OSI SECURITY DEVICES

OMNILOCK®

ACCESS CONTROL SYSTEMS
SERIES OM2000

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.

CAUTION

Use electrostatic discharge protection procedures when the printed circuit board is exposed.

OSI Security Devices
1580 Jayken Way
Chula Vista, Ca. 91911-4644
Phone: (619) 628-1000
Fax: (619) 628-1001 Email:osi@omnilock.com
Website:www.omnilock.com

11068 Rev C

Initial Setup Checklist

- ❑ Complete and mail the **Product Registration** Form. You must register the ID number on your OM2000 Installation CD with OSI Security Devices in order to receive technical support for software or hardware. Ensure that you receive the Lock Installation Instructions and other data from the lock installer.
- ❑ Read the **Administrator's Guide**! Review the Lock Installation Instructions that are shipped with each Lock and verify Lock operation.
- ❑ Install ActiveSync on your Personal Computer (PC) and create a partnership with your ActiveSync compatible Mobile Device per the device manufacturer's instructions (see **Software Installation** page **4**).
- ❑ Close any open applications on your PC. Insert the OM2000 Installation CD into the drive of your PC. Launch the file *(CD drive letter):Setup.exe*. Follow the instructions of the Setup Wizard which will automatically install the software in a sub-directory of the Program Files directory of your C drive (see **Software Installation** page **4**).
- ❑ Connect your partnered Mobile Device to your PC. Select the *Start* key on your PC, select *Programs*, select *OSI Security Devices* and select *Install OMNILOCK Data Link* (ODL) which will download the ODL to your Mobile Device (see **Software Installation** page **4**).
- ❑ From the *OSI Security Devices* directory select *OMNILOCK Facility Manager* (OFM) which will launch the OFM. The OFM toolbar will show but the screen will otherwise be blank, (see **Software Installation** page **4** and **Toolbar** page **16**).
- ❑ To become familiar with the OFM, it is highly recommended that you use the System Tutorial (see **Chapter 6** page **43**).
- ❑ Select *Facility*, then *New* to bring up a property sheet for the new facility that you are about to create. Fill in or select the applicable boxes and then select *Next*. Verify or modify the Daylight Savings Time setting and then select *Finish*. Follow the prompts to protect your database with a password (recommended). Do not check the box for Microsoft Access compatibility, (see **Facilities, Locations, and Locks** page **7**, **Facility Manager Overview** page **15-22**, and **Setting Global Facility Parameters** page **43**).
- ❑ Select the *Group* icon (the multiple human faces). Double click on *Group 1* to bring up a property sheet for that group and fill in the sheet as desired, select *OK* when complete. Identify other groups as required, (see **User Groups** page **12**, **Setting Up Groups** page **22**, and **Groups** page **44**).

- ❑ Select the *User* icon (the single human face). Select the *Add New* button on the toolbar. Since a Programmer must be assigned to a lock when it is defined, fill in the property sheet with the name of the person who will be a Programmer and then complete the property sheet. Select *Next* to make a group assignment. Select *Next*; the Lock enrollment pane will appear, but since no locks are enrolled in the system yet, select *Next.* Select *Next* again and enter any reference information desired. Select *Finish*. Repeat this process to enroll other Users. (see **User Types** page **10**, **Enrolling Users** page **23,** and **Adding Lock Users** page **44**).
- ❑ Select the *Time Schedule* icon and then select the *New* icon. The starting pane for creating a Time Schedule will appear. (see **Time Schedules and Holidays** page **12**, **Setting Up Time Schedules** page **26,** and **Setting Up a Time Schedule** page **45**).
- ❑ Select the *Mobile Device* icon and then select the *New* icon. The OFM will connect to the device and identify it in the Mobile Device Pane. Enter the name of the person to whom it is assigned, if desired, and select *Finish*. . (see **Enrolling a Mobile Device** page **47**).
- ❑ Select the *Lock* icon and then select the *New* icon. Select *Location* or *Lock* to add a new location or lock. (see **Facilities, Locations, and Locks** page **7**, **Enrolling Locks in the System** page **25**, and **Enrolling Locks** page **47**).
- ❑ Select the *Data Exchange* icon (the lightning bolt), the locks requiring programming will appear (see **Transferring Current Data to the Mobile Device** page **48**).
- ❑ Disconnect the Mobile Device from the PC. On the Mobile Device, select *Omnilock Data Link*, a list will show the names and locations of the locks to be programmed. Initiate IR communications between a Lock and the Mobile Device. Then, from the tree view, select the location and lock to be programmed and select *OK*. After programming the locks, exit from the Omnilock Data Link program (see **Using the Mobile Device to Exchange Data with Locks** page **33**, and **Exchanging Data With the Locks** page **49**).
- ❑ Reconnect the Mobile Device to the PC and wait for the units to synchronize. Select the *Data Exchange* icon on the OFM to update the OFM (see **Updating the OFM from the Mobile Device** page **30**).

Table of Contents

Notes:

|| Chapter 1 || Introduction to the OMNILOCK® Access Control System OM2000

Welcome!

Thank you for choosing the OMNILOCK Access Control System OM2000 for your building security needs. The OMNILOCK is a sophisticated building access device, which is fully self-contained (requiring no wiring), battery-operated, and capable of managing entrance security needs for small and large buildings alike. With its rugged housing, robust electronics, and patented low-power motorized locking mechanism, the Lock can provide years of maintenance-free service with infrequent battery replacement.

The accompanying OMNILOCK FACILITY MANAGER (OFM) software for Windows® 9X/2000/NT enables you to easily configure one or more facilities, each with up to 65,000 Locks, for keypad and/or identification card access, design a multitude of access time control plans, define up to 2,000 users per Lock, as well as generate various reports for each Lock and monitor battery condition.

Once a facility access control plan is set up in the software, each Lock is programmed via the infrared port on your ActiveSync-compatible Mobile Device. A quick stroll through your facility is literally all that it takes to manage every Lock.

Each Lock keeps a log of all activity, which you can retrieve at a later time. This log stores the user ID, the date, and time of each entry event. It even records failed attempts to open the Lock!

Lock Package Contents

Each Lock for the Access Control System is shipped with the items listed below. Please check this list to ensure you have received all items.

- ❑ Keyboard/Electronics Housing (Additional electronics housing with weatherized units.)
- ❑ Lockset (not included with the Wall-Mount System)
- ❑ Installation Hardware
- ❑ Hardware Installation Instructions
- ❑ 1 System Default Programmer ID Card for Track 2
- ❑ 1 System Default Programmer ID Card for Track 3
- ❑ Installation Template
- ❑ Warranty registration form

Administrator's Package Contents

- ❑ Software Installation Disk
- ❑ Administrator's Guide
- ❑ 10 Manager programming instruction cards (please call OSI if more are needed)
- ❑ 3 magnetic head cleaning cards
- ❑ Warranty Registration Form

Requirements

The Access Control System requires the following items to function in the keypad-only mode:

- ❑ OM2000 Series Locks
- ❑ OMNILOCK Facility Manager Software
- ❑ OMNILOCK Data Link Software
- ❑ Personal Computer running on Windows 9X/2000/NT, Pentium 133 Mhz w/32 Meg Memory (Minimum)
- ❑ Mobile Device (hand held computer) with ActiveSync and infra-red port

The following additional items are required to function with magnetic cards:

- ❑ Magnetic Cards (According to standards ISO 7810 and 7811)
- ❑ Compatible Keyboard "Wedge" Magnetic Card Reader

Lock Installation

Note: For hardware installation, please refer to the hardware installation instructions included with your OMNILOCK OM2000 Series Lock.

Testing the Lock

After the Lock hardware has been installed, use the included DEFAULT PROGRAMMER ID (Master ID) card to test various functions of the Lock.

1. Briefly insert the card into the card reader (***with the printed side facing the user and the point of the arrow down).*** When the card is removed, the green light on top of the Lock should begin flashing approximately once per second.
2. Turn the Lockset handle within ***three seconds*** to gain entry. The Lock should enable entry; five seconds after five green flashes have started, it will flash the red light and re-lock.

   The next test involves changing the Access Level of the Lock.

   1. Using the keyboard, enter the default Manager Code***: 2…2…2…2***; the green light should flash after the last digit entered. At this point the green light will flash once to indicate successful data entry each time a key is pressed.
   2. Within three seconds, enter the ***2*** once more (note the green flash), then press and hold the ***CL*** key. The green indicator will flash to indicate data entry; continue holding it down until the green light **begins** a sequence of three flashes. This should put the Lock into the Unlocked state (test this by turning the Lockset handle downward).
   3. At the keyboard, enter the default Manager Code again.
   4. Within three seconds, enter the keypad digit ***5*** then press and hold the ***CL*** key until the sequence of three green flashes begins. This should put the Lock back into the Enrolled ID Required state and lock it.
   5. Try turning the Lockset handle to ensure it is locked.
   6. Insert the DEFAULT PROGRAMMER ID card briefly again into the card reader, then remove it.
   7. Turn the Lockset handle again within three seconds to ensure that one-time access is granted. Observe that after about 5 seconds the red light will flash and the Lock will re-lock.

   This concludes testing of the Lock. The Lock is now in the Enrolled ID Required state, and will allow access only for individuals using the factory Default Manager ID(**2222**), the Programmer ID (**1234**) or the Default Programmer ID card. You should now proceed to install the OMNILOCK Facility Manager program.

Software Installation

You will need an ActiveSync (early versions are named “Windows CE Services”) compatible handheld computer (“Mobile Device”) to communicate between your desktop computer and the Locks in your system**. If you already have the Mobile Device, it is recommended that you install its ActiveSync software and serial connection before you start the installation of the OMNILOCK Facility Manager on your system.** When you first establish the serial connection to the Mobile Device, you will be given the option to establish a partnership or connect as a “guest”. Choose “partner” in order for the Device to work with the OMNILOCK Facility Manager. If you do not want to set up the Mobile Device now, you can still run the database manager. This will, for example, allow you to become familiar with its features and even set up your facility before you have the Mobile Device ready, however, **when you later install ActiveSync, you must reinstall the OFM**. The reinstallation will take two steps; first you will remove the original installation, 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.

