CyberAudit®-Web Lite

Notice:
Videx, Inc. reserves the right to make improvements or changes in the product described in this manual at any time, without notice.

Disclaimer of All Warranties and Liability:
Videx, Inc. makes no warranties, either expressed or implied, except as explicitly set forth in the Limited Warranty below, with respect to this manual nor with respect to the product described in this manual, its quality, performance, merchantability, or fitness for any purpose. Videx, Inc. software is sold or licensed "as is." The entire risk as to its quality and performance is with the buyer. Should the programs prove defective following their purchase, the buyer (and not Videx, Inc. its distributors, or its retailers) assumes the entire cost of all necessary servicing, repair, or correction and any incidental or consequential damages. In no event will Videx, Inc. be liable for direct, indirect, incidental, or consequential damages resulting from any defect or the possibility of such damages. Some states do not allow the exclusion or limitation of implied warranties or liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Limited Warranty:
Videx, Inc. warrants this product to be free from defects in material and workmanship for a period of one (1) year from the date of original purchase. Videx, Inc. agrees to repair or, at our option, replace any defective unit without charge. Videx, Inc. assumes no responsibility for any special or consequential damages. No other warranty, either expressed or implied, is authorized by Videx, Inc. Some states do not allow the exclusion or limitation of implied warranties or liability for incidental or consequential damages, so the above limitation may not apply to you.

Copyright Notice:

1105 NE Circle Blvd., Corvallis, OR 97330
Phone (541) 758-0521 Fax (541) 752-5285
http://www.videx.com • sales@videx.com • support@videx.com

Trademarks:

Table of Contents

Introduction

System Setup

Using the Application

Settings and Special Operations

Help and Support

Technical Information

Introduction

CyberAudit-Web Lite is now available as a desktop software application, making it easier for owners of smaller CyberLock installations to control access.

System and Hardware Requirements

CyberAudit-Web Lite may be installed on computers running:

- Microsoft Windows XP or Vista
- Mac OS X 10.4.11 or later with an Intel processor

The computer should have:

- A minimum of 512MB of RAM
- A 1GHz or faster processor
- 4GB of free disk space

The CyberAudit-Web Lite application uses the default web browser to provide a user interface. Supported browsers include:

- Mozilla Firefox (version 2 or later)
- Microsoft Internet Explorer (version 6 or later)
- Apple Safari (version 2 or later)

A complete hardware setup requires one Grand Master CyberKey, an IR Encoder or USB Station, CyberLocks, and CyberKeys.

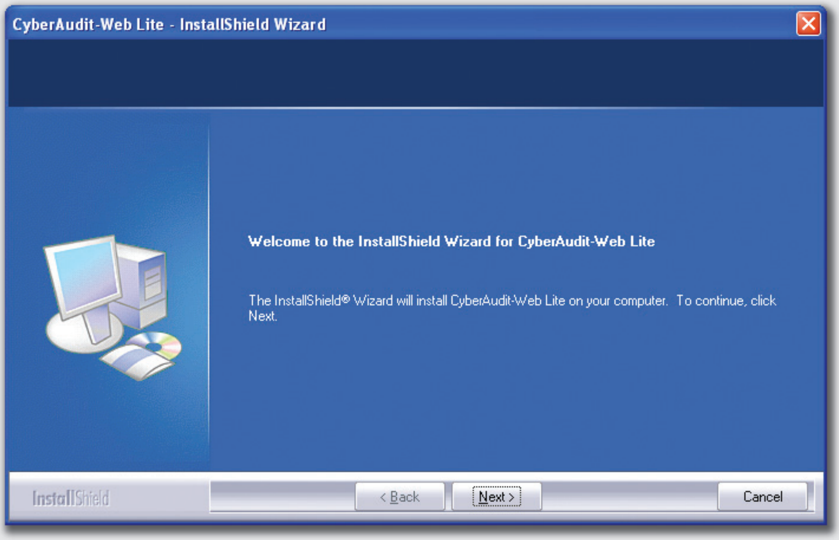
System Setup

Setting up the system includes these steps:

- Installing the software
- Programming locks and keys
- Completing the *Database Initialization Wizard*

Software Installation - Windows

To install the CyberAudit-Web Lite software, insert the application disc into the CD drive. If the InstallShield Wizard does not launch automatically, navigate to the CD drive using the file explorer and double-click the *Lite-Setup* icon.



CyberAudit-Web Lite - InstallShield Wizard

Welcome to the InstallShield Wizard for CyberAudit-Web Lite

The InstallShield® Wizard will install CyberAudit-Web Lite on your computer. To continue, click Next.

Figure 1-1: *Installing the CyberAudit-Web Lite Software*

Software Installation - Macintosh

To begin, insert the CyberAudit-Web Lite installation disc into the computer's CD drive. A window displaying the contents of the disc will appear automatically.

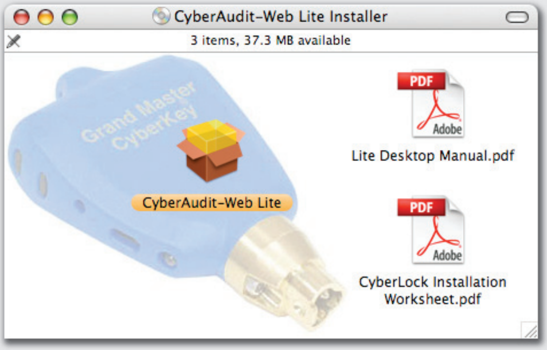
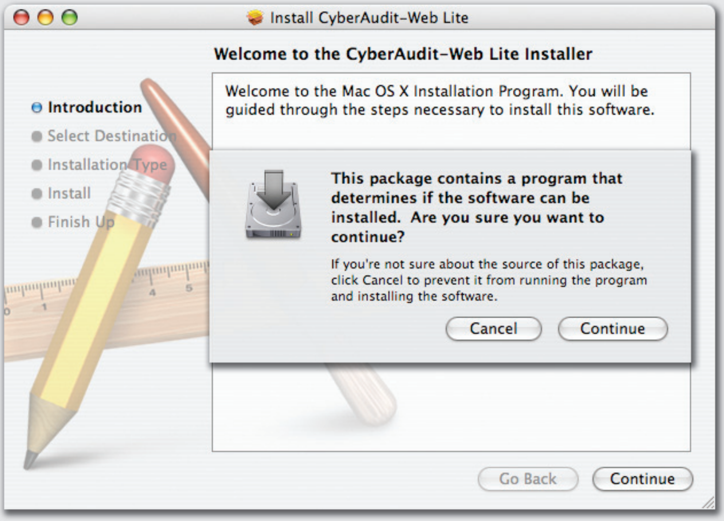

CyberAudit-Web Lite Installer
3 items, 37.3 MB available
Grand Master CyberKey
CyberAudit-Web Lite
PDF
Adobe
Lite Desktop Manual.pdf
PDF
Adobe
CyberLock Installation Worksheet.pdf

Figure 1-2: ***Contents of the CyberAudit-Web Lite Installation Disc***

Double-click the icon for the CyberAudit-Web Lite installer package. The installer will launch and then prompt for confirmation before beginning the installation process. After confirming the install, follow the prompts given on the screen.



Welcome to the CyberAudit-Web Lite Installer

Welcome to the Mac OS X Installation Program. You will be guided through the steps necessary to install this software.

This package contains a program that determines if the software can be installed. Are you sure you want to continue?

If you're not sure about the source of this package, click Cancel to prevent it from running the program and installing the software.

Figure 1-3: ***The CyberAudit-Web Lite Installer with Confirmation Dialog***

Hardware Setup

The simplest method of adding CyberLocks and CyberKeys to the database is to configure them using the Grand Master CyberKey. This special key is used to configure locks and keys. When downloaded, the IDs of the locks and keys it has come into contact with will be automatically added to the database.

Begin by contacting CyberLocks with the Grand Master key. The Grand Master will configure the CyberLocks it contacts with its access codes.

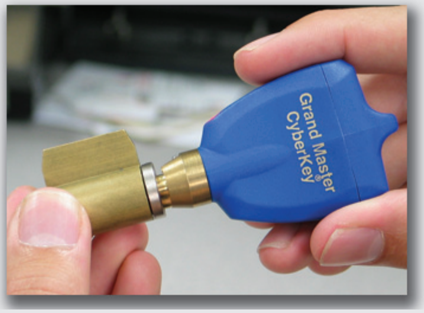


Figure 1-4: ***Configuring a CyberLock Using the Grand Master***

The Grand Master also configures standard CyberKeys using its access code, via infrared communication. Hold the Grand Master and the CyberKey about six inches apart, with the LEDs facing each other. The CyberKey will beep twice when it has been configured. After configuring each key, verify that it will open all of the programmed CyberLocks.

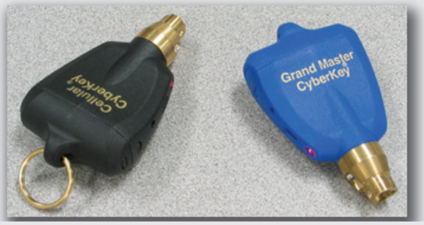
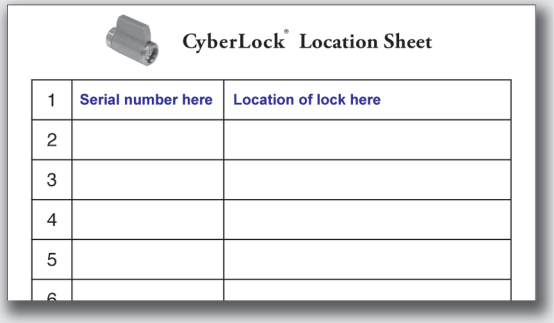


Figure 1-5: ***Configuring a CyberKey Using the Grand Master***

After configuring, install the CyberLocks into their permanent, physical locations. Use the serial number labels and the *CyberLock Location Sheet* (provided in PDF format on the installation disc) to note where each lock is installed.

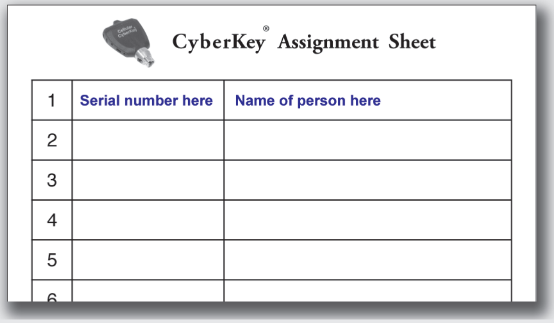


CyberLock® Location Sheet

1	Serial number here	Location of lock here
2		
3		
4		
5		
6		

Figure 1-6: ***Record Serial Numbers and Locations for Future Reference***

Assign the configured CyberKeys to the people who will use them. Use the serial number labels and the *CyberKey Assignment Sheet* (also provided on the installation disc) to record each assignment.



CyberKey® Assignment Sheet

1	Serial number here	Name of person here
2		
3		
4		
5		
6		

Figure 1-7: ***Record Serial Numbers and Persons for Future Reference***

Notes regarding Grand Master keys:

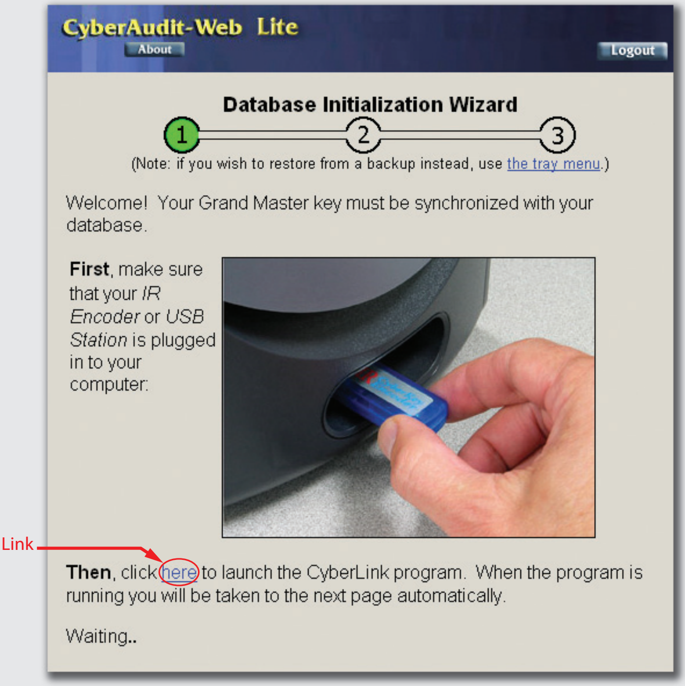
- Grand Masters are able to program CyberKeys for up to two minutes after contacting a CyberLock.
- When Grand Masters are in key program mode, the green LED flashes once per second.
- When Grand Masters are not in key program mode, the green LED flashes once every eight seconds.
- A CyberKey beeps twice to indicate it has been successfully programmed by a Grand Master. If the CyberKey fails to program, remove its battery for approximately five minutes. Then re-insert it and try programming the CyberKey again.

Important: Store the Grand Master key in a safe place when not in use. It is the basis of security for the system!

First Use

After the software has been installed and all locks and keys have been configured, only a few simple steps remain before the CyberAudit-Web Lite system is ready for use. The application assists in the completion of these steps the first time it is run.

To launch the application on a Windows machine, double-click the icon on the desktop. On Macintosh, double-click the icon in the *Applications* folder. Once the application is running, the *Database Initialization Wizard* will appear. This three-step process is designed to help set up the database with information contained in the Grand Master key. Follow the instructions given by the wizard to complete the setup.



