility to review the latest information about the locks. The following information is displayed on all Lock Reports:

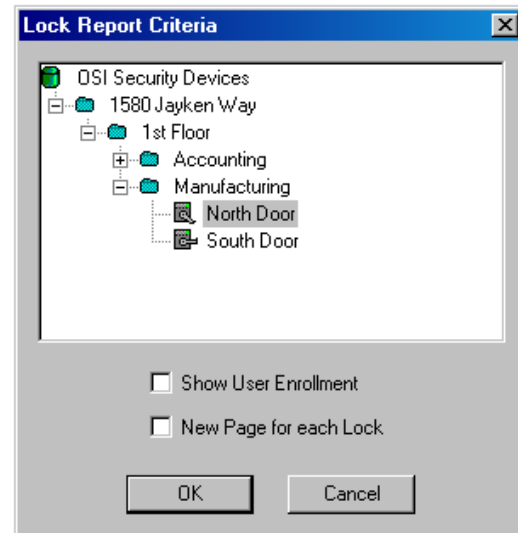
- | | |
|---|--|
| <input type="checkbox"/> Model Number (if entered at time of creation) | <input type="checkbox"/> Pocket PC Assigned |
| <input type="checkbox"/> Serial Number (if entered at time of creation) | <input type="checkbox"/> Last Programming Date |
| <input type="checkbox"/> Open Delay | <input type="checkbox"/> Installation Date |
| <input type="checkbox"/> Time Schedule Assigned | <input type="checkbox"/> Battery Installation Date |

Lock Report Criteria

The Lock Report Criteria dialog is relatively simple. Again, you have the explorer view of your facility.

The “Show User Enrollment” option is available in the event you would like to view the Users are currently enrolled in each lock on the report.

You can also separate each lock so that when the lock information for a different lock will start on a new page.



Running a Lock Report

As with Audit Reports, Lock Reports can also be run in the exact same two ways:

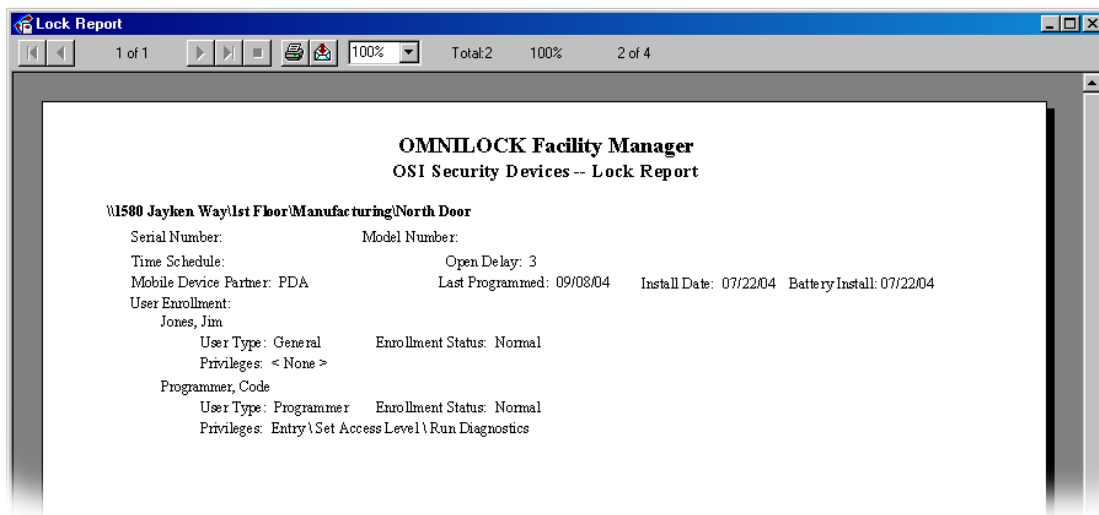
1. Clicking on the Report Menu and select Lock Report.

OR

2. Right-clicking on the lock you wish to run a report on and selecting Lock Report.

Once you’ve started the Lock Report dialog, follow these steps to retrieve the report:

1. Check or uncheck the box for Show User Enrollment.
2. Check or uncheck the option for New Page for each Lock.
3. Click OK. Your report should be similar to the report below:



Users Reports

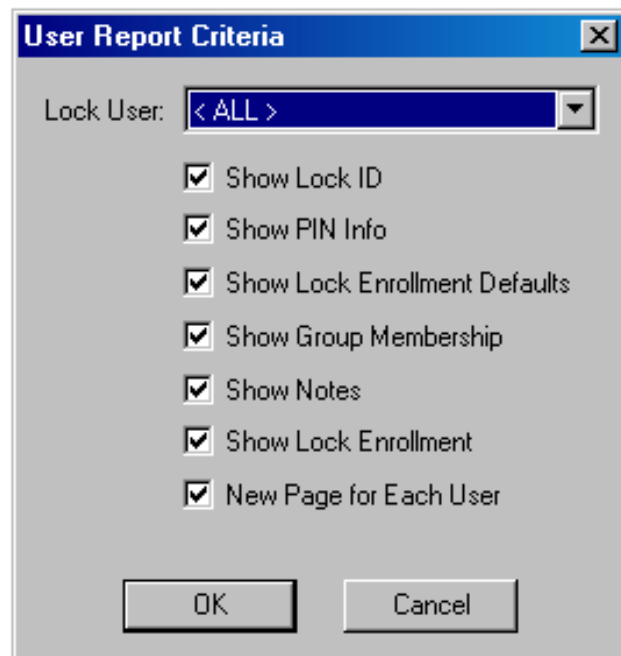
Introduction

User Reports have been designed to assist the administrator in gathering information on all the users within the facility. User reports can be tailored with numerous options in order to filter out any unwanted information. At minimum, each report will contain the first and last name of the selected user.

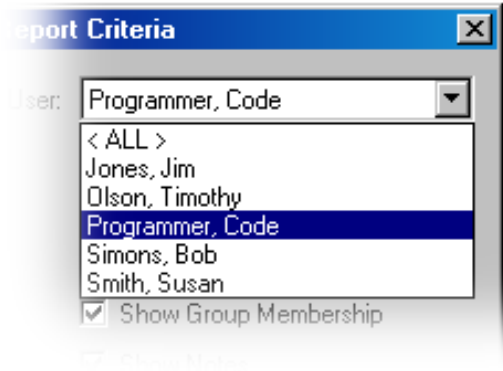
User Report Criteria

The top portion of the Criteria dialog is the "Lock User" filter. You can either display ALL users or you can select one specific user to view.

- Show Lock ID: displays the ID for that user on the report.
- Show PIN Info: Shows the current PIN for that user.
- Show Lock Enrollment Defaults: This shows the default settings for that user when he is enrolled in a lock.
- Show Group Membership: displays the current Home Group and Associate Groups.
- Show Notes: Displays the text inputted in the Contact1, Contact2, and Reference field for that User.
- Show Lock Enrollment: displays the locks that this user is currently enrolled in.
- New Page for Each User: Creates a new page for Each User.



The image to the right shows the filter being used to select only the User named "Programmer, Code." The report will now only show the information for that user and not all the users in the facility.



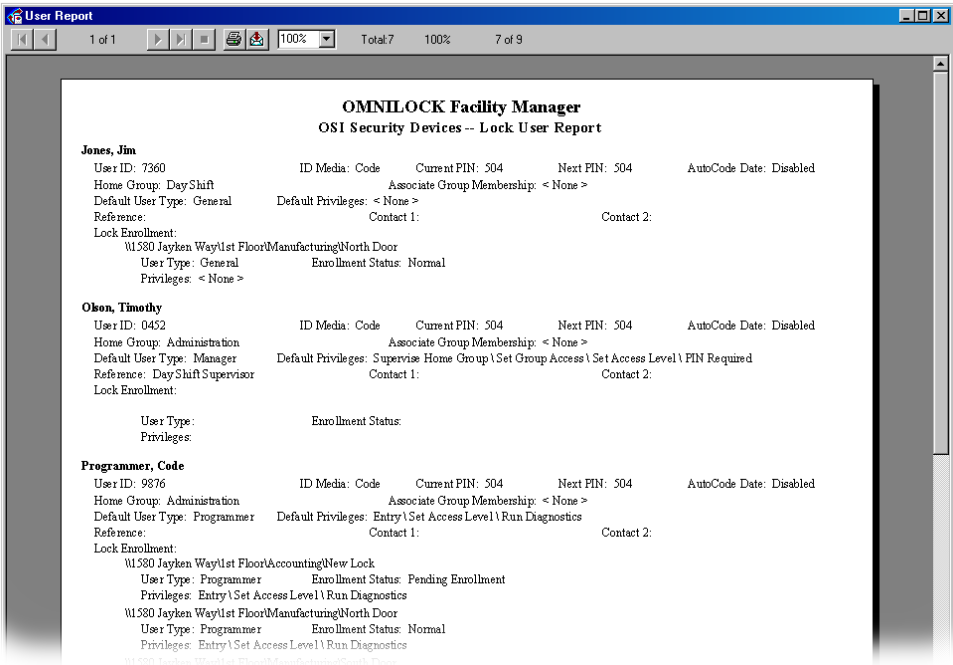
Running a User Report

User reports can be run in one of two ways:

1. Clicking on the Report Menu and select User Report.
- OR*
2. Right-clicking on the User you wish to run a report on and selecting User Report.