Included with your package is a software installation CD. To begin the software installation, follow the instructions below.

1. Close any open applications.
2. Insert the CD into the drive of a Windows 9X/00/NT compatible personal computer.
3. Launch the file “CD drive letter:\Setup.exe” via the Run Command in the Windows Taskbar, or by double-clicking on the set-up icon in the CD drive display window, or by using the “Install/Remove Programs” feature in your computer’s control panel.
4. Follow the Setup Wizard instructions that appear on your screen.
5. When the License Agreement window appears, read the Agreement, then click Yes to accept the terms of the Agreement.
6. You will be asked to enter a user name and company name. Default user and company names will be shown.
7. The Setup Wizard will automatically install the software in a sub-directory of the Program Files directory of your C drive. If you wish to install to a different directory, follow the instructions presented by the installation program.
8. If prompted, click Restart to restart your computer.

When you are ready to use the program, press the Start key on your desktop, move the mouse to Programs, then on the sub-menu OSI Security Devices. There are two choices offered at this point; one launches the OMNILOCK Facility Manager (OFM), and the other downloads the OMNILOCK Data Link (ODL) program onto a Mobile Device connected to the desktop computer. If you have the Mobile Device connected to your computer and set up as a partner, now would be a good time to download the ODL, but it can be done later. Of course, you will need to download the program before the OFM will be able to register the device for communication to any Locks. To download the ODL, click on "Install OMNILOCK Data Link".

To run the OFM, Click on "OMNILOCK Facility Manager". The OFM will launch and will show its toolbar, but the screen will otherwise be blank, as it has not yet connected to a database. In addition, the installation process will have placed an OMNILOCK Facility Manager icon on your desktop. Double clicking on this is an alternative way to launch the OFM. If you prefer not to have this on your desktop, you should highlight it by clicking once on it and then pressing the keyboard Delete key. This will have no effect on your ability to start the program from the Start Menu.

If the OFM screen with the toolbar appeared when launched, the software installation is complete.

Notes:

|| Chapter 2 || Overview of Access Control System Concepts

Real World Versus Virtual World

Your OM2000 Access Control System actually exists in two places: the real world and the virtual world. The real world scheme is comprised of the actual Locks you have installed in the building(s) you occupy, used by the individuals who are authorized to do so, as specified in each Lock's configuration.

The virtual world scheme encompasses all of the same entities, but exists in the OMNILOCK Facility Manager's database. You create this database using the software that is part of the OM2000 system. First, you create an access control plan in the software, then transfer the data from this configuration to each of the Locks in your building(s), using the OMNILOCK Data Link (ODL) software and a Mobile Device. The OMNILOCK Facility Manager (OFM) software helps you manage all of this by keeping track of the state of the system at all times. This includes tracking changes to the system that you enter at your computer using the OFM. These changes are recognized to be in a pending state until they have been transferred to the Lock(s) using the ODL, and the ODL has reported the successful transfer back to the OFM. Various views in the OFM offer an instantaneous "snapshot" showing everything that has been programmed, with items not transferred and reconciled appearing as pending.

Facilities, Locations, and Locks

The uppermost tier of an installation plan is called a Facility. For each database, there is only one Facility. A Facility, however, can be defined quite liberally, usually somewhere from a single building to a large, contiguous campus of buildings. When 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 or a wing, to an entire floor, or even a building.

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 to which it belongs.

Below is an example of a Facility scheme.

Facility:West Campus

Locations: Rasmussen Building
Kirk Room (Lock)
Green Room (Lock)
Kcomt Room (Lock)

Outzs Building
Reilly Room (Lock)
Justin Room (Lock)
Navarro Room (Lock)

Britton Building
Weiland Room (Lock)
Lindros Room (Lock)
Wayne Room (Lock)

Facility:Blue Sky Tower

Locations: Floors 1-20
Third Floor (sub-location)
Room 3137 (Lock)
Seventeenth Floor (sub-location)
Room 17114 (Lock)
Room 17156 (Lock)
Eighteenth Floor (sub-location)
Room 18119 (Lock)

Floors 21-50
Twenty-Second Floor (sub-location)
Room 21107 (Lock)
Room 21108 (Lock)
Room 21112 (Lock)
Twenty-Ninth Floor (sub-location)
Room 29002 (Lock)
Room 29007 (Lock)

Access Levels

A Lock is always in one of eight possible levels of access, as described below. The Lock's Access Level is changed either by a Time Schedule Event (programmed into the Lock), or by the use of the Lock's keypad, using the key indicated below, by an individual with a Manager ID (see Page 38). If the User's ID entered meets the requirements of the operative access level, the Lock will disengage the Locking mechanism, enabling entry access for a specified period of time (usually 2-4 seconds), then re-engage the Locking mechanism and remain Locked until the next valid ID is entered or the Access Level is changed by a Time Schedule event.

Unlocked (Key 2)

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.

Unlocked with first valid ID (Key 3)

A special feature of the Unlocked Access Level is that it can be optionally set to go into the Unlocked state only after initiation by a valid ID (code or card). 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 each day.

Unlocked with first valid ID + PIN (Key 4)

A special feature of the Unlocked Access Level is that it can be optionally set to go into the Unlocked state only after initiation by a valid ID + PIN (Personal Identification Number). For example, you may want a Lock be Unlocked from 8 a.m. to 5 p.m. on weekdays, but only after the first person with a valid Enrolled ID + PIN has entered each day.

Enrolled ID Required (Key 5)

In the Enrolled ID Required state, a valid ID must be given to the Lock, via either an ID card or keypad code entry, for entry access to be granted. This is probably the most frequently used access level.

Enrolled ID + PIN Required (Key 6)

The Lock can be configured to require an ID (code or card) + PIN (Personal Identification Number). Once a valid ID + PIN has been entered, entry access is granted.

Lockout (Key 8)

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.

Any Valid Facility Card ID Required (Key 7)

(Requires special card programming)

Locks at this level will allow access for any valid card ID for 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. It requires that cards have the Facility ID in addition to the User ID programmed on each card within the facility. **Entry gained under this access level is not recorded in the Audit Log.**

Shutdown (No key assigned)

In the shutdown state, the Lock will give entry access only to a user with a Programmer ID. This access level will be forced by the Lock if there is imminent battery failure or a motor drive failure. 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 Types

The system supports four different types of users: Programmer, Manager, General User and Service User. A Service card or code (used in conjunction with a PIN) can be issued for temporary access. Each user has a different level of Lock control.

Programmer

The Programmer ID is to be used by the primary administrator (or administrators) of the Access Control System. There can be multiple Programmer IDs and you can configure multiple Locks to have the same Programmer ID. Each Lock must have at least one Programmer ID. The Programmer ID allows the Mobile Device to set up communication with the Lock through an infrared link. Once communication is established, pending actions from the OFM are posted to the Lock and audit information collected in the Mobile Device. Most use of the Programmer ID will be for this purpose only.

The Programmer ID can allow entry, permit the Lock's Access Level to be set using a dialog box on the Mobile Device, and can allow diagnostic tests to be run from the Mobile Device, depending upon the rights granted to the Programmer when the ID is issued. Since the Programmer can access primary Lock functions, the ID may be set up to always require a PIN in addition to the card or code in order to add additional security.

As indicated above, a Programmer ID can be set such that Lock entry is not permitted. This allows the security administrator to assign an individual who has no access authorization the responsibility of data exchange only with no entry privileges.

Manager

An individual with a Manager ID has the capability to enable or disable access for the manager's home group. A Manager ID can also be granted permission to enable or disable all user groups. Additionally, a manager may have the rights to change the Access Level of the Lock or Locks in a facility.

Although an individual with a Manager ID can make such changes at any time, a subsequent Time Schedule Event will override a setting made by a user with a Manager ID. For example, if a manager sets the Lock Access Level to Unlocked (thereby enabling anyone to have entry access), and a Time Schedule Event (see "Time Schedules and Holidays" page 12) is scheduled to put the Lock into Lockout mode at the end of the day, the Lock will enter the Lockout Access Level at the prescribed time. Of course, the manager can again set the Access Level to the state desired after a Time Schedule Event.

General User

In most applications, the vast majority of system users are General Users. The General Users are only able to gain entry when the Lock access level requires an Enrolled ID or Facility Card. General Users do not have access authorization when the Lock is in the Lockout or Shutdown state, or when they are not a member of a group that is enabled.

Service

Often a building or facility will require maintenance work. This may require access by contractors who need entry rights on a temporary basis. For this purpose a card or code may be issued with an additional PIN. This PIN will automatically change daily, weekly or monthly as desired. Once it has changed, entry will no longer be possible until the service person is given the new PIN.

User IDs

A User ID uniquely identifies every system user. It is normal that no two users have the same User ID. User codes can be anywhere from 4 to 10 numeric digits in length, depending upon the number of users and level of security desired. Codes may be manually entered as desired by the Security Administrator, or codes may be generated using the software's code generator. If a facility desires to use magnetic-stripe cards for access, OSI-supplied cards with magnetic ID codes can be used for access control. Furthermore, the card reader in the Lock will read common identification cards (drivers licenses, credit cards, student IDs, etc.). The system will accept up to the first 19 digits ("Primary Account Number" as specified in ANSI/ISO/IEC 7811) and this digital information may be read into the system software using the Magnetic Card Reader (which may be purchased from OSI Security Devices).

As an additional security feature, a PIN (personal identification number) can be assigned to each user ID. PINs can be from 3 to 6 digits in length. 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. With a user-entered code ID, it simply provides a longer ID. Since the PIN requirement can be made dependent upon the time schedule in the Lock, a longer code ID or a card + PIN can, for example, be set up for periods when there are few people in the area.

User Groups

The Access Control System enables you to set up user groups (Groups) to accommodate time-dependent access requirements for different people. For example, a day shift and a night shift or janitorial service could be set up to have access only during their period of duty. Each Facility can have up to eight different User Groups. Every General User and every Manager must belong to at least one of these groups.