Database Initialization Wizard

(Note: if you wish to restore from a backup instead, use the tray menu.)

Welcome! Your Grand Master key must be synchronized with your database.

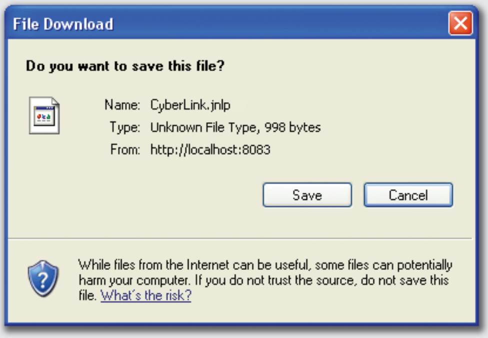
First, make sure that your *IR Encoder* or *USB Station* is plugged in to your computer:

Then, click here to launch the CyberLink program. When the program is running you will be taken to the next page automatically.

Waiting..

Figure 1-8: ***The Database Initialization Wizard - Step 1***

To continue to Step 2, click the link beneath the photo. A file download prompt may appear. Choose to save or open the file and, if available, choose to have the file automatically opened in the future. If a secure certificate warning appears, choose to accept the certificate.



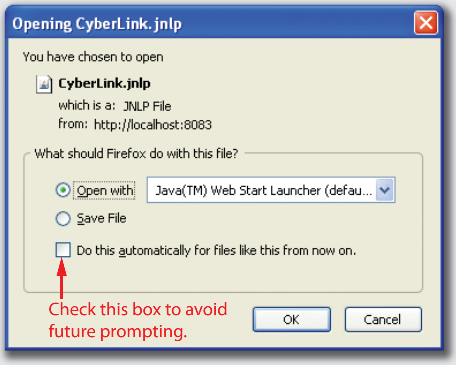
File Download

Do you want to save this file?

Name: CyberLink.jnlp
Type: Unknown File Type, 998 bytes
From: http://localhost:8083

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not save this file. What's the risk?

Figure 1-9: ***Prompt for Action on File Launch (Internet Explorer)***



Opening CyberLink.jnlp

You have chosen to open

CyberLink.jnlp
which is a: JNLP File
from: http://localhost:8083

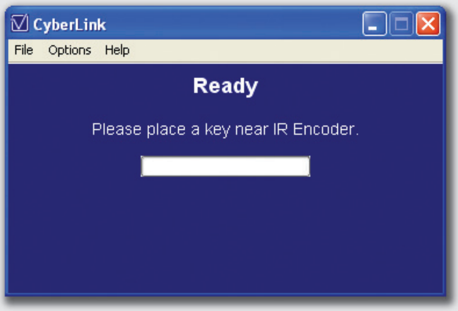
What should Firefox do with this file?

● Open with Java(TM) Web Start Launcher (defau...
○ Save File
□ Do this automatically for files like this from now on.

Check this box to avoid future prompting.

Figure 1-10: ***Prompt for Action on File Launch (Firefox)***

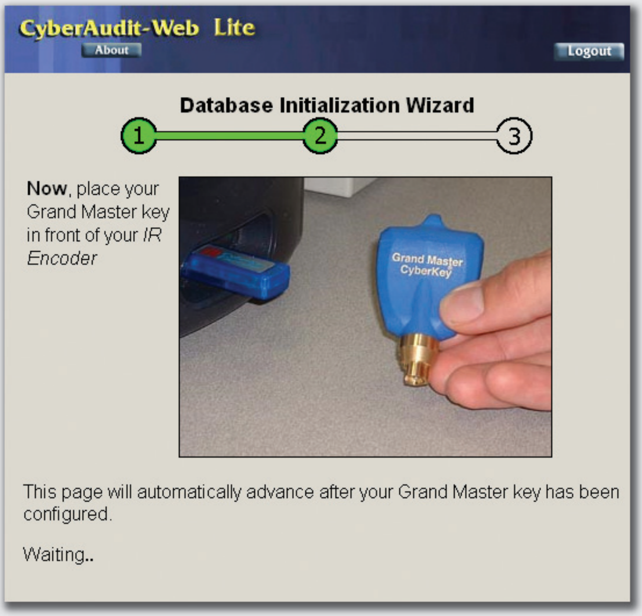
This launches a helper application called *CyberLink*, which serves as a go-between for CyberKeys and the CyberAudit-Web Lite software. When *CyberLink* has finished loading, a ready message will appear, and the wizard will advance to Step 2.



Ready

Please place a key near IR Encoder.

Figure 1-11: *The CyberLink Application*



Database Initialization Wizard

Now, place your Grand Master key in front of your *IR Encoder*

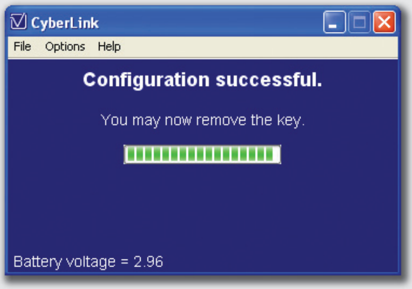
This page will automatically advance after your Grand Master key has been configured.

Waiting..

Figure 1-12: *The Database Initialization Wizard - Step 2*

Note: The use of a USB extension cable in conjunction with the IR Encoder is recommended for convenience.

CyberLink will download the IDs of CyberLocks and CyberKeys that the Grand Master has configured. Once the configuration process is complete, the application will display a success message, and the wizard will advance.

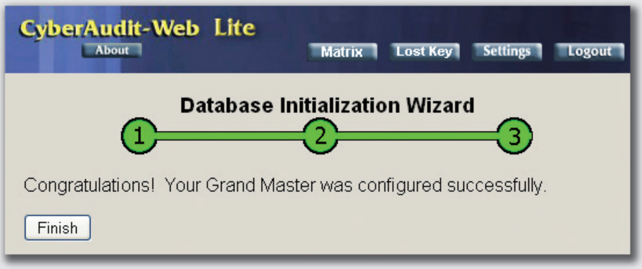


Configuration successful.

You may now remove the key.

Battery voltage = 2.96

Figure 1-13: *Grand Master Configuration Completed*

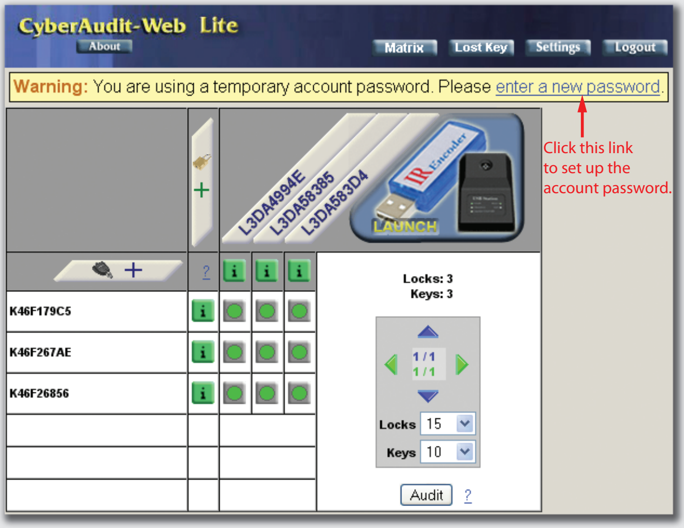


Database Initialization Wizard

Congratulations! Your Grand Master was configured successfully.

Figure 1-14: *The Database Initialization Wizard - Step 3*

Click the *Finish* button to close the wizard and advance to the *Access Matrix* page. The last item to complete is the selection of an account password. This password must be entered at startup and after an extended idle period while logged in to gain access to the application.



Warning: You are using a temporary account password. Please enter a new password.

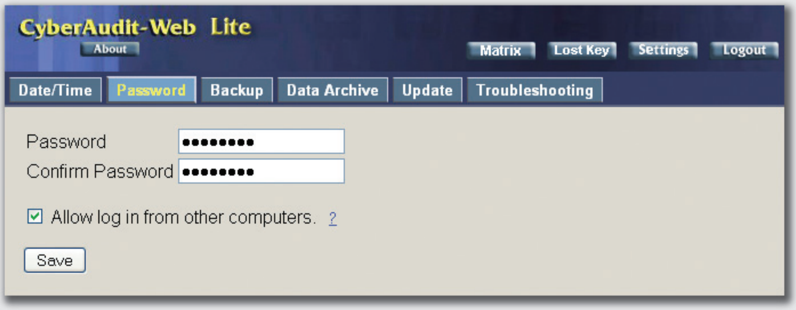
Click this link to set up the account password.

Locks: 3
Keys: 3

Locks 15
Keys 10

Figure 1-15: *The Access Matrix Page with Password Warning*

In the warning box which appears at the top of the *Access Matrix* page, click the link labeled *"enter a new password"* to bring up the password selection page. Enter and confirm a password, then click the *Save* button.



Password ●●●●●●●●●
Confirm Password ●●●●●●●●●

☑ Allow log in from other computers. ?

Figure 1-16: *The Password Selection Page*

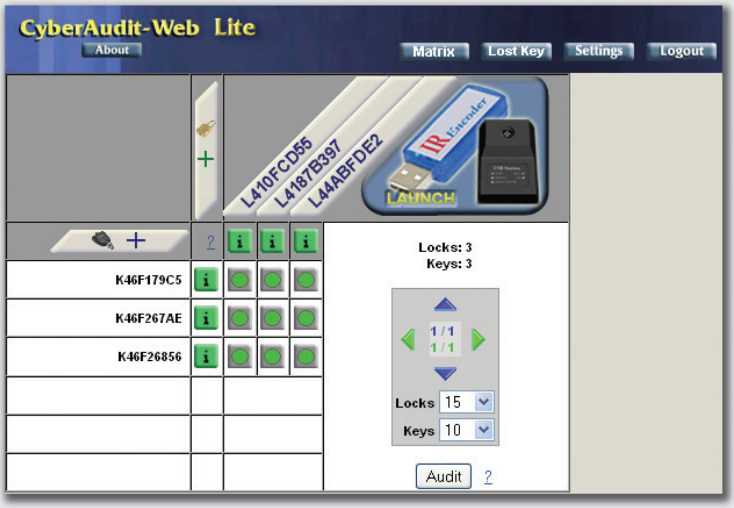
After the password has been set, the CyberAudit-Web Lite system is ready for normal use.

Using the Application

The main purpose of CyberAudit-Web Lite is to control the access that CyberKeys have to CyberLocks in the system. Access times can be easily scheduled using the software, and audit reports of access events can be viewed at the click of a button.

The Access Matrix

The Access Matrix is the main page of CyberAudit-Web Lite. It is the first page displayed after password verification at startup. Each row of the matrix represents a CyberKey, and each column represents a CyberLock. The juncture of a row and a column contains information regarding the schedule by which a key may access a lock.



L410FCD55
L4187B397
L44ABFDE2

K46F179C5
K46F267AE
K46F26856

Locks: 3
Keys: 3

1 / 1
1 / 1

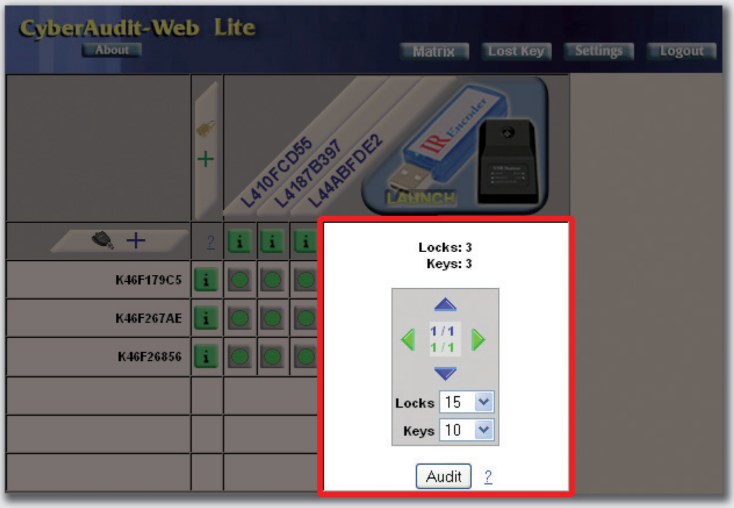
Locks 15
Keys 10

Figure 2-1: ***The Access Matrix Page***

There are several types of icons which appear in the Access Matrix. After completing the *Grand Master Registration Wizard*, every lock and key in the matrix will have a green i icon next to its serial number, and a green ● icon will appear in every square. The i icon represents the status of a lock or key. It indicates that the lock or key has been programmed with the most recent configuration options. The ● icon indicates that a key has access to a lock 24 hours a day, 7 days a week. This icon initially appears in every square of the Access Matrix because the Grand Master configures all CyberKeys with master key access.

Other icons – namely lettered schedule icons and the I icon – will appear in the Access Matrix after lock or key settings have been changed. These icons will be discussed later in this chapter.

Because there may be many more locks and keys in the system than can be shown on the screen at one time, some basic navigation tools have been built into the Access Matrix. To specify how many items are displayed in a matrix "page" at once, select the desired number from the *Locks* or *Keys* drop-down lists in the Navigation Controls section. Move through the pages using the colored triangles.