Once the Report Criteria dialog is displayed, use the steps below to complete the report:

1. Select the User you want to view using the filter on the top of the dialog.
2. Check or Uncheck the features you want to use on the report.
3. Click "OK."
4. The report should appear similar to the report below.



.: Chapter 6 :. Tutorial

Overview

This chapter presents a brief tour of the OMNILOCK Facility Manager software. This will lead you through the process of setting up a simple facility, including setting up groups, registering users, enrolling Locks and establishing a simple time schedule. Then you will enroll a Mobile Device (attached to a laptop or desktop PC) in the facility to transfer data to a lock you have enrolled in the system. To enroll a Mobile Device, ActiveSync must be installed on the host PC. If you install ActiveSync after the OFM has been installed, you must reinstall the OFM. The reinstallation will take two steps; first you will remove the original installation (remembering not to remove any shared files or folders), and then run Setup from the source CD to reinstall the program to properly recognize the recently installed ActiveSync. The reinstallation of the OFM will not destroy any OFM Facility databases that you have created. Of course, communication with the Locks will not be possible until ActiveSync and the Mobile Device(s) are installed.

Setting Up a Sample Facility

A tour of the OFM application begins with launching the program. The installation program will have placed a shortcut (lock) icon on your computer's desktop. Double click this icon to launch the program. Alternatively, select Programs from the Windows Start menu then select OSI Security Devices then OMNILOCK Facility Manager, if you installed the program in the default directory.

First Step, Setting Global Facility Parameters

The first step is to define some parameters that are global throughout the Facility. From the main menu click Facility, then New or click on the New Facility button to bring up a property page for the new facility that you are about to create. Type the name "Sample" for the Facility Name. With the mouse, set the desired Code ID Length, the default is 4, but we will set it to 5 by clicking once on the up arrow at the right edge of this window. The PIN length can be left at the default setting of three. The card ID parameter windows show default values with the ID data on Track 2, starting at the first character on the track. This is typical for credit cards and banking cards. Leave the "ID Issue Number at" box set on the default "Not Used". At this time you can set up to use general Facility Cards. While these cards require special programming, we can set up for a typical Facility Card now. We will use a 5-digit code: type in any 5-digit number. The facility code will often use the second field on the card, i.e., the field just after a field separator. Select Field for the Starts at window and number 2 to set up for the first field after the separator. (The field before the separator is field 1). Leave the "Expiration Starts at" box set on the default "Not Used". At this point you can change and define the "User Defined Note Fields" as necessary. Go ahead and change Contact1 to read Phone Number, Contact 2 to E-Mail, and Reference to Access Level. The last Field that we are concerned with is the "Prox Reader Config" drop down list box. If you are not going to be using Proximity you may leave this box "Not used", if you plan on using Proximity then change it to COM 1 or the appropriate COM port. If these settings are all correct, click the OK button.

Day Light Savings

The system automatically adjusts the clocks in the Locks for Daylight Savings time changes. North American is the default; you may want to try some different selections while this dialog box is up, but select North America at the end. At this point you have finished setting up the global parameters for the facility. If you want to review them, select the Back Button(s). Once Locks have been programmed, any changes to these global parameters will require reprogramming all of the Locks in the system. If you are satisfied with the settings, select Finish.

Chapter 6: Tutorial

A window will appear allowing the choice to protect the database with a password (Recommended). Click Yes. The next box requires you to type a password that is 6 to 14 characters in length; type a word you can remember, or write it down immediately. It is recommended that your password include upper case and lower case, numbers, and even special characters (\$%^&*) in your password. You will have to type it again to confirm that you typed it correctly. Do not check the box for Microsoft Access compatibility. Click OK, and you will be warned that you will not be able to open the database without the correct password. If you are satisfied with these settings, click "Yes."

Second Step, Setting Up Groups

Since users are assigned to groups, the next step is to set up the required groups and their properties. In this example, three groups of a possible eight will be defined. They are:

Group 1: Office staff, no PIN required for access to the office area.

Group 2: Cryptographers, Card and PIN required for access to the data security room.

Group 3: Service group, Card and PIN required for short-term access.

To set up the first group, click on the Group icon (the multiple human faces). The Group pane will appear with a list of the eight possible groups, all shown as <untitled>. Double click on group 1 to bring up a property page for that group. Type the name "Office Staff" in the name window. You may wish to enter a name or point of contact for this group in the Reference box. Since no PIN will be required, click OK to establish the Office Staff as group 1.

For the second group, double click on it, and enter the name "Programmers". This group requires a PIN and the PIN should auto recode, so check the Autocode box (to manually set PINs for this group leave the Autocode box unchecked). Set the recode interval to 3 months using the up arrow to the right of the number box, and the next PIN effective date to the fifteenth of the next month, then click OK.

For the third group, enter the name "Service", check the Autocode checkbox, and Recode every 2 days, with the next PIN effective date for tomorrow. Again, click OK when you are done.

Third Step, Adding Lock Users to the Database

Since a Programmer must be assigned to a lock when it is defined (created), establishing the user database is the logical third step in setting up a Facility. To bring up the User Page, click on the User icon (the single human face). To add a new user, select the "New (Wand)" icon on the toolbar, or right click on any blank area of the pane and select New. A property page will appear where you type the last and first name and, optionally, the middle initial of the new user.

The first user will be a Programmer (every lock must have at least one programmer enrolled). Type the last name, "Programmer" and the first name "Ima". A unique code ID has already been selected by the system; you can accept it or type in one of your own choosing. If you type a code ID that is already in use, a message box will inform you of this when you click the Next button and force you to try another code. Type a simple 5-digit code, such as 31416, or select the Recode button to change the code. Next is the Current PIN box. By default, the "Current PIN" box will allow you to manually change the PIN. Entering a PIN here does not mean that this user will be required to use a PIN, it is just defining what the PIN will be if you decide later to require users to use a PIN. Setting a requirement to use PINs is accomplished when setting up a schedule. Next, select Programmer from the default ID type drop down list. You will now have the choice of privileges; select Entry, Set access level, and Run Diagnostics. Do not select PIN Required. Click Next.

Group Membership

In the Home Group at the top of the page, select Home Group 1 - Office Staff. Click Next.

Lock Enrollment

Since no Locks are in the system yet, no locks will appear on this page so click Next again. Now the Notes page will allow reference information to be added to the database. This is optional; it might include a home phone number or other pertinent information. Remember that the names of these fields may be changed on the Facility Property page at any time. Click Finish to complete the user enrollment process.

The next user will be a Manager. Click on the New User (Wand) icon to open a New user page and type a name and leave the code and PIN as they are. Select Manager for the default lock ID type. Select Supervise Home Group, Set Group Access, and Set Access Level, then Next. On the Group page, this user is also an office staff member, so select Home Group 1 and no associate groups. Click Next, Next, and Finish to enroll this user.

The last user we will set up will be a General User. Click on the New User (Wand) icon to open a New user page and type a name, and select Mag Card. If you have a card reader connected inline with your keyboard port, swipe a card through it (such as the Programmer card that you received with your lock, or a bank card). Otherwise, you can type in the number encoded on the magnetic stripe (if known). With a bankcard, the number embossed on it will generally work. If there are more than 19 digits, type only the first 19. If you use your Programmer card, type 1234567890123456789. Select General for the user type and click Next. Place this user in Home Group 2 and no associate groups, Cryptographers, and step through the remaining two pages to enroll the user.

Fourth Step, Setting Up a Time Schedule

Time schedules can be very complex, but the process of setting one up can be illustrated simply; more complex schedules result from more steps like the ones we will use in this example. As usual, bring up the Time Schedule page by clicking on the Time Schedule icon (the one with the clock and schedule book) on the tool bar. Select the New (Wand) icon, or right click on the blank area and select New.