At any given time, for each Lock where a user is enrolled, the user's group is either enabled or disabled. When a Group is enabled, all members of that Group have access rights 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 of access. All users belong to a home group, but may also have an associate membership in another group or groups. The distinction between home and associate groups is important only for users of the Manager type.

Time Schedules and Holidays

The feature that brings the most versatility and flexibility to the Access Control System is its ability to be configured for a multitude of access control timing schemes, including unlimited time-based Access Level changes, automatic accommodation of daylight savings time (DST) changes, and observation of up to 32 holiday periods annually.

With time-based Access Level changes, called Time Schedule Events, a Lock can be configured to automatically change to a different Access Level. Any of seven Access Levels can be set via a Time Schedule Event (Shutdown cannot be set). Of course, such a change can also be overridden by a subsequent Time Schedule Event. For example, a Lock can be configured to go into the Unlocked state every weekday at 8:00 a.m., and go into the Enrolled ID Required state every weekday at 5:00 p.m.

Group Access Privileges are controllable through the time schedule, allowing different groups access at different times.

Changes in daylight savings time can be configured in the Lock to occur automatically, by 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.

The access control system supports up to 32 holiday periods. Although this may seem an excessive number, the extras come in handy for events such as company shut down periods, extended holidays, open house days, etc.

Audit Log

In addition to the access and timing features of the system, supplementary security is provided via audit logging and anti-tamper control.

The Audit Log is a log of all entry attempts, successful and/or unsuccessful. For each successful entry, the log records the user ID, and date and time of entry. Entry attempts by registered users without current access rights and Anti-Tamper conditions are also recorded with a date and time.

Anti-Tamper Features

The Anti-Tamper feature is designed to discourage repeated unauthorized entry attempts. After three unsuccessful entry attempts, the Lock will automatically go into the Shutdown Access Level for ten seconds. During this time, the Lock does not recognize any keypad or card input (including input of a Programmer ID). After the ten-second interval has passed, the Lock will return to the mode it was previously in. However, if an invalid code is then entered before a valid code, the Lock will again go to shutdown for ten seconds. This makes it impossible for a person trying to gain access to rapidly try a series of numbers and thus reduces the probability of a "hit" on an enrolled number.

Magnetic Card Features

The standard magnetic cards available from OSI Security Devices are encoded on Track 2 and have an eleven digit ID number followed by a field with a four digit Lot number. The Lot number is for manufacturing purposes and is not used by the system.

The maximum number of characters that the system can read on Track 2 is the first twenty-five (25) encoded on a card. The character count includes Digits and Field Separators.

The system will also accept cards that are encoded on Track 3. Track 2 cards and Track 3 cards cannot be mixed in the same facility.

The system is flexible and may accept coding from existing Track 2 or Track 3 magnetic cards or cards may be encoded to include the following features as long as the total of the characters including Field Separators does not exceed twenty-five (25):

User ID 19 digits maximum (see "User IDs" page 12)

Facility ID (see "Any Valid Facility Card ID Required (Key 7)" page 10)

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 a higher Card Issue ID in a lock, that lock will no longer accept cards with the same User ID but 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 at that date. 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, MMYY, MMYYYY, YY, YYDDMM, YYMM, YYMMDD, YYYY, YYYYDDMM, YYYYMM OR YYYYMMDD.

For more detailed information on card encoding, see "Defining User IDs, Facility IDs, Card Issue IDs and Expiration Dates." on page 20.

|| Chapter 3 || The OMNILOCK Facility Manager

Facility Manager Overview

The OMNILOCK Facility Manager (OFM) running on a desktop or portable PC is the tool for managing and controlling access and maintaining records for a facility. The Locks and Mobile Device are subservient to and controlled by the OFM. There are a limited number of modifications to access levels and groups enabled that can be accomplished at the Lock without the intervention of the OFM, but even these are recorded and made a part of the audit data. Since the OFM is the kernel of the system, it is essential that the security manager become thoroughly familiar with the OFM. Time taken to carefully read this section and the example in the Software Tour will pay off when actually setting up your own facility database.

The OFM is a Windows application and makes use of the capabilities provided by the operating system. Consequently, many of the features and functions are accessed in a way that will be obvious to anyone generally familiar with Windows applications. The details of the various windows presented by the OFM are described below.

The OMNILOCK Facility Manager (OFM) allows the security administrator to perform the functions required to add and remove Locks and users for the security system and to control all Lock functions. Audit data collected from the Locks can be displayed and searched for relevant information as required. The OFM has internal mechanisms for checking entries to ensure that actions, which could result in improper system operation, are not permitted. For example, you will never be allowed to remove the last Programmer from a Lock, because to do so would make communication with that Lock impossible.

There are certain basic actions that must be taken to manage the security system through the OFM. The administrator will need to:

- ❑ Set up a facility to contain all of the Locks and users assigned to that facility and set the global facility parameters.
- ❑ Enroll Users, assign a card or keypad-code ID and assign a PIN if one will be required. Group membership and special user types are assigned as part of the enrollment process.
- ❑ Set up Programmer IDs to allow for transfer of data between the Locks, Mobile Devices and the OFM. Assign rights to these IDs to allow data collection with or without entry rights or advanced programming rights.
- ❑ Set up Manager IDs for group supervision and access level control beyond that provided by time schedules, and assign desired rights to the Manager IDs.

- ❑ Set up a time schedule for each Lock in the system. While each Lock can have a different schedule, in most cases this will not be required and each schedule can be simply copied to numerous Locks.
- ❑ Assign a name and location for each Lock in the system
- ❑ Assign Users to each Lock in the system.
- ❑ Transfer data between the OFM and the Locks using a Mobile Device.
- ❑ View audit information from the Locks.

When using the OFM, selecting an item from the toolbar gives access to the key programming functions. The toolbar buttons presented (L to R) are:

Figure 1

Toolbar

	New Facility	Presents a window for defining a new facility
	Open Facility	Presents a window for selecting established facilities
	View Facility Explorer	Shows a “Tree” of locations & Locks within the facility
	View Lock Users	Presents an alphabetical table of all users in the facility
	View User Groups	Presents a table of users, arranged by groups
	View Time Schedules	Presents a list of operational time schedules
	View Mobile Devices	Shows the properties of registered Mobile Devices
	New--	Allows you to add a new item to the current list etc.
	Copy--	Copies selected item to the clipboard
	Paste--	Pastes clipboard item to selected area
	Delete--	Deletes selected item
	Properties--	Displays property sheet(s) for the selection
	Data Exchange	Allows you to synchronize data with a Mobile Device

It is not necessary to show the Toolbar; it can be enabled or disabled under the View menu. Setting up a new facility or modifying an existing one can be done by selecting Facility from main menu. Any one of the five views can be selected from View on the main menu. Right-clicking on an item or highlighting it and selecting Edit from the menu will allow you to Add New, Cut, Paste, Delete or view its Properties as appropriate. Data exchange can be accomplished from the Tools item in the menu.

Facility properties are viewed and set by clicking on Facility Properties. The facility properties should be set before any other programming actions are taken. Facility properties are global throughout the facility, so if they are changed, all users' codes will change and all Locks will require reprogramming. The Facility must have a name assigned to it. The facility name becomes part of a code that uniquely identifies the facility. Any attempt to communicate with Locks of a facility using a Mobile Device registered to another facility will fail, so that unauthorized re-programming from another OFM cannot occur. Other properties that can be set include the code length required for keypad entry, the PIN length (you should set one even if you don't intend to immediately use one, as you might want to later) and card parameters. For card parameters, you will probably just want to use the default parameters if you are using OSI-supplied cards. If you are encoding your own cards and use an encoded card Issue ID or Expiration Date, these parameters must be set.

Additions or changes to the Lock users, user groups and time schedules are all accomplished similarly. For example, in the user table a user is selected for viewing or modification by right-clicking the mouse with the arrow positioned on that user. When this is done, choices are presented: New to add a new user, Copy to take the properties of the selected user and copy them to a new user (of course you have to add the name and ID for the new user, but the type of user and group membership etc. will be copied) Delete to remove the selected user from the list, and Properties to show the properties for the selected user.

The data entry process is governed by a series of screens, sometimes called "Wizards", because they step you through entries required. If an essential field is left unfilled, you will be reminded that you must fill it in before going on. Finally, in the case of data modification which must be downloaded to a specific Lock or group of Locks, after selection, a pending icon shows up indicating that enrollment will not be complete until the Lock(s) have been visited and connection to the appropriate Mobile Device established to update each Lock's internal database. When the Mobile Device returns from its journey around the facility and has been re-connected to the computer, the pending icon will be removed if there is confirmation that all Locks subject to the new enrollment have been updated.

Mobile Devices used to exchange data between the Locks and the OFM are registered in the system by the operating system using Microsoft ActiveSync. Their properties will appear when Mobile Devices is selected. A Lock is partnered (for programming) with a single Mobile Device, so that the OFM will transfer data for a specific Lock with the correct Mobile Device. In many cases, only a single Mobile Device will be used within a facility. However, if the facility is large enough to warrant the use of multiple Mobile Devices, a fixed subset of the Locks must be assigned to each Mobile Device for programming. Lock assignments are made and modified using the Lock-listing window for a selected Mobile Device. While only one Mobile Device is allowed to program a specific Lock, other Mobile Devices can be used to collect audit data, as long as they are registered in the facility (as Guest Mobile Devices).

Setting Up a Facility

Overview

There are a number of things that need to be determined at the beginning. Defining a Facility attaches a database with the Facility name to the OFM. When you set up a Facility, several “global” (i.e. affecting all Locks in the facility etc.) items are determined. It is therefore important that some thought be given to the choices, as all the Locks in the facility will have to be reprogrammed if a global item is changed later.

To set up the Facility, click on Facility in the main menu, or select the New Facility button at the left end of the toolbar. A property sheet will show your choices. Determine a unique descriptive name for your facility and type it in the box provided.

