



Professional

Version 1.1

Reference Manual

Table of Contents

System Setup

Recommended Order of Implementation.....	1
------------------------------------------	---

Software Overview

User Interface and Navigation	3
Menus	3
Item Choosers.....	6
Tags	8
Getting Help.....	10
Access Matrix Functionality	12
Granting Access to Locks.....	13
Controlling the Display	14
Navigation	15
Operations Menu	15
Filters.....	17
Matrix Options	19
Locks Menus and Functionality	21
Filters.....	23
Lock Properties.....	24
Bulk Editing	26
Lock Tags	27
Lock Tag Properties.....	28
The CyberPoint List	29
CyberPoint Properties	31
Programming Jobs.....	32
Programming Job Properties	33
Importing Lock Data	34
CSV File Format For Importing Locks	35
Lock Options	36
People & Keys Menus and Functionality	37
People Properties.....	39
Bulk Editing	41
People Tags.....	42
People Tag Properties.....	44

System Keys	45
System Key Properties	47
Importing People	48
Lost Keys.....	50
Lost Key Properties	51
People & Key Options.....	52
People & Key Options - Expiration	53
People & Key Options - Master Keys	53
People & Key Options - Memory Full Behavior	54
People & Key Options - “No Access” Behavior	54
People & Key Options - “Removed . . .” Behavior	55
People & Key Options - CyberKey IrDA Control	56
People & Key Options - Low Battery Warning Level	56
People & Key Options - Default Expiration Rule.....	57
Schedules Menus and Functionality	60
Schedule Properties	61
Holidays	62
Holiday Properties.....	64
Reports Menus and Functionality	64
Notifications	67
Notifications Properties	68
Journal of Changes	69
Email Setup	70
Communicators Menus and Functionality	71
Web Authorizers	71
Web Authorizer Properties	72
Stations	74
Station Properties	76
LAN Authorizers	77
LAN Authorizer Properties	78
IR Encoders	80
IR Encoder Properties	81
Communicators Options.....	82
Administrators Menu and Functionality	83
Administrator Properties	84
System Menus and Functionality	86
Access Matrix Options	86
Lock Options	87
Key Options.....	87
Email Notification Setup	88
Communicators Options.....	89
Date & Time Preferences	90
Archive/Restore Options	90
Backup Options	91

Remote Access	91
Re-Keying All Locks.....	92
System Logs	93
System Backup and Restore.....	94
Software Updates	95
System Help	96

CyberLink

Installing and Using CyberLink.....	97
Upgrading Key Firmware	103

Operations Reference

Access Matrix Operations.....	107
Administrators Operations.....	116
Communicators Operations	118
Locks Operations	132
People & Keys Operations.....	141
Reports Operations.....	159
Schedules Operations.....	163
Database Backup and Restore Operations	167
Miscellaneous Operations.....	169

Additional Information

Glossary of Terms	171
Lock Contact Diagrams	182
CSV File Format Descriptions.....	185
For Importing Locks.....	185
For Importing People	185
Modem Control.....	186
Event Descriptions	187
CyberKey Support Information	197
Rechargeable CyberKey Flash Patterns	199
CyberKey Tones and Descriptions.....	201
Infrared Communication Sounds.....	203
Warranty Information.....	205
Videx Limited Warranty on CyberLock Hardware	205

Introduction

CyberAudit-Web software is the platform for creating your CyberLock access control system. Designed with the mid-sized business in mind, CyberAudit-Web Professional offers a suite of features in addition to the basics of scheduled access and auditing: key expiration and lost key settings for a high degree of key control, reporting options using the data from the locks and keys, and email notification of specific events such as denied entries or weekend activity.

Installation is flexible: CyberAudit-Web Professional installs on either a PC or Mac for local control, or on a server to support a small number of concurrent software users. The software is accessible through a web browser on any terminal that can be connected to the application server. Up to 500 locks and 500 keys can be easily managed using CyberAudit-Web Professional.

The CyberAudit-Web *Access Matrix* displays the people and CyberLocks in the system and facilitates granting access. Access schedules are designated in the matrix and are represented by icons or letters. The number of displayed CyberLocks and CyberKeys is controlled in the display settings. Navigation controls are available for when there is more data than can be displayed on a single page of the Access Matrix. In addition to the Positioning Box, navigation controls are available for scrolling data up, down, right, or left. Single arrow controls scroll one row or column at a time. Double arrow controls scroll one full page.

Another feature to aid in managing locks, lock tags, people, or people tags are the Access Matrix filters. To find a person, lock or tag quickly, enter the sequence of characters to filter on in the filter link and it will find the records containing those letters.

People and *Lock* page navigation is controlled by the arrows bracketing the page number link. Clicking the link will open more page options including browsing to the first and last pages, selecting a page to jump to, or the number of people/locks per page.

System Setup

For detailed instructions on installing and preparing the software for use, refer to the “*CyberAudit-Web Professional Installation and Troubleshooting Guide*,” included in the box with the software. Following these instructions completely will result in the creation of a new database. As an alternative, an existing database may be imported from a CyberAudit Professional 2.0, CyberAudit-Web Lite, or CyberAudit-Web Professional backup file.

Recommended Order of Implementation

The order of implementation is not critical. However, for efficiency in programming locks and keys, the following sequence is recommended:

- I. Specify System Options
 - A. Set Lock Options
 - B. Set People and Key Options
 - i. Key Options
 - ii. Default Expiration
 - C. Add Additional Administrators
 - D. Set Communicator Options
 - i. Default URL
 - ii. Proxy Settings
 - iii. Key Associations
- II. Add Communicators
- III. Add Locks
- IV. Add Schedules and Holidays
 - A. Add Holidays
 - B. Add Schedules
 - i. (Optional) Add Icons for Schedules

- V. Add People and Keys
- VI. Set Access
 - A. Establish and Assign Tags
 - B. Assign Access
- VII. Update Keys
- VIII. (Optional) Define Reports and Notifications

Software Overview

Inside this chapter:

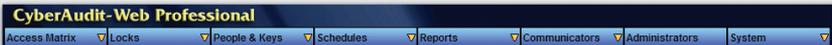
- *User Interface and Navigation*
- *Access Matrix Functionality*
- *Locks Menus and Functionality*
- *People & Keys Menus and Functionality*
- *Schedules Menus and Functionality*
- *Reports Menus and Functionality*
- *Communicators Menus and Functionality*
- *Administrators Menu and Functionality*
- *System Menus and Functionality*

This chapter will introduce the major sections of the software and how to interact with each one.

User Interface and Navigation

Menus

CyberAudit-Web Professional uses menus to manage a CyberLock system.



The CyberAudit-Web Professional Menu Bar

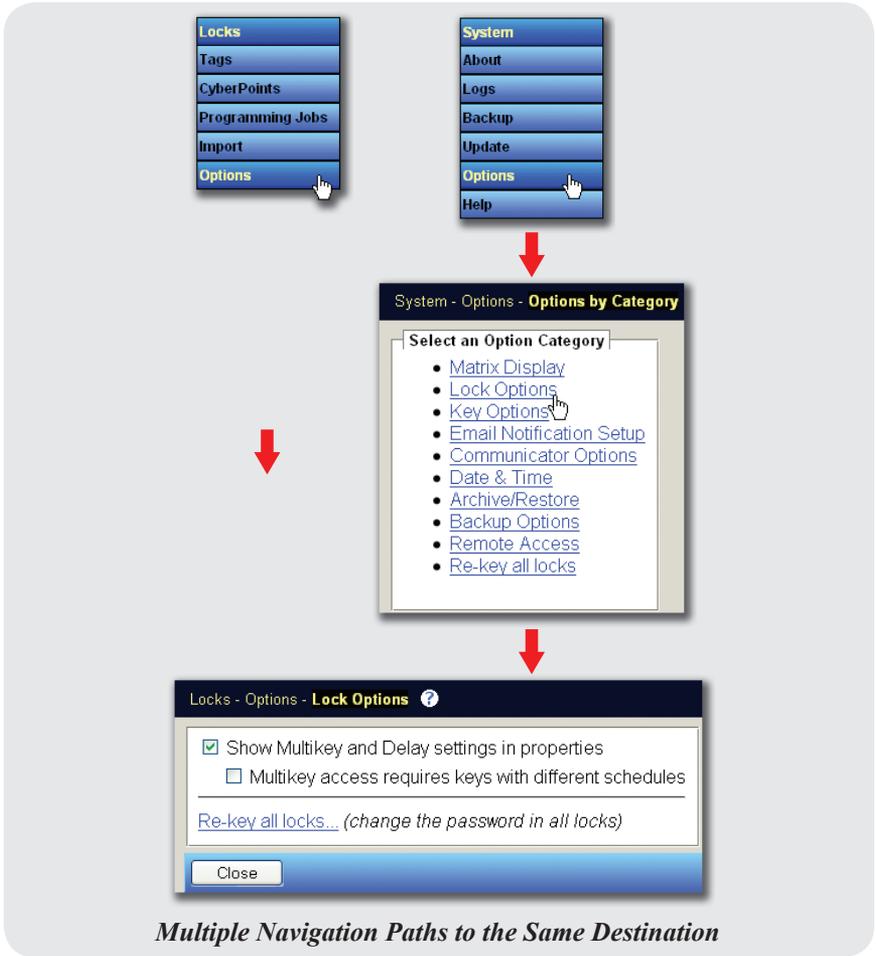
The presence of submenus is indicated by a yellow ▼ icon in the menu header.

Submenus are accessed by hovering the mouse pointer over a menu header.



An Expanded Submenu

There are often multiple navigation paths to reach the same part of the software. For example, the global options for locks may be accessed by choosing *Options* from the *Locks* menu, or it may be found by selecting *Options* from the *System* menu, then choosing the *Lock Options* category from the *Options by Category* page.



Multiple Navigation Paths to the Same Destination

The operations which apply to a particular item (a lock, key, person, etc.) appear in a pop-up menu when the mouse is clicked inside the item’s table cell.

The screenshot shows a web application interface titled "People & Keys - People List". It features a search bar, a filter menu on the left, and a table of people. A context menu is open over the "LaFleur, Nancy" row, showing options like "Properties", "Show in Matrix", "Audit Report", "Comm Log", and "Delete".

Click inside a cell to view available item operations.

Name	Key Serial / Issue Number	Next Expiration	Master Key	Tagged with	Accessible Locks
Adams, Mark	K44A3EABE	Never		Engineering	5
Baker, Daniel	K600017CF	6/4/2009 11:59 PM			2
Baxter Rita					0
Charger, Robert	K438B5F70	Key Not Configured			0
Corzine, Jean	K4195AD19	Key Not Configured		Accounting Day	10
Gorski, Stan	K3E36DCA2	1/17/2064 3:59 PM			8
Grady, Margaret				Night Support	10
Jones, Mario				Night Support	10
Keller, Martha					0
Knuston, Ben	K42B3285D	5/15/2009 11:59 PM			1
LaFleur, Nancy		Key Not Configured			5
Master key		1/18/2016 11:59 PM	✓		28
Moore, Patricia					0
Muhammad, Abd		1/18/2016 11:59 PM		Accounting	3
Norris, Christoph				Day Production	10
Powell, Edwin	K3EA43148	8/1/2005 4:59 PM			10
Pyle, Nellie	K3E36DB54	1/17/2064 3:59 PM			5
Sanchez, Andy	K3E36D880	1/17/2064 3:59 PM			0
Simms, Carol	K3FDF7C8E	1/17/2064 3:59 PM			1
Tamal, Srini				Night Production	10
Trujillo, Lanny	81857273	Key Not Configured			1
Wells, Homer				Day Production	10

An Available Operations Pop-Up Menu

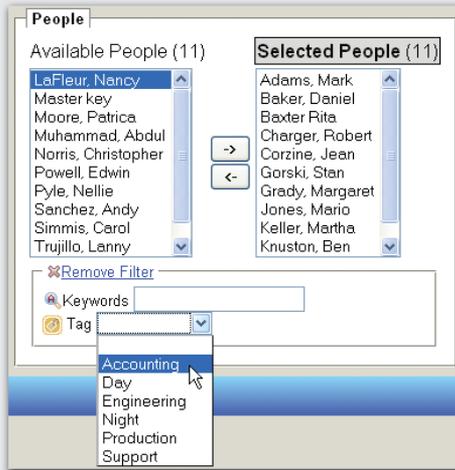
Item Choosers

Some pages, such as the *People Properties* page, contain *Item Chooser* controls with keyword filtering, which are used to select multiple items and build lists. Available items are displayed on the left-hand side of an Item Chooser, and selected items are displayed on the right. Items may be moved from one side to the other by clicking the and buttons. Multiple items may be chosen simultaneously by holding down the *Ctrl* key (Windows) or the key (Mac) on the keyboard and clicking on individual items. Hold down the *Shift* key and click two items to select the range of items between them.



Selecting Multiple Items in an Item Chooser

The number of available items shown in an Item Chooser may be reduced to aid selection. Click the  icon or the adjacent link to enable the list filter controls.



Filtering an Item Chooser List

Keyword filtering works not only in Item Choosers, but also in the Access Matrix and other lists. Matching items are found based on the pattern entered as the search string.

Pattern Matching Rules for Keyword Filtering:

- Character sequences containing the search text will return a match. The text *“he”* will match *“she”* and *“there.”*
- Searching is case-insensitive. Searching for *“a”* will match both *“a”* and *“A.”*
- Adding additional search terms, separated by spaces, will expand the number of returned results, not limit them. For example, searching for *“Mary Smith”* will return both *“Mary Taylor”* and *“John Smith.”*
- Search terms enclosed in quotation marks, including spaces, must match exactly as entered to return a result.
- Both quoted and unquoted search terms may be used simultaneously, separated by spaces.
- Quotation mark characters are interpreted only as operators, and cannot be searched for themselves.
- Patterns are searched for in both names and IDs of items.

Tags

In CyberAudit-Web, tags help organize people and locks into logical categories by providing an unlimited number of ways to describe them. There is no wrong choice for how to use them. Instead of belonging to one “group,” people and locks may have any number of tags.

Here are some examples of how tags may be used:

- ABC Enterprises uses people tags to organize their employees by department. The departments are Accounting, Engineering, Human Resources, Maintenance, Marketing, Production, and Support. Employees of each department have a set of locks they must be able to open.

ABC creates lock tags to group CyberLocks for access. Finally, using the Access Matrix, ABC grants each people tag access to each of the groups of CyberLocks it requires.

“Maintenance” is a lock tag. It tags CyberLocks needed to do the Maintenance functions at ABC. The “Maintenance” tag also includes some locks that are tagged with “Production” and “Human Resources” because all three departments require common access to some locks.

Gail Ash, as supervisor of Marketing and Support, is tagged with both “Marketing” and “Support” people tags. This allows her to access both “Marketing” and “Support” tagged CyberLocks. Norman Cooper, normally tagged with Production, temporarily gets the “Maintenance” tag when Eric Montoya, the regular Maintenance employee, goes on vacation.

- Green Construction Company employs electricians, plumbers, carpenters, and other specialists. Each employee serves a role in the construction process. Green uses CyberLocks to help them maintain control on their supply of raw materials. They use people tags to classify their employees by the role they play in the company. They use lock tags to identify the CyberLocks each employee group must access.

When Green adds a new electrician, Kashif Saleem, they simply tag his record with the “Electrician” people tag. When they issue him a CyberKey, it will automatically be programmed to open the locks that electricians at Green Construction need to open.

(Continues on next page . . .)