Master - The first page (Master) is for setting timing events that set the access level of the lock. Click on Monday and select the New button on the right and type an event time of 8:00 (You can use either 12 hour or 24 hour format, i.e. 4:00 PM or 16:00). Use the arrow to the right of the Access Level window to show a list of levels. Select Unlock with ID. Do not check any restrictions. Select OK. You have created the first event.

Continue Monday's schedule by adding and setting the scheduled events as shown below:

TIME	ACCESS LEVEL
8:00 AM	Unlock with ID
12:00 PM	ID Required
1:00 PM	Unlock with ID
4:00 PM	ID Required
5:00 PM	ID Required, PIN Required
10:00 PM	Lockout

Note that to set ID Required, PIN Required, you have to check the box below the Access Level window.

For the remaining weekdays, you can copy this schedule. Highlight Monday (only) and select the Copy button. Now highlight Tuesday and select Paste. Repeat the Paste for the remaining weekdays. (You only have to Copy once, as the copy remains on the clipboard until you copy another object).

For the weekend, set two events for Saturday: 08:00 –ID Required and PIN Required, and at 17:00 – Lockout. Copy this to Sunday. This completes setting the access level for the weeks. Click Next to move on to the groups.

Chapter 6: Tutorial

Group - With everyone out to lunch between 12:00 and 12:30, the office staff will not be allowed access during that period, but cryptographers will not be restricted. Highlight Monday for the Office Staff, click New and set an event time for 12:00 and select Deny Access and OK. Repeat, but set the Event Time for 12:30, and Allow Access.

As you did for the Master Access Level Events, Copy the Monday schedule to the rest of the weekdays. This completes the Group events page; click Next to advance to the Holiday page.

Holidays - For this example we will set one Holiday period. Click New to bring up a dialog box to set up the holiday period. Our holiday will be "Spring Break"; type this in the name window. The period is from March 15 to March 25; type these dates in the appropriate fields using MM/DD format. (Ex. 03/15) Set the start time to 12:01 AM and the stop time to 11:59 PM. The schedule for the holiday period will be set to be just like a weekend day. To set this, check Use Daily Schedule and select Saturday. Select OK to establish this schedule. Click Next, if you are satisfied with the holiday set up. This will bring up the lock enrollment page to allow you to enroll the schedule in Locks, but since no Locks are set up, just click Next to move on to the final page.

The final page allows you to give the entire schedule a name. In this case we will just use "General Schedule" (or you can give it another name if you wish). Click Finish to save the schedule.

Fifth Step, Enrolling a Mobile Device

These steps require that you have a Mobile Device connected and synchronized to your computer and have an established partnership through ActiveSync. Furthermore, you must have already run "Install OMNILOCK Data Link" from Programs: OSI Security Devices on the Windows Start Menu Bar (If you haven't done so do so now). In other words, your Mobile Device must be set up and ready to go. If you install ActiveSync after the OFM has been installed, you must reinstall the OFM. The reinstallation will take two steps; first you will remove the original installation (Select NO every time you are asked to remove a shared file or folder), then run Setup from the source CD to reinstall the program to properly recognize the recently installed ActiveSync. The reinstallation of the OFM will not destroy any OFM Facility databases that you have created. Of course, communication with the Locks will not be possible until ActiveSync and the Mobile Device(s) are installed and enrolled into your Facility on the Mobile Device page.

Click on the Mobile Device icon to bring up the Mobile Device page. Click on the New Device (Wand) icon or right click on the blank portion of this page and select New. The OFM will connect to the device, identify it, and enroll it automatically if it is synchronized correctly. Now your Mobile Device is enrolled. Double click on the mobile device's name that will open the Mobile Device Property page. Here you have the option of typing the name of the person to whom it is assigned in the text box. If there were any Locks enrolled at this point they could be enrolled in the device by selecting the lock Enrollment tab. Since there is none enrolled, just click OK to finish the enrollment of the device.

Sixth Step, Enrolling (Creating) Locks and Locations

Click on the lock icon to bring up the Facility Explorer. The first thing to notice about this window is that it very much resembles the appearance of the Windows Explorer program. If you are already familiar with Windows Explorer, you will quickly understand the Facility Explorer.

On the upper left corner of the left pane (under the toolbar) is an icon representing the entire facility, and it will have the name you gave the facility shown next to it (in this case "Sample"). We will add two locations under the facility.

Locations -To add a location, highlight the facility by right clicking on the icon. Right clicking the facility will bring up a menu; move the cursor to New and a sub-menu will appear. Click Location to cause a folder icon to appear on the tree below the facility with "New Location" highlighted for editing. Type in the name "Office Building" followed by the Enter key. To illustrate another way of adding a location, left click the Office Building folder icon to highlight it. Select the New Item (Wand) icon on the toolbar and select Location. A new location folder will appear under the Office Building folder; type in "Communication Division" and Enter. You now should have a tree with the Office Building under the facility, and the Communication Division under the Office Building.

Locks - Adding a lock starts the same way as adding a location. Right click the Office Building folder and select lock from the New sub-menu to bring up a property sheet for the new lock. The name “New lock” will appear highlighted for editing; type in “Main Door”, but do not press enter. The default Open Delay of three seconds (the minimum) is shown below the name; use the control to the right of this box to adjust it to 4 seconds. Next, select the button to the right of the Time Schedule text box and you will see “General Schedule”. If there were several schedules defined, all would appear as choices, but since we just have one defined, select General Schedule. The lock and battery installation dates are shown as today’s date, but they can be changed if desired. The optional fields for Serial Number and Model Number can be filled in to help keep track of the lock if desired. Click Next to move on to the User Enrollment page.

The User Enrollment page is a list box showing all the users currently enrolled in the Facility database. In a large Facility, it may be necessary to narrow the list to just a single group of users. You may do this by selecting a group from the User Group drop down list. A much shorter list of users will now be displayed. Select User Group 2 – Cryptographers and only one name should appear as this is the only user enrolled in this group at this time. After doing this, select All Groups. We will enroll all the users in the Main Door. Simply click each user and the Enroll button (the standard Windows Control-click and Shift-click selection extensions also work). Click Finish when the selection is complete.

A selection box will appear to allow you to select a Mobile Device to be assigned to program the lock. The box will initially show <None>, but selecting the button on the right will bring up a list of devices enrolled in the OFM. Since we have only enrolled one, select it as the Mobile Device partner for the lock. Select OK to save the lock enrollment in the database.

We will now add a new lock to the Communication Division. To save steps, right click on the Main Door lock you have just created and select Copy. Now right click on the Communication Division folder icon and select Paste lock. As before, the property sheet for that lock appears. You still have to give it a name (“Code Room”), but you will notice that the open delay is already set to 4 seconds and that the General Schedule has already been selected. You can edit these items if you want, but you don’t have to. Click Next and you will see that all the users are already enrolled. If you want to add or remove a user you can do so at this time, but for this simple example, we will just click Finish to move on to the Mobile Device enrollment, which also has been copied. Click OK and you have completed the enrollment of the Code Room lock in the facility database. At this point, the Sample Facility has been set up and you are almost ready to program the Locks.

Transferring Data to the Locks

Transferring Current Data to the Mobile Device

At this stage, you would normally update the Locks in the system. This section will go through the procedure, but you may not want to actually carry out the transfer, as you will ultimately have to remove any Locks you have programmed from their doors and lightly press the reset button on the lock (until you the green light flashes) in order to use them as new Locks in a real facility. If they are not already mounted, this might not be too much trouble. A Programmer may also reset a lock without removing it from the door by running Diagnostics and selecting “Upgrade OS”, even if the new OS is the same version as is currently in the lock microprocessor. This will return the lock to a factory default condition.

Data Exchange - With the Mobile Device connected and synchronized; select the Data Exchange icon (the lightning bolt). After a short delay while various updates occur, a tree view of Locks requiring programming will be displayed. Click on a lock and then click on the Select button; repeat for each of the Locks shown. After you have selected the Locks to program, click on the Program button to transfer data to the Mobile Device. When the data exchange is complete, the Mobile Device is ready to transfer programming data to the selected Locks.

Exchanging Data With the Locks

From the Start menu on the Mobile Device, select OMNILOCK Data Link. You will see that two Locks are pending, and a list will show you their names and locations. Go to the first lock to be programmed and point the IR port of the Mobile Device at the lock's IR window (it's just above the handle). Then enter the default Programmer code of 1-2-3-4, or use the default Programmer Card to activate the lock. The Mobile Device will present a split view of the Facility Explorer with the locations and Locks to program. On the lower half of the screen, using the stylus, select the location for the lock then select the lock itself. The name of the lock and its location should now appear in the text box on the bottom of the screen; when it does, press OK. Note: Make sure that the lock that you selected is the correct one before pressing OK, otherwise you will have to reset the lock and refresh the lock data in the OFM and perform another data exchange.