The Locks in the system will accept a keypad-entered code or a card insertion. Either of these may have an optional keypad-entered PIN (Personal Identification Number) attached for additional security. Usually a PIN is used in conjunction with a card ID, as it reduces the possibility of entry with a lost or stolen card. With a code ID, a PIN essentially just makes a longer code. PINs can be set to automatically change (recode) at specified periodic intervals. The code length and PIN length should be set to a desired value, even it they aren’t going to be immediately used, to avoid reprogramming all Locks if you decide to use a length other than the default value later. Codes can be from 4 to 10 numeric digits long and PINs can be 3 to 6 numeric digits in length.

Setting Up to Use Cards in the Facility

Normal magnetic card parameters are set to default values on the property sheet. If you are using standard OSI-supplied magnetic cards, these parameters will be satisfactory. They will also work with other ANSI 7811 type cards typically used by banks, driver's licenses, and for student IDs, etc. The card coding must follow ANSI 7811, which requires that the first character of the magnetic data be a Start Sentinel generally represented as a ";". To avoid data entry errors, a keyboard "wedge" reader is recommended. With this device connected in line between the PC and its keyboard, you can simply scan the magnetic stripe directly to enter the card ID. Since the data output format is not standardized for these readers, it is recommended that you purchase a certified card reader from OSI Security Devices to guarantee compatibility.

New Locks are normally shipped from the factory set up to read Track 2 on the card. This track has low-density data, is very durable, is the most common track for this application and it appears on all cards. Using Track 2 is strongly recommended unless there is a good reason for using Track 3. This might be necessary if Track 2 is already being used in the system in a way that makes it unusable for user identification. Track 3 can be used by changing a jumper plug on the circuit board inside each Lock. You cannot mix Track 2 and Track 3 Locks in the facility; all Locks must be set for one or the other and the selection on the property sheet must agree with the Lock jumper placement. If you decide to use Track 3, you must be sure to purchase cards that include magnetic material printed on the Track 3 location. Also, a keyboard wedge reader capable of reading Track 3 must be installed if you want to enroll cards by scanning them at the PC running the OFM. The total number of characters (Digits plus Field Separators) that the Lock can read is 25 on Track 2. The maximum number of digits allowed for an ID under ANSI 7811 is 19 and they are the first recorded on the card. The card can have more than 19 characters, but only the first 19 will be used for the ID. If you are encoding your own cards and are using an encoded Issue ID, Facility ID, or Expiration Date in addition to the Card ID, this data must appear in the first 25 characters. See "Using Fields", page 20 and "Using Digit Count", page 21

Setting up for Global Facility Card Entry

The access control system allows for cards with two identification numbers encoded on the magnetic track. One is the normal identification number or ID for the user; the other is identical for all cards within the facility. The purpose, as described more fully elsewhere (see Page 10), is to allow everyone to enter common areas. It is not necessary to use this feature or to have more than just one ID on the card. If you do want to use the feature, cards must be programmed specially for your facility. There is some flexibility in the way the cards can be programmed so that compatibility with pre-existing card systems may be possible. The choices available relate to the placement of the data disired. See "Using Fields", page 20 and "Using Digit Count", page 21

Defining User IDs, Facility IDs, Card Issue IDs and Expiration Dates.

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:

1576=3492657182=0=060101

- FIELD 4
  CARD EXPIRATION DATE
  June 1, 2001
  (MAY BE SPECIFIED AS "TO" OR THROUGH THE DATE)
  See "Card Expiration Date" page 14
- FIELD 3
  CARD ISSUE ID (MAXIMUM 1 DIGIT, 0 TO 9)
  (NEW ISSUES OF THE CARD MUST HAVE
  THE SAME OR A HIGHER ISSUE NUMBER)
  See "Card Issue ID" page 14
- FIELD 2
  USER ID NUMBER (MAXIMUM OF 19 DIGITS)
  See "User IDs" page 12
- FIELD 1
  FACILITY ID NUMBER
  See "Any Valid Facility Card ID Required (Key 7)" page 10

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 must have a fixed number of digits and that the total number of digits not exceed 25.

Example of encoded data using character count:

1576349265718200601 01

- CARD EXPIRATION DATE
  (STARTS AT COUNT 16)
  June 1, 2001
  (MAY BE SPECIFIED AS "TO" OR THROUGH THE DATE)
  See "Card Expiration Date" page 14
- CARD ISSUE ID
  (STARTS AT COUNT 15) (MAXIMUM 1 DIGIT, 0 TO 9)
  (NEW ISSUES OF THE CARD MUST HAVE
  THE SAME OR A HIGHER ISSUE NUMBER)
  See "Card Issue ID" page 14
- USER ID NUMBER
  (STARTS AT COUNT 5) (MAXIMUM OF 19 DIGITS)
  See "User IDs" page 12
- FACILITY ID NUMBER
  (STARTS AT COUNT 1)
  See "Any Valid Facility Card ID Required (Key 7)" page 10

Daylight Savings/Standard Time

The access control system is able to automatically change its internal time clock at the daylight savings/standard changeover time, setting itself one hour ahead or back, as required. The Daylight Savings tab on the Facility property sheet allows you to select when the changeovers will occur. The drop down box lets you select the North American, European, or Southern Hemisphere normal changeover times. If these don't meet your needs, the Other selection enables you to fill in desired changeover times in the boxes below, or as you fill in the boxes with your custom selection, the drop down box will automatically change to Other.

After completing your selections, click the Finish button. A dialog box will then appear to allow you to select a password for the facility.

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 or alpha (case sensitive) characters and must be between 6 and 14 characters long. To ensure that the password has been typed correctly, it must be typed into the confirmation box as well. If the two entries agree, a message box warning that if you lose the password that the database will be forever inaccessible; at the bottom of the box you can select YES or NO. **If you select YES, the database will be inaccessible without the password.**

Unless a password is set up, anyone can view the database using Microsoft Access. If changes are made to the database using Microsoft Access, the database will become unusable by the OFM! Nevertheless, Microsoft Access may be useful for advanced users who wish to use, but not modify the database. In general, it is not recommended to make the database available to Microsoft Access. The Access Compatibility box in the password dialog should remain unchecked when setting up passwords unless you have a very good reason to allow compatibility. Even if Microsoft Access compatibility is allowed, the password protection will still apply in any case. Microsoft Access will demand the password before opening the password-protected database.

Setting Up Groups

General

Click on the User Groups (it is the two-headed icon) button on the toolbar to bring up the list box showing the eight groups. The groups are numbered 1 through 8, and are accessed by number at the Locks by Managers and Programmers. For easy reference, each group can be given a name, such as Accounting, Mail Room, Janitorial, etc. A reference field is also available for any other descriptive information that you may wish to add. For convenience, group names are used throughout the OFM to refer to the groups. Group membership is assigned from the Users toolbar button. A member of a group can be assigned a Personal Identification Number (PIN) which can be set to automatically change (recode) at specified periodic intervals. PINs are required for General Users only if a Lock's access level is set to require one, so they don't have to be used even if they are set up.

To modify the properties of a group, double click or right click on the line for the group you want to modify to bring up a property sheet for that group. Or select the line with a single click and select Edit then Properties. You can change the group name or reference information at anytime without requiring a download to the Locks, as this affects the OFM only. Changes affecting PINs will have to be downloaded to all Locks in the system. Once PIN specifications have been downloaded, the Locks automatically recalculate the PINs at the specified intervals, and the OFM always shows both the current and the next PIN for each user. It will generally save time if PIN specifications for each group are set up initially when setting up the facility.

Setting the PIN Recode Interval

To set the PIN recode interval, click on the Autocode check box so that the check appears. This will enable the selections in the autocode window. You can select the interval in days (up to 30) or months (up to 12). For months, the default date for recoding is the first of the month, but you can change it. If you select a month-day greater than 28, the day will slip to the first of the next month when the recode day is not on the calendar for the interval. For this reason, it may be wise not to select a recode month-day greater than 28. PIN specifications can be different for each group. If you do not check the Autocode box, the PIN will not change.

Service Group

If there is a need for service, maintenance or for other temporary workers who will need access for a brief period, you may want to set up a Service group with a recode interval of 1 or a few days. Individual users may be set up (using the Users button on the toolbar) to be of type Service. This type of user must always enter a PIN for entry as well as a card or code. As soon as the current PIN expires, the Service User will not be able to enter. Of course, you can inform the user of the new PIN and entry will again be possible until the next recode date. Alternatively, you could issue a card (or code) to an individual or to a company that is frequently used for service calls. Then, when they are needed, you just have to inform them of the current PIN and possibly the next one as well (if the current one is about to expire, for instance) and they can enter for the recode period. Service User IDs can be assigned to any group, but it is usual to have only one group with a short recode interval.

Enrolling, Removing Users and Modifying User Properties

General

Use the *Users* button on the toolbar to access the user list box. The box shows the users in alphabetical order, their ID number (whether they are identified by a card or code), and their home group. Existing users can have their data edited by double or right clicking on the user line in the table. New users can be added by right clicking anywhere on open space not part of a line, or selecting the *New* button on the toolbar. A series of dialog boxes will appear to allow you to enter the individual user information. You cannot set up any Locks until you have established a *Programmer* to assign to that Lock. Therefore, you must set up at least one user as a Programmer.

New users

New users can be added by either "filling out" the dialog boxes obtained by selecting *New*, or by double clicking on an existing user and selecting Copy. Selecting *New* will, of course, necessitate filling in at least the required information. If the user database includes a user with the same enrollment characteristics (or most of them), then time can be saved by copying that user profile to the new user with the *Copy* choice after double or right clicking on the prototype user. If you choose to copy, the dialog boxes that appear will have selections made for ID card or code, ID type, privileges (if any) assigned to the ID, group membership and Lock enrollment.