(. . . continued from previous page)

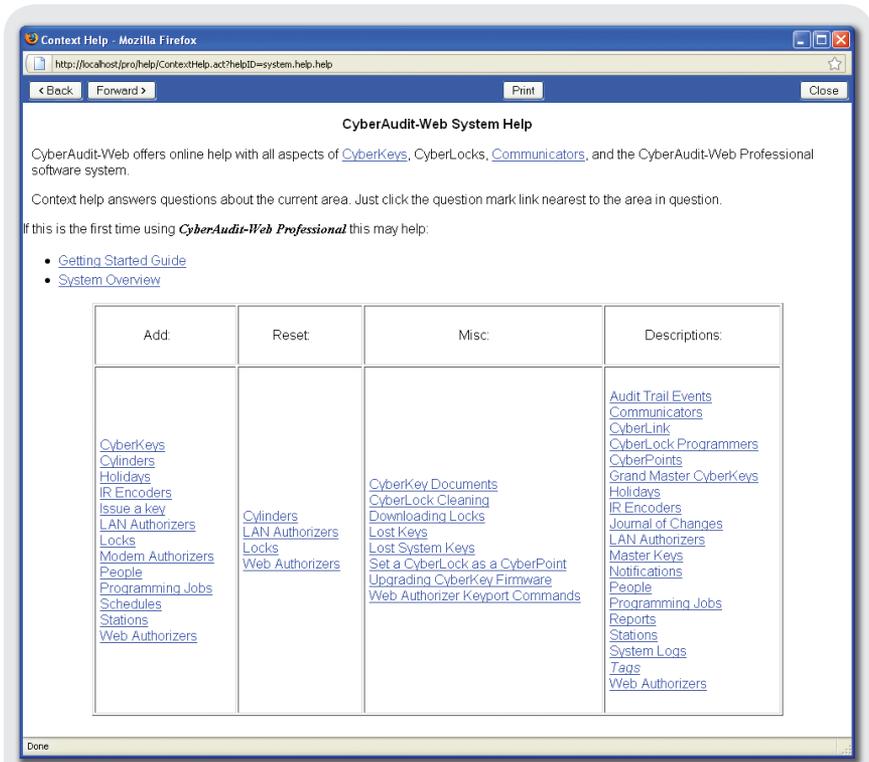
- Wilson Vending uses CyberLocks on their vending machines to prevent key duplication and to maintain an audit trail of activity for each vending machine asset. Most key holders are either route drivers or service technicians. Wilson uses lock tags to identify the assets and CyberLocks on each route. Then they use people tags to identify the drivers that will service each route.

The service technicians must be able to open a broader group of locks. Wilson again uses lock tags, this time to identify the assets that fall into each service area. As a result, each asset (CyberLock) gets two tags; one for its route and one for its service area. The service technicians are then tagged with a descriptor for their service area and access is granted to the appropriate group of locks.

Finally, auditors for Wilson want to classify the vending assets by the “type” of product they dispense (snacks, cold beverage, hot beverage, money token.) They create additional lock tags using these descriptors and apply them to the locks. They then use the descriptors to help them create customized reports for audit trails from these locks.

Getting Help

Online help is available for an in-depth explanation of all aspects of CyberKeys, CyberLocks, Communicators, and the CyberAudit-Web Professional software system. The *System Help* page is accessed by selecting the *Help* option from the *System* menu. It is displayed in a separate window for convenience.



The System Help Page

Context help answers questions about the current area. Just click the question mark link (?) nearest the area in question. Context help pages contain links to other subjects within the same page. The following page contains an example of context help for the Item Chooser control.

The CyberAudit-Web Item Chooser Control

The CyberAudit-Web Item Chooser is a control used to select items and create lists. Below are two examples of Item Choosers.

Tags

Available Tags:

- Marketing
- Human Resources
- Engineering
- Maintenance
- Accounting
- Night
- Support

-> <-

Selected Tags:

- Production
- Day

[Filter these lists](#)

People

Available People

- Adams, Mark
- Alcazar, Ernesto
- Anderson, Kathrine
- Ash, Gail
- Baker, Daniel
- Baxter, Rita
- Bickford, Mary Lou
- Cooper, Norman
- Corzine, Jean
- Curtis, Fred

-> <-

Selected People

[Filter these lists](#)

Item Chooser for applying [tags](#) to people

Item Chooser for selecting People to include in a [report](#)

To use the Item Chooser control, select items from one list and click the direction arrow to move them to the other list. Use Ctrl-Click to add individual items to the selection or Shift-Click to select a range of items.

Click on [Filter these lists](#) to further reduce the list of choices in the item chooser.

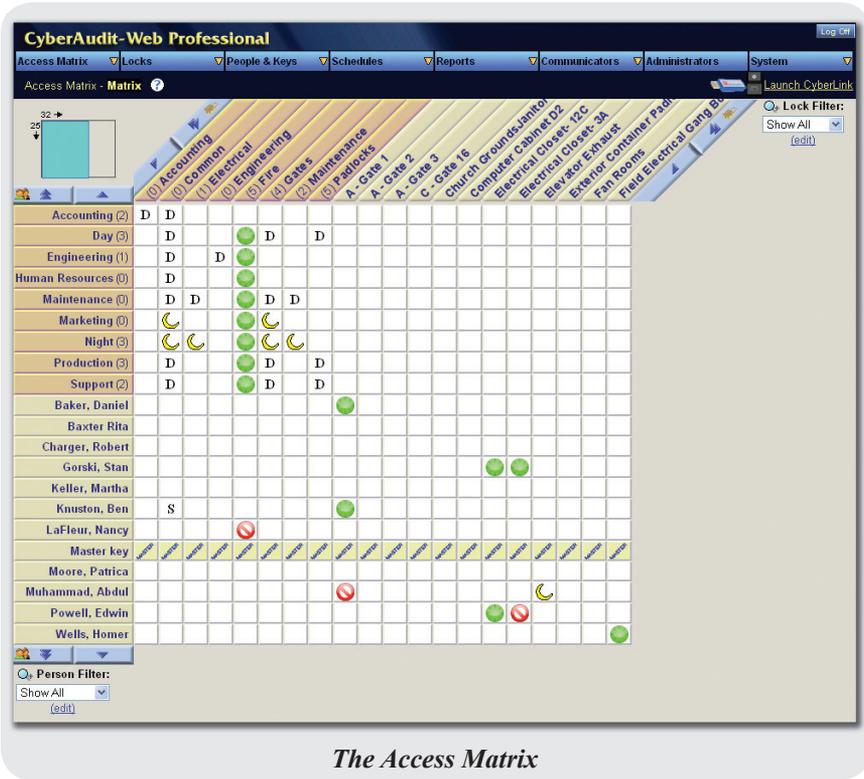
All items may be filtered by [Keywords](#). The Keyword filter supports pattern matching by these rules:

- Matching looks for substrings. *he* would match *she* and *there*.
- All matching ignores differences between upper case and lower case.
- Additional substrings may be added to increase the possible matches. Separate each substring with a *space*. For example, searching for *ma* against a list containing *Peter, Paul, and Mary* would result in a list of *Mary and Paul*.
- Use double quotes to look for a phrase. Within double quotes a *space* is meaningful. For example, "*he sat*" would not match *she sat*.
- Quoted phrases and substrings may be used at the same time. Separate each with a *space*.
- A quote character (") cannot be searched.
- The search is done on both names and IDs.

The Context Help Page for Item Chooser Controls

Access Matrix Functionality

The *Access Matrix* displays the people and locks in the database and enables granting access to CyberLocks. People and people tags are shown vertically (rows), and locks and lock tags are shown horizontally (columns).

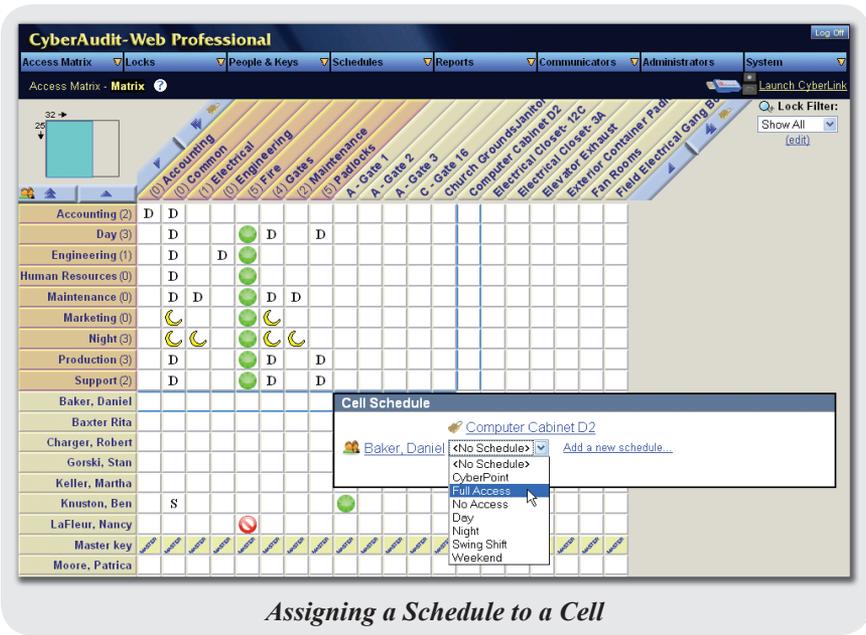


The Access Matrix

The schedule by which a person may access a lock is indicated by a letter or icon in the cell where the row and column intersect.

Granting Access to Locks

Access is granted by assigning a schedule to the cell at the intersection of the desired person and CyberLock. To apply a schedule, click on the cell. The *Cell Schedule* overlay will appear, showing the names of the person and lock (or tags) as links. Clicking one of these links will open the corresponding properties page. Select an existing schedule to assign from the drop-down menu, or click the *Add a new schedule* link to create a new one.



Assigning a Schedule to a Cell

Controlling the Display

The Position Box is located above the list of People and illustrates which portion of the Access Matrix is currently visible on the screen. The blue section represents the currently visible subset of the matrix, and the grey section represents the remainder. The view is navigated by the arrows framing the CyberLock and People lists or by dragging the blue box to the desired location in the position box. The numbers at the top, left-hand corner of the box represent how many total people and locks are displayed with the current filter settings.

32 locks and 25 people are currently displayed.

The Position Box

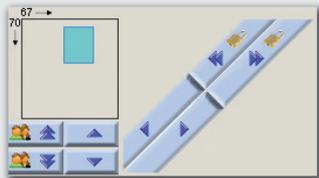
Use these buttons (at both ends) to scroll the display.



The Position Box

Navigation

In addition to the Position Box, Navigation Controls are available for scrolling the matrix up, down, right, or left. Single-arrow controls scroll one row or column at a time. Double-arrow controls scroll one page at a time.



The Access Matrix Navigation Controls

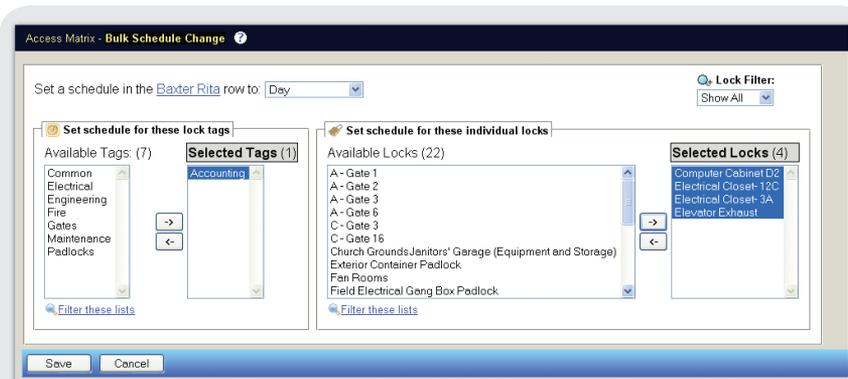
Operations Menu

A special pop-up menu is displayed when a header cell (the name of a lock, person, or tag) is clicked. This menu includes options which affect the selected intersection only and options which can affect multiple intersections at one time.



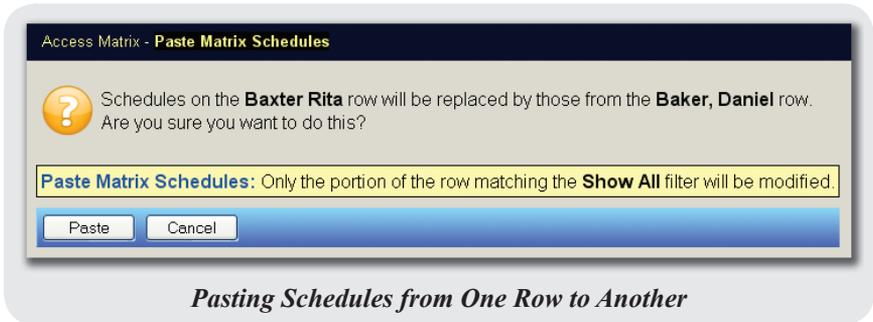
The Operations Menu for a Row Header

The *Bulk Schedule Change* option enables an administrator to set a schedule for a row or column in the Access Matrix. Schedules may be set for a person against a selected set of locks and lock tags. Schedules for a lock are set against selected people and people tags.



The Bulk Schedule Change Page

Schedules from one row or column may be copied and pasted to another, using the *Copy Row Schedule* command from the menu. The menu also includes an option to clear all schedules from a row or column.

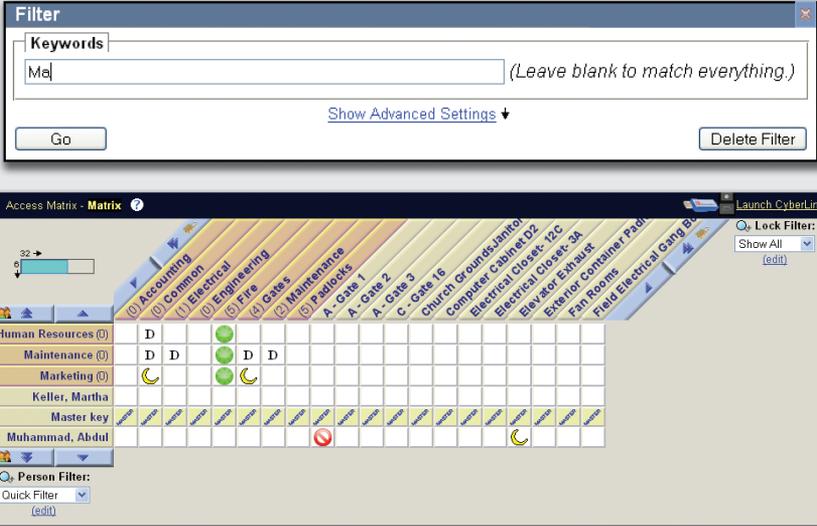


Filters

Another feature to aid in managing locks, people, and tags are the Access Matrix filters, found at the end of the header row and column. To create a filter, click on the *(edit)* link, or choose *New Filter* from the pull-down list.



In the *Filter* overlay that appears, type a string of characters. Person and Lock filters match patterns based on the same rules outlined earlier in this chapter.



A Person Filter and the Resulting Matrix

The most recent search will be saved as *Quick Filter* in the drop-down list. If the same search will be performed often, it can be given a name and saved in the list. Click on the *Show Advanced Settings* link in the *Filter* overlay, then type a name in the *Filter Name* field. Other advanced options for filters include finding tags only (as opposed to individual persons or locks), hiding unused tags, sorting the results so that tags appear at the top, and customizing the dimensions of the results matrix. Tags are covered later in this chapter, in the sections titled “Lock Tags” and “People Tags.”

Advanced Filter Options

Matrix Options

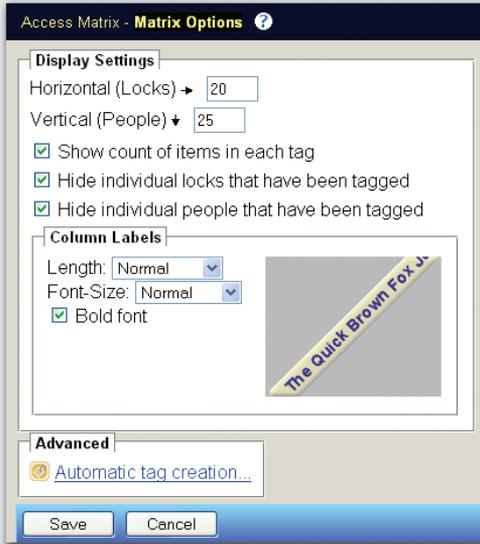
The *Matrix Options* page is accessed by choosing *Options* from the *Access Matrix* menu. To manage the total number of CyberLocks and people displayed in the matrix per frame, adjust the horizontal and vertical limits. The number in the *Horizontal* field will change the number of locks displayed. The *Vertical* field changes the number of people displayed. To display the number of people or locks that belong to each tag, check the box next to *Show count of items in each tag*.

By default, CyberAudit-Web attempts to hide individual locks and people in the matrix when they are a member of one or more tags and have no individual schedules designated. Clear the *Hide individual locks/people that have been tagged* checkboxes to prevent CyberAudit-Web from hiding the individual items.

Some lock names may be too long to display in the allocated space for the column label graphic. Both the length of the label and the font size used to generate the graphic may be changed to a preferred setting.