Locks: 3
Keys: 3

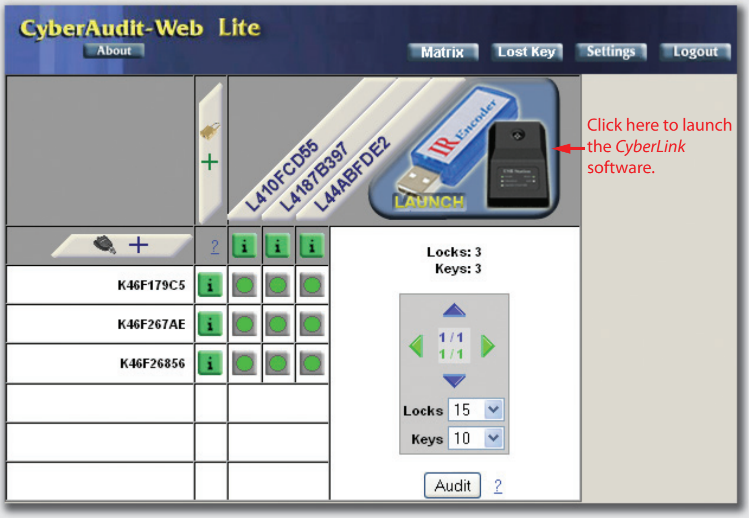
1 / 1
1 / 1

Locks 15
Keys 10

Figure 2-2: *The Access Matrix - Navigation Controls Section*

Using the CyberLink Software

The *CyberLink* application is used whenever CyberKeys need to be downloaded and configured. To launch it, ensure that an IR Encoder or USB Station is connected, then click on the blue *Launch* button which contains an image of the two devices.



Locks: 3
Keys: 3

K46F179C5	i	●	●	●
K46F267AE	i	●	●	●
K46F26856	i	●	●	●

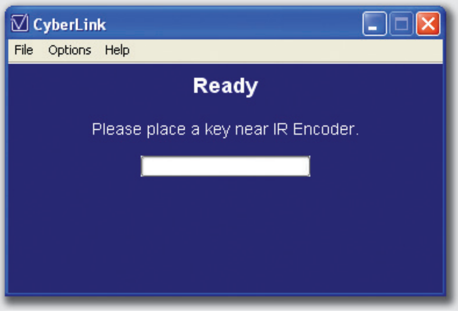
1 / 1
1 / 1

Locks 15
Keys 10

Click here to launch the *CyberLink* software.

Figure 2-3: ***The CyberLink Launch Button***

When the ready message appears in the *CyberLink* window, place a CyberKey or the Grand Master into the USB Station or near the IR Encoder (see Figure 1-10) to download and configure the key.



Ready

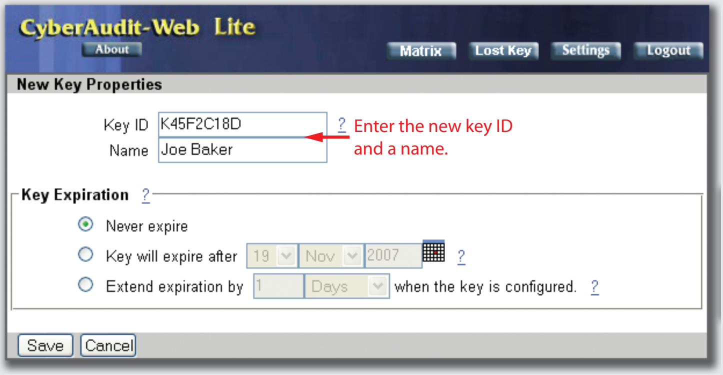
Please place a key near IR Encoder.

Figure 2-4: ***The CyberLink Application Ready Screen***

Adding New Locks and Keys

Additional locks and keys can easily be added to the system after the basic setup has been completed. The simplest method is to configure each item using the Grand Master, then download the information using an IR Encoder or USB Station to add the new items to the database.

Locks and keys can also be added manually, which can be useful for assigning names prior to programming them with the Grand Master. To do so, click the 🔑 + or 🔒 + button in the Access Matrix to bring up either the *New Key Properties* or *New Lock Properties* page.



New Key Properties

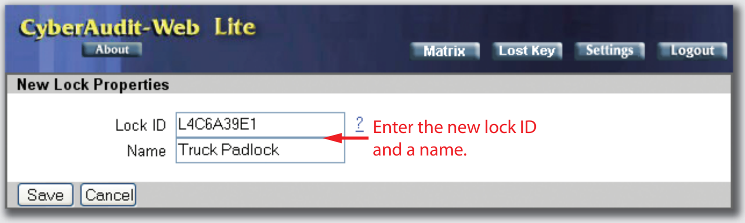
Key ID: K45F2C18D ?
Name: Joe Baker

Enter the new key ID and a name.

Key Expiration ?

● Never expire
○ Key will expire after 19 Nov 2007 ?
○ Extend expiration by 1 Days when the key is configured. ?

Figure 2-5: *The New Key Properties Page*



New Lock Properties

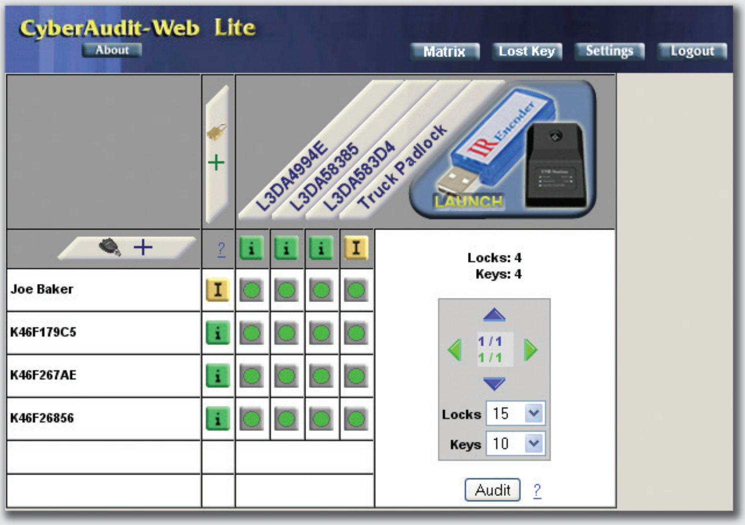
Lock ID: L4C6A39E1 ?
Name: Truck Padlock

Enter the new lock ID and a name.

Figure 2-6: *The New Lock Properties Page*

Enter the ID of the new item, along with a descriptive name. Naming items makes it easier to keep track of where locks are installed and the people to whom keys are assigned. After entering the name and ID of the new item, click the *Save* button. Until CyberAudit-Web Lite has communicated with a manually added item, the Access Matrix displays a yellow I icon beside its name, indicating that it needs to be updated.

Note: Renaming a lock or a key does not cause the I icon to appear.



	?	L3DA4994E	L3DA58385	L3DA583D4	Truck Padlock
		i	i	i	I
Joe Baker	I	●	●	●	●
K46F179C5	i	●	●	●	●
K46F267AE	i	●	●	●	●
K46F26856	i	●	●	●	●

Locks: 4
Keys: 4

1 / 1
1 / 1

Locks 15
Keys 10

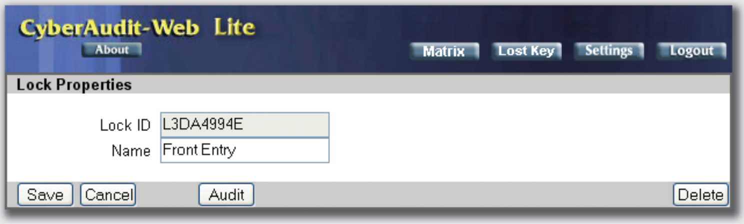
Figure 2-7: ***The Access Matrix Showing Items to Update***

To clear the I icon for CyberKeys, simply configure the key using the *CyberLink* application. For CyberLocks, contact the new lock with the Grand Master to set the access code, then download the Grand Master using *CyberLink.*

Viewing and Editing Item Properties

To view or edit the current properties of a lock or key, click on the item's i or I icon to access the *Lock Properties* or *Key Properties* page. These pages are identical to the respective *New* pages shown in Figures 2-5 and 2-6 on page 16, but the item ID field is not editable, and the *Key Properties* page includes additional options. CyberKey properties are discussed in detail in the following section.

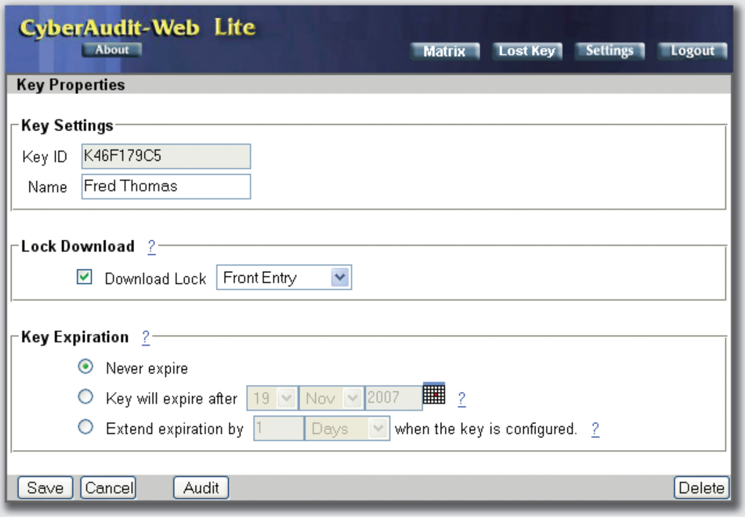
After making any changes to item properties, click the *Save* button.



Lock Properties

Lock ID L3DA4994E
Name Front Entry

Figure 2-8: ***Editing Lock Properties***



Key Properties

Key Settings

Key ID K46F179C5
Name Fred Thomas

Lock Download ?

☑ Download Lock Front Entry

Key Expiration ?

● Never expire
○ Key will expire after 19 Nov 2007 ?
○ Extend expiration by 1 Days when the key is configured. ?

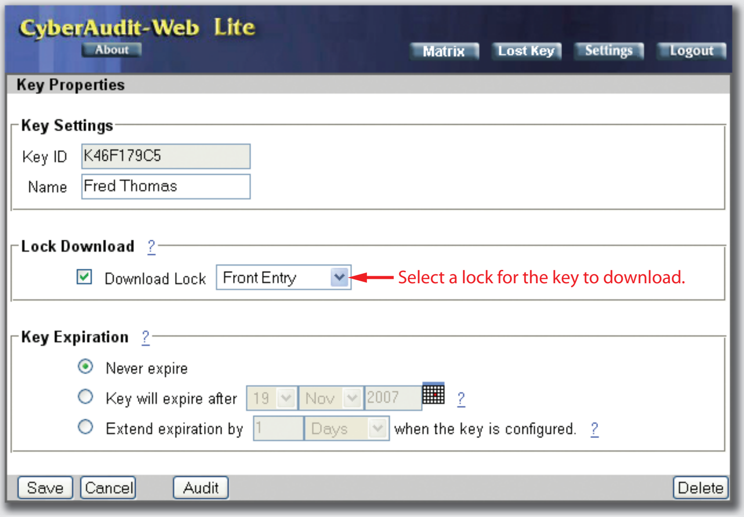
Figure 2-9: ***Editing Key Properties***

Properties of CyberKeys

CyberKeys have two important properties in addition to their names. The first is the ability to download events from a lock, and the second is the key expiration rule.

Each CyberKey in the system may be configured to download events from one selected lock. Every time a person attempts to open a CyberLock, an access event is recorded in both the lock and the key. Events from keys are added to the database when the key is downloaded by *CyberLink*. However, CyberLocks never directly communicate with the software, so the system relies on CyberKeys to carry the information to the database.

To specify which CyberLock a CyberKey will download, check the box in the *Lock Download* section of the *Key Properties* page, and select the desired lock from the adjacent pull-down list.



Key Properties

Key Settings

Key ID K46F179C5

Name Fred Thomas

Lock Download ?

☑ Download Lock Front Entry

Select a lock for the key to download.

Key Expiration ?

● Never expire

○ Key will expire after 19 Nov 2007 ?

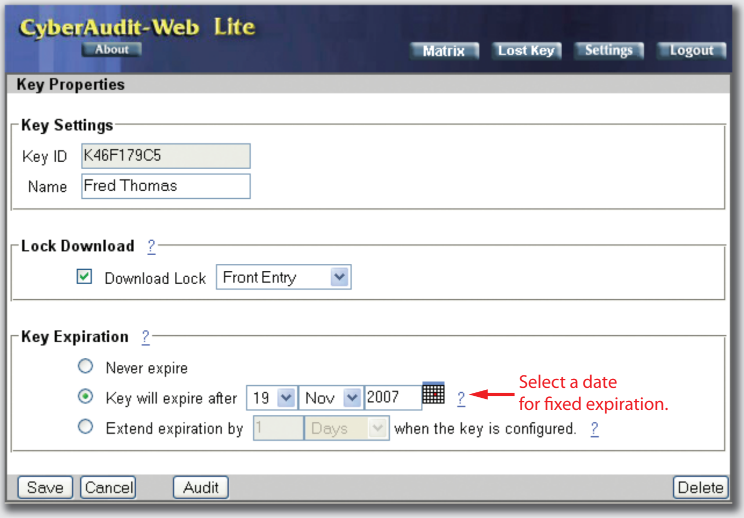
○ Extend expiration by 1 Days when the key is configured. ?

Figure 2-10: *Selecting a Lock for a Key to Download*

Key control is best achieved by configuring CyberKeys to expire on a regular basis, because expired keys cannot open locks.

There are two types of expiration: *fixed* and *rolling*. Setting a fixed expiration rule causes keys to expire at the end of the specified date. Selecting rolling expiration causes the software to renew the expiration timer each time the key is configured. If the specified interval of time elapses between key configurations, the key expires and loses its access to CyberLocks. This process also ensures that audit trail data is captured on a regular basis, which makes audit reports more accurate.