In all cases, an ID number will be assigned by the system. If you want to change that number, simply type the number you want to use or press the *Recode* button for the system to assign a different one. The system will check to be sure that the number you select has not already been assigned. Bear in mind that for user entered codes, the number of digits must be the same throughout the facility. Card IDs are normally entered through a card reader, but they can be entered manually if the magnetically encoded number is known. Using the card reader will minimize the possibility of error. Card IDs are limited to 19 characters. If a card has more than 19 characters for the ID portion, all characters in excess of 19 will be ignored.

A first and last name is required by the database manager; the middle initial is optional. If you try to move on to the next dialog box without entering one for each, you will be reminded. The PIN information will not appear during the enrollment process. When you are finished, you can see the PIN information by double or right clicking on the user and selecting Properties.

There are optional fields offered by the dialog boxes in addition to the middle initial. These are named Reference, Contact 1, and Contact 2. You may use these boxes to include other relevant information about a user in the database (i.e. emergency telephone number, dormitory room number, etc.).

Removing a User

To remove a user, double or right click on the user line and select Delete. If a user is removed in error, but not yet removed from the Lock(s), you can use the Restore selector to allow you to reactivate that user.

Changing a User's Profile

To change a user profile, double or right click on the user line. The property sheet for that user will appear. Simply change any selectable item to the desired state or value and select Apply or OK.

Lock Enrollment from User Property Sheets

The user can optionally be enrolled into Locks from the Enrollment page of the User Profile. This will be useful if the system has already been set up with all the Locks enrolled in the system. For example, if you are enrolling a new employee into the system, you can select Locks to which the employee will have access at this time. If you haven't set up the Locks in the system yet (you are enrolling users first), then you can easily select the users for each Lock from the Lock property sheet (see Page 26).

Enrolling Locks in the System

The process of enrolling Locks is accomplished by building a hierarchical "tree". The highest level is always the Facility. When you first open the Facility Explorer (Lock Icon) it will only show the Facility with its name. At this level one can add either a new location or a new Lock. Locations show as a file folder that can contain additional locations and/or Locks. Locations are simply a convenient way to break up a facility into easily identified units. There is no requirement to use locations and if you only have a very few Locks to manage, you may choose to simply attach all Locks directly to the Facility. In general, it is advisable to set up locations that are easy to find and are easily referenced to the individual Locks in the system.

Adding Locations

A sensible way to begin is to set up a hierarchy of locations before adding the Locks. This will generate a tree that you can decorate with the Locks as required. Of course, you can modify the tree if you want a different facility arrangement. Select the point where you want to add a location by either right clicking on it or left clicking on it and clicking on the Add New button on the toolbar. Select Location from the drop down list and click. A folder will appear below and to the side of the item selected. A highlighted box for you to type the location name appears to the right of the location folder. When you have entered the name the location has been added.

You can add as many sub-locations as you wish. For example, the Collins Building (location), Basement (location), Furnace Room (lock). A location can have both a sub-location and a Lock of the same name. This is useful if the location has an entry door with controlled access. However, one cannot have two identical items attached to a single node with the same name. In the example above, "Basement" could be the name of a Lock attached to the Collins Building as well as the location. There could not be two locations named "Basement" attached to the Collins Building. The OFM will not prevent you from repeating names if they are not attached directly to the same node. However, using identical names for different points in the hierarchy can be confusing and should not be done without a good reason.

Adding Locks

Adding Locks to the tree is done in a manner similar to that of adding locations. However, when you select Lock, a property sheet will appear for you to enter some information. At the top of the page is a field to enter a descriptive name for the Lock. Next is a drop down box to select among time schedules that have been defined. If you haven't defined any at this point the choice will be "none". You can add this later. A Lock and battery installation date are set to today's date by default, but they can be changed by typing in a desired date. A serial number and model number can optionally be entered to facilitate recording history of the Lock.

The Next button brings up a display of users in the Facility that can be assigned to the new Lock. At least one user must be a Programmer, but all the other users may be assigned as desired at this point. Please note that users may be added from their individual user groups, or users may be selectively added from a list of All users. When all desired users have been added, click Finish, and you will see a window allowing you to select a Mobile Device to be a partner to the Lock. Once this selection is made, all the necessary steps to enroll a Lock in the system have been completed. All that remains is to update the Mobile Device (the lightning symbol on the toolbar) and to visit the Lock. At the new Lock, you will have to specifically select it on the Mobile Device's screen for initial programming. After this one-time selective programming, the Lock's identity has been established and future connections will be automatic.

Setting Up Time Schedules

Overview

Time schedules are established to change the access level and group enablement at specific times for each Lock in the system. Schedules may be different for each Lock or group of Locks, but generally there will be a small number of schedules in use in the facility. After a schedule has been set up, it can be installed on a set of Locks by simply selecting the Locks for application. The schedules are set up to repeat on a weekly basis. Each day of the week can be programmed to be different, or a daily schedule can be copied to other days of the week. For example, a schedule can be set up for Monday then copied to the rest of the workweek, ending on Friday. A separate schedule for Saturday and Sunday can be made. In addition to the regular schedule, Holidays may be added which will override the daily schedule on the date of the Holiday.

The Master Schedule sets the access level for each scheduled event. For example, at 8:00 AM the schedule may call for ID Required, then at 10:00 AM Unlocked, then at 5:00 PM ID Required again, and finally at 10:00 PM Lockout. As explained earlier, all groups are subject to a single set of access level restrictions, but when an ID is required, entry permission for each group can be enabled or disabled at the times determined by the Group Schedule. In fact, in some installations, ID is always required, but the groups are enabled or disabled according to schedule.

Setting Up a Master Schedule

Click on the Time Schedule Icon on the toolbar to bring up a list of time schedules. If this is the first schedule to be installed in the system, you will not see any schedule names listed; otherwise there will be a list of previously defined schedules. Either right click and select New or click on the New Item on the toolbar to bring up a wizard to lead you through the process of making a new schedule.

The first box is for the master schedule. You must select a day of the week and the New button to bring up a dialog box to set up a Time Schedule Event for that day. This box allows you to set a time for the event and, by clicking on the small arrow at the edge of the access level box, you can then select an access level to become active at that time. If ID will be required, you can select whether a PIN will also be required using the check box. You also have a check box to prevent the normal manager override if you don't want manager control of the access level after the event time. At this time you should normally set up all of the events for the day.

Once the day's schedule has been established you can set up the schedules in the same way for other days. However, you probably will want to use the schedule you have just set up for other days of the week. To copy the schedule, highlight the day you have set up and click Copy; now click the target day you want to copy to and click Paste. You can repeatedly paste from a single copy. Before you leave the Master dialog box, you should have set up schedules for every day. Note that if no schedule is set for a day, the Lock just stays in the last level set for the previous day(s). This may be OK, as for example if ID is required on Friday evening, it may be that this is the desired level for the weekend and no other levels need be set for Saturday or Sunday. The Delete button works in the normal way, serving to delete any selected item. When you are satisfied with the Master Schedule, click Next (if you later decide to change something, you can go back).

Setting Up Group Schedules

After clicking Next on the Schedule Wizard, the Group List will show up. All the available groups will be listed. Click on a group expand button and you will see the days of the week shown. Select a day of the week and right click or select the New button to bring up the dialog box to add a group event. Here you set the time for the event and make the choice to deny or allow access by clicking on the desired button. Add as many events as you need. Each group you want to set up can be done separately, but the copy feature is also available.

You can copy events using the same process as for the Master Schedule. Individual events can be copied to the clipboard and pasted to any day and any group. Once copied, the event is on the clipboard and it can be repeatedly pasted as required. If you want to copy an entire schedule from one group to any other, just select a group you have set up and copy it to the clipboard. You can paste the copied group schedule to another group or set of groups. Use the Delete button to remove any selected item that is incorrect, or that you want to change.

After setting up the group events, the next step is to set up special schedules for Holiday periods.

Setting Up Holidays

Holiday schedules override the normal daily Lock schedule for a specified period. It is common for a year's holiday periods to be set up at once. The OFM allows for setting up Holiday Periods for up to one year in advance. Each holiday is set up separately; Click New to bring up a dialog box to be used to define the holiday. For convenience, each holiday is assigned a name. The Start and Stop times must be set as well.

The access level can be set once for the entire period, or one of the daily schedules previously created can be used. For example, the holiday period might be set up to use Sunday's schedule because the holiday requirements might be identical to a non-working day. Alternatively, it might be desirable to set Lockout during the entire period. If a daily schedule is selected, all of the events associated with the daily schedule, including group enablement, will apply for the period of the holiday. If a fixed access level is set, there are further choices to be made. If an ID will be required, there are the usual options of requiring a PIN during the period and whether manager override will be allowed. These are set using the check boxes. Also, different groups can be enabled as desired using the group check boxes.

After the desired holidays have been set up, the next step is to enroll the time schedule in the Locks to be governed by it.

Lock Enrollment

A tree view of the Locks in the facility allows selecting the Locks for enrollment. 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, the next window provides an opportunity to assign a name to the Time Schedule.

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.

Deleting, Modifying Existing Schedules, 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 Properties (double left clicking also brings up the property sheets). The properties of the schedule will be shown on a tabulated table. Select the tab for the property you need to modify, select the property to modify and change it as desired. Once in a tab window, the process is identical to using that part of the Wizard to create a new schedule.

Right clicking on an existing schedule and selecting Copy sets it up as a template for a new one. From here on the process is just like creating an all new schedule, but all of the events in the template have already entered. The schedule-creating wizard shows up and you can modify any event, 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.

Reporting Features

The Locks keep a record of every significant access control event. This includes, among other things, user entries, access level changes and entry attempts by unauthorized users. An audit report allows the security manager to see each event. Another report shows user properties and facilitates the distribution of new PINs when required. The Lock report shows who is enrolled in each Lock and other properties of the Lock that assist in maintaining the system. To generate a report, start by clicking Reports on the main menu. Choose between Audit, Lock or User to bring up dialog boxes for entry of desired report characteristics.

The Audit Report

Audit reports can be set up and used in a variety of ways. Some security requirements call for maintaining a continuous and complete log of all audit events. Others may only want to print or view a report when a breach of security has occurred. The OFM provides a flexible way to generate reports to accommodate a variety of requirements.