CyberAudit-Web Professional can automatically create lock and people tags to simplify the Access Matrix. This will ease access

control management within the system. When the same group of people have access to the same lock or locks using the same schedule, they will be grouped together in a single tag.



The Matrix Options Page

Click the *Automatic tag creation* link and follow the on-screen instructions to have CyberAudit-Web automatically generate tags. If the results of the automatic tagging are undesirable, restore the database to its previous state. Select *Backup* from the *System* menu and restore the most recent file named “*Before Automatic Tag Creation.*”

Locks Menus and Functionality

The *Lock List* page is accessed by clicking on the *Locks* menu header. This page allows new CyberLocks to be added and edited. Each row contains information about a lock.

The screenshot shows the 'Locks - Lock List' page. It features a navigation bar with 'New' and 'Edit All (28)' buttons, and a 'Locks (28) 2 Page 1 of 1' indicator. A search filter is available. On the left, there is a 'Filter By Tag' section with a list of tags: Accounting (0), Common (0), Electrical (1), Engineering (0), Fire (5), Gates (4), Maintenance (2), and Padlocks (5). The main table displays the following data:

Name	Serial	Reset	Multi-key Mode / Open Delay	Tagged with	People with Access
A - Gate 1	L3A55F1B9		Single Key / No Delay		4
A - Gate 2	L11111111		Single Key / No Delay		1
A - Gate 3	L11111112		Single Key / No Delay		1
C - Gate 16	L11111114		Single Key / No Delay		1
Computer Cabinet D2	L11111116		Single Key / No Delay		1

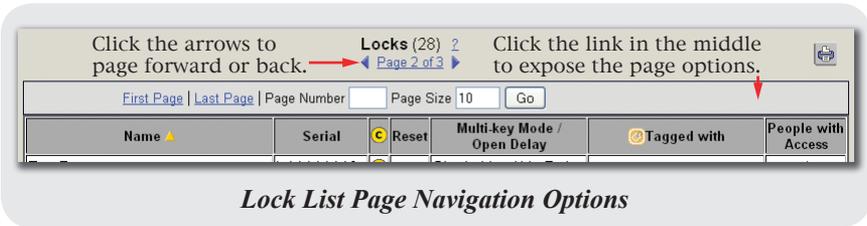
The Locks List Page

The *Locks* table displays the following in each row:

- The lock name.
- The serial number of the lock.
- The icon. This is displayed only if the lock needs to be updated.
- The icon. If this icon is displayed without a icon in the same row, it indicates that the lock is not programmed with any access codes. If the icon is also present, the lock needs to be reset.
- The multi-key/delay setting.
- The tags applied to the lock. Clicking a tag name brings up the properties page for that tag.
- The number of people who may open the CyberLock. Clicking the link will generate a report listing authorized personnel.

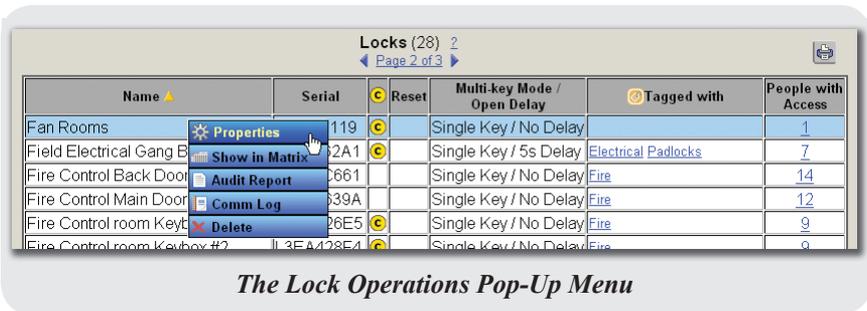
Note: Once a lock is updated or reset, the CyberLock Programmer or Grand Master that communicated the change to the lock must be downloaded to CyberAudit-Web to clear the yellow **C** icon.

Page navigation is controlled by the arrows bracketing the link which displays the current page number. Clicking the link will expose more page options.



In the upper left-hand corner of the *Lock List* page are two buttons. Clicking the **+ New** button brings up the *New Lock* page. Clicking the **Edit All (28)** button allows for bulk editing of the locks in the list.

Clicking in a table cell which does not contain a link displays a pop-up menu of available operations for the selected lock.



Choosing the *Properties* option displays the properties of the selected lock. The *Show in Matrix* option creates a filter in the Access Matrix to display the people and people tags which have access to the lock. The *Audit Report* option generates a report of audit trail data associated with the selected lock. The *Comm Log*

option generates a report of CyberLock status retrieved from the lock when downloaded by a CyberKey, Grand Master, CyberLock Programmer, or USB Programmer. Selecting the *Delete* option removes the selected lock from the system (after a confirmation).

Filters

There are two types of filters which may be used to reduce the number of locks displayed in the table. The text filter matches patterns based on the rules explained earlier in this chapter. The tag filter matches locks to which the selected tag has been applied, and may be used in conjunction with the keyword filter to further reduce the number of rows shown in the table.



The Lock List Filters

To remove all filters and display all of the locks, click the *Remove Filter* link near the page controls at the top of the list.

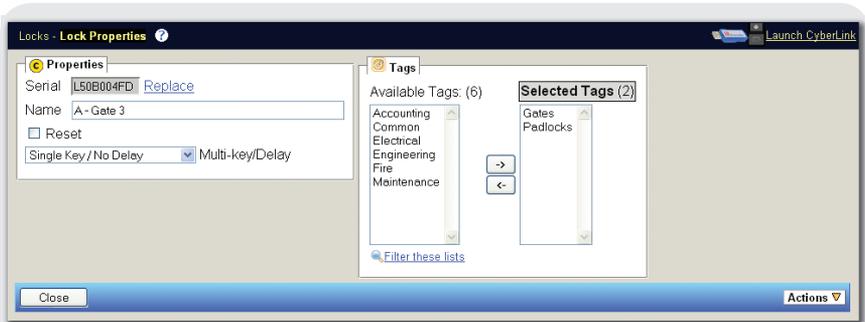
Click this link to remove the filter.



Removing the Lock Filter

Lock Properties

The *Lock Properties* page, accessed by selecting *Properties* from the lock operations pop-up menu, displays the properties for an individual CyberLock and allows them to be edited.



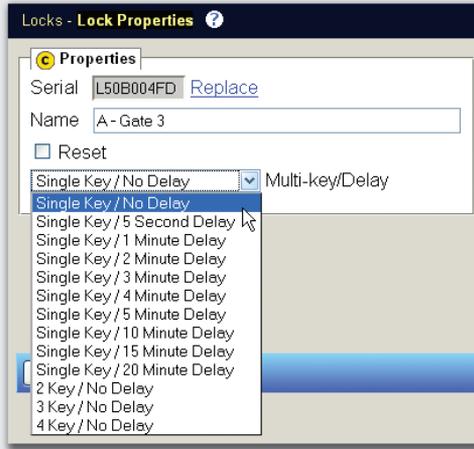
The Lock Properties Page

The *Serial* field displays the unique ID of the CyberLock. This cannot be edited. The CyberLock can, however, be replaced by clicking the adjacent link.

The description entered in the *Name* field is displayed in the audit trail data downloaded from CyberKeys or downloaded from the CyberLock.

Checking the *Reset* box tells CyberAudit-Web that the CyberLock is to be reset. This will clear all access codes from the lock and return it to factory settings the next time it is updated.

Selecting an option other than *Single Key/No Delay* from the *Multi-key/Delay* drop-down list will modify the behavior of the CyberLock when contacted by an authorized key. The lock can be set to delay opening for a specified interval of time, or it can be set to require contacts from multiple keys before opening.



Available Multi-Key/Delay Options

The *Lock Properties* page also includes an item chooser used to associate the selected lock with the necessary tags.

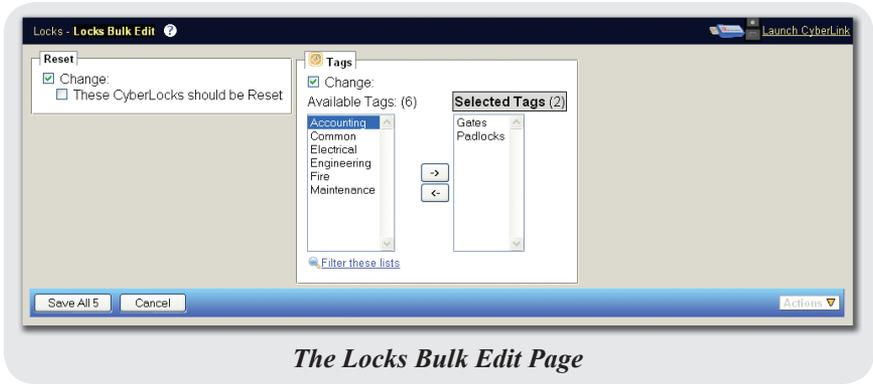
Clicking on the **Actions** button in the blue bar at the bottom of the page will expose an operations menu identical to the one from the *Lock List* page, with the exception that there is no *Properties* option.



The Lock Properties Page Actions Button Menu

Bulk Editing

The *Locks Bulk Edit* page allows the same settings and tags to be applied to the selected group of CyberLocks. First, use Lock Filters to select the desired locks from the *Locks List* page, then click the  button to access the *Locks Bulk Edit* page.



All of the selected locks may be marked for reset or associated with the selected tags at the same time.

Note: CyberPoints may not be reset.

The  button menu on this page only contains the option to delete all of the selected locks (after confirmation).



The Locks Bulk Edit Page Actions Button Menu

Lock Tags

Lock tags are used to group CyberLocks together for both management and function. The *Lock Tag List* page is accessed by selecting *Tags* from the *Locks* menu. It displays the list of tags which have been created, the number of locks associated with each tag, and the number of people who have access to those locks.



The Lock Tag List Page

The number of locks and people associated with a tag are displayed in the list as links. Clicking one of these links brings up either the *Locks List* page, filtered to display only those locks associated with the selected tag, or a report page showing the associated people and the schedule by which they can access the locks in the tag.

Clicking in one of the cells of the *Lock Tags* table displays an operations pop-up menu similar to that from the *Locks* table, with the addition of the *Locks Tagged* option. Selecting this option is equivalent to clicking the locks link in the table.



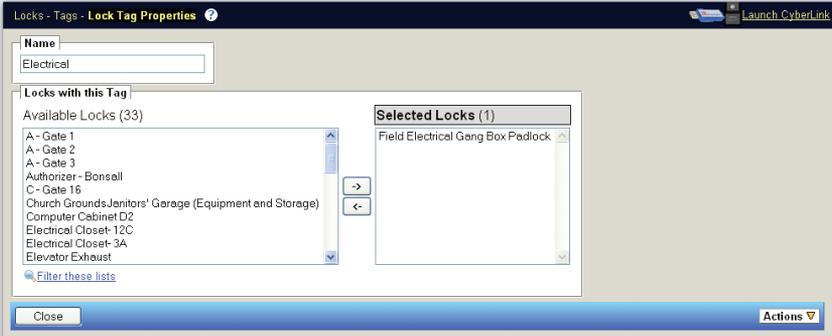
Tag Name	Locks with this Tag	People with Access
Accounting	0	3
Common	0	10
Electrical	1	4
Engineering		
Fire		
Gates		
Maintenance		
Padlocks		

The context menu for the 'Engineering' row includes the following options: Properties, Show in Matrix, Audit Report, Comm Log, Locks Tagged, and Delete.

The Lock Tags Operations Pop-Up Menu

Lock Tag Properties

The *Lock Tag Properties* page is accessed by selecting the *Properties* option from the operations pop-up menu in the *Lock Tags* table. It allows the tag name to be set or changed, and contains an item chooser which allows the tag to be associated with a specified set of locks.



The screenshot shows the 'Lock Tag Properties' page. At the top, the title is 'Locks - Tags - Lock Tag Properties'. Below the title is a 'Name' field containing the text 'Electrical'. Underneath is a section titled 'Locks with this Tag' which contains two lists: 'Available Locks (33)' and 'Selected Locks (1)'. The 'Available Locks' list includes items like 'A - Gate 1', 'A - Gate 2', 'A - Gate 3', 'Authorizer - Bonsall', 'C - Gate 16', 'Church Grounds/Jenitors' Garage (Equipment and Storage)', 'Computer Cabinet D2', 'Electrical Closet-12C', 'Electrical Closet-3A', and 'Elevator Exhaust'. The 'Selected Locks' list contains 'Field Electrical Gang Box Padlock'. At the bottom of the page, there is a 'Close' button and an 'Actions' button with a dropdown arrow.

The Lock Tag Properties Page

The **Actions** button menu on this page contains the same options as the *Lock Tags* operations menu, minus the *Properties* option.

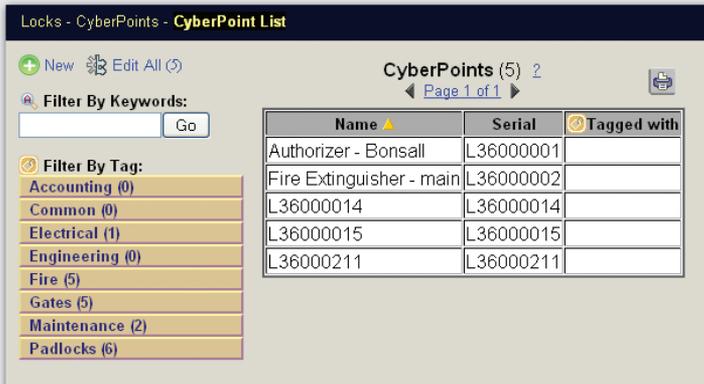


The Lock Tag Properties Actions Button Menu

The CyberPoint List

A CyberPoint is an electronic core designed to serve as a data checkpoint during security guard tours. CyberPoints differ from CyberLocks in that they have no moving parts or editable settings in the software. There is no need to program CyberPoints. They are ready to install and use right out of the box.

The *CyberPoint List* page, accessed by selecting the *CyberPoints* option from the *Locks* menu, displays the list of CyberPoints which have been added to the system.



The CyberPoint List Page

The *CyberPoints* table displays the name, serial number, and tags associated with the CyberPoint in each row. This table displays less information than the *Locks* table, because CyberPoints do not have the same properties as CyberLocks. The remainder of the page is identical to the *Lock List* page, explained earlier in this chapter section.

Clicking in one of the table cells displays the operations pop-up menu for CyberPoints. This menu is identical to the one for locks, minus the *Show in Matrix* option. Since CyberPoints cannot be assigned an access schedule, they do not appear in the Access Matrix.



The CyberPoint Operations Pop-Up Menu

CyberPoint Properties

The *CyberPoint Properties* page is accessed by selecting the *Properties* option from the operations pop-up menu in the *CyberPoints* table. This page is identical to the *Lock Properties* page, minus the *Reset* and *Multi-key/Delay* options. Since CyberPoints have no configurations, they cannot be reset. The name may be set in the *Name* field, and the CyberPoint may be associated with tags in the item chooser.



The CyberPoint Properties Page

The **Actions** button menu on this page contains the same options as the CyberPoint operations menu, minus the *Properties* option.



The CyberPoint Properties Page Actions Button Menu

Programming Jobs

Programming Jobs are a means by which selected groups of CyberLocks (up to 1,250 at a time) can be configured or downloaded. They provide a way to explicitly select the list of locks to process and enable an administrator to delegate the task of performing the job to others.

The *Job List* page, accessed by selecting the *Programming Jobs* option from the *Locks* menu, displays the Programming Jobs which have been added to the system.



Each Programming Job has a unique ID. When a Programmer or Grand Master is presented to a communicator, the system will prompt for a Job Number. Entering the Job Number tells CyberAudit-Web which set of instructions to load into the key.

The Job Number of '11111111' is reserved. Using that number will load a Programmer or Grand Master with configurations for all of the CyberLocks in the system that need be updated, up to the 1250 lock maximum.

The *Programming Jobs* table lists the Job Number, name, type, and number of locks included for each job. The job type can be either *configure* or *download*.