A message window will appear and after a brief period a progress bar will indicate that programming is active. At the end, a message box will indicate that programming has been completed. Press OK on the message box. You can now go to the next lock and program it the same way. When you are finished, be sure to exit out of the OMNILOCK Data Link (by pressing the "X" at the upper right hand corner of the window). If you do not exit, the connection to the computer will fail. If you forget, just disconnect the Mobile Device from its docking station or serial cable, exit from the OMNILOCK Data Link (ODL) program on the Mobile Device and replace the Mobile Device in the dock.

Updating the OFM

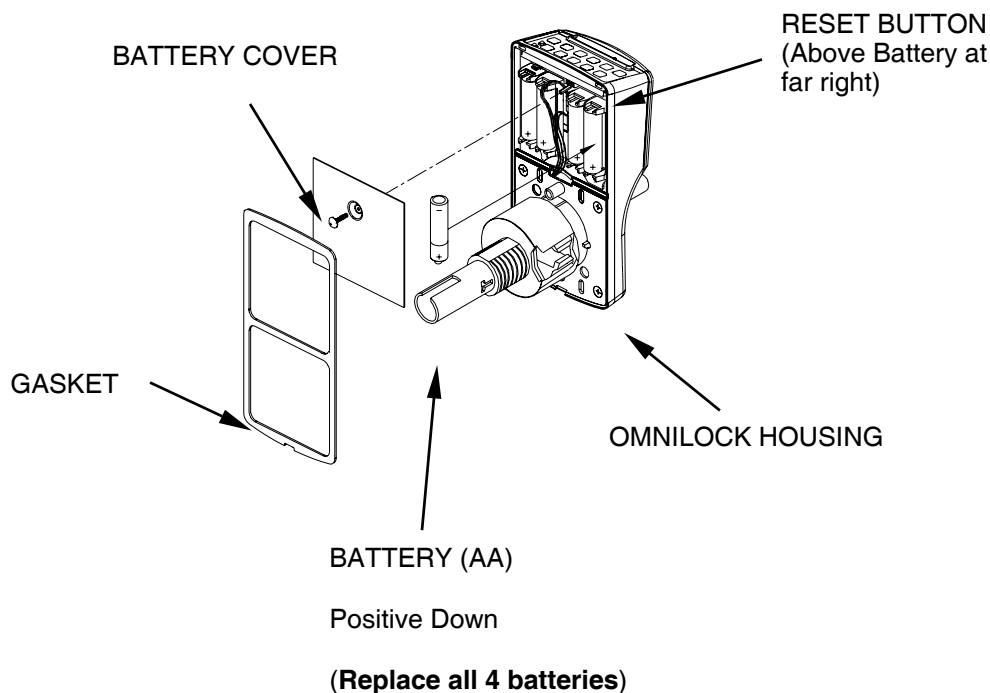
After exchanging data between the Mobile Device and the locks and exiting the ODL program, connect the Mobile Device to the PC and allow them to synchronize. On the OFM screen, select the Data Exchange icon (Lightning Bolt). A screen will appear showing any locks that are pending programming. Select Cancel to bypass this screen and the OFM will be updated with the collected data. On the Mobile Device page the Data Exchange Status should be CURRENT. In the lock Property page click on the Status Tab and verify the Data Exchange status is CURRENT. If it reads "Pending Collection" then the system is telling you that the lock may have information for collection and you will need to visit the lock in question and perform a Data Exchange at the lock and upon returning to the OFM before the system will go Current. If the status reads "Pending Update" then you need to update the lock in question by performing a Data Exchange in the OFM (remembering to select & program the locks requiring updating) then visiting and programming the lock and return to the OFM and perform the data exchange before all will be current.

.: Chapter 7 .: Maintenance

Lock Maintenance

Battery Replacement

Battery replacement will be required when the voltage of the batteries indicates that long term continued operation would not be possible. When the battery level falls below 4.3 Volts, establishing an Infrared connection with your Mobile Device may not be possible. When an IR connection is made, the Mobile Device screen will indicate that replacement is required. The OFM will show the battery level under the lock status tab. When replacement is first indicated, approximately 1000 operations will be possible, so that replacement can be timely but it doesn't have to be on an emergency basis. If the batteries are not replaced in due time, however, the lock will enter Shutdown, and only the Programmer will have access. This reduces the possibility of total battery failure and resultant loss of programming information and audit data.



To replace the batteries in non-weatherized units, the electronics module must be removed from the door and the battery cover removed by unscrewing the screw in the center of the battery cover. For weatherized units, remove the cover from the electronics module on the protected side of the door. If each cell is removed singly and its replacement installed, so that only one cell is absent at any time, the data in the memory will be preserved. All Batteries need to be replaced with Alkaline type. Use Of Lithium type batteries will not only void the warranty, it will also nullify the UL listing on the lockset.

Note: You must replace the batteries from Left to Right and one at a time.

Normally the batteries should be replaced soon after the red indicator starts to flash twice after the green entry indication. However, if allowed to discharge after this indication for well over a thousand entries, the battery level will be low enough to force the lock into Shutdown access level. It will still respond to the Programmer code, thus entry can be gained so that the batteries can be exchanged. Note: After the new batteries have been installed, the Programmer must reset the access level to the desired level using the Mobile Device.

Chapter 7: Maintenance

Resetting the Lock

If the batteries are completely dead, or if they have been removed altogether, the memory contents will be lost. In this case, after replacing the batteries, you will have to reset the lock. Here's how:

1. Remove the battery cover from the lock.
2. Ensure the motor or relay cable is connected to the electronics module. If this is a mortise lock, you must have the mortise chassis plugged into the electronics module.
3. In the top right corner of the board is a small button. Gently press and hold the button for about three to five seconds until you observe on Green flash.
4. Release the button.
5. After a few seconds you may hear the lock cycle the motor a few times. If it is a Wall Mount, there may be no sound, but perhaps one soft click.
6. The lock will now flash Five times immediately following the cycles. They should ALL be Green flashes. If you receive a Red flash at any time, refer to the table below for troubleshooting.

Red Flash	Component Tested	Resolution
1	Memory	Return to Factory for repair.
2	Clock	Return to Factory for repair.
3	Drive Status	Check Motor Connection. Lock Chassis must be connected during reset. Check wires thoroughly for any pinches or breaks.
4	Drive Polarity	Check that the Drive wires are plugged in correctly. Red with Red and Black with Black.
5	Battery Level	Replace Batteries with New Batteries.

Magnetic Read Head Cleaning

From time to time, the card reading head should be cleaned. The frequency of cleaning will depend on the cleanliness of the environment and the frequency of use. After some experience, you will learn how long the lock can go before the build up of a dirt film begins to interfere with accurate reading of the card data. To clean the head, use a special cleaning card. These have a solvent impregnated surface that will remove most films. Simply slide the card in and out a few times to clean the head, with a fresh area of the cleaning surface facing the keypad. Magnetic Head Cleaning Cards are available from OSI Security Devices, order part number 11071.

Running Diagnostics

All 2000 Series locks have onboard diagnostics capabilities. These diagnostic capabilities include:

- Drive Tests
- Keypad Tests

Other features of the Diagnostics include”

- LOS Update capability
- Audit Log Collection

To do this, you will need your Pocket PC and an enrolled Programmer ID.

1. At the lock, start the OmniLink program.
2. Select Lock.
3. Select Diagnostics.
4. Enter the Programmer Card or Code. The Diagnostics information will be loaded and displayed.
5. Tap Drive Test to run the Motor or Relay. You should hear the drive actuate approximately 5 times.
6. Tap Audit Log and the Pocket PC will collect all Audit information still contained in the lock.



7. Tap Test Keypad in order to begin the keypad test. Once it starts, you can press any button on the lock and the corresponding button on the Pocket PC display should "illuminate."
8. Tap "End Test" when finished.
9. Tap Refresh to re-display the lock information on the screen.
10. Tap Log Off when finished.



Lubrication

In normal environments, the lock will give many years of service without additional lubrication. Lubrication Kits are available from OSI Security Devices, order part number 10277.