The Audit Report dialog box allows for the selection of specific Locks and users to include. The tree view on the left shows the Locks in the facility. Selecting a folder will include all of the Locks in that folder and its sub-folders. Thus you can make a report for the entire facility by clicking on the top Facility icon. Or you can make a report for just one Lock in the system. Select users from the text box to the right. Here you can select All, or by selecting the button to the right, a list appears for selection. A starting and ending date and time can be set, to just show the period of interest. You can choose to show the selection criteria on the first page of the report and to print each Lock's report on a separate page.

Lock Report

As is typical of the OFM, the Locks are shown on the tree view and any level can be selected to create a report showing a single Lock or all the Locks in an entire location or facility. All the pertinent properties of the Lock(s) are shown. Enrolled users can optionally be left off to produce a shorter report geared for Lock maintenance.

Users Report

By selecting the obvious check boxes, a report can be configured to show various properties for each user, or a selection of users. The various report possibilities permit the printing and dissemination of desired information without disclosing confidential data. If PINs are used, users need to be informed of their new PIN in conjunction with a recode period. For this purpose, you may find it convenient to print a new page to be delivered to each individual user.

Updating the OFM from the Mobile Device

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. 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

|| Chapter 4 || The OMNILOCK Data Link(ODL)

Overview

The OMNILOCK Data Link (ODL) runs on a Mobile Device. To install the program on a new Mobile Device, first connect the device to the PC docking adapter. Assuming that you have already established a partnership between the host PC and this Mobile Device using ActiveSync before you installed the OFM, you can install the ODL program. This program is installed from the Windows Start Menu. Select Programs, then OSI Security Devices, and finally Set up New Mobile Device. Ideally all of this should have been accomplished at the time you installed the system software on your 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, 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

Data synchronization with the OFM is described in the OFM section. Once programming data has been transferred to the Mobile Device, it is ready to transfer data to the Locks enrolled with it. To run the ODL, select the Start menu of the Mobile Device with the stylus. Select OMNILOCK Link and the main window will appear. It will show the OSI logo and, prominently in the center, the number of Locks requiring programming. Below that is an actual list of the Locks that must be visited to transfer data. The menu at the top accesses the Facility Explorer and, under Lock, a choice to run diagnostics, to set the access level, and to download a new operating system to a Lock. The latter choice will be gray and inaccessible unless a file with the Lock operating system has been placed in the Mobile Device.

How the Mobile Device Works with the OFM

Data is transferred between the OMNILOCK Facility Manager and the Locks in the system using the Mobile Device. These devices require a serial (RS-232) connection to the host PC running the OFM, typically through a docking station that also provides power to recharge the Mobile Device's battery. Data is transferred between the host and the Mobile Device using ActiveSync, a program normally supplied with the Mobile Device for installation on the host PC. The serial communications and the partnership between the host PC and the Mobile Device should be set up according to the instructions provided by the manufacturer of the Mobile Device. Note that the OFM requires a "partnership" with the Mobile Device for programming; it will not work with a Mobile Device registered as a "guest". However, a guest device can be used to collect audit data from the Locks, as long as it is registered within the Facility. To set up the partnership, select Data Exchange on the dialog box that appears after the first connection. See the ActiveSync instructions that came with your Mobile Device for more information.

To ensure unambiguous reconciliation of downloaded data to the OFM database, the OFM allows only one Mobile Device to transfer programming data with each individual Lock. Multiple Mobile Devices can be assigned to a facility, which makes possible simultaneous data transfer to various parts of the facility. Clearly this can be advantageous for a large facility, as the work of transferring data can be accomplished by several employees working independently. In such cases, each Mobile Device has its own private set of Locks to program and there is no possibility of a Lock appearing on more than one Mobile Device. Once the Mobile Device has been connected to the PC running the OFM, updated data is exchanged between the Mobile Device and the host PC when requested by the user through the OFM. Programming actions taken at the PC will show a "pending" status until the Mobile Device has made a successful data exchange with the affected Lock(s) and confirming data has been exchanged back to the OFM.

Using the Mobile Device to Exchange Data with Locks

Upon completion of the desired programming actions at the OFM, and selection of the Data Exchange button, data will be downloaded to the Mobile Device. To transfer the data to the Locks, remove the Mobile Device from its docking station. You can launch the ODL program on the Mobile Device either by selecting the program from the program choice bar, or (if you have one set up to launch the ODL) by pressing a hot button on the Mobile Device. See the instructions that came with your Mobile Devices for Information on setting up a hot button. When the ODL launches, you will see the OSI Logo and a window showing the number of Locks to program along with their names. The Mobile Device must be carried to each Lock requiring programming. With the ODL launched on the Mobile Device enter a Programmer ID at the Lock. The infrared communication window of the Mobile Device must be held within range of the Lock's window within six seconds (or the open delay time) after the ID has been entered. The following diagram shows the region for effective communications at the front of the Lock. The distance over which communication can be maintained depends upon the Mobile Device. Many will work up to 2 feet (60 cm) or more, but those with low-powered infrared ports must be held within 6 inches (15 cm). Once the IR ports are in range of each other, the ODL program will initiate a connection with the Lock, and then automatically transfer pending data to the Lock, as well as collect Audit Log and pertinent Lock status data.

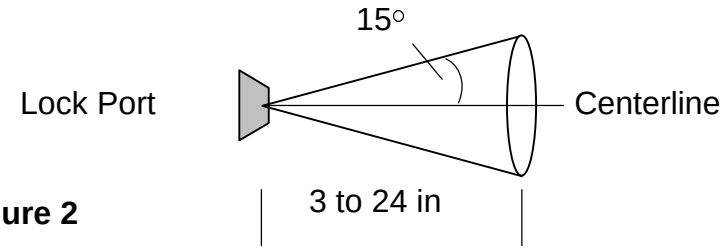

Figure 2

Programming a Lock for the First Time

When a new Lock is first placed in service, it will not be known by location and name to the system. The list of Locks to be programmed will show on the main pane of the ODL with their locations. To assist in finding them, you can select Facility Explorer and see a convenient tree view of the facility. This works similarly to the Facility Explorer of the OFM, but because of the shape of the screen on the Mobile Device, the listing of items in the open folder is below the tree view rather than next to it. You will have to select the Lock for programming and this will determine its identity thereafter. Accordingly, you should be careful not to make a mistake and select the wrong Lock or you will have to reset the Lock and start over.

When you are in front of the Lock, launch the ODL and point the Mobile Device's IR port at the IR window of the Lock (it's just above the lever handle on a cylindrical lock and just above the key cylinder on a wall mount or mortise system). Key in the default Programmer code (1-2-3-4) to activate the Lock. The device will establish a communication link with the Lock and you will then have to select (carefully!) the named Lock to be programmed. Once selected, the programming will proceed without further intervention. When programming has been completed, a message window will inform you that data exchange is complete. Select OK to acknowledge the message and you can proceed to the next Lock.

Programming Locks Already in the System

Once a Lock has been programmed for the first time, it will be known to the ODL. If its programming data needs to be changed (for example, the enrolled user list has changed), it will show up on the Mobile Device as a Lock requiring programming. As above, the Mobile Device must be running the ODL and pointed at the Lock. Now the programmer will have to enter his or her Programmer ID to the Lock (either by card or code) to allow the ODL to log on to the Lock. Immediately after the Lock has verified the Logon ID, the data exchange will take place automatically. In this case, it is not required to select the Lock, because it is automatically identified by the system. At the same time, any outstanding audit data is collected.

Setting Access Levels and Running Diagnostics

If a user has a Programmer ID with the right of access, it will be possible to change the access level, enable groups and to run diagnostics for a Lock. From the main menu, select Lock; selecting this brings a choice of two views, Access level and Diagnostics. Selecting Access level provides a drop-down box allowing a selection of access levels to be set, and a set of check boxes, one for each group. To use this window, first run the ODL and select Access Level, then enter a Programmer ID to establish the infrared connection. The drop-down box will show the current access level and the check boxes will display checks for each group enabled. If you want to change the access level, click on the arrow button at the side of the drop down box to see the possible selections. Click on one of these to select it. Then click on any of the group check boxes you wish to change. Click on the Apply button when you have completed your selections. If you want to check that the Lock is now in the desired state, click on Refresh and the display will read the state as collected from the Lock. When you are done, click Log off and the connection will be terminated.

To run diagnostics, select Diagnostics, as above. The Mobile Device will display the diagnostics window and, as soon as you have established the infrared connection to the Lock, will display:

The hardware version, the second number is the firmware revision number and the third is the firmware release number.

1) The battery voltage in millivolts, typically about 5000 mV
2) The number of samples, a number indicative of the length of the motor running period, typically about 8.
3) The motor voltage and current, typically about 1250 mV and a few hundred milliamperes.

There are three buttons immediately below the diagnostic data display. One activates a Drive test, which runs the Lock through a number of unlock/lock cycles. Another button brings up a Keyboard test window with a dummy keyboard depicted on the screen. When you press each key on the Lock, the corresponding "key" on the display should appear as depressed, then return when the key is released. The third, Update OS, replaces the operating system in the Lock with one from a file that has been loaded into the Mobile Device. **Do not use this function unless you understand the results of this action**. The Maintenance section of this manual contains detailed information about this. (see Page 56)

At the bottom of the display are two additional buttons. The Refresh button brings new data to the display from the Lock. For example, after running the drive test, you might want to recheck the battery and motor voltages. Use the Log off button when you are finished with the tests to disconnect from the Lock. If you just leave without logging off, the Lock will time out in 30 seconds anyway, but this wastes battery energy, and the lock is in the unlocked mode during this period.

Closing the ODL–A Word About Synchronization

Before you return the Mobile Device to its dock at the PC, you must click the X (you may have to do this more than once, depending upon the view that is displayed) at the upper right hand corner of its display to terminate the ODL program. Depending upon the Mobile Device, failure to do this will make it impossible 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 ODL program and plug it in anyway, simply unplug the device, close down the ODL, and reconnect it to the PC.