To set a fixed expiration rule for a key, select the second option in the *Key Expiration* section of the *Key Properties* page and specify the date after which the key should expire.



Key Properties

Key Settings

Key ID: K46F179C5

Name: Fred Thomas

Lock Download ?

☑ Download Lock: Front Entry

Key Expiration ?

○ Never expire

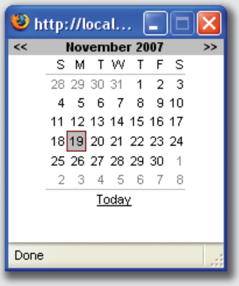
● Key will expire after 19 Nov 2007 ?

○ Extend expiration by 1 Days when the key is configured. ?

Select a date for fixed expiration.

Figure 2-11: ***Setting a Fixed Expiration Rule for a Key***

Clicking the ▦ icon beside the pull-down list will cause a small calendar to appear in a pop-up window. This may be used for easy date selection.



http://local...

<< November 2007 >>

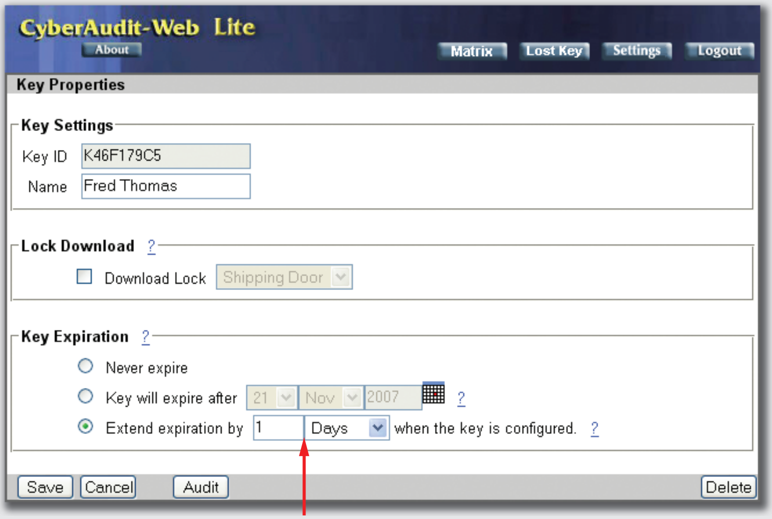
S	M	T	W	T	F	S
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	1
2	3	4	5	6	7	8

Today

Done

Figure 2-12: ***The Pop-up Calendar***

To set a rolling expiration, select the third option in the section and specify the expiration time interval (days, weeks, or months) in the adjacent fields.



Key Properties

Key Settings

Key ID K46F179C5

Name Fred Thomas

Lock Download ?

□ Download Lock Shipping Door

Key Expiration ?

○ Never expire

○ Key will expire after 21 Nov 2007 ▦ ?

● Extend expiration by 1 Days when the key is configured. ?

Select a time interval for rolling expiration.

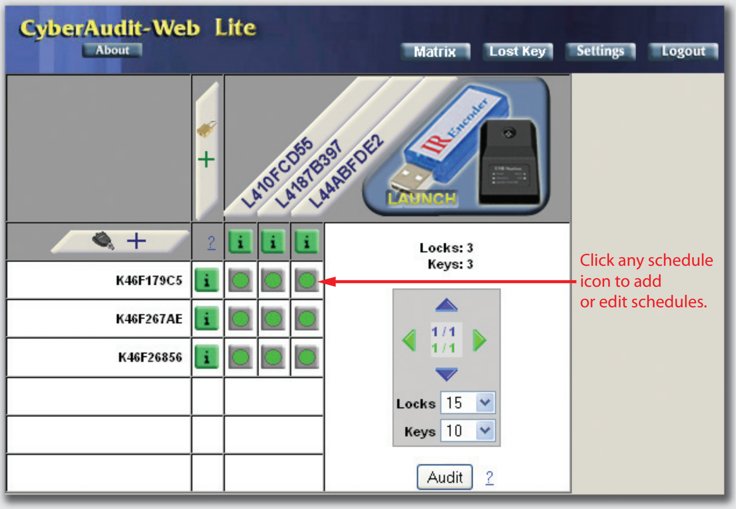
Figure 2-13: ***Setting a Rolling Expiration Rule for a Key***

Creating Schedules

Schedules are another powerful access control feature of the CyberAudit-Web Lite system. CyberKeys may open CyberLocks only during time frames defined within their assigned schedule.

Two pre-made schedules exist in CyberAudit-Web Lite: *Full Access* and *No Access*. All keys are assigned the *Full Access* schedule for every lock when they are added to the system. This schedule allows access to all locks in the system at all times. In addition to the two pre-made schedules, up to 26 custom schedules may be created. Each one will be associated with a letter of the alphabet which will represent the schedule in the Access Matrix.

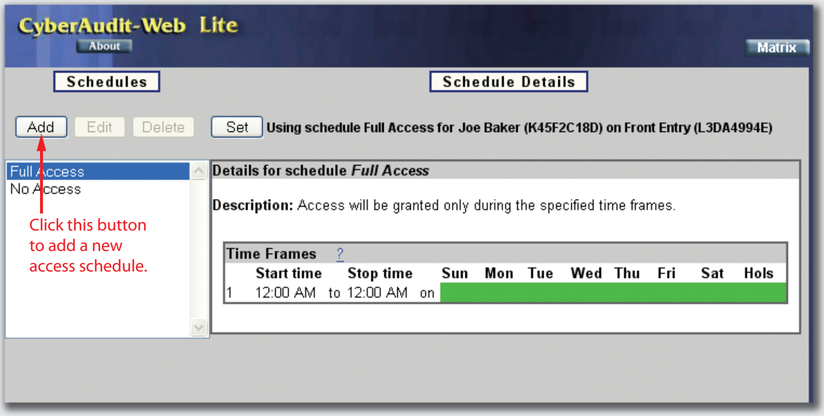
To create a new schedule, click on any schedule cell in the Access Matrix to bring up the *Schedules/Schedule Details* page. The *Holidays* section also appears on this page, but will be discussed separately in the section titled *Entering Holidays*.



Click any schedule icon to add or edit schedules.

Figure 2-14: ***Access the Schedules/Schedule Details Page***

In the *Schedules* section, click the *Add* button to create a new schedule. This will bring up the *Add or Edit Schedule* page.



Using schedule Full Access for Joe Baker (K45F2C18D) on Front Entry (L3DA4994E)

Full Access
No Access

Click this button to add a new access schedule.

Details for schedule *Full Access*

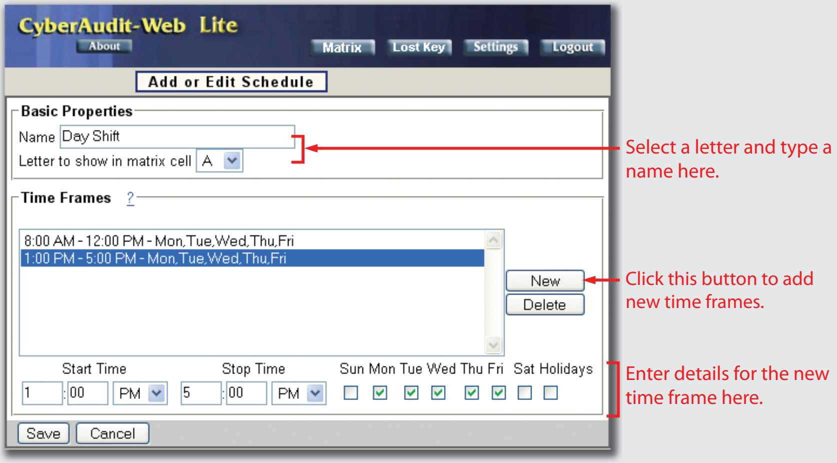
Description: Access will be granted only during the specified time frames.

Time Frames ?

	Start time		Stop time		Sun	Mon	Tue	Wed	Thu	Fri	Sat	Hols
1	12:00 AM	to	12:00 AM	on	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

Figure 2-15: *The Schedules/Schedule Details Page*

Select a letter from the pull-down list in the *Basic Properties* section and type a name for the new schedule into the adjacent text entry field.



Basic Properties

Name Day Shift

Letter to show in matrix cell A

Select a letter and type a name here.

Time Frames ?

8:00 AM - 12:00 PM - Mon,Tue,Wed,Thu,Fri
1:00 PM - 5:00 PM - Mon,Tue,Wed,Thu,Fri

Click this button to add new time frames.

Start Time			Stop Time			Sun	Mon	Tue	Wed	Thu	Fri	Sat	Holidays
1	:00	PM	5	:00	PM	☐	☑	☑	☑	☑	☑	☐	☐

Enter details for the new time frame here.

Figure 2-16: *Creating a New Schedule*

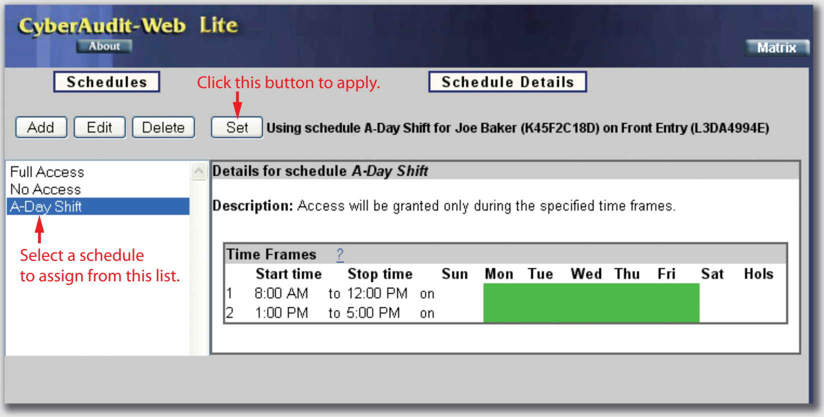
Next, one or more time frames must be added to the schedule. A key will only be able to access a lock during one of the time frames contained in its schedule for that lock, and then only on days of the week specified. For example, a schedule containing time frames of 8:00 AM to 12:00 PM and 1:00 PM to 5:00 PM with only Monday through Friday checked for days of the week would allow access only on weekdays during normal business hours, but not during the lunch hour.

To add a time frame to the schedule, click the *New* button in the *Time Frames* section, (see Figure 2-16, on the previous page). Enter start and stop times for the new time frame and check the box corresponding to each day of the week to which the schedule should apply. If access should be granted on holidays, check the box labeled *Holidays*. Otherwise, keys using the schedule will be denied access on dates that have been entered into the system as holidays. For more information on holidays, see the section entitled *Entering Holidays*.

When finished entering schedule details, click the *Save* button to confirm the changes and return to the *Schedule Details* screen.

Assigning Schedules to Keys

By default, all CyberKeys are assigned the *Full Access* schedule for every lock. Keys which should not have access to certain locks should be assigned the *No Access* schedule. To assign a new schedule for a key to access a lock, click on the juncture of the key's row and the lock's column in the Access Matrix. This will bring up the *Schedules/Schedule Details/Holidays* page for the selected key/lock combination. Choose a schedule to assign from the *Schedules* section of the page, then click the *Set* button in the *Schedule Details* section.



Click this button to apply.

Using schedule A-Day Shift for Joe Baker (K45F2C18D) on Front Entry (L3DA4994E)

Full Access
No Access
A-Day Shift

Select a schedule to assign from this list.

Details for schedule *A-Day Shift*

Description: Access will be granted only during the specified time frames.

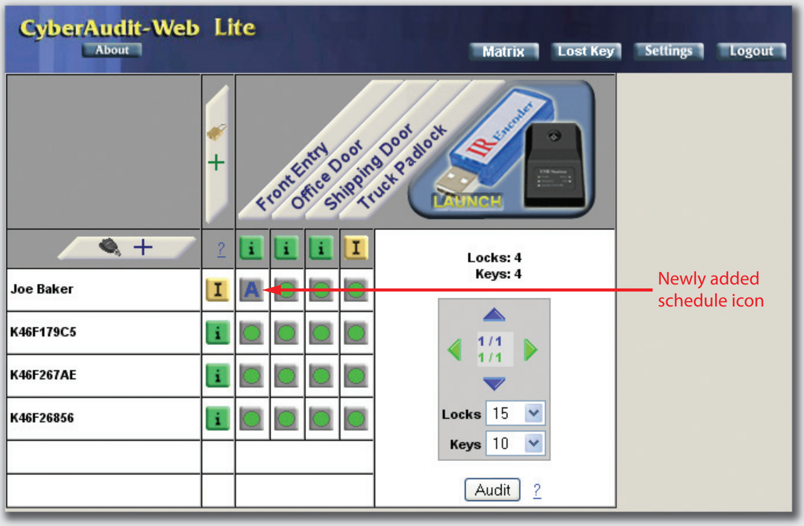
Time Frames ?

	Start time	Stop time		Sun	Mon	Tue	Wed	Thu	Fri	Sat	Hols
1	8:00 AM	to 12:00 PM	on		🟩	🟩	🟩	🟩	🟩		
2	1:00 PM	to 5:00 PM	on		🟩	🟩	🟩	🟩	🟩		

Figure 2-17: *Assigning a Schedule to a Key*

After applying a schedule for the current key and lock combination, click the *Close* button to return to the Access Matrix. An icon which corresponds to the letter of the newly applied schedule, like A, will appear at the juncture of the key's row and the lock's column. Since access information has changed, the yellow I icon will be displayed for the key. Configure the key using an IR Encoder or USB Station to transfer the new settings and clear the icon.