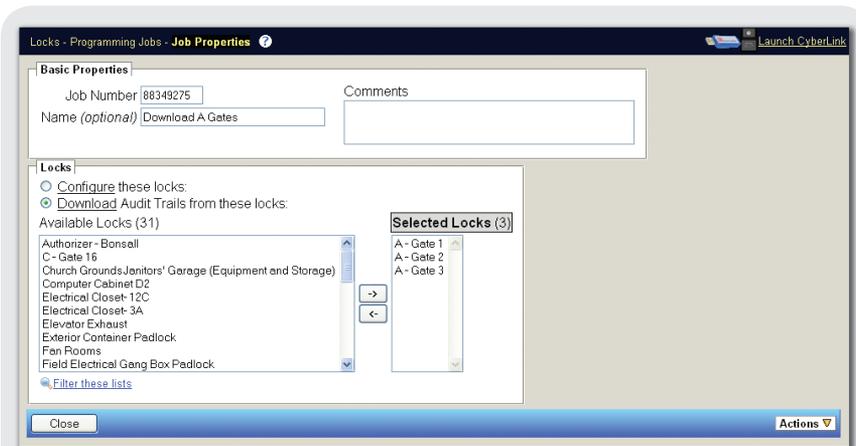
Clicking in one of the table cells displays the operations pop-up menu for Programming Jobs. The available options are to view the properties of the job or to delete it (after confirmation).



The Programming Jobs Operations Pop-Up Menu

Programming Job Properties

Selecting the *Properties* option from the operations pop-up menu for Programming Jobs brings up the *Job Properties* page.



The Job Properties Page

The Job Number is a random 8-digit number generated by the system when the Job is created. It may be changed on this page. The job may optionally be given a name and comments. Locks may be added to the job using the item chooser. Select the *Configure* option to load the latest settings for the locks into the Programmer or Grand Master when it is used with the job number. Selecting the *Download* option will cause the Programmer or Grand Master to download audit trail data from the included locks.

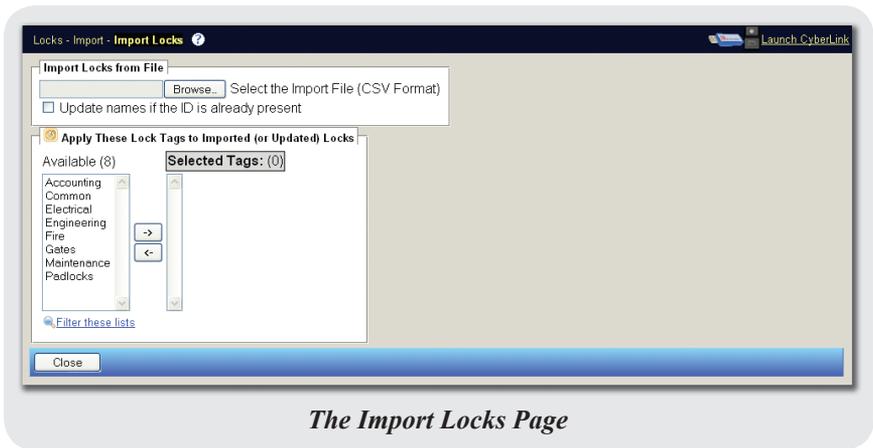
The **Actions** button menu on this page contains only the option to delete the current Programming Job.



The Job Properties Page Actions Button Menu

Importing Lock Data

Selecting the *Import* option from the *Locks* menu brings up the *Import Locks* page. This page allows lock data to be imported from a comma-separated values (CSV) file. Existing locks may also be updated with names using this method.



The Import Locks Page

A CSV file must have the following properties to import:

- One lock per line
- Commas separate the values
- Fields with embedded commas must be surrounded by double quotes
- Fields with embedded double quotes must have all the double quotes doubled then the entire field is surrounded with double quotes
- New-line and carriage return characters embedded in a field are not permitted

The fields accepted by the import are *Lock ID* and *Lock Name*, in that order. The ID field is required, but the name is optional. A lock ID starts with 'L' and is followed by 8 hexadecimal digits. Lower case letters in the ID will be promoted to upper case. If the lock name field is omitted, the ID will be used as the name. Names may be a maximum of 128 characters.

If there are any errors on the import due to invalid ID or name formats, the error will be reported on the *Import Locks* page and no rows from the import file will be inserted or updated.

Once the locks have been imported, they may need to be updated with a Grand Master or a CyberLock or USB Programmer.

CSV File Format For Importing Locks

Field	Required	Information
Lock ID	Yes	Starts with 'L', followed by 8 hexadecimal digits. Lower case letters in the ID will be promoted to upper case.
Lock Name	No	If left blank, the CyberLock or CyberPoint will be named with the ID. Names may be a maximum of 128 characters.

Lock Options

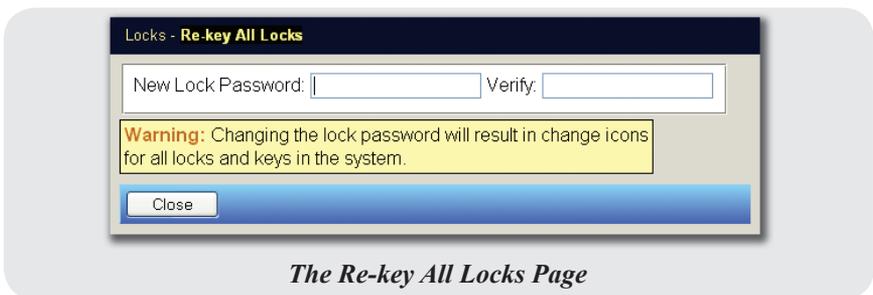
The *Lock Options* page, accessed by selecting *Options* from the *Locks* menu, contains options for multi-key/delay settings and changing the access codes for all locks in the system.



Multi-key mode and open delay are advanced settings for a CyberLock. A lock may require two, three, or four different keys, or a delay, before access is granted.

In order for CyberLocks to be configured with multi-key or delayed opening settings, the option must first be enabled from this page. There is also an option to require that the keys used to open a lock with a multi-key setting have different schedules. With this option enabled, each person needs to have access at the time the lock is contacted to meet the multi-key requirement.

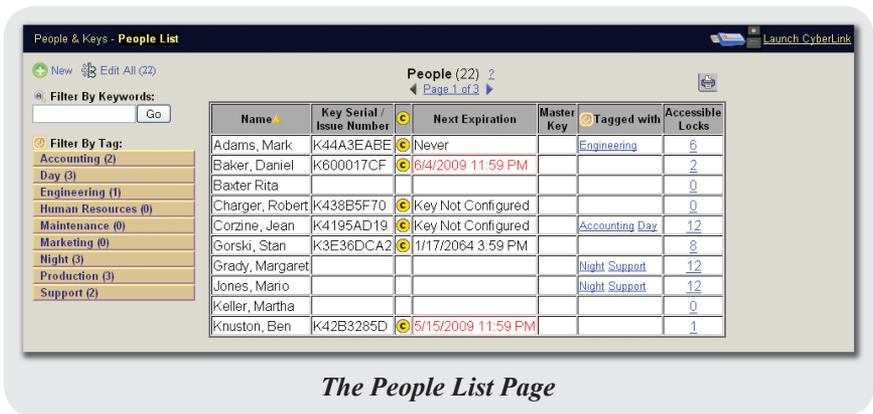
If the system was created using manual passwords, the *Re-key all locks* link is shown on this page. This link brings up the *Re-key All Locks* page, where a new access password may be set. After changing the password, all locks in the system must be updated.



People & Keys Menus and Functionality

In CyberAudit-Web, people are potential key holders or software administrators. They may be granted access to CyberLocks using the Access Matrix, issued a CyberKey that has a set of access permissions and behaviors, and assigned tags in order to group them with other people having similar access. Individual persons may be granted permission to log in to the software to administer the system.

The *People List* page, accessed by clicking on the *People & Keys* menu header, displays information about people who have been added to the system.



The People List Page

The *People* table displays the following in each row:

- The person’s name.
- The serial or issue number of the CyberKey which has been assigned to the person. (Key numbers begin with ‘K’.)
- The  icon, if the person’s key needs to be updated.
- The date the key is set to expire.
- The  icon, if the key is a master key.
- The tags with which the person has been associated. Clicking a tag link will bring up the tag’s *Properties* page.
- The total number of locks to which the person has been assigned access, displayed as a link. Clicking the number link will display a report showing those locks.

The table and page navigation controls are the same as those on the *Locks List* page, explained in the previous chapter section. The same set of filters are also available.

Clicking in a table cell which doesn’t contain a link displays a pop-up menu of available operations for that person.

People (22) [?](#)
 Page 1 of 1

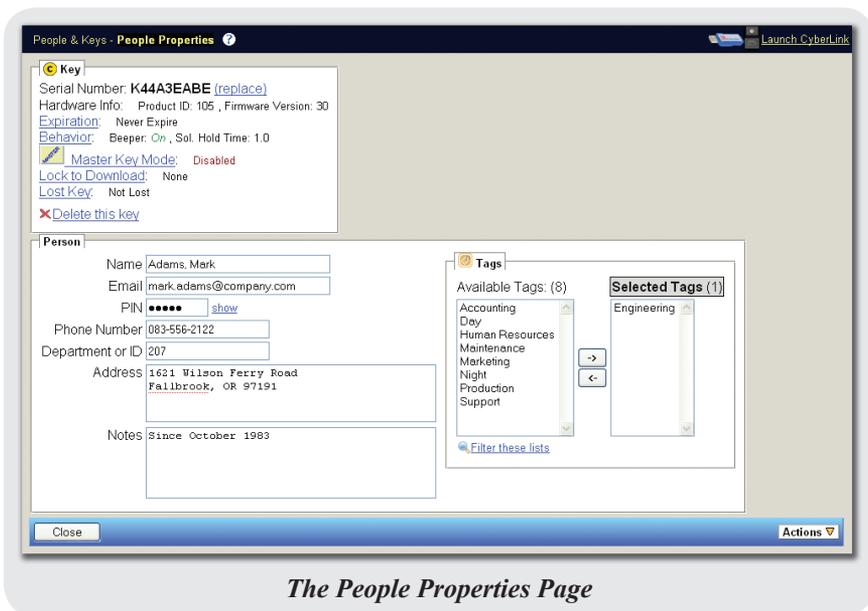
Name ▲	Key Serial / Issue Number		Next Expiration	Master Key	 Tagged with	Accessible Locks
Adams, Mark	K44A3EABE		Never		Engineering	5
Baker, Daniel	K600017CF		6/4/2009 11:59 PM			2
Baxter Rita						0
Charger, Robert	K438B5F70		Key Not Configured			0
Corzine, Jean	K4195AD19		Key Not Configured		Accounting Day	10
Knuston, Ben	K42B3285D		5/15/2009 11:59 PM			1
LaFleur, Nancy			Key Not Configured			5
Master key			1/18/2016 11:59 PM			28
Moore, Patrica						0
Muhammad, Abd			1/18/2016 11:59 PM		Accounting	3
Norris, Christoph					Day Production	10
Powell, Edwin	K3FA43148		8/1/2005 4:59 PM			10

The People Operations Pop-Up Menu

Choosing the *Properties* option displays the properties of the selected person. The *Show in Matrix* option creates a filter in the Access Matrix to display the locks and lock tags to which the person has access. The *Audit Report* option generates a report of audit trail data associated with the selected person. The *Comm Log* option generates a report of the key status logged by communicators when the person's CyberKey is downloaded. Selecting the *Delete* option removes the selected person from the system (after a confirmation).

People Properties

The *People Properties* page is accessed by selecting the *Properties* option from the operations pop-up menu for people. It includes information about the selected person, the tags with which they are associated, and their CyberKey.



The People Properties Page

One CyberKey may be issued to each person. Its settings are controlled in the *Key* frame.

The following settings may be specified in the *Key* frame:

- To replace the key if it is lost or broken, click the (*replace*) link. The new key will automatically be configured with the same settings as the original.
- Click the *Expiration* link to change the key's expiration.
- The key's beeper and solenoid hold time (the number of seconds the lock is held open by the key after access is granted) may be changed by clicking the *Behavior* link.
- To grant master access, click the *Master Key Mode* link.
- The key may be configured to download an audit trail from a lock when it makes contact. To select the lock, click the *Lock to Download* link.
- If the key is lost or stolen, click the *Lost Key* link to set disabling points.
- To remove the key from the system, click *Delete this key*.

Details for a person may be entered in the *Person* section:

- The person's name will be displayed in reports and email notifications exactly as it is entered in the *Name* field.
- If a PIN is required to update CyberKeys, set one for the selected person in the *PIN* field.
- The *Phone Number*, *Department or ID*, *Address*, and *Notes* fields are all for information purposes only.

The *Person* section also includes an item chooser for assigning tags to the selected person.

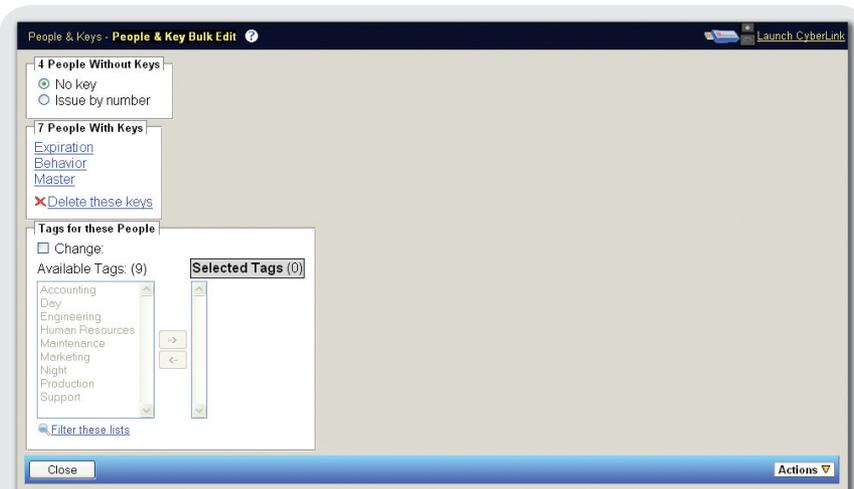
The **Actions** button menu on this page contains the same items as the operations pop-up menu for people, minus the *Properties* option.



The People Properties Page Actions Button Menu

Bulk Editing

The *People & Key Bulk Edit* page allows the same settings and tags to be applied to the selected group of persons and keys. First, use filters to select the desired persons from the *People List* page, then click the **Edit All (28)** button to access the *People & Key Bulk Edit* page.



The People & Key Bulk Edit Page

People in the selected group who do not yet have a CyberKey can be assigned an issue number. The issue number appears in the *People* table beside the person's name after changes on the *People & Key Bulk Edit* page have been saved.

The same rules for expiration, behavior, and master key settings can be applied at once to all of the persons who have a CyberKey. All of the assigned keys may also be deleted in one operation.

This page also includes an item chooser for assigning the same set of tags to the selected group of people.

The **Actions** button menu on this page contains only the option to delete the currently selected group of people (after confirmation).



The People & Key Bulk Edit Page Actions Button Menu

People Tags

People tags are used to group keyholders together for both management and function.

The *People Tags* page is accessed by selecting the *Tags* option from the *People & Keys* menu.



People & Keys - Tags - **People Tags**

[+ New](#) **People Tags (9)** [2](#) 

 Tag Name ▲	People with this Tag	Locks with Access
Accounting	1	1
Day	0	12
Engineering	1	6
Human Resources	0	7
Maintenance	0	14
Marketing	0	11
Night	2	12
Production	1	12
Support	1	12

The People Tags Page

The number of people and locks associated with a tag are displayed in the list as links. Clicking one of these links brings up either the *People List* page, filtered to display only the persons associated with the selected tag, or a report page showing the associated locks and the schedule by which they can be accessed by people associated with the tag.

Clicking in one of the cells of the *People Tags* table displays an operations pop-up menu similar to that from the *Lock Tags* table, with a *People Tagged* option in place of the *Locks Tagged* option. Selecting this option is equivalent to clicking the people link in the table.



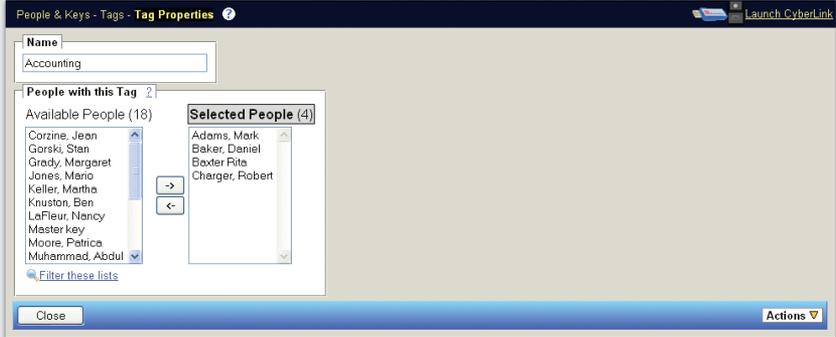
The screenshot shows a table titled "People Tags (9) ?" with three columns: "Tag Name", "People with this Tag", and "Locks with Access". A context menu is open over the "Accounting" tag, listing options: Properties, Show in Matrix, Audit Report, Comm Log, People Tagged, and Delete. The "Accounting" row in the table shows 12 people and 1 lock.