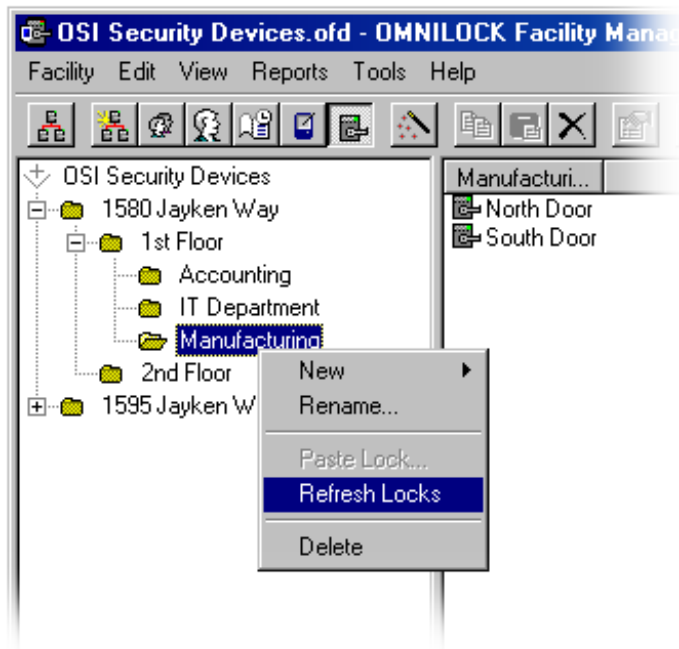
Refreshing a Lock

Refreshing a lock is the process of telling the database that you need to reprogram the lock. This could be because you have a replacement lock, or the lock has lost power and you need to reprogram it. In whatever the case may be, refreshing a lock is only done in emergency situations. Only refresh a lock if the lock is **not** working at all. If you constantly refresh the lock, you will be losing valuable audit data on the lock.

Chapter 7: Maintenance

To refresh a lock, follow these steps:

1. Open your database.
2. Navigate to the lock you want to refresh.
3. If you want to refresh a group of locks, you will need to navigate to the upper most location of those locks.
(i.e. Manufacturing)
4. Right-click the location or lock and select Refresh.
5. A warning will be displayed about refreshing the locks. Simply click "Yes" if you are sure you want to Refresh.



Pocket PC Maintenance

In most cases, your Pocket PC will have come with a cradle. This cradle will usually continuously charge the battery while it is in place. If you did not get a cradle, you will have received a sync cable and a charging cable. When the battery reaches a full charge, the Pocket PC will internally "disconnect" itself so as not to overcharge the battery. This is a safety feature that can become a nuisance if you do not use the Pocket PC on a regular basis., as the Pocket PC will discharge completely while connected.

It is HIGHLY recommended that if you do not program the locks on a daily basis, that you at least disconnect and reconnect your Pocket PC to ensure that the battery remains fully charged. Failure to do so, will result in the Pocket PC becoming discharged on its own.

The battery of the Mobile Device should be kept charged at all times, otherwise data can be lost. If the device becomes discharged to the point where its memory is lost, it will lose its identity within the system. If this happens, you must download the ODL program again and refresh the device as described below.

Refreshing the Pocket PC

If a Mobile Device has been lost, damaged or has lost its data (for example, both the main and backup batteries have discharged), the OFM will no longer recognize it. You must, therefore, re-establish the partnership with your database and the Mobile Device. There are three steps involved.

1. Re-establish a new ActiveSync Partnership. (See Installing ActiveSync on Page 17)
2. Re-install the OmniLink Application to the Pocket PC. (See Installing the Omnilock Facility Manager and OmniLink on Page 18)
3. Refresh the Mobile Device with your Database.

There are times when a Data Exchange is not going accordingly. If you are experiencing problems retrieving information from your Pocket PC or downloading to it, there may be a case where the database on the Pocket PC is corrupt. You will have to refresh the Pocket PC using the steps below.

To Refresh the Pocket PC with your database, follow the steps below:

1. Select View > Mobile Devices.
2. Right click the currently listed Pocket PC.
3. Select Refresh.
4. Click Ok on the Mobile Device Properties dialog.
5. Select Yes to Update Device Directory Now.

Database Maintenance

The database for a Facility contains all the information pertinent to that facility. As such, it grows continuously with each audit record returned from the lock. In addition, this type of database will grow as changes are made, because the database engine does not automatically “fill in the holes” left by the removal of obsolete data. Eventually, it may take up more disk space than is convenient on your desktop computer. Furthermore, the database can be corrupted, for example, by a power failure occurring when a critical action is in process. The OFM provides for this with utilities that attempt to repair the database, compact the database, and allow for you to select stale audit data for removal.

Before using these tools, a backup copy of the database should be made. If you want to keep audit data for an extended period, but don't want to waste the space on your hard drive, you should keep the backup copy for as long as you want to have the audit records saved. You can then remove all the audit records up to a convenient past date.

To compact the database, select Facility, and Compact from the Facility menu. A dialog box will appear giving you the choice of purging or not purging old audit data. If you choose the Purge button, you should enter the date for which you want the more recent audit records retained. To prevent data loss if the compaction process should fail, the process creates a backup file with the Facility name, but with the extension .old. After you are satisfied that the compacted database is functional, you can delete this .old file to save disk space.

Since the file has changed during the compaction process, it must be reloaded into the OFM. The OFM will present you with a request for a password if the database was password protected, in order to start loading.

Backing Up the Database

By default, the database files are located in the Facilities folder of the installation directory. If you have chosen the default choices at the time of installation, it will be found in:

“C:\Program Files\OSI Security Devices\OMNILOCK Facility Manager\Facilities”

The database file will have the form (name of your facility).ofd (i.e., Blue Sky Tower.ofd).

Of course, you can use the Windows Find utility to locate the file; just set it to find “*.ofd”. The database files have the extension “.ofd”. These files can be copied to any suitable backup media such as a floppy disk, Zip[®] drive, tape drive or CD depending on the configuration of your PC. Follow the instructions that came with your PC for copying files. Be sure that the storage media has sufficient capacity to accept the file. Prudence would dictate that backups should be created at regular and frequent intervals and should be handled and stored in accordance with security procedures.

Disaster Recovery

In case of a major PC failure, such as a hard drive failure; return the PC to service in accordance with the PC manufacturer's instructions. If you have a system backup for restoring your programs and data, you should use it. Otherwise, you will have to install your programs using the original media. You may then copy the current backup file of your OFM database to the Facilities folder on your PC. Of course, any data that had been entered into the database between the time the last backup was made and the time of the Failure may have been lost.

The Lock Operating System (LOS)

Lock Operating System (LOS) replacement is not a periodic maintenance item. You should only replace the lock operating system for a good reason. The most obvious reason for replacement is that a newer version has been made available by OSI Security Devices offering improved performance or features. The steps that must be followed to replace the operating system must be followed carefully, as you need to be sure that you really have the desired operating system in place when you are done.

Replacing the LOS will destroy all audit data and programming information in the lock; i.e. the lock will be "new" after LOS replacement. Therefore, you should be sure to collect the audit information prior to replacing the LOS. When you have finished replacing the LOS, you can refresh the lock to restore all of the programming information. The audit trail in the lock will, of course, begin from the point at which the lock is reprogrammed.

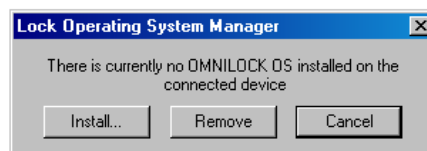
Upgrading the LOS

To Upgrade (or update) the LOS in your lock, follow the instructions below:

1. Open your database (facility)
2. Go to the Tools menu on the top of the OFM screen and select Lock OS Manager.

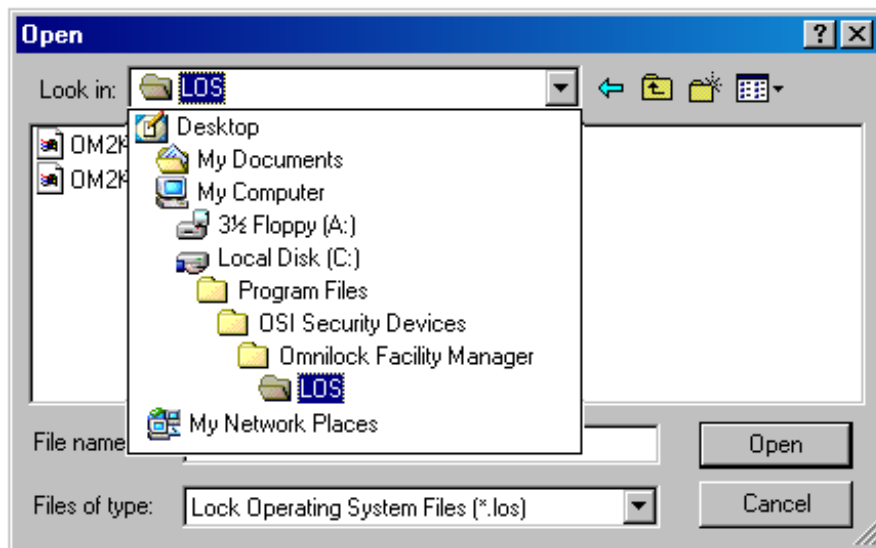


Note: At this point the pop-up menu should tell you which LOS (if any) is loaded on the Mobile device.