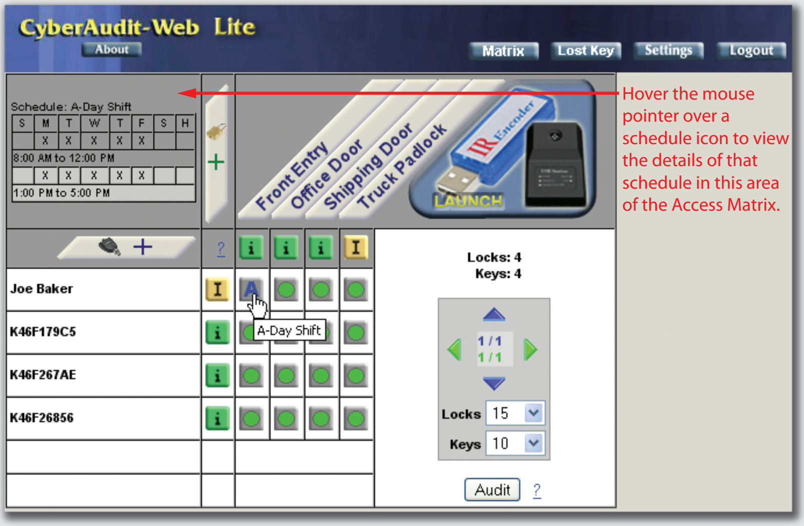
]



Newly added schedule icon

Figure 2-18: *The Access Matrix Showing a Newly Applied Schedule*

For easy viewing, hovering the mouse pointer over a schedule icon will cause the details of that schedule to be displayed in the upper left-hand corner of the matrix.

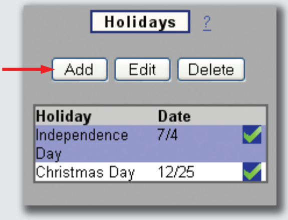


Hover the mouse pointer over a schedule icon to view the details of that schedule in this area of the Access Matrix.

Figure 2-19: *The Access Matrix Showing Schedule Details*

Entering Holidays

Holidays, which do not have to be literal (calendar) holidays, are meant to be schedule exceptions in CyberAudit-Web Lite. Any day of the year may be designated a holiday. To add holidays to the system, click any schedule icon in the Access Matrix to bring up the *Schedules/Schedule Details/Holidays* screen. In the *Holidays* section, click the *Add* button to bring up the *Add or Edit Holiday* page.

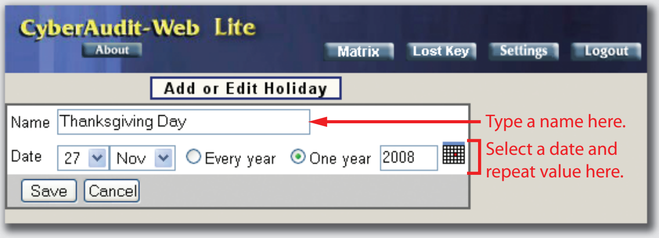


Holiday	Date	
Independence Day	7/4	✓
Christmas Day	12/25	✓

Click this button to add a new holiday.

Figure 2-20: *The Holidays List*

In the *Add or Edit Holiday* page, type a name for the new holiday into the *Name* field, then set the date using the pull-down lists and specify whether the holiday will be a one-time exception to access, or if it occurs every year. When finished entering details for the new holiday, click the *Save* button to return to the *Holidays* page. The new holiday will appear in the list. This list is sorted by holiday status (one-time or recurring) and then by date. Recurring holidays are marked with a ✓ icon.



Name: Thanksgiving Day

Date: 27 Nov ○ Every year ● One year 2008

Type a name here.

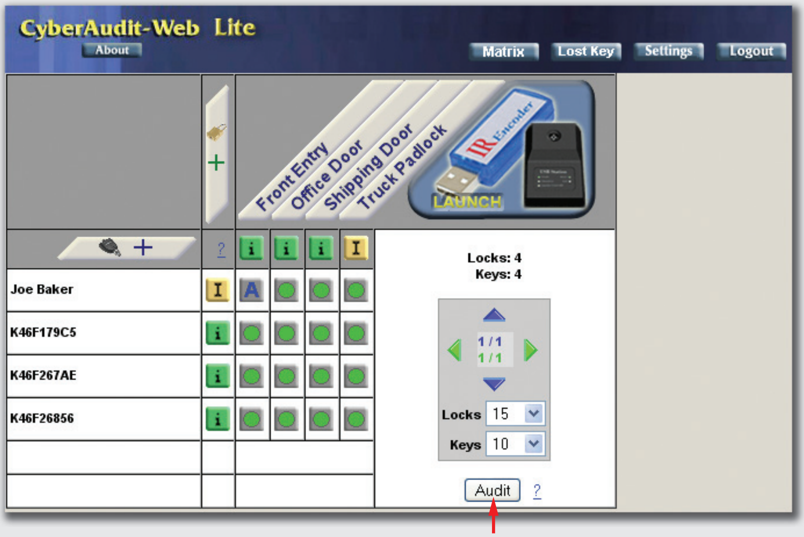
Select a date and repeat value here.

Figure 2-21: *The Add or Edit Holiday Page*

Auditing the System

In addition to controlling access, CyberAudit-Web Lite gives users the ability to view audit trails from keys and locks. The system records the time and date of every event, the key and lock involved, and a short description of what took place.

To view audit entries for the system as a whole, click the *Audit* button in the Access Matrix Navigation Controls. A new browser window will be opened to display the data.



	?	Front Entry	Office Door	Shipping Door	Truck Padlock
		i	i	i	I
Joe Baker	I	A	●	●	●
K46F179C5	i	●	●	●	●
K46F267AE	i	●	●	●	●
K46F26856	i	●	●	●	●

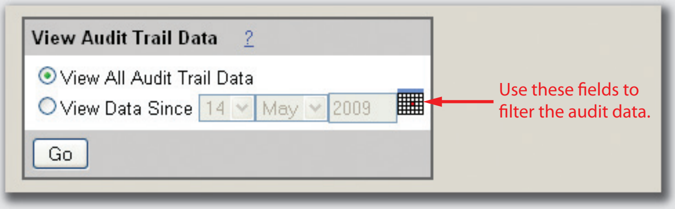
Locks: 4
Keys: 4

Locks 15
Keys 10

Click this button to view audit information for all keys and locks combined.

Figure 2-22: *Auditing the System*

Since the number of audit entries can be quite large, the system allows the user to choose a starting date to use as a filter before displaying information. Only events occurring on or after the date selected will be included in the audit report.



View Audit Trail Data ?

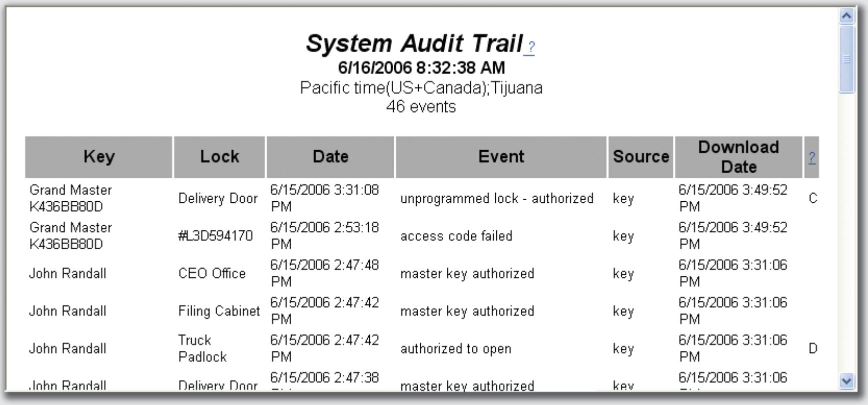
● View All Audit Trail Data

○ View Data Since 14 May 2009

Use these fields to filter the audit data.

Figure 2-23: ***Specifying a Starting Date to Filter the Display of Information***

After selecting a starting date using the pull-down lists, click the *Go* button to view the report of audit information.



System Audit Trail ?

6/16/2006 8:32:38 AM

Pacific time(US+Canada);Tijuana

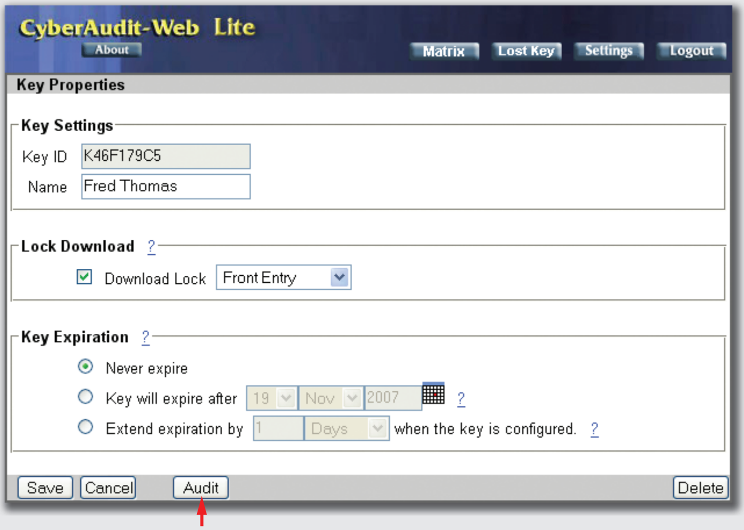
46 events

Key	Lock	Date	Event	Source	Download Date	?
Grand Master K436BB80D	Delivery Door	6/15/2006 3:31:08 PM	unprogrammed lock - authorized	key	6/15/2006 3:49:52 PM	C
Grand Master K436BB80D	#L3D594170	6/15/2006 2:53:18 PM	access code failed	key	6/15/2006 3:49:52 PM	
John Randall	CEO Office	6/15/2006 2:47:48 PM	master key authorized	key	6/15/2006 3:31:06 PM	
John Randall	Filing Cabinet	6/15/2006 2:47:42 PM	master key authorized	key	6/15/2006 3:31:06 PM	
John Randall	Truck Padlock	6/15/2006 2:47:42 PM	authorized to open	key	6/15/2006 3:31:06 PM	D
John Randall	Delivery Door	6/15/2006 2:47:38	master key authorized	key	6/15/2006 3:31:06	

Figure 2-24: ***System-Wide Audit Information Report***

The letters *"C"* or *"D"* can be seen in the last column of the report. *"C"* indicates that a key or lock was configured by the Grand Master. *"D"* indicates that a lock was downloaded by a CyberKey.

Similar reports can be generated for a specific lock or key. To view such a report, first click on a lock or key's i or I icon to enter the item's *Properties* page, then click the *Audit* button on that page to bring up the date filter option.



Key Properties

Key Settings

Key ID: K46F179C5

Name: Fred Thomas

Lock Download

☑ Download Lock: Front Entry

Key Expiration

● Never expire

○ Key will expire after 19 Nov 2007

○ Extend expiration by 1 Days when the key is configured.

Click this button to view audit data specific to the selected item.

Figure 2-25: *Retrieving a Single-Item Audit Report*

Settings and Special Operations

This chapter contains advanced information on settings and operations which fall outside normal use of the system. The software pages discussed are accessed through the buttons found in the banner area, located at the top of the application window.

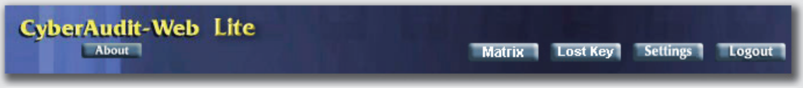
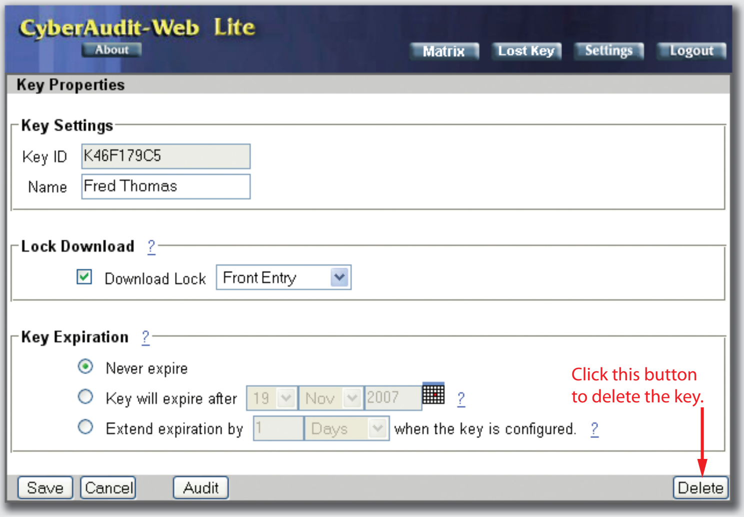


Figure 3-1: ***Buttons in the Banner Area***

Deleting Locks and Keys

If necessary, such as when replacing an item, locks and keys may be deleted from the system via the appropriate properties page. Click on the lock or key's i or I icon to access the page, then click the *Delete* button to remove the item from the system.

Note: Audit trail data for a lock or key will no longer be readily available after the item has been deleted from the system.



Key Properties

Key Settings

Key ID K46F179C5

Name Fred Thomas

Lock Download ?

☑ Download Lock Front Entry

Key Expiration ?