Tag Name	People with this Tag	Locks with Access
Accounting	12	1
Day	12	12
Engineering	6	6
Human Resou	7	7
Maintenance	14	14
Marketing	11	11
Night	12	12
Production	1	12
Support	1	12

The People Tags Operations Pop-Up Menu

People Tag Properties

The *People Tag Properties* page is accessed by selecting the *Properties* option from the operations pop-up menu in the *People Tags* table. It allows the tag name to be set or changed, and contains an item chooser which allows the tag to be associated with a specified set of people.



The screenshot shows the "People & Keys - Tags - Tag Properties" page. It features a "Name" field containing "Accounting". Below it, there are two lists: "Available People (18)" and "Selected People (4)". The "Available People" list includes names like Corzine, Jean; Gorski, Stan; Grady, Margaret; Jones, Mario; Keller, Martha; Knuston, Ben; LaFleur, Nancy; Masterkey; Moore, Patricia; and Muhammad, Abdul. The "Selected People" list includes Adams, Merk; Baker, Daniel; Baxter, Rita; and Charger, Robert. There are navigation arrows between the lists and a "Filter these lists" link. At the bottom, there is a "Close" button and an "Actions" dropdown menu.

The People Tag Properties Page

The **Actions** button menu on this page contains the same options as the People Tags operations menu, minus the *Properties* option.



The People Tag Properties Actions Button Menu

System Keys

System keys are a special class of CyberKey used to perform specific tasks within a CyberLock system. The *System Key List* page, accessed by selecting the *System Keys* option from the *People & Keys* menu, displays the special keys which have been added to the system.

Name	Serial or Issue #	C	Base GM	Type
Reset Key 1	K61EE27C8	C		Reset
Grand Master Programmer 1	K436BB80D	C		Grand Master

The System Keys List Page

The *System Keys* table displays the following in each row:

- The name given to the key.
- The serial or issue number of the key (key numbers begin with ‘K’).
- The **C** icon, if the key needs to be updated.
- The **⚓** icon, if the key is the Grand Master that was used as the source of access codes for the system.
- The key type. This can be either *Grand Master* or *Reset* (for systems whose access codes originate from manually entered passwords).

Clicking in one of the table cells displays the operations pop-up menu for system keys.



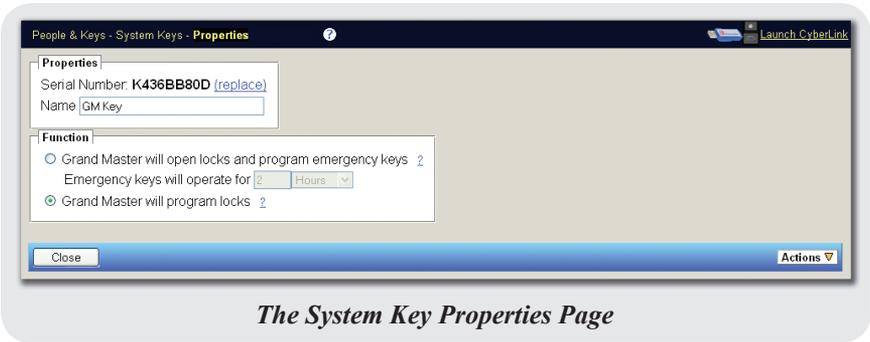
The System Keys List Operations Pop-Up Menu

The following operations are available in the pop-up menu:

- Choosing the *Properties* option displays the properties of the selected key.
- The *Audit Report* option generates a report of audit trail data associated with the key.
- The *Comm Log* option generates a report of the key status logged by communicators when the key is downloaded.
- Selecting the *Lost* option initiates the steps necessary to mark the key as lost in the system.
- Selecting the *Delete* option removes the selected key from the system (after a confirmation).

System Key Properties

The *System Key Properties* page, accessed by selecting the *Properties* option from the operations pop-up menu on the *System Keys* page, contains options for naming system keys and specifying their function.



Grand Masters can be set to open locks and program emergency keys that will open any lock for the specified time. They can also be set to program locks with one touch.

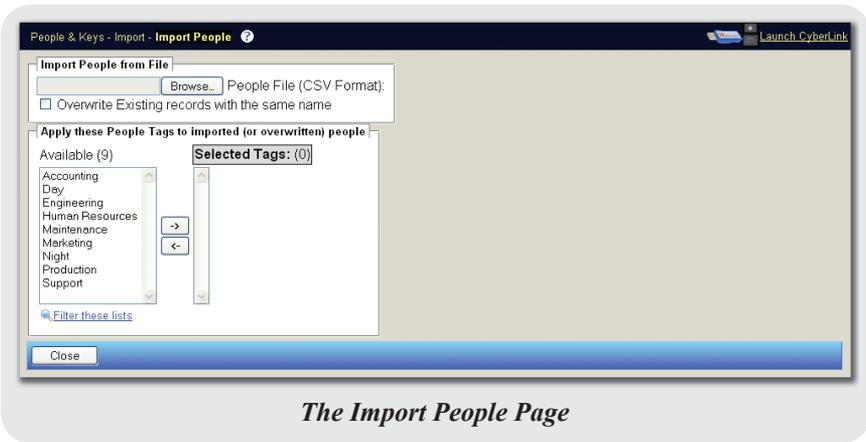
Reset keys restore locks to their factory settings. After a lock is reset, any CyberKey will open it.

The **Actions** button menu on this page contains the same options as the System Keys operations menu, minus the *Properties* option.



Importing People

The *Import People* page, accessed by selecting the *Import* option from the *People & Keys* menu, allows people records to be imported from a file to populate CyberAudit-Web, or to update existing records. The page also includes an item chooser which allows the imported people to be associated with the selected tags.



The import file must be in standard CSV (comma-separated values) format, as exported from most spreadsheet applications.

A CSV file must have the following properties to import:

- One person record per line
- Commas must separate the values
- Fields with embedded commas must be surrounded by double quotes
- Fields with embedded double quotes must have all the double quotes doubled then the entire field is surrounded with double quotes
- New-line and carriage return characters embedded in a field are not permitted

The field structure of an import file is as follows:

Column No.	Name	Max. Size	Details
1	Name	64	Required. Row is skipped if empty.
2	Department or ID	64	
3	External	255	Not used. May be left empty.
4	Email Address	255	
5	Address	255	
6	Phone Number	64	
7	PIN	8	Must be between 4-8 digits.
8	Notes	255	

Lost Keys

The *Lost Key List* page, accessed by selecting the *Lost Keys* option from the *People & Keys* menu, displays the keys which have been marked in the system as lost.



The screenshot shows a web browser window titled "People & Keys - Lost Keys - Lost Key List". The main content area is titled "Lost Keys (1) ?" and contains a table with the following data:

Key Serial	Next Expiration	KeyType	Master Key	Last Issued To	Disable Points
K420D04D5	Key Not Configured	Standard		Adams, Mark	0

The Lost Key List Page

The *Lost Keys* table displays the following in each row:

- The serial number of the lost key.
- The  icon, if the system has not received confirmation that the lost key has been disabled.
- The date the key is set to expire. A lost key is no longer a threat to security after it has expired.
- The key type. This can be *Standard*, *Grand Master*, or *Reset*.
- The  icon, if the key is a master key.
- The name of the person to whom the key was last issued.
- The number of locks which have been configured as disable points for the lost key.

Clicking in a table cell displays the operations pop-up menu for lost keys. Choosing the *Properties* option displays the properties of the selected key. The *Audit Report* option generates a report of audit trail data associated with the key. The *Comm Log* option generates a report of the key status logged by communicators when the key is downloaded. Selecting the *Delete* option removes the selected key from the system.

Lost Keys (1) ?					
Key Serial	Next Expiration	KeyType	Master Key	Last Issued To	Disable Points
K420D04D5	Properties	Standard		Adams, Mark	1
<div style="display: flex; justify-content: space-between;"> Audit Report Comm Log </div> <div style="display: flex; justify-content: space-between;"> Delete </div>					

The Lost Keys Operations Pop-Up Menu

Lost Key Properties

The *Lost Key* page, accessed by selecting the *Properties* option from the operations pop-up menu on the *Lost Key List* page, displays settings and disable points for the selected key.

The Lost Key Page

The lost or found status of the selected key can be toggled from this page. This page also includes an item chooser which is used to select locks to be disable points for the key, and the option to automatically create a programming job which includes the selected locks. Any locks which are selected to be disable points must be updated. If the lost key contacts one of these locks, it will be denied access and all of its access permissions will be removed.

If a lost key is found, it may be marked as “not lost” in its *Properties* page. The locks which have been configured as disable points must then be updated again, or they will continue to disable the key when it contacts them.

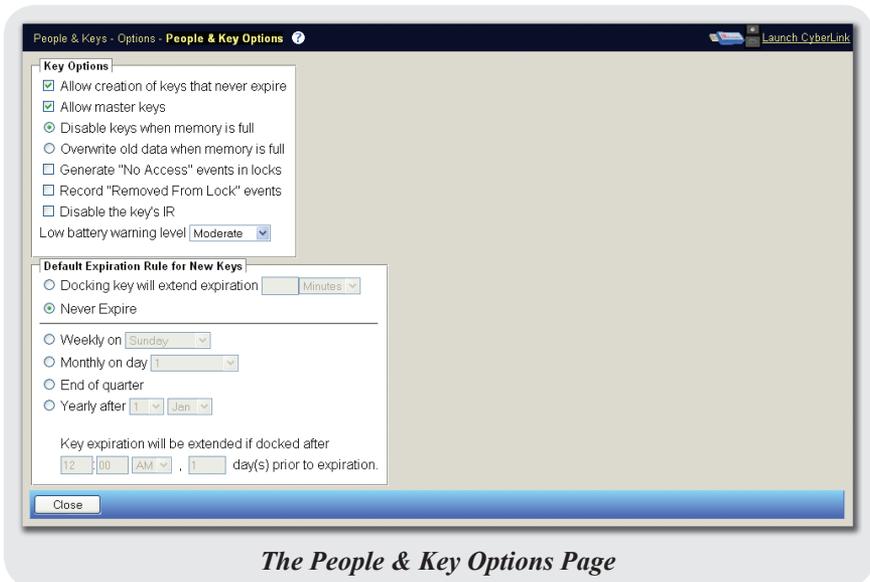
The **Actions** button menu on this page contains the same options as the Lost Keys operations menu, minus the *Properties* option.



The Lost Key Page Actions Button Menu

People & Key Options

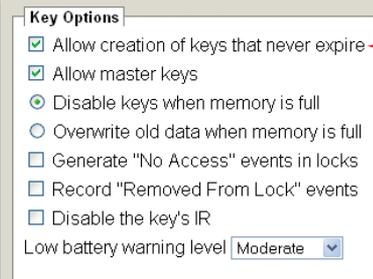
The *People & Key Options* page, accessed by selecting *Options* from the *People & Keys* menu, defines rules and defaults for behavior of CyberKeys added to the system.



The People & Key Options Page

People & Key Options - Expiration

Expiration is an important means to achieve key control. Regular expiration and renewal reduces the exposure and subsequent risk of a lost or stolen key, because an expired key will not open locks. However, there are some cases where expiration may not be desirable, so this page includes the option to allow creation of keys that never expire.

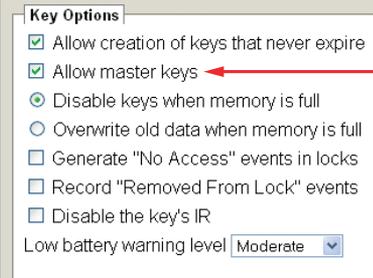


Select this option to allow the use of non-expiring keys.

Allowing Non-Expiring Key Creation

People & Key Options - Master Keys

To enable keys to be configured with access to all locks in the system, select the *Allow master keys* option.

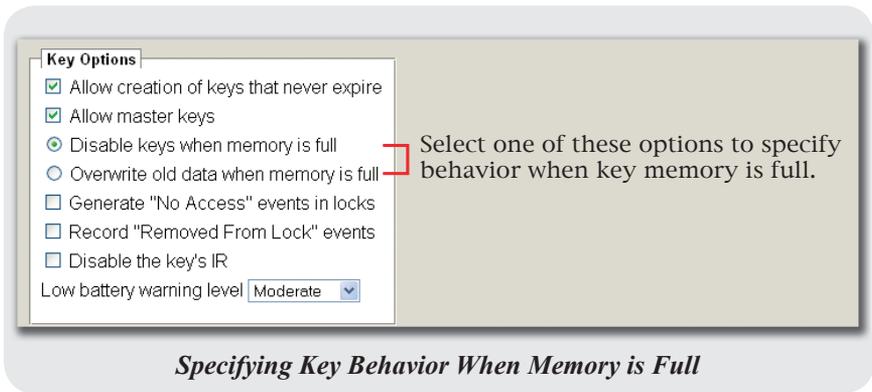


Select this option to allow the use of master keys.

Allowing Master Key Creation

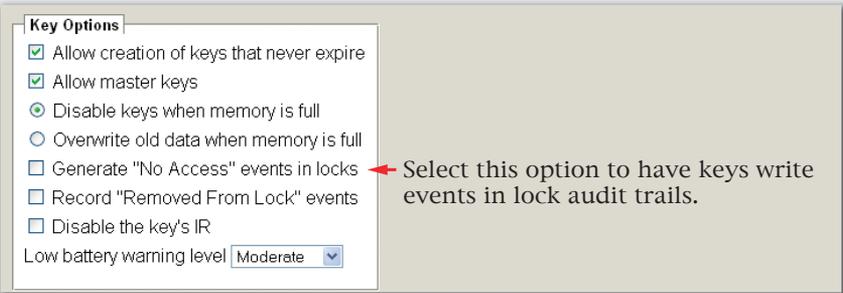
People & Key Options - Memory Full Behavior

The importance of audit trail data versus key operation must be weighed by administrators. If the audit trail data is deemed more valuable than the operation of a key, select the option to disable keys when their memory is full. If it is more important that key operation is not interrupted, select the option to overwrite old data when the key memory is full.



People & Key Options - “No Access” Behavior

CyberKeys always record “No Access” type events in their audit trail. By default, CyberLocks do not record most events where the key is not permitted access. To make keys write an event to the audit trail of a lock when they are denied access, select the *Generate “No Access” events in locks* option.



The screenshot shows a 'Key Options' dialog box with the following settings:

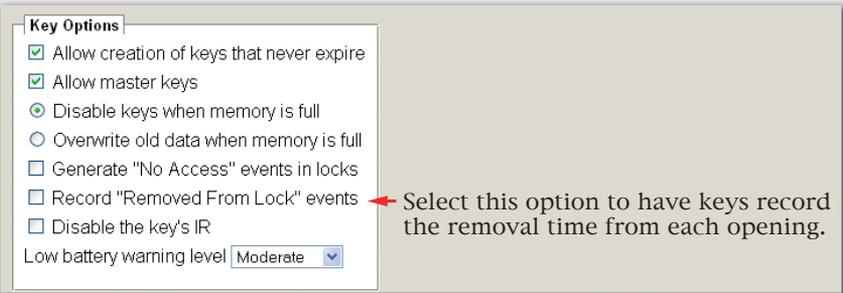
- Allow creation of keys that never expire
- Allow master keys
- Disable keys when memory is full
- Overwrite old data when memory is full
- Generate "No Access" events in locks
- Record "Removed From Lock" events
- Disable the key's IR
- Low battery warning level: Moderate

A red arrow points to the 'Generate "No Access" events in locks' option, with the text: "Select this option to have keys write events in lock audit trails."

Making Keys Generate "No Access" Events in Lock Audit Trails

People & Key Options - "Removed . . ." Behavior

Normally, CyberKeys only record a "Removed From Lock" event if they are left in contact with the lock for more than one minute. If the option *Record "Removed From Lock" events* is selected, CyberKeys will record the time at which they were removed from a lock, regardless of how long they are left in contact.