3. Select Install.
4. Navigate through the directories and select the LOS you wish to upgrade to. By default, all the LOS files are located in the following directory:

C:\Program files\OSI Security Devices\Omnilock Facility Manager\LOS



5. Double-click the LOS you wish to install. The OFM should automatically begin uploading it into the Pocket PC.
6. Up-load time into the mobile device ranges from 3-15 minutes depending on file size and the connection. Simply click "OK" when installation is complete.

7. Click on the View Menu

8. Select Facility Explorer..

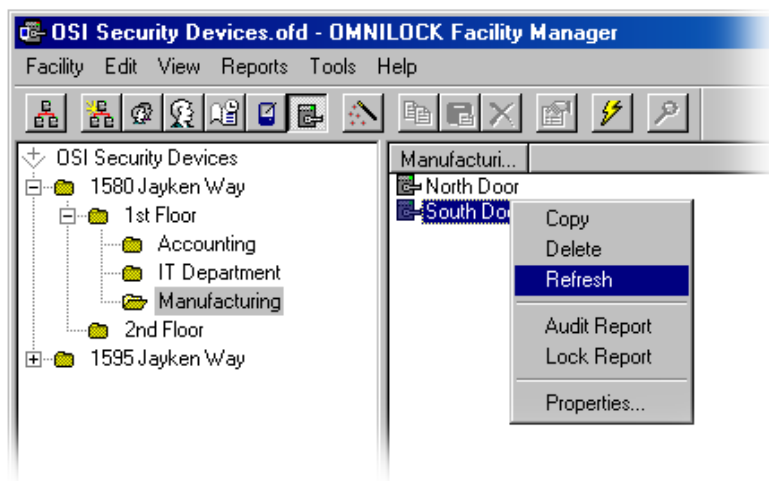
9. Right-click each lock you wish to upgrade and select Refresh.

10. Click "Yes" to the warning about refreshing the lock.

11. Press the lightening bolt to begin the Data Exchange Process.

12. Complete the Data Exchange with your computer and ensure that all the necessary locks are pending on your Pocket PC.

13. It is now time to visit the locks.



IMPORTANT: DO NOT log on or enter any codes or cards until you have completed steps 14 through 20!!

Chapter 7: Maintenance

14. At the lock, start the OmniLink program.
15. Select Lock.
16. Select Diagnostics.
17. Enter the Programmer Card or Code. The Diagnostics information will be loaded and displayed.
18. On the diagnostics screen select "Upgrade OS."
19. Select "Yes" when prompted if you want to replace the current LOS.
20. Upgrading the LOS at the lock will take 45-60 seconds. If successful the lock will be automatically reset in order to load the new LOS. All codes will be erased and the factory default code of 1234 will be reactivated.
21. Close the Diagnostics screen.
22. Enter 1234 into the keypad of the lock. You should be prompted to select the lock you want to program.
23. Highlight the lock at the bottom of the screen and tap "Ok."
24. Test and verify any codes or cards and functionality of the lockset.



.: Chapter 8 :. Help!!

Troubleshooting Tips

The following table lists some common problems and the associated remedies for the Omnilock. Please read through these problems carefully prior to contacting technical support.

Lock Troubleshooting

Indication	Possible Problem	Resolution
Lock flashes Red and Green simultaneously with every button and card.	Lock was not reset properly.	Remove the lock from the door and follow the reset procedures in the maintenance section of this manual.
Lock alternately flashes Red-Green-Red-Green with all IDs.	Motor Failure	Check for pinched or damaged wires. Verify that battery cable is connected properly. Red and black wires should match up to red and black connector.
Lock does not respond when any ID is introduced.	Lock is in Anti-Tamper.	Wait 10 seconds, press the CL key. Use a valid Programmer ID. If an invalid ID is used, the lock will return to Anti-Tamper.
	Lock does not have power or lock is "hung up" due to short in system.	Check batteries are in place. Check for pinched or damaged wires. Hit reset button and then press Default Code 1234.
Lock flashed Green-Green when card or code is introduced, but does not open.	Lock requires a PIN	Either the ID you are using requires a PIN or the lock is in a PIN Required state. You must use that ID + PIN. If your ID is a Code, then you must use the Code ID in addition to the PIN.
Lock flashes Green, but does not open. OR Lock is Unlocked at all times and it is NOT in the Unlocked Access Level.	Possible broken drive spring.	Return to factory for servicing.
	Internal drive mechanism is binding.	Remove lock and inspect installation. If no fault found, return to factory for servicing.
	No power being sent to electrified hardware. WALL MOUNT SYSTEMS ONLY	Have an electrician verify that power is coming out of the power supply. Test strike by applying power directly to strike, thus bypassing the Omnilock altogether.

Chapter 8: Help!!

Indication	Possible Problem	Resolution
	Power sent to motor is insufficient.	Check for pinched or damaged wires. Check or Replace batteries.
Lock flashes Green-Green-Green and remains unlocked. It will not relock.	The lock is the Unlocked Access Level.	You must change the lock to ID Required if you want it to relock during operation.
Lock flashes Red with some General User IDs, but not all.	ID is not enrolled in the lock	Verify that the User ID you are attempting to use is enrolled in the system. Verify the User ID is enrolled into the lock. You can double-click the User ID and click "Lock Enrollment" to check this.
	Necessary Groups are not Enabled	Verify that all necessary Groups are enabled with either the Pocket PC or by using a Manager who has Group Access Privileges.
Lock flashes Red with my General Users, but not my Managers or Programmers.	Lock is in Lockout.	Lockout only allows Manager IDs and Programmer IDs to gain access. Change the Access Level to ID Required to allow General User IDs to gain entry.
Lock flashes Red with all other IDs except for Programmer IDs.	Lock is in Shutdown	You must use the Programmer ID and the Pocket PC to take the Access Level out of Shutdown.
Lock flashes Green, but sometimes it does not unlock. Sometimes it does.	Low power	Lock may need the batteries replaced. For some reason the system is unable to recognize the batteries are low.
	Faulty connection with chassis.	Lock should be inspected thoroughly for good connections. It may be necessary to return the lock to the factory for servicing.

OmniLink Troubleshooting

Indication	Possible Problem	Resolution
I get the error "Unable to Open IR Serial Port" when starting the OmniLink program.	OBEX services are not disabled.	You must disable the Beam setting on the Pocket PC. On your Pocket PC, go to Start > Settings > Connections > Beam and uncheck "Receive all Incoming Beams."

Indication	Possible Problem	Resolution
	Infrared may have malfunctioned on Pocket PC.	Perform a soft reset with your Pocket PC in accordance with the User Manual for that Pocket PC. This is usually a small button on the back, side or bottom of the Pocket PC.
	OmniLink software is incompatible with your Pocket PC	Contact Technical support to get the latest version of software.
	No Infrared on the Pocket PC	You must use a Pocket PC that has a usable IR Port.
I get the error "Unable to Open Facility Directory."	Pocket PC has not been enrolled in to the database.	Refresh the Pocket PC with your database or enroll the Pocket PC into your database.
Pocket PC says "Invalid Logon: Connection Terminated" every time I try to connect with the Omnilock. (continued on next page.)	Pocket PC is not enrolled into that database.	You must use a Pocket PC that is enrolled into the database that the particular lock is a part of. You can not use your Pocket PC to log onto someone else's locks.
	Pocket PC is not enrolled into that lock.	You must ensure that your Pocket PC is enrolled in the lock. Double-click the Pocket PC in your database and check the Lock Enrollment Tab.
Pocket PC says "Logging On..." but never finishes connecting.	Infrared may have malfunctioned on Pocket PC.	Perform a soft reset with your Pocket PC in accordance with the User Manual for that Pocket PC. This is usually a small button on the back, side or bottom of the Pocket PC.
	Alignment of Pocket PC is not stable.	You must hold the Pocket PC 6-8" away from the lock and you cannot move it. Moving the Pocket PC around will cause the connection to become unstable and fail.
	Infrared on lock has failed.	Lock must be returned to factory for servicing or main circuit board must be replaced.

Chapter 8: Help!!