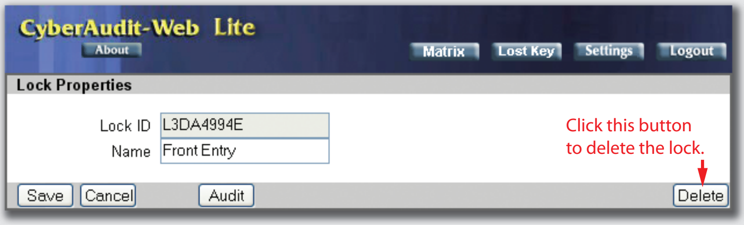
● Never expire

○ Key will expire after 19 Nov 2007 ?

○ Extend expiration by 1 Days when the key is configured. ?

Click this button
to delete the key.

Figure 3-2: *Deleting a CyberKey*



Lock Properties

Lock ID L3DA4994E

Name Front Entry

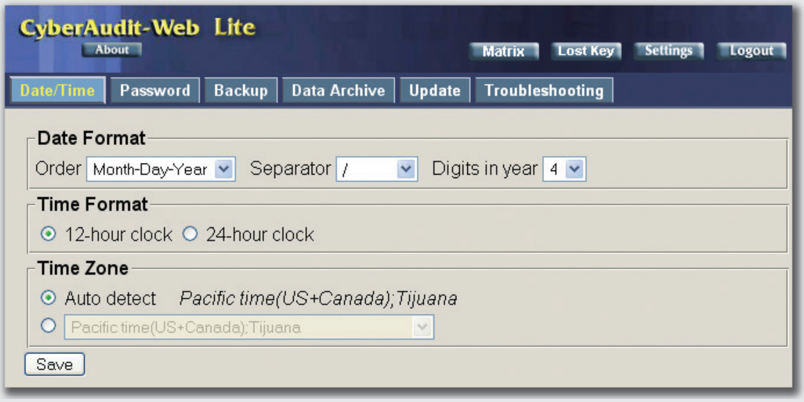
Click this button
to delete the lock.

Figure 3-3: *Deleting a CyberLock*

Settings and Preferences

Clicking on the Settings button in the banner area will bring up the *Date/Time* tab of the system settings page. The various subsections of settings may be navigated by clicking on the named tabs.

The formats and time zone chosen on the *Date/Time* tab affect how the date and time are displayed in audit reports.



Date Format

Order: Month-Day-Year   Separator: /   Digits in year: 4

Time Format

● 12-hour clock ○ 24-hour clock

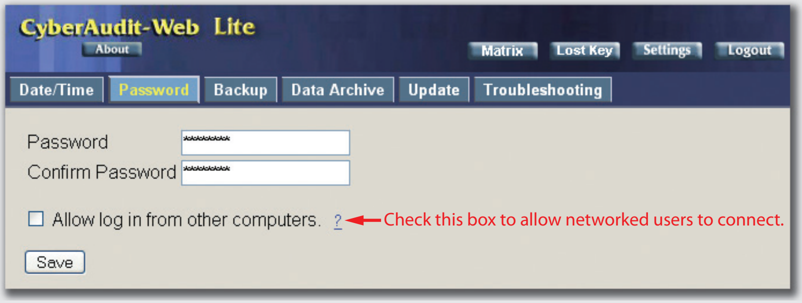
Time Zone

● Auto detect *Pacific time(US+Canada);Tijuana*

○ Pacific time(US+Canada);Tijuana

Figure 3-4: ***The Date/Time Tab***

As seen in Figure 3-5, on the following page, the *Password* tab is identical to the one seen when setting up the system for first use. It allows the login password to be changed, and also includes the option of allowing people to connect from other computers. Checking this box will allow networked users who have been given the system password to use the software or allow them to download and configure CyberKeys.

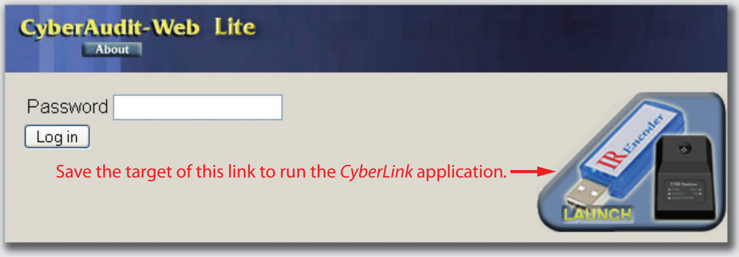


Password ********
Confirm Password ********

□ Allow log in from other computers. ? ← Check this box to allow networked users to connect.

Figure 3-5: *The Password/Log In Tab*

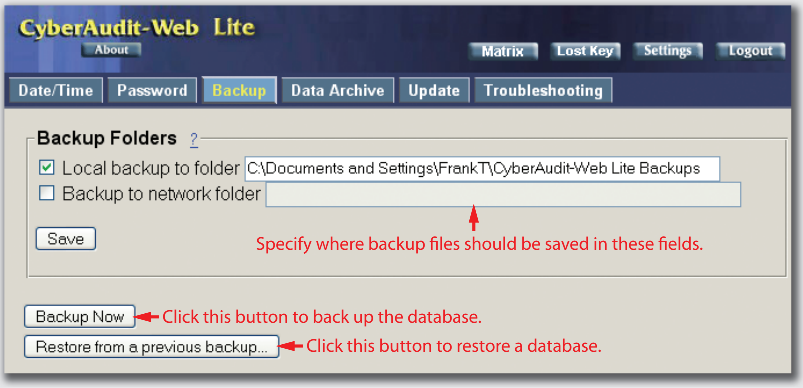
Users who should be able to update and download keys without having access to the CyberAudit-Web Lite application can open a web browser and enter the system URL *(http://<Host IP Address>:8083/CyberAuditLite/)* to download the CyberLink software. At the login page, right-click on the *Launch* button and choose *"Save target as..."* from the pop-up menu. Specify a conveniently accessible location for the file, such as the Desktop. This will allow the user to run CyberLink without needing to log in to CyberAudit-Web Lite.



Save the target of this link to run the *CyberLink* application. →

Figure 3-6: *Downloading CyberLink From a Remote Computer*

The *Backup* tab is where the path to backup files may be specified. Database files may be backed up to both a local and/or network folder. This page also allows a previously saved backup to be restored.



Backup Folders ?

☑ Local backup to folder C:\Documents and Settings\FrankT\CyberAudit-Web Lite Backups

☐ Backup to network folder

Specify where backup files should be saved in these fields.

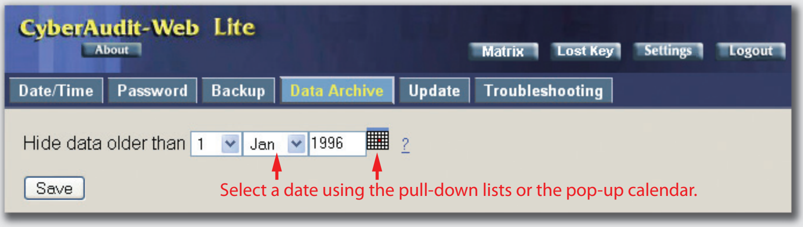
Click this button to back up the database.

Click this button to restore a database.

Figure 3-7: ***The Backup Tab***

The amount of collected audit trail data continues to grow with every key download. At some point, older data may no longer be useful, and may be archived to reduce volume and improve system performance. When data is archived, it is moved to different tables in the database and will no longer be viewable through the user interface.

To archive data, select a date on the *Data Archive* tab to function as a cutoff point, then click the *Save* button. Events which occurred before the selected date will be moved to the archive tables. To restore archived data, select an earlier date and click the *Save* button. The data will be retrieved from the archive tables and will once again be viewable through the user interface.

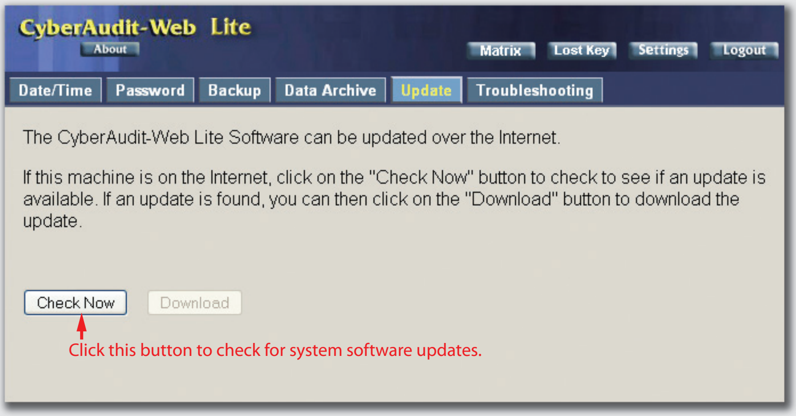


Hide data older than 1 Jan 1996

Select a date using the pull-down lists or the pop-up calendar.

Figure 3-8: ***The Data Archive Tab***

The *Update* tab allows the user to check for and download any available system software updates.



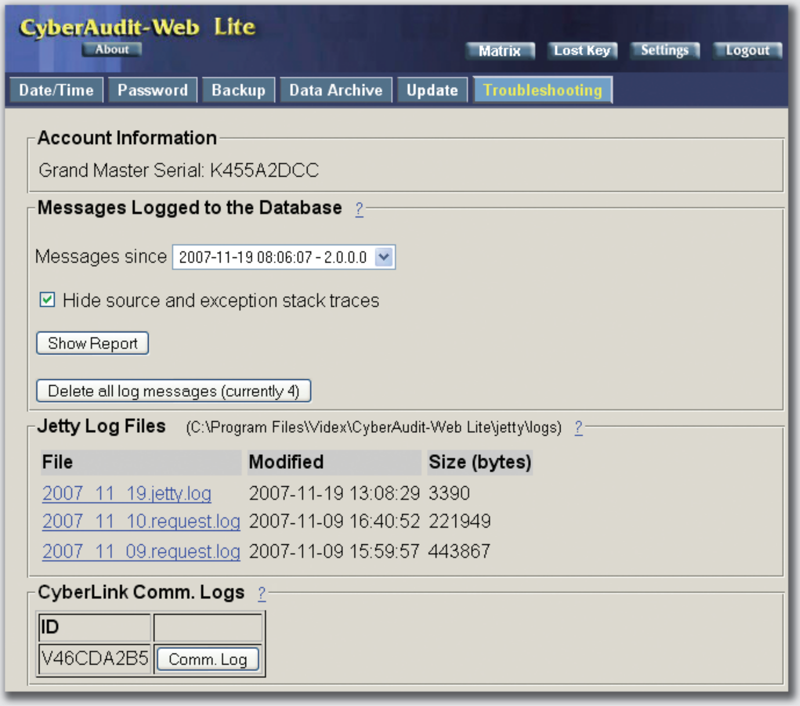
The CyberAudit-Web Lite Software can be updated over the Internet.

If this machine is on the Internet, click on the "Check Now" button to check to see if an update is available. If an update is found, you can then click on the "Download" button to download the update.

Click this button to check for system software updates.

Figure 3-9: ***The Update Tab***

The *Troubleshooting* tab contains information that is useful to advanced users or Technical Support personnel for the purpose of diagnosing problems with a CyberAudit-Web Lite installation.



Account Information

Grand Master Serial: K455A2DCC

Messages Logged to the Database ?

Messages since 2007-11-19 08:06:07 - 2.0.0.0

☑ Hide source and exception stack traces

Jetty Log Files (C:\Program Files\Videx\CyberAudit-Web Lite\jetty\logs) ?

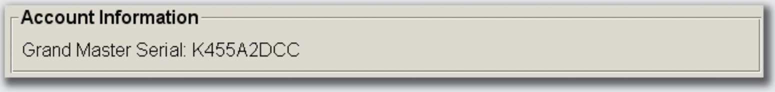
File	Modified	Size (bytes)
2007_11_19.jetty.log	2007-11-19 13:08:29	3390
2007_11_10.request.log	2007-11-09 16:40:52	221949
2007_11_09.request.log	2007-11-09 15:59:57	443867

CyberLink Comm. Logs ?

ID	
V46CDA2B5	Comm. Log

Figure 3-10: ***The Troubleshooting Tab***

The *Account Information* section displays the ID of the Grand Master CyberKey currently associated with the system.

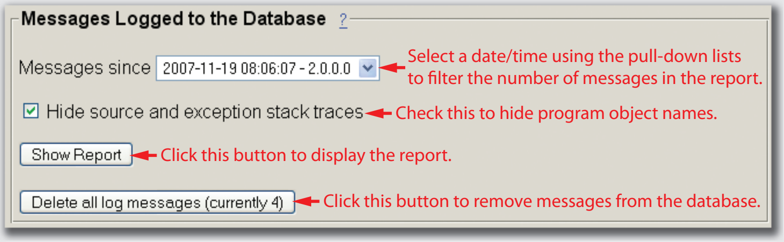


Account Information

Grand Master Serial: K455A2DCC

Figure 3-11: ***The Troubleshooting Tab - Account Information Section***

The *Messages Logged to the Database* section can generate a report which shows information generated by the software, such as startup warnings or error messages. The number of messages displayed may be filtered by selecting a date and time from the pull-down list labeled *"Messages since."* Checking the box labeled *"Hide source and exception stack traces"* will cause the report to be displayed without detailing the exact function or object in the application code which generated the message. If the messages are no longer needed, they can be removed from the database by clicking the button labeled *"Delete all log messages . . . ."*



Messages Logged to the Database ?

Messages since 2007-11-19 08:06:07 - 2.0.0.0 ← Select a date/time using the pull-down lists to filter the number of messages in the report.