The screenshot shows a 'Key Options' dialog box with the following settings:

- Allow creation of keys that never expire
- Allow master keys
- Disable keys when memory is full
- Overwrite old data when memory is full
- Generate "No Access" events in locks
- Record "Removed From Lock" events
- Disable the key's IR
- Low battery warning level: Moderate

A red arrow points to the 'Record "Removed From Lock" events' option, with the text: "Select this option to have keys record the removal time from each opening."

Making Keys Record "Removed From Lock" Events

People & Key Options - CyberKey IrDA Control

CyberKeys use an infrared transceiver to communicate with some communicators using the IrDA protocol. Other IrDA devices, including some laptop computers and PCs, may cause a CyberKey to “chatter” when it is in proximity. There is no security risk associated with this behavior, but if no infrared communicators will be used with the system, selecting the *Disable the key's IR* option will stop CyberKeys from responding to other devices.

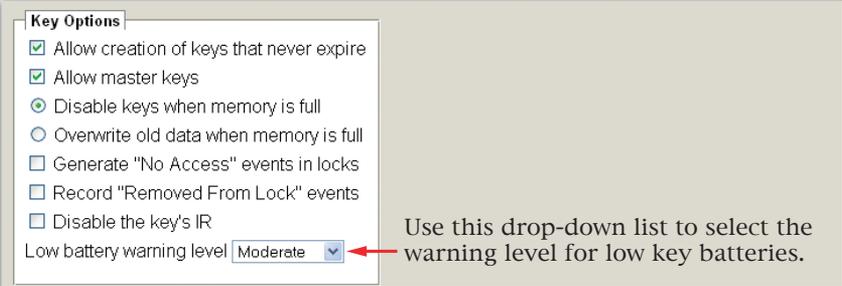


People & Key Options - Low Battery Warning Level

For systems that have standard CyberKeys manufactured before January 2009, a *Low battery warning level* drop-down list is available to set the level at which CyberKeys, communicators, and CyberAudit-Web warn that a key's CR2 lithium battery is nearing end of life. CyberKeys measure their battery each time they open a lock and during communications. If their battery voltage is below the low battery warning level for *five or more consecutive readings*, these keys will emit a low battery warning beep once every 8 seconds for a minute.

Guidelines for setting the low battery warning level:

- **Low** - use this setting if CyberKeys will perform 75 or more lock openings per day.
- **Moderate** - use this setting if CyberKeys will perform 25-75 openings per day. (This is the default setting.)
- **Aggressive** - use this setting if CyberKeys will perform less than 25 openings per day or if there is a strong requirement for key holders to get the low battery warning prior to the battery's end of life.



Selecting the Low Battery Warning Level

People & Key Options - Default Expiration Rule

As explained in the “*People & Key Options - Expiration*” subsection, it is recommended for reasons of security and data integrity that CyberKeys be set to expire on a regular basis. The *Default Expiration Rule for New Keys* frame contains several choices which will be applied to all keys when they are added to the system.

One option is to have the expiration move further ahead each time the key is updated. This is called *rolling expiration*. Since there is no set day or date, the key's next expiration is calculated when the key is updated via a communicator device. Each time the key is

updated, the time until expiration is reset to the interval specified in the input fields.

Default Expiration Rule for New Keys

Docking key will extend expiration Minutes ← Select this option and specify a duration for “rolling” key expiration.

Never Expire

Weekly on

Monthly on day

End of quarter

Yearly after

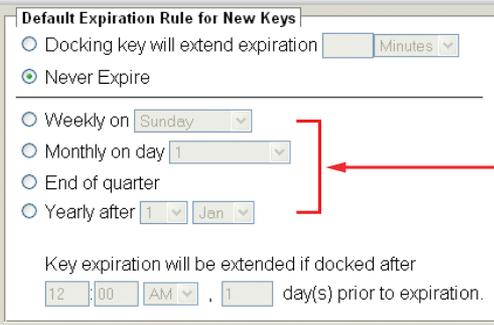
Key expiration will be extended if docked after , day(s) prior to expiration.

Specifying a Rolling Expiration for CyberKeys

A rolling expiration by days, weeks, or months extends the key’s expiration to midnight of the last day. For example, a key having a one day rolling expiration will be set to expire at the end of the following day each time it is updated. Expiration rules of “minutes” or “hours” will set the key to stop working at a specific hour and minute of the day.

Note that a rolling expiration of minutes or hours takes priority over the time frames assigned to master keys. For example, if a master key has a 24 hour rolling expiration and the key is updated at 10:00 am on Wednesday, it will continue to operate until 10:00 am on Thursday, even if the time frames for the master key indicate that it cannot operate on a Thursday.

To set keys to expire on a periodic schedule, select one of the options for fixed expiration.



Default Expiration Rule for New Keys

Docking key will extend expiration Minutes

Never Expire

Weekly on Sunday

Monthly on day 1

End of quarter

Yearly after 1 Jan

Key expiration will be extended if docked after
 12 : 00 AM , 1 day(s) prior to expiration.

Select one of these options for fixed key expiration.

Specifying a Fixed Expiration for CyberKeys

Options for fixed expiration include:

- *Weekly on* - Sunday, Monday, Tuesday, etc.
- *Monthly on day* - The numbered day of the month. Includes an option for the final day of each month, since the number of days in each month varies.
- *End of quarter* - The final day of every third month (March, June, September, and December).
- *Yearly after* - A specific month and day.

The final option in the *Default Expiration Rule for New Keys* frame specifies a window of time before expiration. If the key is presented to a communicator during this time period, its expiration will be moved to the next date. For example, assume that a key is set to expire weekly on Fridays, and the extension period is set to 12:00 PM, 1 day prior to expiration. The key's expiration date will be moved to the following Friday if the key is presented to a communicator any time after 12:00 PM on Friday. Since a key expires as soon as the date advances (midnight on Saturday, in this example), Fridays equate to one day prior to expiration.

Default Expiration Rule for New Keys

Docking key will extend expiration Minutes

Never Expire

Weekly on

Monthly on day

End of quarter

Yearly after

Key expiration will be extended if docked after : , day(s) prior to expiration.

Specify the expiration renewal window with this option.

Specifying the Expiration Renewal Window

Schedules Menus and Functionality

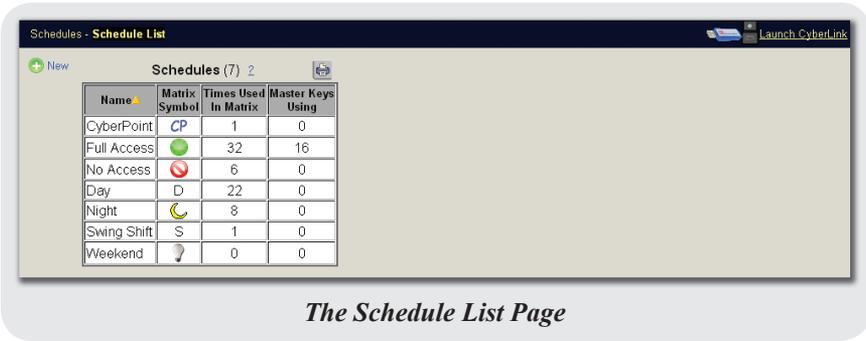
Schedules dictate the times at which locks may be opened. CyberAudit-Web Professional supports a maximum of 49 schedules. Three schedules are always present in CyberAudit-Web Professional: *CyberPoint*, *Full Access*, and *No Access*.

CyberPoint schedules do not allow access to locks. Instead, they cause keys to beep 3 times and record the time at which the lock was contacted. Security guard rounds are a great application of this schedule type. CyberPoint schedules are valid at all times, including holidays.

The Full Access schedule allows locks to be accessed at all times, including holidays.

The No Access schedule is assigned to restrict master key access. When this schedule is used in the Access Matrix for a person or tag with a master key, it will prevent the master key from accessing those locks.

The *Schedule List* page, accessed by clicking on the *Schedules* menu header, displays a table of information about the schedules which have been added to the system.



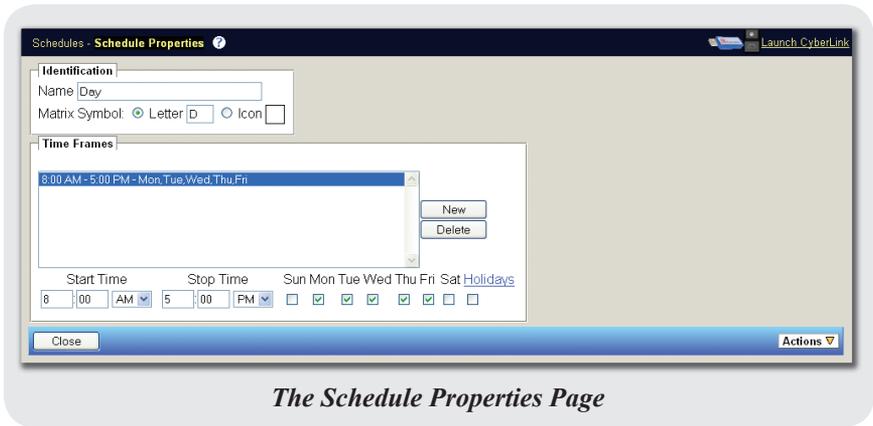
The *Schedules* table displays the following in each row:

- The name of the schedule
- The letter or icon used to represent the schedule in the Access Matrix
- The number of squares in the Access Matrix to which the schedule has been applied
- The number of master keys which are restricted by the schedule

Clicking in a table cell displays the operations pop-up menu for schedules. Choosing the *Properties* option displays the properties of the selected schedule. Selecting the *Delete* option removes the selected schedule from the system.

Schedule Properties

The *Schedule Properties* page, accessed by selecting the *Properties* option from the operations pop-up menu in the *Schedules* table, displays settings for the selected schedule.



Schedules should be given a descriptive name in the *Identification* frame. They can be represented in the Access Matrix by either a letter or an icon. Additional icons may be added to the system via the link that appears when the *Icon* option is selected in the *Matrix Symbol* field. CyberAudit-Web accepts .png, .gif, and .jpg images, and will automatically resize them to 23 x 23 pixels. The *Time Frames* added to schedules specify the times at which locks may be opened.

The **Actions** button menu on this page contains only the option to delete the currently selected schedule (after confirmation).



Holidays

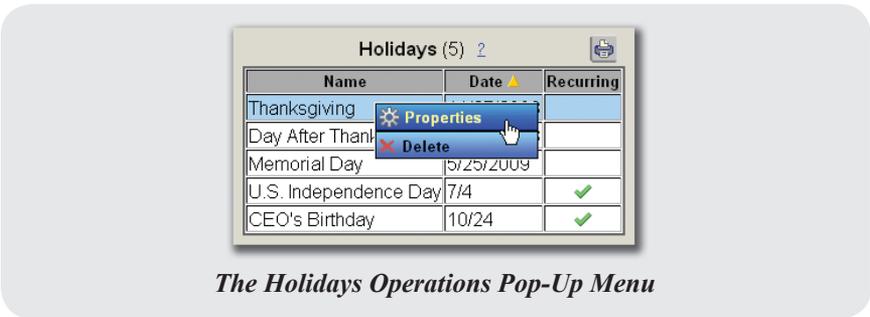
Holidays are utilized as schedule exceptions in CyberAudit-Web Professional. They do not have to be literal holidays – any day of the year can be designated as a holiday. The rules specified for holidays in a schedule time frame take priority over normal access. For example, if access is allowed on Wednesdays, but not on

holidays, then the key will not be granted access on Wednesdays that are also holidays.

The *Holiday List* page, accessed by selecting the *Holidays* option from the *Schedules* menu, lists the holidays which have been added to the system. The *Holidays* table lists the name and date of each holiday, and displays a green ✓ if the holiday is recurring.



Clicking in a table cell displays the operations pop-up menu for holidays. Choosing the *Properties* option displays the properties of the selected holiday. Selecting the *Delete* option removes the selected holiday from the system.



Holiday Properties

The *Holiday Properties* page, accessed by selecting the *Properties* option from the operations pop-up menu in the *Holidays* table, displays settings for the selected holiday.



Holidays must be configured with a name and a date, and whether the holiday occurs on the same date every year must be specified.

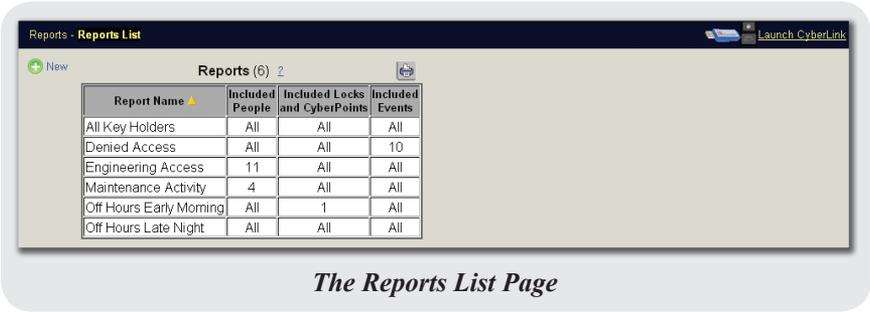
The **Actions** button menu on this page contains only the option to delete the currently selected holiday.



Reports Menus and Functionality

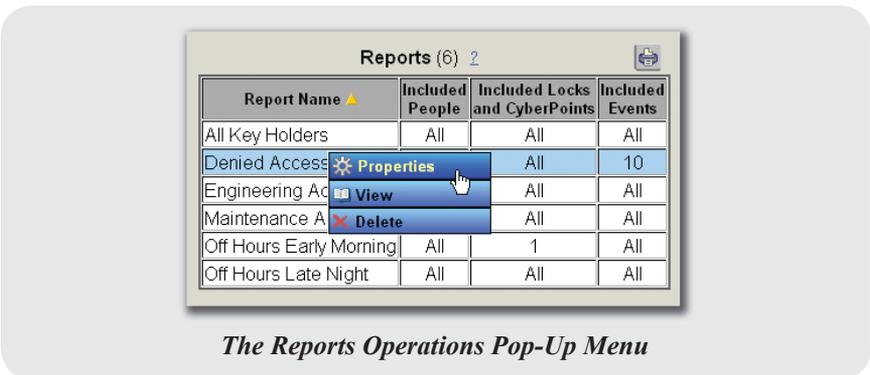
Reports are an excellent way to organize audit trail data. The items included in the report can be specified by the administrator, as well as the order in which the columns appear (left to right) and the order in which the rows are sorted (top to bottom).

The *Reports List* page, accessed by clicking the *Reports* menu header, displays the list of reports which have been created in the system.

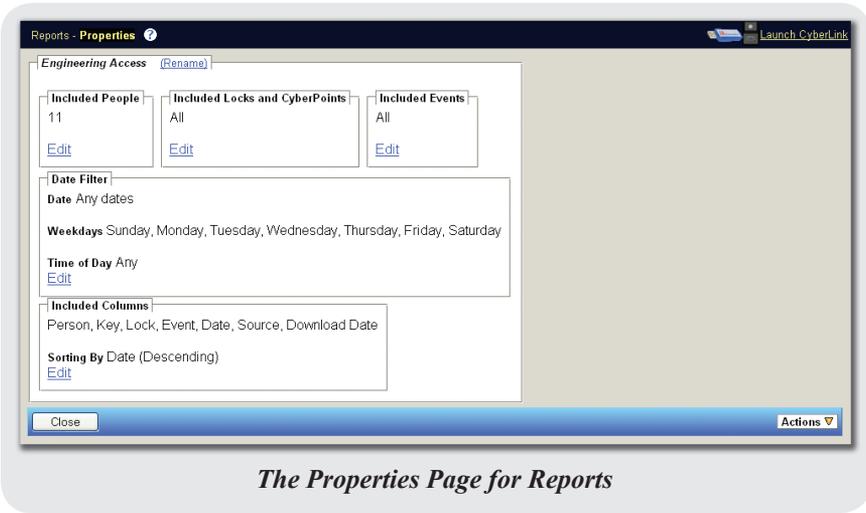


The *Reports* table lists the name of each report, the number of included people, the number of included locks and CyberPoints, and the number of included events.

Clicking in one of the table cells displays the operations pop-up menu for reports. Selecting the *Properties* option will display the properties page. Selecting the *View* option will execute the report, displaying the results in a new browser window. Selecting *Delete* will remove the selected report from the system.