Updating the OMNILOCK Facility Manager

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. 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

Notes:

|| Chapter 5 || Lock Operation

Introduction

While almost all of the control of the Lock is done by transferring programming information using the Mobile Device, there is some control over the Lock state, which is accomplished without direct interaction with the OFM, by the holder of a Programmer ID or a Manager ID. The Lock responds to user keypad programming inputs by flashing its red or green light when a Manager uses it to make programming inputs. A General User may notice that the Lock will occasionally flash different color lights, depending upon its state. The meaning of these responses will be fully described below.

User Type General

Enrolled ID Required or Facility Card Required

The General User can only gain entry. There are no control features available for modification by a General User. If the Lock is locked, entry is obtained by either entering a code or inserting and removing a magnetic ID Card. If the Lock recognizes the ID and entry is permitted, the green light will flash once and the Lock will unlock. The Lock will remain unlocked for the Open Delay Period, then the red light will flash once and the Lock will relock. If the Lock doesn't recognize the ID, or entry is not permitted (e.g. the User's group is disabled at that time), the red light will flash once, but the Lock will not unlock. In the event that the Lock is unlocked, entering the ID will cause the green light to flash three times, indicating that the Lock is already unlocked and that no ID is required.

Enrolled ID + PIN Required

The Lock may be in a state where a PIN is required in addition to the card or code ID. When this state is active, the green light will flash twice when the Lock recognizes the ID and the user has the right of entry. This signifies that the Lock has accepted the ID and that the user must now enter a PIN to complete the identification process. Once the PIN has been entered, the Lock action will be as described above.

Low Battery Warning

If the red light flashes twice immediately after the green entry indication, the battery energy level is low and management should be informed so that replacement can be scheduled.

User Type Manager

Manager Rights

Managers have certain rights assigned to them. The Lock will respond in accordance with those rights. In addition, because the manager has these rights, a PIN may always be required for access, depending upon how the manager has been defined by the OFM. If a PIN is required, the green light will flash twice when the ID has been successfully entered, indicating that a PIN must be entered. If the PIN is entered correctly (or if one wasn't required) the green light will flash once and the Lock will then be unlocked. For a period of five seconds (or the Open Delay Time, if longer) the Lock will wait for a further key-press, and if none is detected, it will flash red twice and relock (unless the Lock is in the unlocked state in which case it will just remain unlocked).

Lock Management Actions

The management functions which may be authorized are: (1) Enabling or disabling entry for the manager's home group, (2) Enabling or disabling all groups, (3) Setting the access level. A manager ID with no rights assigned can be useful, because that manager ID will always have right of entry regardless of access level, except *Shutdown*. The OFM Manager Enrollment dialog box controls the right to use each function. The functions are hierarchical in that (3) implies (1) and (2), and (2) implies (1). For example, if the manager has the right to set the access level, he will also be able to enable and disable any group etc. At the Lock, these functions are accessed through the keypad, during the open interval. During this interval, any detected key-press will cause the green light to immediately flash once. This indicates to the manager that the Lock has detected the key-press. The instructions below assume that a Manager ID has been successfully entered and the actions described are taken during the Open Delay Interval.

Home Group Supervision

Enabling or disabling the manager's home group is a toggle function accessed by **pressing** and **holding** the ***CL*** key until the green light starts its three-flash sequence. If the home group was disabled it will now be enabled and vice-versa. Since the manager may not be certain whether the home group is currently enabled or disabled, the status may be checked by *briefly* pressing the ***CL*** key during the open interval. If enabled, the green light will flash when the key is pressed (confirming the key-press) then, after a short delay, green again; if disabled, the flash immediately following the key press will again be green, but the second flash will be red.

Group Control

Groups may be enabled individually or generally. Pressing ***1,*** followed by holding the ***CL*** key down until the three-light sequence starts, enables all groups. Similarly, pressing ***0…CL (HOLD)*** will disable all groups. For individual groups, press either ***1*** or ***0*** to enable or disable, then the group number(s) followed by ***CL (HOLD).*** Thus ***0…3…5…CL (HOLD)*** will disable groups ***3*** and ***5***. If a mistake is made when entering numbers, press the ***CL*** key and re-enter the entire sequence.

Group control is an overlay of enabled groups. For example, assume that the Lock is in the Enrolled *ID Required* state, but with no groups enabled. Manager John arrives and enables groups 1 and 2, and later Manager Alice enables groups 3 and 6. At this time, groups 1, 2, 3, and 6 will be enabled.

Setting the Access Level

The table below describes the access level corresponding to each numeric keypad entry. To set the access level, press the numeric key corresponding to the desired access level, then press and hold the ***CL*** key. This action will set the new access level, and for levels 3, 4, 5 and 6, enable all groups. For these levels, if you only want to enable one or more group(s), enter the group number(s) after the access level. For example, to allow entry with enrolled ID for groups 3 and 5 only, press (during the open interval) ***5…3…5…CL (HOLD)****.* Group settings do not overlay when set in conjunction with setting the access level. Thus, only those groups *specifically selected*, regardless of any previous actions, will be enabled when setting the access level; all others will be disabled**.** Of course, once the access level has been set, you can enable or disable groups as described above.

Access Level Description	**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 (Manager or Programmer only)	8

User Type Programmer

Like the Manager ID, the Programmer ID has rights that can be assigned to it by means of the OFM dialog box. Since the main function of the Programmer is to transfer information to/from the Lock and entry is not a requirement for this, unlike other IDs, the Programmer may or may not have the right of entry. This allows for personnel who are not cleared to enter an area to nevertheless distribute and collect data at the Lock. Other rights are (1) Setting the access level and groups enabled and (2) Running diagnostics. Right of entry is required for either of the two rights. In effect, without entry rights, the only activity allowed is data exchange. As with the Manager ID, the Programmer can be set up to always require a PIN in addition to the basic ID. As usual, the green light will flash twice upon entering the ID correctly, indicating that the PIN must now be entered.

Once the correct ID (or ID + PIN) has been entered, the Lock will flash green once per second. (The first flash indicates correct ID entry, the next flash will occur anytime from immediately to one second later.) This indicates that the Lock is ready to communicate with the Mobile Device assigned to it. If the ID has the right of entry, the Lock will also unlock. The Lock continues to be ready for five seconds (or the open delay time, if longer); if communication is not established within that period, it relocks (if not in the unlocked state) and flashes the red light. As a practical matter, the Mobile Device should be set up for communication before entering the ID; then it will be ready to communicate as soon as the ID is entered and the Lock starts flashing its green light.

As soon as the communication connection is established, the Lock will send the audit data to the Mobile Device and the Mobile Device will send any pending programming data to the Lock. The user may then proceed to run diagnostics or set levels and group access using the dialog boxes on the Mobile Device, assuming rights associated with the ID allow it. Upon logging off, the Lock will relock, if appropriate, and communications will be terminated.

User with a Facility Card

A Facility Card can be used in any Lock within a facility when the Lock's access level is set for Facility Card entry. This is useful for common areas that all users need to enter. For example, the lobby or rest room of an office building would be accessible to all users, but a specific ID would be required for entry to an individual office. This feature of the system requires card access and that all Users' cards be programmed with a common facility ID in addition to their personal ID. When a Lock is set for Facility Card access level, any card with the common facility ID can unlock the Lock. Operation is normal; i.e. after inserting and removing the card, the Lock will unlock, flash a green light, wait for the open period, then flash the red light and relock. No audit record of entry is made when in Facility Card access level. Programming actions by Managers or Programmers will be recorded, however.

User with a Service ID

The service ID feature is useful for short-term entry by personnel who will not need access on a long-term basis. For example, contractors employed to perform a single equipment service or repair. The service ID is assigned to a separate group and always requires an ID + PIN. The recode interval for the PIN can be made as short as one day. After the recode interval, a new PIN is required. After correctly entering the ID card or code, the green light will flash twice, and then the PIN is entered. The green light will flash once and the Lock will unlock. After the Open Delay Time the Lock will relock and the red light will flash.

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. The event is recorded in the Audit Log.

Key Detection (Option 1)

This Feature detects when the Lock has been unlocked with a standard key and makes an entry in the Audit Log.

Notes:

|| Chapter 6 || Access Control System 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 the 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, 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 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 sheet for the new facility that you are about to create. Type in "Sample" for your facility on the top line. 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. 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 a 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". If these settings are all correct, click the OK button.

The system automatically adjusts the clocks in the Locks for Daylight Savings time changes. North American practice 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, select Finish.

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. 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, 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:

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

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

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 sheet for that group. Type the name “Office Staff” in the name window. 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. 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”, set Autocode, 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, establishing the user database is the logical third step in setting up a Facility. To bring up the User Pane, click on the User icon (the single human face). To add a new user, either select the Add New button on the toolbar, or right click on any blank area of the pane and select New. A property sheet 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 (obviously, 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 Next 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. Select a default ID type of Programmer. You will now have the choice of privileges; select Entry, Set access level, and Run Diagnostics. Do not select PIN Required. Click Next to make a group assignment. Select group 1, Office Staff. Click Next; this will bring up a Lock enrollment pane, but since no Locks are in the system yet, click Next again. Now the Pane will allow reference information to be added to the database. This is optional; it might include a home phone number or other pertinent information. Click Finish to enroll the user in the system.

The next user will be a Manager. Type a name and leave the code as it is. Select Manager for the default Lock ID type. Select Supervise Home Group, Set Group Access, and Set Access Level, then Next. This user is also an office staff member, so select group 1. Click Next and Finish to enroll this user.

The last user we will set up will be a general user. Type a name, and select Card. If you have a card reader connected to 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. 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 group 2, Cryptographers, and step through the remaining two panes 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 pane by clicking on the Time Schedule icon (the one with the clock and schedule book) on the tool bar. Select the New tool bar button, or right click on the blank area and select New. The first pane 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.

Repeat this five times for Monday, setting the schedule 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 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 persists on the clipboard).