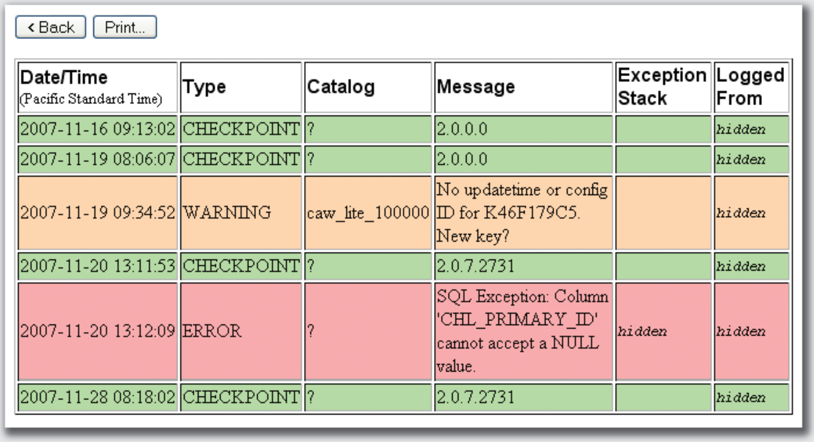
☑ Hide source and exception stack traces ← Check this to hide program object names.

Show Report ← Click this button to display the report.

Delete all log messages (currently 4) ← Click this button to remove messages from the database.

Figure 3-12: ***The Troubleshooting Tab - Logged Messages Section***

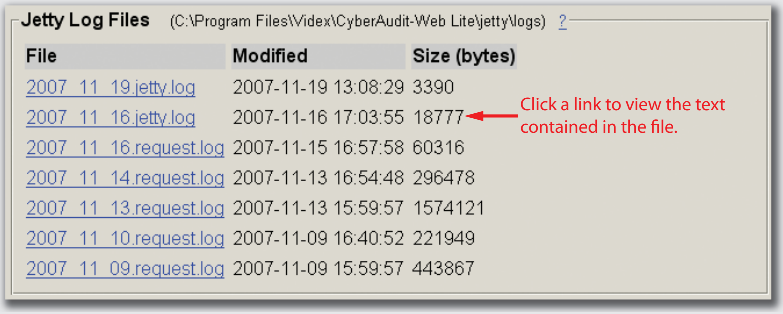
After selecting the desired options, click the *Show Report* button to display the report.



Date/Time (Pacific Standard Time)	Type	Catalog	Message	Exception Stack	Logged From
2007-11-16 09:13:02	CHECKPOINT	?	2.0.0.0		*hidden*
2007-11-19 08:06:07	CHECKPOINT	?	2.0.0.0		*hidden*
2007-11-19 09:34:52	WARNING	caw_lite_100000	No updatetime or config ID for K46F179C5. New key?		*hidden*
2007-11-20 13:11:53	CHECKPOINT	?	2.0.7.2731		*hidden*
2007-11-20 13:12:09	ERROR	?	SQL Exception: Column 'CHL_PRIMARY_ID' cannot accept a NULL value.	*hidden*	*hidden*
2007-11-28 08:18:02	CHECKPOINT	?	2.0.7.2731		*hidden*

Figure 3-13: ***A Sample System Message Report***

The *Jetty Log Files* section of the *Troubleshooting* page contains links to the log files generated by the server which runs the CyberAudit-Web Lite application.



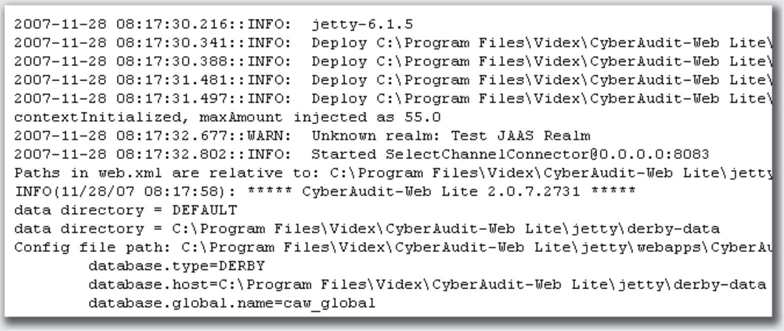
Jetty Log Files (C:\Program Files\Videx\CyberAudit-Web Lite\jetty\logs) ?

File	Modified	Size (bytes)
2007_11_19.jetty.log	2007-11-19 13:08:29	3390
2007_11_16.jetty.log	2007-11-16 17:03:55	18777
2007_11_16.request.log	2007-11-15 16:57:58	60316
2007_11_14.request.log	2007-11-13 16:54:48	296478
2007_11_13.request.log	2007-11-13 15:59:57	1574121
2007_11_10.request.log	2007-11-09 16:40:52	221949
2007_11_09.request.log	2007-11-09 15:59:57	443867

Click a link to view the text contained in the file.

Figure 3-14: ***The Troubleshooting Tab - Jetty Logs Section***

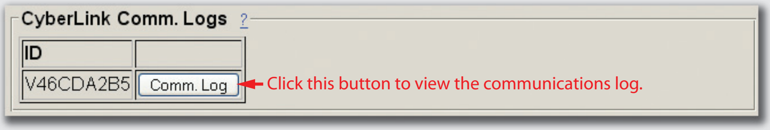
Clicking on any of the links in this section will display the text contained in the linked file.



```
2007-11-28 08:17:30.216::INFO:  jetty-6.1.5
2007-11-28 08:17:30.341::INFO:  Deploy C:\Program Files\Videx\CyberAudit-Web Lite\
2007-11-28 08:17:30.388::INFO:  Deploy C:\Program Files\Videx\CyberAudit-Web Lite\
2007-11-28 08:17:31.481::INFO:  Deploy C:\Program Files\Videx\CyberAudit-Web Lite\
2007-11-28 08:17:31.497::INFO:  Deploy C:\Program Files\Videx\CyberAudit-Web Lite\
contextInitialized, maxAmount injected as 55.0
2007-11-28 08:17:32.677::WARN:  Unknown realm: Test JAAS Realm
2007-11-28 08:17:32.802::INFO:  Started SelectChannelConnector@0.0.0.0:8083
Paths in web.xml are relative to: C:\Program Files\Videx\CyberAudit-Web Lite\jetty
INFO(11/28/07 08:17:58): ***** CyberAudit-Web Lite 2.0.7.2731 *****
data directory = DEFAULT
data directory = C:\Program Files\Videx\CyberAudit-Web Lite\jetty\derby-data
Config file path: C:\Program Files\Videx\CyberAudit-Web Lite\jetty\webapps\CyberAu
        database.type=DERBY
        database.host=C:\Program Files\Videx\CyberAudit-Web Lite\jetty\derby-data
        database.global.name=caw_global
```

Figure 3-15: ***A Sample Jetty Log File***

The last section of the *Troubleshooting* page, the *CyberLink Comm. Logs* section, displays a table which contains the serial numbers of any IR Encoders or USB Stations which have been used with the CyberAudit-Web Lite installation.



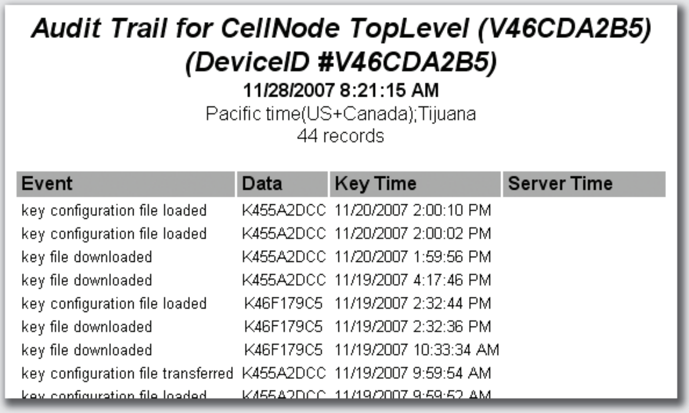
CyberLink Comm. Logs ?

ID	
V46CDA2B5	Comm. Log

Click this button to view the communications log.

Figure 3-16: ***The Troubleshooting Tab - CyberLink Comm. Logs Section***

Clicking on the *Comm. Log* button will display another type of audit report. This report details communication sessions between the CyberAudit-Web Lite application and hardware components.



Audit Trail for CellNode TopLevel (V46CDA2B5) (DeviceID #V46CDA2B5)
11/28/2007 8:21:15 AM
Pacific time(US+Canada);Tijuana
44 records

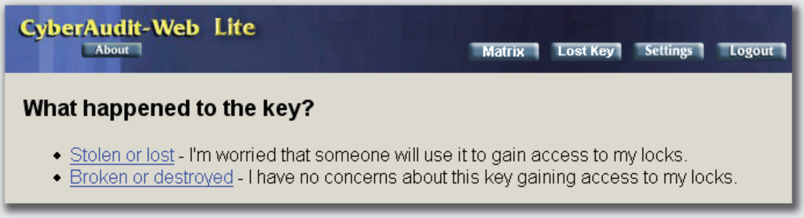
Event	Data	Key Time	Server Time
key configuration file loaded	K455A2DCC	11/20/2007 2:00:10 PM	
key configuration file loaded	K455A2DCC	11/20/2007 2:00:02 PM	
key file downloaded	K455A2DCC	11/20/2007 1:59:56 PM	
key file downloaded	K455A2DCC	11/19/2007 4:17:46 PM	
key configuration file loaded	K46F179C5	11/19/2007 2:32:44 PM	
key file downloaded	K46F179C5	11/19/2007 2:32:36 PM	
key file downloaded	K46F179C5	11/19/2007 10:33:34 AM	
key configuration file transferred	K455A2DCC	11/19/2007 9:59:54 AM	
key configuration file loaded	K455A2DCC	11/19/2007 9:59:52 AM	

Figure 3-17: ***A Sample CyberLink Communications Log***

Handling Lost or Damaged Keys

Lost or stolen CyberKeys can pose a threat to the security of a CyberLock installation. Unless the system is updated to deny access to the lost key, or the key expires, an unauthorized person may be able to gain access to locks. As soon as it is discovered that a key is missing, steps should be taken to protect system integrity.

To begin the process, click on the Lost Key button, found in the banner area at the top of the CyberAudit-Web Lite window. A wizard-like series of pages will gather information on the scenario and present a recommended course of action to protect system security. This process also assists with the replacement of damaged keys, including the Grand Master.

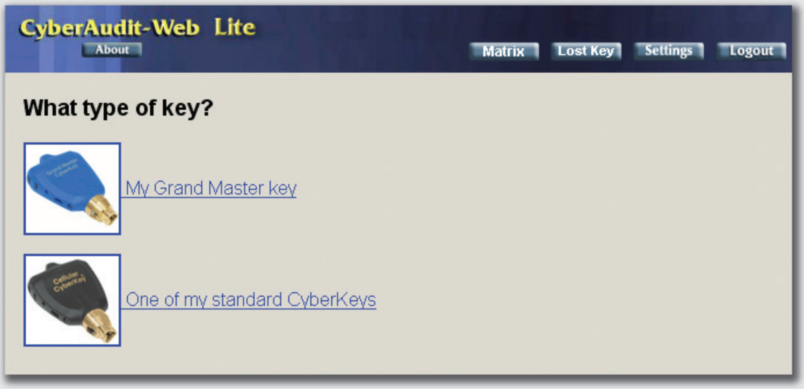


What happened to the key?

- Stolen or lost - I'm worried that someone will use it to gain access to my locks.
- Broken or destroyed - I have no concerns about this key gaining access to my locks.

Figure 3-18: *Handling a Lost or Damaged Key - Select Situation*

Click the link to the left of the sentence that best describes the current situation. Either choice will lead to a prompt for the type of key to be dealt with.



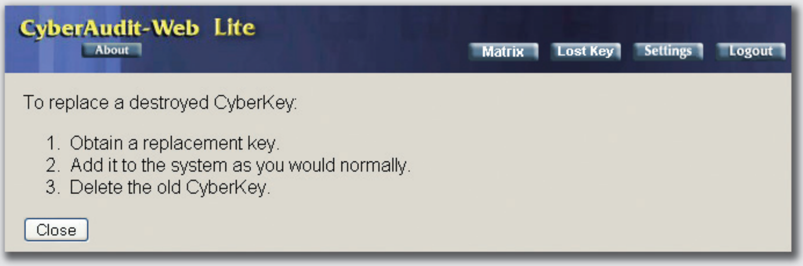
What type of key?

My Grand Master key

One of my standard CyberKeys

Figure 3-19: *Select the Type of Key*

Broken or destroyed keys are easier to process than lost or stolen keys, as they only need to be replaced by new keys and then deleted from the system. If replacing a standard CyberKey, simply follow the instructions given on the page. Deleting CyberKeys will be discussed in the following section.

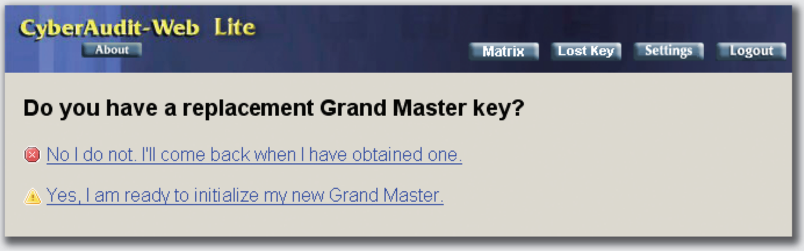


To replace a destroyed CyberKey:

1. Obtain a replacement key.
2. Add it to the system as you would normally.
3. Delete the old CyberKey.

Figure 3-20: ***Instructions for Replacing a Broken or Destroyed CyberKey***

If replacing a broken or destroyed Grand Master, the page will verify that a replacement has been obtained before continuing. The same *Grand Master Configuration Wizard* encountered the first time the application was launched will appear after clicking on the *"Yes . . ."* link. The *"No . . ."* link will return the user to the Access Matrix when clicked. The replacement process must be completed from the beginning after a new Grand Master has been obtained.