Indication	Possible Problem	Resolution
<p>Pocket PC still says 0 locks pending even after I just downloaded information from the OFM.</p>	<p>OmniLink was running during download.</p>	<p>You cannot have the OmniLink application running on the Pocket PC while downloading to it. It will not refresh otherwise.</p> <p>Try closing and reopening the OmniLink Program. If that does not work, try performing a soft reset with your Pocket PC in accordance with the User Manual for that Pocket PC. This is usually a small button on the back, side or bottom of the Pocket PC.</p> <p>If still unsuccessful, you may have to re-download the information with the OmniLink program closed.</p>
<p>Pocket PC does not log onto the lock. I tried aligning it with varying distances, still nothing.</p>	<p>Infrared may have malfunctioned on Pocket PC.</p>	<p>Perform a soft reset with your Pocket PC in accordance with the User Manual for that Pocket PC. This is usually a small button on the back, side or bottom of the Pocket PC.</p>
	<p>OmniLink software is incompatible with your Pocket PC</p>	<p>Contact Technical support to get the latest version of software.</p>
<p>Pocket PC logs on as "Guest"</p>	<p>Lock ID has been lost.</p>	<p>This is an error that usually occurs from older version of the OFM. On versions prior to 1.25, compacting the database would cause some locks to lose their ID. This is an ID that is set automatically and never seen by the administrator. Best solution is to reset the lock and reprogram.</p>
<p>Facility Explorer on the Pocket PC will not let me select a lock to program. It just says Data Exchange Complete.</p>	<p>Facility Explorer is used when trying to program the lock.</p>	<p>You do not use the Facility explorer on the Pocket PC to program. Close the Facility Explorer. Program the lock with the OSI screen. You will be prompted to select a lock from this point on.</p>
<p>OmniLink program is no longer on the Pocket PC.</p>	<p>Pocket PC may have lost power completely or lost its memory.</p>	<p>See Refreshing the Pocket PC instructions in this manual.</p>

Indication	Possible Problem	Resolution
I programmed the lock, but it seems to do random things. Not what I told it to do.	Incorrect version of the OmniLink for your Pocket PC.	Pocket PCs with Windows Mobile 2002 or previous have a different version of OmniLink than those with Windows Mobile 2003 or later. Contact OSI to ensure you have the correct version for your Pocket PC.
Lock will sometimes accept cards, but sometimes won't. All codes work fine.	Magnetic Reader head is dirty.	Review the Lock Maintenance section of this manual.

Omnilock Facility Manager Troubleshooting

Indication	Possible Problem	Resolution
"Failed to establish Connection" Error	Active Sync displays "Not Connected."	<p>The OFM communicates with your Pocket PC through Active Sync. If Active Sync does not say connected, then the OFM will not be able to connect to the Pocket PC. Ensure you establish a connection with ActiveSync by checking all cables.</p> <p>Try disconnecting and reconnecting your Pocket PC as well.</p> <p>For more troubleshooting of ActiveSync, contact the manufacturer of the Pocket PC.</p>
	ActiveSync says Guest.	Your Pocket PC must be connected through a Partnership. If it says guest, disconnect it, reset it, and reconnect it. Then set up a partnership when prompted.
	Bad installation of ActiveSync	Even if ActiveSync says connected, a faulty connection. Reinstall ActiveSync.
"Unable to find Partnership Information" Error	ActiveSync says Guest.	Your Pocket PC must be connected through a Partnership. If it says guest, disconnect it, reset it, and reconnect it. Then set up a partnership when prompted.

Chapter 8: Help!!

Indication	Possible Problem	Resolution
“Connected Mobile Device is not Enrolled in this Facility” error	Pocket PC is not enrolled in the open facility.	Your Pocket PC must be enrolled in the database. If this is a new Pocket PC, or it had lost power, you must Refresh the Pocket PC or Enroll it into the database.
“Unable to Create Report” error	Registry Entries for Reports are not accessible.	<p>For OFM versions of 1.21 or prior, you must have Administrative privileges on the PC in order to run reports. OSI always recommends upgrading to the latest version of the OFM.</p> <p>For later versions of the OFM you must have certain registry entries under your profile. Contact OSI Technical Support for help with this.</p>
“Unable to Open Database”	Currently installed Crystal Report libraries are incompatible with the OFM.	The OFM uses Crystal Reports v7 to generate reports. If you have another application that uses Crystal Reports in some fashion, the libraries that are installed by that application are incompatible with the OFM. We recommend you install the OFM or that application on a separate machine.
<p>“Locks at location locks not found”</p> <p>OR</p> <p>“Users at location Users not found”</p>	Currently installed Crystal Report libraries are incompatible with the OFM.	The OFM uses Crystal Reports v7 to generate reports. If you have another application that uses Crystal Reports in some fashion, the libraries that are installed by that application are incompatible with the OFM. We recommend you install the OFM or that application on a separate machine.
“No audit data found for specified criteria.”	No Audit data has ever been collected from lock.	You must collect audit from the lock prior to running a report.
	There is no audit for the criteria you specified in the audit log criteria dialog.	Check the Date and Time settings of the criteria dialog again. Make sure they are correct.
“You must enroll at least one Programmer”	There are no programmers enrolled in the lock.	All locks must have at LEAST one programmer enrolled in the lock, otherwise, you will never be able to make changes to the lock.

Indication	Possible Problem	Resolution
“Unable to remove [User name]. User is last remaining enrolled programmer ID in lock”	This is the last programmer in the lock.	You must either enroll a new programmer into the lock prior to removing the old, or leave the programmer in the lock.
“Unrecognized Database Format”	OFM version is older than database version.	Make sure you are running the latest version of software. Contact OSI to obtain the latest.
“Error updating Database”	OFM has internal error.	Close the OFM and restart.
“Prox Reader COM Port failed to open. Please select a different Port.”	The Prox Reader Config setting on the Facility Properties is invalid.	Try a different setting under the Facility Properties.
	Prox Reader is not connected correctly.	Check the proximity enrollment reader to ensure that all cables are connected. If you are using a serial type reader, BOTH connectors must be connected.
	Software is incompatible with connected pcProx.	Check that you have the latest version of software. Contact Technical Support to obtain the latest version.
“A sharing violation occurred while Accessing [<i>database filename and path</i>]”	Database is already open	<p>Check your task bar to see if you already have the OFM open. Likewise, you can close all your programs and try reopening just to be sure.</p> <p>Also, if the database is on a shared drive, someone else may have the database open on another computer.</p>
	OFM crashed and left database open.	Restart your computer and try to open again.
	The database is Read-Only.	<p>Check the file to make sure it is not read only.</p> <p>If it is on a shared drive, make sure you have proper rights security privileges. You may need to contact your IT department for help with this.</p>
	The database is on a CD or some other media that is not “Write” enabled.	You must either copy the database to another media that is “Write” enable or disable the “Read-Only” portion of the media.

Chapter 8: Help!!

Indication	Possible Problem	Resolution
“Unable to find last used facility. [Database filename and path.]”	The database has been deleted, moved, or renamed.	This is a general error. If the database has been moved or renamed, you must re-open it directly by clicking Facility then Open. Point the OFM to the new location or the new facility database. If it has been deleted, you can ignore the error and create a new database.
“Unhandled Error loading facility Directory.”	Database name that was used to create database is too long.	You must recreate database with a shorter name.
“The Field is too small to accept the amount of data you attempted to add. Try inserting or pasting less data.”	The facility name you chose is too long.	Limit the database name to 32 characters or less, including spaces.

Miscellaneous Troubleshooting

Indication	Possible Problem	Resolution
My Pocket PC has lost all power. How do I reestablish the database connection?	Pocket PC must be Refreshed.	Review the Pocket PC Maintenance section of this manual.
I accidentally deleted my database. What do I do?	Lost database.	If you have a backup, use the backup instead. If you do not have a backup, all your locks must be removed and reset. You will have to recreate the entire database and all Users. Review the database maintenance section to prevent this from happening.
I forgot my password for my database. What do I do?	Database is locked out.	You must contact OSI. We have the means of unlocking secured databases. A fee may be incurred for cracking end user databases.
My Prox Enrollment Reader light does not turn on. OR My Magnetic Card Enrollment reader light does not turn on.	Reader is not plugged in. Faulty Reader	Check all cable connections to ensure all cables to the reader have a proper connection. Reader must be sent to OSI for evaluation.

Customer Service / Technical Support

If you wish to return material for credit, contact the dealer from whom you purchased the product, otherwise, our Customer Support staff is available Monday through Friday 7:00 AM to 5:00 PM, Pacific time. Contact Customer Service concerning product pricing, availability and order status. Contact Technical Support concerning technical problems and repairs. If you have not previously registered your OM2000 Software with OSI Security Devices, have the ID Number from your Installation CD available when you call for service. They can be reached by:

Calling our corporate telephone number: (619) 628-1000

Corresponding by E-mail: techsupport@omnilock.com

Warranty Service

OSI Security Devices will service any product we sell when you return it to the factory complete, free and clear of all liens and encumbrances. You must prepay transportation and accompany the product by an RMA Number. For warranty service on products that have not been registered with our Customer Service Department, include your sales receipt or other documentary proof of when you bought your OMNILOCK product. If the product requires warranty related service, we will repair or replace it and return it to you, shipping prepaid.