The *Properties* page for reports, accessed by selecting the *Properties* option from the pop-up menu in the *Reports* table, allows reports to be tailored to a specific purpose. The report name, included people, locks and CyberPoints, events, dates, and columns may all be customized.



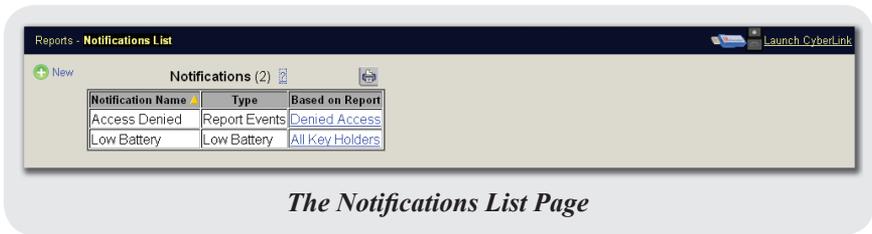
The **Actions** button menu on this page contains the same options as the Reports List page operations pop-up menu, with the exception of the *Properties* option.



Notifications

Notifications are reports sent by email. After a CyberKey is downloaded, the system scans the new data to determine if it matches the criteria of a notification. An available email server must be specified in the setup for notifications.

The *Notifications List* page, accessed by selecting the *Notifications* option from the *Reports* menu, displays the list of notifications which have been added to the system.



The *Notifications* table displays the following in each row:

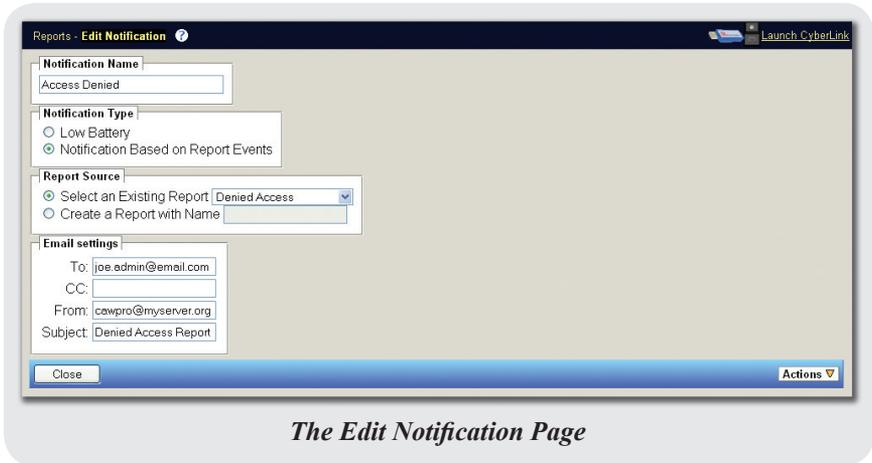
- The name of the notification
- The type – either *Report Events* or *Low Battery*
- The name of the report on which the notification is based

Clicking in a table cell that does not contain a link displays the operations pop-up menu for notifications. Selecting *Properties* displays the properties page for the current notification. Selecting the *Delete* option removes the notification from the system.



Notifications Properties

The *Edit Notification* page, accessed by selecting the *Properties* option from the operations pop-up menu in the *Notifications* table, displays the properties of the selected notification.



If the *Low Battery* type is selected, an email will be sent to the specified recipient when the system detects a low battery voltage (checked when a CyberKey is downloaded) for any of the people included in the report on which the notification is based.

If the *Notification Based on Report Events* type is selected, an email will be sent to the specified recipient whenever one of the events included in the base report is detected in an audit trail downloaded from a CyberKey.

If none of the existing reports in the system will serve as a basis for the notification, the creation of a new report can be triggered by selecting the *Create a Report with Name* option.

In the *Email Settings* frame, the *To:* and *From:* fields are required to have values.

The **Actions** button menu on this page contains only the option to delete the currently selected notification.

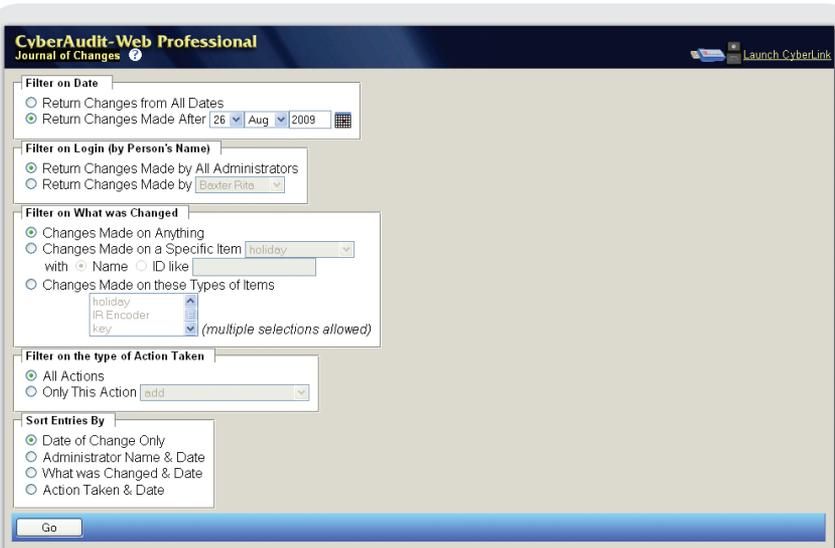


The Edit Notification Page Actions Button Menu

Journal of Changes

The Journal of Changes is a record of all changes that have been made in the CyberAudit-Web system, either by administrators or by the system background processes.

Selecting the *Journal* option from the *Reports* menu will display the *Journal of Changes* page inside a new browser window.



The Journal of Changes Page

Because the number of entries can grow quite large, there are several filters to aid in displaying only the entries of interest. For detailed information about each of the filters, click the context help link (?). After setting filters and clicking the *Go* button, the Journal of Changes will be displayed as a report.

Email Setup

In order to send email notifications, CyberAudit-Web Professional relays messages through an email server. The server details must be entered on the *Email Notifications* page, accessed by selecting the *Email Setup* option from the *Reports* menu.



Consult the administrator of the email server and enter the necessary server details. Note: By default, the email server must support SMTP on port 25 without secure sockets (TLS).

Communicators Menus and Functionality

Communicators are the devices used to transfer configurations and audit trail data between CyberAudit-Web Professional and CyberKeys, Programmers, and Grand Masters.

Web Authorizers

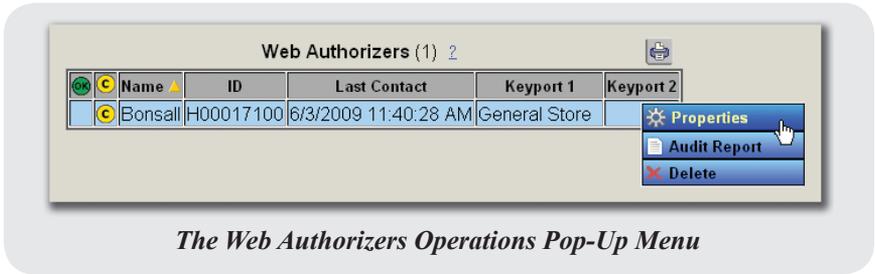
Clicking on the *Communicators* menu header or selecting the *Web Authorizers* option displays the *Web Authorizers List* page, which displays information about the Web Authorizers which have been added to the system.



The *Web Authorizers* table displays the following:

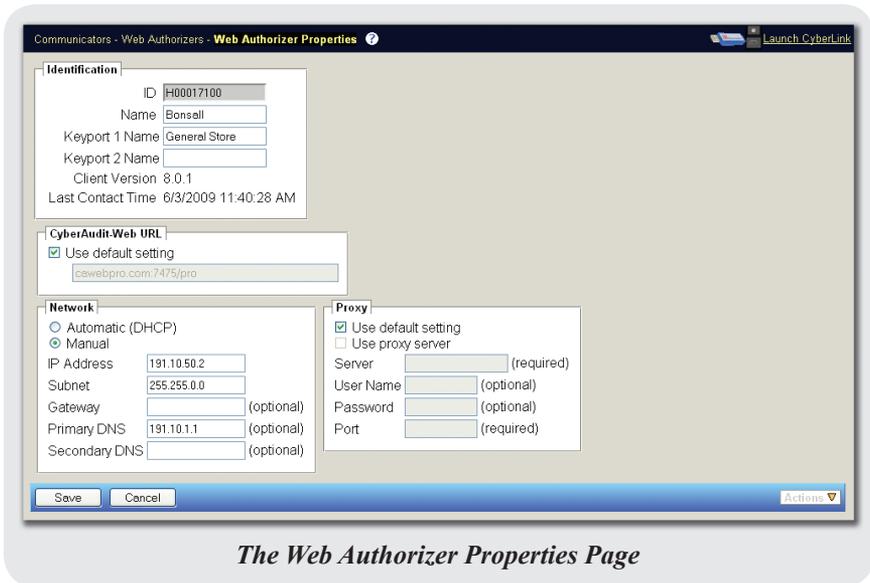
- The  icon, if an Authorizer has communicated with the server within the last minute
- The  icon, if the settings for the Authorizer have changed in CyberAudit-Web but the device still needs to be updated
- The name of the Authorizer
- The serial number of the Authorizer
- The last time the Authorizer contacted the server
- The names of the Keypoint(s) attached to the Authorizer

Clicking in a table cell displays the operations pop-up menu for Web Authorizers. Choosing the *Properties* option displays the properties of the selected Authorizer. The *Audit Report* option generates a report of activities logged by the Authorizer. Selecting the *Delete* option removes the selected Authorizer from the system.



Web Authorizer Properties

The *Web Authorizer Properties* page, accessed by selecting the *Properties* option from the operations pop-up menu in the *Web Authorizers* table, displays the properties and settings for the selected Authorizer.



The Web Authorizer Properties Page

The *Identification* frame displays the serial number of the Authorizer, the firmware version it is currently using, and the last time it contacted the server. The frame also includes entry fields which can be used to assign names to the Authorizer and its attached Keyports.

The default value in the *CyberAudit-Web URL* frame comes from the *Communicator Options* page, but may be changed by removing the checkbox.

Authorizers request a dynamic IP address by default, but a manual address may be assigned in the *Network* frame. Check with a network administrator for the proper values to enter into both the *Network* and *Proxy* frames.

If any of the following conditions are true, a Web Authorizer must be configured via USB:

- The Authorizer must use a static IP address
- CyberAudit-Web can only be reached by name or cannot be reached on the default `https://` port 443
- A proxy server is required to reach CyberAudit-Web

The **Actions** button menu on this page contains the same options as the *Web Authorizers List* page operations pop-up menu, with the exception of the *Properties* option.



The Web Authorizer Properties Page Actions Button Menu

Stations

The *Stations List* page, accessed by selecting the *Stations* option from the *Communicators* menu, displays information about the USB and Web Stations which have been added to the system.

A screenshot of a web browser window displaying the 'Stations List' page. The page title is 'Communicators - Stations - Stations List'. The main content is a table with the following data:

	Name	ID	Last Contact	Type	Key Name	Battery Level
👤	Jones	72817855	None	USB Station		
👤	Lunch Room	W00020F76	5/8/2009 4:59:24 PM	Web Station		
	Stanton	v48034389	None	USB Station		

The Stations List Page

The *Stations* table displays the following in each row:

- The  icon, if the Station has communicated with the server within the last minute
- The  icon, if the settings for the Station have changed in CyberAudit-Web but the device still needs to be updated
- The name of the Station
- The serial number of the Station
- The last time the Station contacted the server
- The Station type – either *USB* or *Web*
- The name of the key currently inserted into the Station, if applicable
- The battery voltage of the currently inserted key, if applicable

Clicking in one of the table cells displays the operations pop-up menu for Stations. Selecting the *Properties* option displays the properties page for Stations. The *Audit Report* option generates a report of audit trail data associated with the Station. Selecting the *Delete* option removes the selected Station from the system.



Stations (3) 2							
		Name ▲	ID	Last Contact	Type	Key Name	Battery Level
		Jones	72817855	None	USB Station		
		Lunch Room	W00020F76	5/8/2009 4:59:24 PM	Web Station		
		Stanton	v48034389	None	USB Station		

 Properties

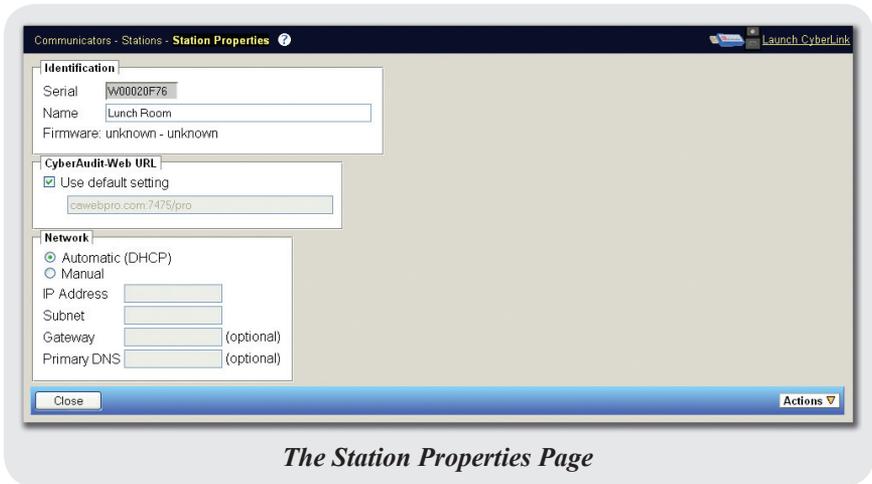
 Audit Report

 Delete

The Stations Operations Pop-Up Menu

Station Properties

Selecting the *Properties* option from the operations pop-up menu on the *Stations List* page displays the *Station Properties* page. This page displays information about the selected Station.



The *Station Properties* page for USB Stations contains only the *Identification* frame, which displays the serial number, name, and firmware version of the Station. The page for Web Stations also contains the *CyberAudit-Web URL* and *Network* frames.

The default value in the *CyberAudit-Web URL* frame comes from the *Communicator Options* page, but may be changed by removing the checkbox.

Web Stations request a dynamic IP address by default, but a manual address may be assigned in the *Network* frame. Check with a network administrator for the proper values to enter into the *Network* frame.

The **Actions** button menu on this page contains the same options as the *Stations List* page operations pop-up menu, with the exception of the *Properties* option.



The Station Properties Page Actions Button Menu

LAN Authorizers

The *LAN Authorizers List* page, accessed by selecting the *LAN Authorizers* option from the *Communicators* menu, displays information about the LAN Authorizers which have been added to the system.

 A screenshot of a web browser window showing the 'LAN Authorizers List' page. The browser title is 'Communicators - LAN Authorizers - LAN Authorizers List'. The page has a 'New' button and a 'Launch CyberAudit-Web' button. Below is a table with the following data:

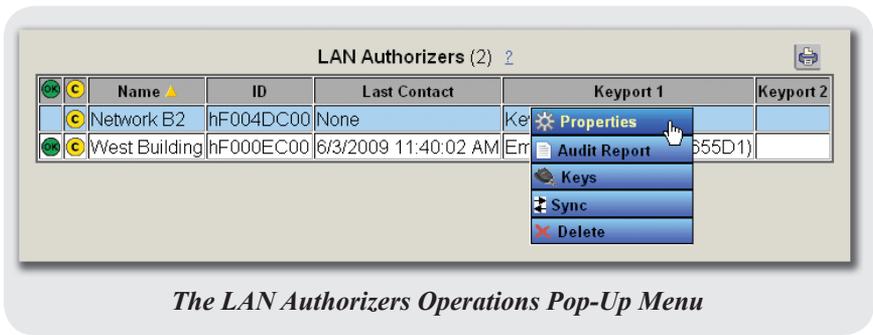
	Name	ID	Last Contact	Keypoint 1	Keypoint 2
OK	Network B2	hF004DC00	None	Keypoint B2	
C	West Building	hF000EC00	6/3/2009 11:40:02 AM	Employee Lobby (t3F4655D1)	

The LAN Authorizers List Page

The *LAN Authorizers* table displays the following:

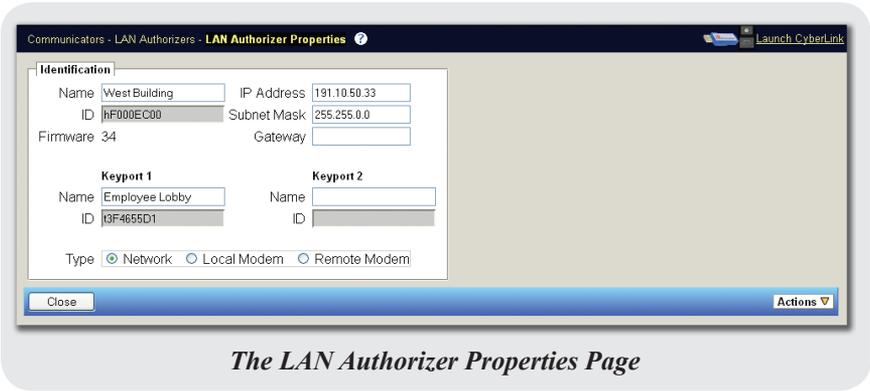
- The **OK** icon, if an Authorizer has communicated with the server within the last minute
- The **C** icon, if the settings for the Authorizer have changed in CyberAudit-Web but the device still needs to be updated
- The name of the Authorizer
- The serial number of the Authorizer
- The last time the Authorizer contacted the server
- The names of the Keypoint(s) attached to the Authorizer

Clicking in one of the table cells displays the operations pop-up menu for LAN Authorizers. Selecting the *Properties* option will display the properties page for the selected Authorizer. The *Audit Report* option generates a report of audit trail data associated with the Authorizer. If LAN Authorizers store key records (based on the setting from the *Communicator Options* page,) selecting the *Keys* option will display the list of keys that have configurations stored in the selected Authorizer. The *Sync* option causes the Authorizer to attempt contact with the server. Selecting the *Delete* option removes the selected Authorizer from the system.