For the weekend, set two events for Saturday: 8:00 –ID Required, PIN Required, and 17:00 –Lockout. Copy this to Sunday. This completes setting the access level for the weeks. Click Next to move on to the groups.

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 pane; click Next to advance to the Holiday pane.

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 a pane 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 pane.

The final pane 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

This step requires that you have a Mobile Device you wish to enroll connected to your computer and established as a partner through ActiveSync. Furthermore, you must have already run "Install OMNILOCK Data Link" from Programs: OSI Security Devices on the Windows Start Menu Bar. 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, 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

Click on the Mobile Device icon to bring up the Mobile Device pane. Click on the New icon or right click and select New from the menu. The OFM will connect to the device and identify it. 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 at this time by selecting the Locks tab. Since there is none enrolled, just click OK to finish the enrollment of the device.

Sixth Step, Enrolling Locks

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 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. 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 button 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.

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 pane.

The User Enrollment pane is a list box showing all the users currently enrolled in the OFM database. If you just want users from a specific group listed, you can select that group by clicking on the button to the right of the User Groups test box to display the individual groups. You can try this, but finally 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 added 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.

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 press the reset button (for 3 seconds) 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.

With the Mobile Device you have partnered with the Locks connected to the computer, 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 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 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 enter the default Programmer code of 1-2-3-4, or use the default Programmer Card to activate the Lock. Immediately point the IR port of the Mobile Device at the Lock's IR window (it's just above the handle). The tree view on the Mobile Device will present a Facility Explorer with the locations and Locks to program. Using the stylus, select the location for the Lock then select the Lock itself, then press OK.

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 remove the Mobile Device from its dock, exit 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. 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

Notes:

|| Chapter 7 || Maintenance

Lock Maintenance

Battery Replacement

Battery replacement will be required when the voltage of the batteries indicates that long term continued operation will not be possible. The Lock gives a red warning light with each entry, and, when 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, more than a thousand 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.

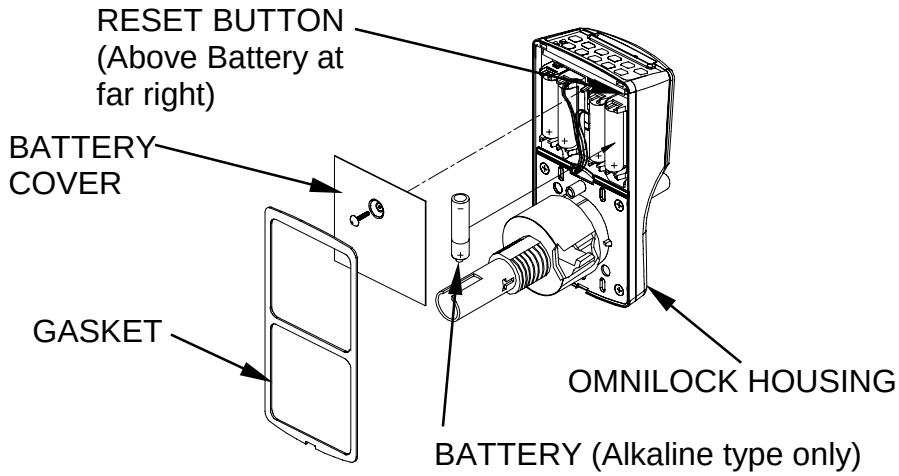

Figure 3

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 void warranty.**

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. After the new batteries have been installed, the Programmer must reset the access level to the desired level using the Mobile Device.

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, press and hold the Reset Button for about three seconds until you observe the green indicator on the Lock keyboard flash, then release the button.(see Fig 3 Page 51) After several seconds you should hear the Lock operate and the green indicator should flash several times. (A red flash indicates an inoperative component on the PC board or the drive system.) The Lock will now be in a reset state, and will not be recognized as an enrolled device by the system. It is the same as a new Lock as far as the system is concerned, however, it can be refreshed by the system. (see Page 53)

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.**

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**.

Mobile Device Maintenance

The Mobile Device connects to the desktop computer and its battery charger with a connector built into its desktop stand. It is important that the contacts remain clean. In a normal office environment, the regular removal and replacement of the device in its stand should keep the contacts clean. However, if they do get dirty enough to be unreliable, a small amount of contact cleaning spray (available at electronics stores) can be sprayed on and the contacts gently cleaned with a soft brush.

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. (see Page 53)

Maintenance Features of the OMNILOCK Facility Manager

Refreshing a Lock

If a Lock is new or has been reset so it has the default programmer ID, it will not be known to the system. If the reset Lock replaces a Lock in the system, in all likelihood you will want the replacement Lock to replicate the one removed. If the Lock has not been reset and is still functional, you should collect all audit data before you refresh it, and be sure to connect and synchronize the Mobile Device before you set up to do the refresh.

For the new or reset Lock, simply select the Lock using the Facility Explorer and right click on it (or select Edit), select Refresh and then select Yes. When you are ready to update the Lock(s) press the Data Exchange (lightning icon) button and select the appropriate Lock for programming. The Mobile Device is now ready to be taken to the Lock(s) to accomplish the refresh.

The screen of the Mobile Device will show the Lock(s) requiring programming. Enter the Programmer code (1-2-3-4 for a reset or new Lock) to obtain a connection to the Mobile Device. Select the desired Lock on the Mobile Device tree view, then OK, and a complete set of replacement data will be downloaded to the Lock.

While it is possible to refresh a Lock already known to the system, it is almost inconceivable that this would ever be required, and is not recommended. However, if you decide to do it anyway, the process is almost the same. In the case of an enrolled Lock, you will not have to select it for programming on the Mobile Device; it will identify and program the Lock as soon as the infrared connection has been established.

Refreshing a Mobile Device

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. It can be refreshed (or a new device programmed to replace the old one). First it will have to be partnered with the desktop computer using the normal procedure with ActiveSync, and then run “Install the OMNILOCK Data Link” from Programs:OSI Security Devices under the Windows Start menu. Be sure the device is connected to the desktop PC. After it has the ODL installed, under View Mobile Devices in the OFM, select the device that has been lost and right click on it (or select Edit) and select Refresh. The recharged or replacement device will now have the identity of the old one. Audit data collected on the original device will, of course, be lost.

If you feel that the audit data is important enough to go to some extra trouble, you can collect what audit data still remains in the Locks. To do this, you must refresh the partnered Mobile Device used to program the Locks with potentially lost audit data. You can then visit the affected Locks and collect all the audit data in each Lock that is partnered with the Mobile Device. This will take a minute or two for each Lock, but you will have all the data that is available.

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 Data

The database files are located in the Facilities folder under the OFM executable file. 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, 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.

Lock Operating System Replacement

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 it 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.

Importing the Lock Operating System File

First, there must be a file containing the replacement operating system that the OFM is able to access. This file may be on a disk, downloaded from the Internet or other media, etc. In any case, it must be accessible from the OFM. The default location of the Lock Operating System file is the "LOS" folder under the OMNILOCK Facility Manager folder

"C:\Program Files\OSI Security Devices\OMNILOCK Facility Manager\LOS"

on your PC. The "LOS" folder will normally be empty until you receive and install a file with a more recent version of firmware than the version that is currently in your Locks. The file name includes hardware and firmware revision codes with the extension ".los", ie. Om2kv105.los, where 105 is the version number "1.05".

The OFM can only transfer the LOS to a partnered Mobile Device registered in a Facility. Be sure that the Mobile Device you intend to use to transfer the new LOS is connected and registered in the Facility containing the Locks to update. With the OFM running on your PC, click on Tools located on the menu at the top of the window. Select Lock OS Manager. A dialog box will appear offering the following 3 choices: Install, Remove, and Cancel. If a file has already been installed into the Mobile Device, the current version number will be displayed above the buttons. Otherwise, the message will state that there is no file installed on the Mobile Device. Selecting Install will cause a Windows file browser box to be displayed so that you can select the location where the file you want to download is located on the PC.

After you select the file to transfer, the download will start. This will take several minutes, due to the way that Microsoft ActiveSync handles the file transfer to the Mobile Device. During the course of the transfer a progress bar will indicate that the file is in the process of being transferred to the Mobile Device. When the transfer completes, the Mobile Device will then be able to transfer the LOS to any Lock in the Facility, or to a new or reset Lock.

When all of the Locks requiring a new LOS have been updated, it is good practice to remove the LOS from the Mobile Device in order to avoid an inadvertent update and attendant loss of data.

Transferring the Lock Operating System to a Lock

The Mobile Device must be enrolled in the facility containing the Lock in order to be able to connect with it, or the Lock must be in a reset state. To put a Lock in the reset state, remove the rear cover and press the button in the upper right hand corner for three seconds, until the green light flashes, then release the button. Launch the OMNILOCK Data Link on the Mobile Device and select Lock and Diagnostics. Make the infrared connection to the Lock in the usual way; after the diagnostic data display shows the Lock data, select Update OS. This will cause a dialog box to appear asking for confirmation that you want to replace the version number on the Lock with the version number on the Mobile Device. You will also be warned if you are about to replace a newer version with an older one. After confirmation, you will see a progress bar showing that the download process is running. The download will take about one and one-quarter minutes, then another 15 seconds for the Lock to reprogram the flash memory.

When the memory has been reprogrammed, the Lock will run a self-test and clear all data memory. When this is finished, the Lock will flash the green indicator five times if self-test has passed. The Lock is now in the “new” state and will respond to the Default Programmer ID (1-2-3-4), or a Default Programmer ID Card. It can be refreshed as described in Maintenance Features of the OFM, Refreshing a Lock (see Page 53).

|| Chapter 8 || Help!!

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 CD available when you call for service. They can be reached by:

- calling our corporate telephone number: (619) 628-1000
- sending a Fax: (619) 628-1001*
- corresponding through our website: http://www.omnilock.com*
- or corresponding by E-mail: osi@omnilock.com*

*Every effort will be made to respond by the next business day.

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 a Return Material Authorization Number (see Page 58). 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

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, either 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 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.

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; nor that the Product will prevent any personal injury or property loss.

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

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

Notes:

|| Index ||

(Back Cover)