Do you have a replacement Grand Master key?

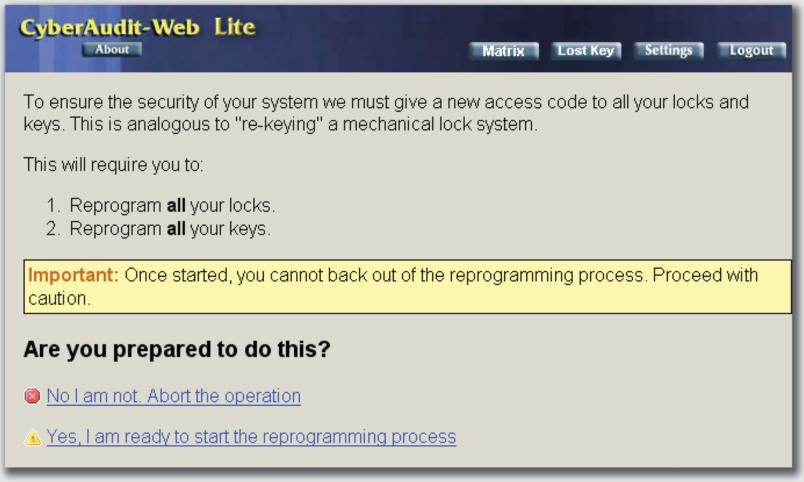
No I do not. I'll come back when I have obtained one.

Yes, I am ready to initialize my new Grand Master.

Figure 3-21: ***Replacing a Broken or Destroyed Grand Master***

Protecting the system from a lost or stolen CyberKey or Grand Master requires changing the access code that is used by the locks and keys. This means that the Grand Master (assuming that a standard user key was lost or stolen) must be updated using *CyberLink*. After the Grand Master has been re-configured, it must contact all the CyberLocks. This will ensure that each lock gets the new access code. Finally, all CyberKeys in the system must be reprogrammed.

If protecting against a lost or stolen CyberKey, the page will issue a warning before generating a new access code. Click the *"Yes . . ."* link to continue, or the *"No . . ."* link to return to the Access Matrix.



To ensure the security of your system we must give a new access code to all your locks and keys. This is analogous to "re-keying" a mechanical lock system.

This will require you to:

1. Reprogram **all** your locks.
2. Reprogram **all** your keys.

Important: Once started, you cannot back out of the reprogramming process. Proceed with caution.

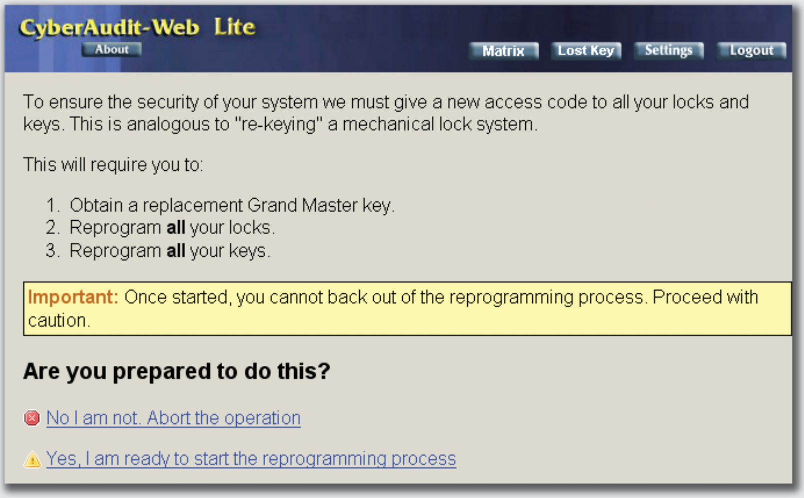
Are you prepared to do this?

☒ No I am not. Abort the operation

⚠ Yes, I am ready to start the reprogramming process

Figure 3-22: ***Preparing to Reprogram the System - Lost or Stolen User Key***

If a Grand Master has been lost or stolen, a replacement must be obtained before the system can be reprogrammed. After clicking the *"Yes . . ."* link, the *Grand Master Configuration Wizard* will appear. After the Grand Master has been programmed with the new access code, all locks in the system must be configured by contact, and all CyberKeys must be updated.



To ensure the security of your system we must give a new access code to all your locks and keys. This is analogous to "re-keying" a mechanical lock system.

This will require you to:

1. Obtain a replacement Grand Master key.
2. Reprogram **all** your locks.
3. Reprogram **all** your keys.

Important: Once started, you cannot back out of the reprogramming process. Proceed with caution.

Are you prepared to do this?

No I am not. Abort the operation

Yes, I am ready to start the reprogramming process

Figure 3-23: ***Preparing to Reprogram the System - Missing Grand Master***

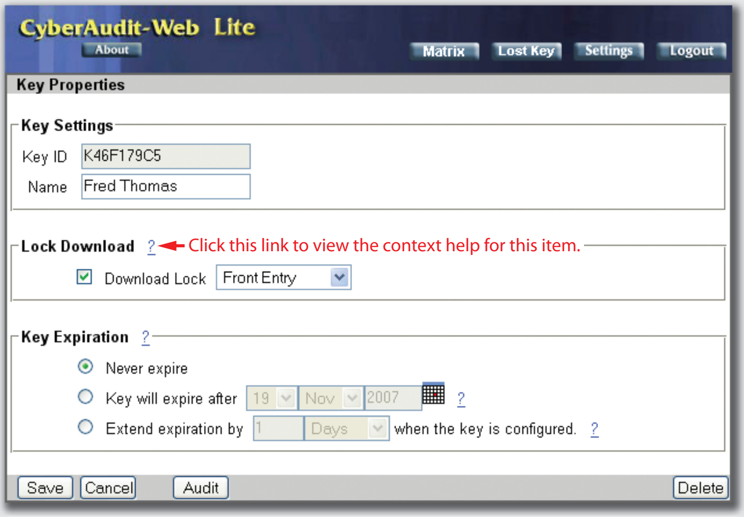
Help and Support

Help pages are available within the CyberAudit-Web Lite application. If the information available on these pages is not sufficient to answer any questions, please contact the reseller from whom the system was purchased or Videx Technical Support:

Phone: (541) 758-0521
Email: support@videx.com
Hours of Operation: 8:00am - 4:30pm (Pacific), M - F

Context Help

Most pages within the CyberAudit-Web Lite application contain at least one hyperlink in the shape of a question mark. These links appear next to items for which context help is available.



Key Properties

Key Settings

Key ID K46F179C5

Name Fred Thomas

Lock Download ? Click this link to view the context help for this item.

☑ Download Lock Front Entry

Key Expiration ?

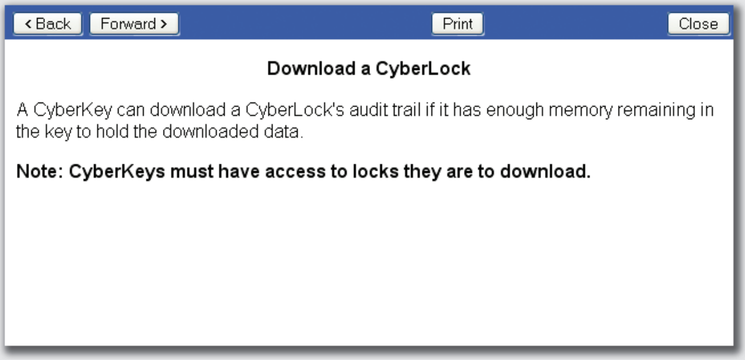
● Never expire

○ Key will expire after 19 Nov 2007 ?

○ Extend expiration by 1 Days when the key is configured. ?

Figure 4-1: ***A Sample Context Help Link***

When clicked, the link will open a small browser window containing helpful hints about the associated item or page section.



Download a CyberLock

A CyberKey can download a CyberLock's audit trail if it has enough memory remaining in the key to hold the downloaded data.

Note: CyberKeys must have access to locks they are to download.

Figure 4-2: ***A Sample Context Help Page***

Customer Support

Videx has a commitment to provide excellent customer support. In the event you experience any problems with Videx equipment, please contact the Videx Technical Support Department and our technicians will assist you:

Phone: (541) 758-0521
Fax: (541) 752-5285
E-mail: support@videx.com
Web: www.videx.com
Hours of Operation: 8:00am - 4:30pm (Pacific), M - F

If, after contacting Technical Support, it has been determined that a product is to be returned, please carefully pack the product together with your purchase receipt or other proof of the date of original purchase, and send it prepaid and adequately insured to:

Videx, Inc.
1105 NE Circle Blvd.
Corvallis, OR 97330
USA

A note detailing the problem is most helpful and should be included in the box.

APPENDIX I

Technical Information

WARNING:

This section contains information for advanced users only! Modifying system setups described in this appendix could cause irreparable damage to databases if not properly executed. Be extremely certain of your actions before making any changes!

Application Specifics

The CyberAudit-Web Lite software is written in Java. Version 1.5 or higher (of Java) must be installed on the system in order for it to run. To find out which version of Java is installed on the system, click the *"About..."* button in the Java control panel, or type *"java -version"* at the system command prompt.

Application pages are served to the web browser by a program called Jetty, but Tomcat could also be used. For more information on Jetty, visit *www.mortbay.org*. Jetty may be started or stopped by right-clicking on the 🟩 icon in the Windows system tray.

Date and time data is stored by the application in Videx UTC format. This is an integer representation of the number of seconds which have elapsed since midnight on January 1, 1996.

Database Information

The default database server is Derby, though it is possible to use MySQL or SQL-Server. For more information on Derby, visit the Apache Group’s website at *www.apache.org*.

The type of database used and its necessary configuration options may be changed by editing the file named *“CyberAuditLite.properties”* located in the *“webapps”* subfolder of the Jetty installation directory. By default, Jetty is installed in *“C:\Program Files\Videx\CyberAudit-Web Lite\jetty”*, though it is possible to select a different directory when installing the software. To change the type of database used, uncomment the appropriate section of the file and comment out the default section (commented lines begin with *‘#’*). Specify the appropriate location of the database, its name, and the required username and password.

A sample *CyberAuditLite.properties* file is shown below.

```
# derby
database.type=Derby
database.host=USER_HOME\\CyberAuditLite
database.global.name=lite_global
database.user=APP
database.pswd=APP

# SQL-SERVER
#database.type=SqlServer
#database.host=172.10.1.92;
#database.global.name=lite_global
#database.user=sql-CAW
#database.pswd=cawpw

# MYSQL
#database.type=MySql
#database.host=localhost
#database.global.name=lite_global
#database.user=mysql-CAW
#database.pswd=cawpw

# common
database.connections.poolsize=10
database.connections.detectleaks=0
```

The default database location is
C:\Documents and Settings\<username>\CyberAuditLite”.

Server Installation

Because a web browser is used to interface with the application, it is possible to install the CyberAudit-Web Lite software on a server machine and access it over a LAN or the Internet. Multiple persons will be able to use the application simultaneously (up to a maximum of 10), and all data will be stored in the same database.

On Windows servers, to change the port number on which Jetty communicates (so as not to interfere with other TCP/IP services), two files must be modified. Both are located beneath the Jetty installation directory.

The first file, *“url.txt”*, contains only one line:

```
http://localhost:8083/CyberAuditLite/
```

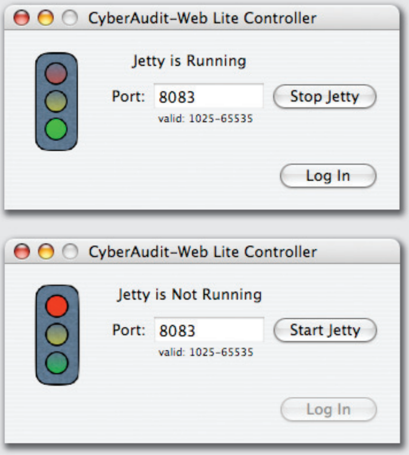
To change the port, simply replace the value *“8083”* with the new port number.

The second file, *“jetty.xml”*, is located in the *“etc”* subfolder of the Jetty directory and contains all the information needed to launch the web server. The parameter named *“jetty.port”* must be edited to reflect the desired port number. Locate the following line in the file:

```
<Set name=”port”><SystemProperty name=”jetty.port” default=”8083”/></Set>
```

Replace *“8083”* with the same value entered for the new port number in the first file.

Changing the Jetty port number on Mac servers is much easier. While the application is running, choose *"Preferences..."* from the *CyberAudit-Web Lite* application menu to display the *CyberAudit-Web Lite Controller* window. The network port on which the Jetty server listens may be changed in this window, provided that the server is stopped first.



CyberAudit-Web Lite Controller

Jetty is Running

Port: 8083

valid: 1025-65535

CyberAudit-Web Lite Controller

Jetty is Not Running

Port: 8083

valid: 1025-65535

Figure I-1: ***The CyberAudit-Web Lite Controller Dialog***

The server status may also be seen at a glance in this window. If the server is running, a green traffic light is displayed. If the server is stopped, a red traffic light is displayed. The server may be started and stopped using the applicable buttons.

Finally, if the CyberAudit-Web Lite browser window has been closed, but the server is still running, the application window can be re-launched by clicking the *Log In* button.