Important!

If we find no faults with the product sent to us for warranty service, we reserve the right to charge a diagnostic fee and handling fee. Also, we will charge for repairing all damage not covered by the Limited Warranty.

Out-of-Warranty Service

We handle out-of-warranty repairs or replacement similar to the manner for warranty service. In this case, there will be a charge for parts, labor and return shipping costs.

Return Material Authorization (RMA)

Before you return any product to OSI Security Devices for any reason, you must first get a Return Material Authorization (RMA) number.

To get an RMA number, call Technical Support and describe the problem. If we determine your System needs to be returned to us for repair, we will give you an RMA number. **Please mark this number clearly on the outside of your shipping package.** You can also help by marking the RMA number on a tag and attaching it to the System.

BE SURE TO INCLUDE THE KEY FOR THE LOCK OR ADDITIONAL CHARGES MAY BE APPLIED FOR LOCKSMITH SERVICES.

Limited Warranty

OSI Security Devices ("OSI") warrants the products manufactured by it (the "Product") to be free of defects in material and workmanship for a period of **ONE YEAR (the "Warranty Period")** from the date of original purchase. Only units specified as weatherized are warranted for outside use. If ownership of the Product is transferred, the warranty is automatically transferred to the new owner and remains in effect for the balance of the Warranty Period. During the Warranty Period OSI shall, at its option, repair or replace, free of charge, any Product or part thereof found, upon OSI's inspection, to be defective. OSI is not responsible for warranty service should the Product fail to be properly maintained or fail to function properly as a result of accident, misuse, abuse, vandalism, disassembly, modification, improper installation, corrosion, ordinary wear and tear or neglect or damage caused by natural disasters such as, but not limited to, fire, flood, earthquake, and lightning. Batteries (and damage caused by the batteries) are not covered by this warranty. Consult with the battery manufacturer about battery and battery leakage warranties. Postage, insurance, and/or shipping costs incurred in presenting the Product for warranty service are your responsibility. If claimed defect cannot be identified or reproduced in service, you may ① be held responsible for costs incurred.

Products are sold on the basis of specifications applicable at the time of manufacture. OSI shall have no obligation to modify or update the Product once sold.

THE WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER EXPRESSED WARRANTIES AND, UNLESS STATED HEREIN, ANY STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR FIRM ARE VOID. THE DURATION OF ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ON THE PRODUCT SHALL BE LIMITED TO THE DURATION OF THE EXPRESSED WARRANTY SET FORTH ABOVE. EXCEPT AS PROVIDED IN THIS WRITTEN WARRANTY, NEITHER OSI SECURITY DEVICES NOR ITS AFFILIATES SHALL BE LIABLE FOR ANY LOSS, INCONVENIENCE, OR DAMAGE, INCLUDING DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR INABILITY TO USE THE PRODUCT, WHETHER RESULTING FROM BREACH OF WARRANTY OR ANY OTHER LEGAL THEORY, AND ALL OTHER IMPLIED AND EXPRESS WARRANTIES, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND AGAINST INFRINGEMENT, ARE EXPRESSLY DISCLAIMED.

Some states do not allow limitations on how long an implied warranty lasts and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitations and exclusions may not apply to you.

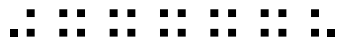
This warranty gives you specific rights and you may also have other rights that vary from state to state, province to province, or country to country.



NOTE: It is the responsibility of the distributor or installing dealer to educate the end user upon completion of the installation project.

OSI Security Devices and its sales representatives are **not** responsible for programming. If required to do so, the end user may incur a fee.

Warning: When properly installed and maintained, the Product may reduce risk of property loss due to burglary, robbery, or otherwise, but is not insurance or a guarantee that these events will not occur. OSI makes no representation that the Product may not be compromised or circumvented; or that the Product will prevent any personal injury or property loss.



Index

A

Access Control System Tutorial, 49
 Overview, 49
Access Level Description, 41
Access Levels
 Enrolled ID Required, 13
 Shutdown, 14
Access Levels, 12
Adding Locations, 32
Additional Lock Features, 43
Address, i
Administrator's Package Contents, 6

B

Backing Up Data, 59
Battery Replacement, 55

C

Card Expiration Date, 18
Card Issue ID, 18
Closing the ODL—A Word About
 Synchronization, 38
Contact Information, i
Customer Service
 E-mail, 71
Customer Service, 71
 Limited Warranty, 72
 Out-of-Warranty Service, 71
 Returning Material, 71
 Warranty Service, 71

D

Data communication, 8
Database, 9
Database Maintenance, 59
Diagnostics, 39
Disaster Recovery, 60

E

Enrolling Locks in the System
 Adding Locks, 33
Enrolling Locks in the System, 32
Enrolling, Removing Users and Modifying
 User Properties
 Changing a User's Profile, 28

 Removing a User, 27
Enrolling, Removing Users and Modifying
 User Properties, 26

F

Facility, 49
Field Separator, 19
Fifth Step, Enrolling a Mobile Device, 52
First Step, Setting Global Facility
 Parameters, 49
Fourth Step, Setting Up a Time Schedule, 51

G

General User, 12
Group PIN Re-coding, 15
Groups, 25, 50

H

Head Cleaning, 56
Help!!, 63
Holidays, 30

K

Key Detection (Option 1), 43

L

Lock Installation, 7
Lock Maintenance
 Battery Replacement, 55
 Head Cleaning, 56
 Lubrication, 57
Lock Management Actions
 Group Control, 42
 Home Group Supervision, 42
Lock Operating System Replacement, 60
Lock Operation, 39
 Introduction, 39
Lock Package Contents, 6
Lockout, 14
LOS, 60
Lubrication, 57

M

Maintenance
 Lock Maintenance, 55
 Mobile Device Maintenance, 58

Index

Maintenance, 55, 57
Maintenance Features of the OMNILOCK
Facility Manager
Backing Up Data, 59
Database Maintenance, 59
Refreshing a Mobile Device, 58
Manager, 11
Mobile Device, 52
Mobile Device Maintenance, 58

O

OFM, 8
OSI Address, i
Overview of Access Control System
Concepts, 8

P

Password, 9
Phone Number, i
PIN, 10, 15
PIN Re-coding, 15
Programmer, 11
Programming a Lock for the First Time, 36

R

Re-coding, 15
Refreshing a Lock, 57
Refreshing a Mobile Device, 58
Remote Switch Operation, 43
Reporting Features
Lock Report, 45
The Audit Report, 44
Users Report, 47
Reporting Features, 44
Reports
Audit Report, 44
Lock Report, 45
Users Report, 47
Requirements, 6
Reset Button, 56
Resetting the Lock, 56
Return Material Authorization, 71
RMA, 71

S

Second Step, Setting Up Groups, 50
Service User, 12

Setting Access Levels and Running
Diagnostics, 39
Setting Up a Facility
Passwords and Microsoft Access
Compatibility, 9
Setting Up a Facility, 24
Setting Up a Sample Facility
1st Step, Setting Global Facility
Parameters, 49
2nd Step, Setting Up Groups, 50
3rd Step, Adding Lock Users to the
Database, 50
4th Step, Setting Up a Time Schedule, 51
5th Step, Enrolling a Mobile Device, 52
6th Step, Enrolling Locks, 52
Setting Up a Sample Facility, 49
Setting Up Groups, 25
Setting Up Time Schedules
Deleting, Modifying Existing Schedules,
and Using a Schedule as a Template, 31
Lock Enrollment, 31
Schedule Names, 31
Setting Up Group Schedules, 29
Setting Up Holidays, 30
Setting Up Time Schedules, 28
Shutdown, 14, 55
Sixth Step, Enrolling Locks, 52
Software Installation, 7
Synchronization, 38

T

Third Step, Adding Lock Users to the
Database, 50
Time Schedule
Access Level, 51
Time Schedules, 28
Time Schedules and Holidays, 15
Transferring Data to the Locks
Exchanging Data With the Locks, 54
Transferring Current Data to the Mobile
Device, 53
Transferring Data to the Locks, 53
Tutorial, 49

U

Unlocked, 13
Unlocked with first valid ID, 13
Updating the OFM, 54
User Groups, 14, 15

User IDs, 10
 PIN, 10
User Types
 General User, 12
 Manager, 11
 Programmer, 11
Using Digit Count, 19

Using Fields, 19

W

Warranty, 72
Welcome!, 6