LAN Authorizer Properties

Selecting the *Properties* option from the *LAN Authorizers* operations pop-up menu displays the *LAN Authorizer Properties* page, which contains settings and information about the selected Authorizer.



The LAN Authorizer Properties Page

The Authorizer and its Keypoints should be given descriptive names. Their ID and firmware numbers are also displayed, but not editable.

If the Authorizer type is set to *Network*, the IP, subnet, and gateway address fields will be enabled for editing. Consult a network administrator for the proper values to enter.

If the Authorizer type is set to *Local Modem*, the *Local Modem* properties frame is displayed. A local modem Authorizer communicates with the server by a network connection. Its modem serves as a communication link between CyberAudit-Web and remote modem Authorizers. Local modem Authorizers may be toggled to either dial any remote modem Authorizer in the database or only those on a given list.



The Local Modem Properties Frame

A remote modem Authorizer communicates with the server by phone line, via one or two local modem Authorizers. Remote modem Authorizers must have at least one local Authorizer to dial. A second one may be selected if desired.

The **Actions** button menu on this page contains the same options as the *LAN Authorizers List* page operations pop-up menu, with the exception of the *Properties* option.



The LAN Authorizer Properties Page Actions Button Menu

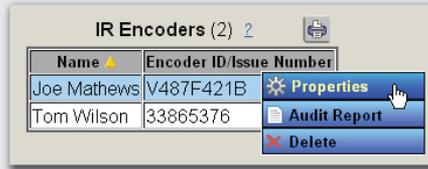
IR Encoders

The *IR Encoder List* page, accessed by selecting the *IR Encoders* option from the *Communicators* menu, lists the IR Encoder devices which have been added to the system.



The IR Encoder List Page

The *IR Encoders* table lists the name and ID or issue number of each IR Encoder in the system. Clicking in one of the table cells displays the operations pop-up menu for IR Encoders. Selecting the *Properties* option displays the properties page for IR Encoders. The *Audit Report* option generates a report of audit trail data associated with the selected IR Encoder. Selecting the *Delete* option removes the IR Encoder from the system.

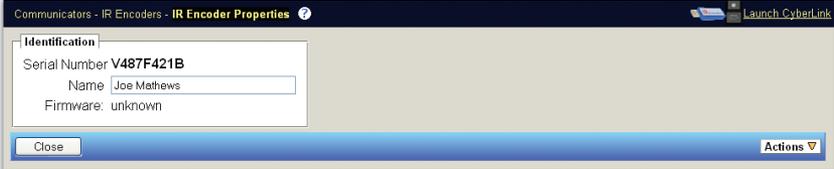


The IR Encoders Operations Pop-Up Menu

IR Encoder Properties

The *IR Encoder Properties* page, accessed by selecting the *Properties* option from the *IR Encoders* operations pop-up menu, displays information about the selected IR Encoder.

The only editable property of IR Encoders is the name. The entered value will appear in CyberKey communications logs if the IR Encoder is used to download a key.



The IR Encoder Properties Page

The **Actions** button menu on this page contains the same options as the *IR Encoder List* page operations pop-up menu, with the exception of the *Properties* option.



The IR Encoder Properties Page Actions Button Menu

Communicators Options

The *Communicators Options* page, accessed by selecting *Options* from the *Communicators* menu, is used for setting default networking values and behavior of certain communicator devices.



The Communicators Options Page

The *CyberAudit-Web Default URL* frame contains the IP address or DNS name of the computer running the CyberAudit-Web Professional software.

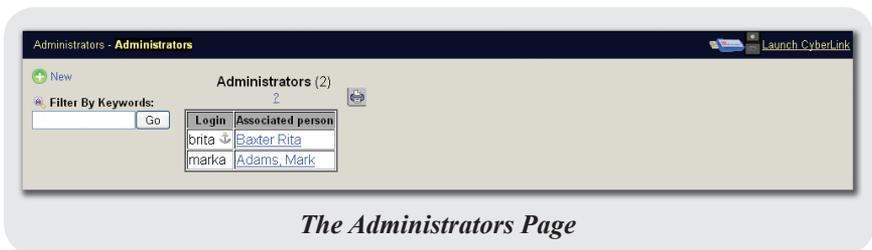
Many larger networks route web browsing through a proxy server to reach the Internet. Because the Web Authorizer is fundamentally a web client, its web traffic must also be routed through the proxy. Consult a network administrator to determine the proper settings to enter into the *Web Authorizers Default Proxy* frame.

Both Web Authorizers and LAN Authorizers are able to store CyberKey records locally. This allows the Authorizer to program the CyberKey with the stored access and expiration rules without first contacting CyberAudit-Web. If the server is not available, CyberKeys may still be updated.

If a key record is not stored locally, the Authorizer will contact CyberAudit-Web for instructions when a CyberKey is inserted into an attached Keyport. With network connections, Authorizers can normally contact the server quickly and program the key in a few seconds. Remote modem Authorizers, however, must dial and communicate with the server via modem, which will take noticeably longer. In this case, it is better to pre-load the key records into the Authorizer so that keys update quickly. This is done by selecting *Keys* from the Authorizer list operations menu and using the Item Chooser to associate keys with an Authorizer.

Administrators Menu and Functionality

The *Administrators* page, accessed by clicking on the header for the *Administrators* menu, lists the administrators which have been added to the system. Having multiple administrators is useful when the task of managing CyberLocks and CyberKeys needs to be delegated.



The *Administrators* table lists login names and their associated person. It is possible for a single person to have multiple logins, each with different permissions for performing various actions within the system. The first row of the table will always display the primary, or *root* administrator login. This login may never be deleted and no other administrator accounts may change its password. The login is marked with the  icon.

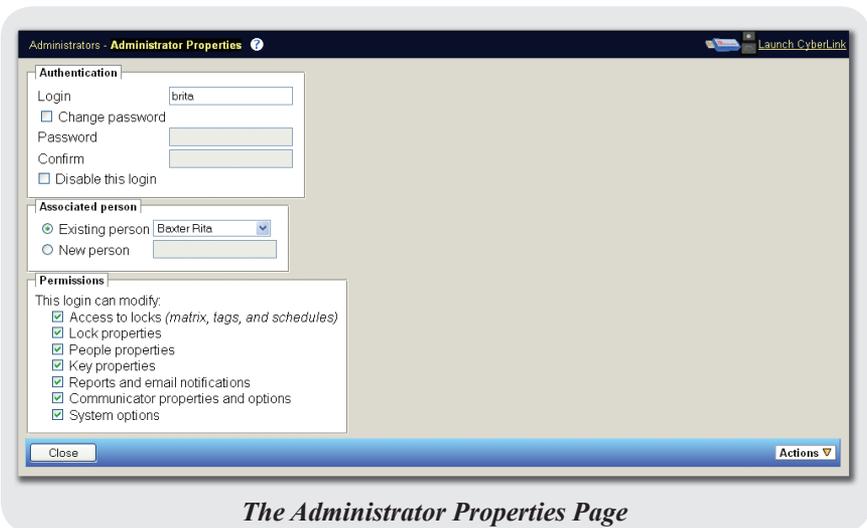
Clicking in one of the table cells displays the operations pop-up menu for Administrators. Selecting the *Properties* option displays the properties page for the selected administrator. The *Journal* option generates a report of changes that the administrator has made to the system. Selecting the *Delete* option removes the Administrator from the system.



The Administrators Operations Pop-Up Menu

Administrator Properties

The *Administrator Properties* page, accessed by selecting the *Properties* option from the operations pop-up menu on the *Administrators* page, lists information about the selected administrator login.



The Administrator Properties Page

The login and password may be changed in the *Authentication* frame, and the account may be temporarily disabled, so that it cannot be used to access the system. The system will automatically disable an administrator account (except for the root administrator login, which cannot be disabled) after three consecutive attempts to enter the password have failed. To re-enable a login, simply uncheck the *Disable this login* checkbox.

Use the *Associated Person* frame to link the administrator account with a person already in the system, or choose to add a new person.

The options selected in the *Permissions* frame determine which areas of the system an administrator login is able to modify. The requisite permissions to perform various actions are described in the table below:

Action	Permission(s)
Create/modify people tags and associate people with them	<i>Access to locks + People properties</i>
Create/modify lock tags and associate locks with them	<i>Access to locks + Lock properties</i>
Automatic tag creation	<i>Access to locks + Lock properties + People properties</i>
Master key designation	<i>Access to locks + Key properties</i>
Create/modify system keys	<i>Access to locks + Key properties + System options</i>
Re-key all locks in the system	<i>Access to locks + Lock properties + System options</i>
Create/modify Notifications	<i>Communicator properties and options OR System options</i>
Create/modify Programming Jobs	<i>Lock properties OR Reports and email notifications OR Key properties</i>

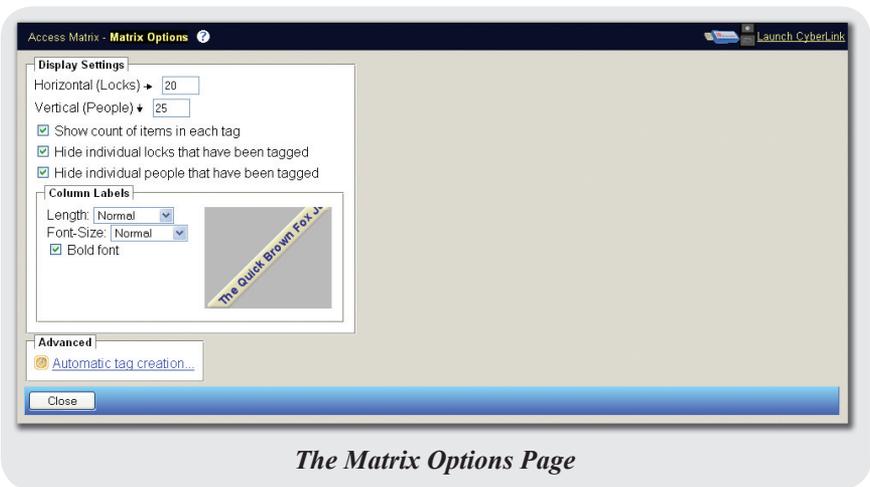
System Menus and Functionality

Clicking on the *System* menu header displays the *Options by Category* page, which contains links to the various sections of system options that may be configured by administrators.



Access Matrix Options

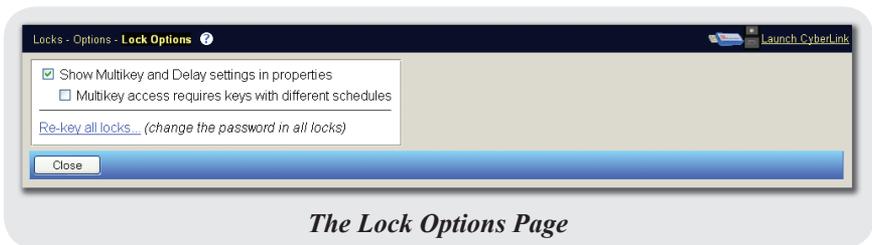
The *Matrix Options* page, accessed by clicking the *Matrix Display* link on the *Options by Category* page, contains options for controlling the display of the Access Matrix.



This page is also accessible by choosing *Options* from the *Access Matrix* menu, and its contents are explained in the “*Access Matrix Functionality*” section at the beginning of this chapter.

Lock Options

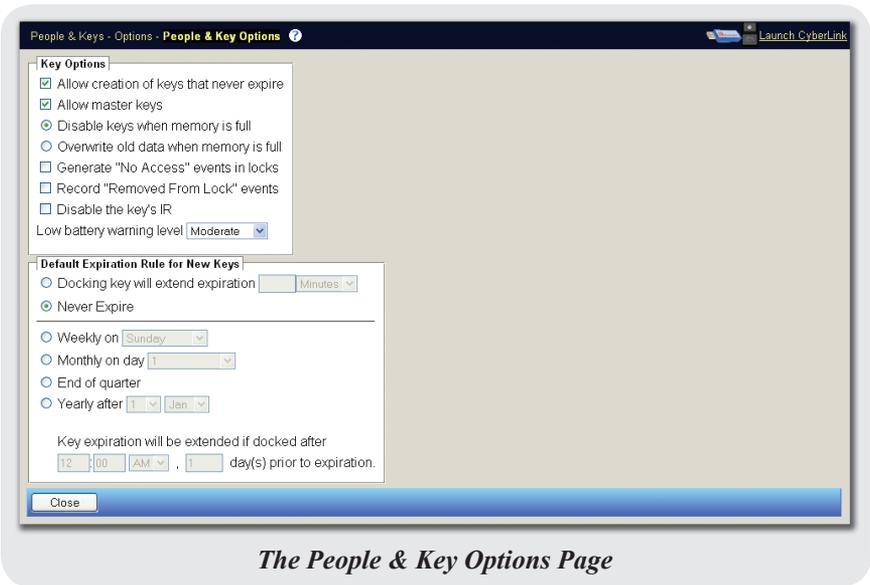
The *Lock Options* page, accessed by clicking the *Lock Options* link on the *Options by Category* page, contains options for multi-key/delay settings and changing the access codes for all locks in the system.



This page is also accessible by choosing *Options* from the *Locks* menu, and its contents are explained in the “*Locks Menus and Functionality*” section earlier in this chapter.

Key Options

The *People & Key Options* page, accessed by clicking the *Key Options* link on the *Options by Category* page, defines rules and defaults for behavior of CyberKeys added to the system.



This page is also accessible by choosing *Options* from the *People & Keys* menu, and its contents are explained in the “*People & Keys Menus and Functionality*” section earlier in this chapter.

Email Notification Setup

The *Email Notifications* page, accessed by clicking the *Email Notification Setup* link on the *Options by Category* page, contains the details of the email server used by CyberAudit-Web Professional to send email notifications.



This page is also accessible by selecting the *Email Setup* option from the *Reports* menu, and its contents are explained in the “*Reports Menus and Functionality*” section earlier in this chapter.

Communicators Options

The *Communicators Options* page, accessed by clicking the *Communicator Options* link on the *Options by Category* page, is used for setting default networking values and behavior of certain communicator devices.



This page is also accessible by selecting *Options* from the *Communicators* menu, and its contents are explained in the “*Communicators Menus and Functionality*” section earlier in this chapter.

Date & Time Preferences

The *System Settings* page, accessed by clicking the *Date & Time* link on the *Options by Category* page, contains options for date and time formats, and allows the system time zone to be set.



The System Settings Page

The format options chosen on this page will be reflected in audit trail reports.

Note: Changing the system time zone will require reprogramming all keys in the system.

Archive/Restore Options

The *Archive/Restore* page, accessed by clicking the *Archive/Restore* link on the *Options by Category* page, is used to hide or show old data from the system. Archiving moves data in CyberAudit-Web from active tables to archive tables. It can help reduce clutter in reports and improve performance.

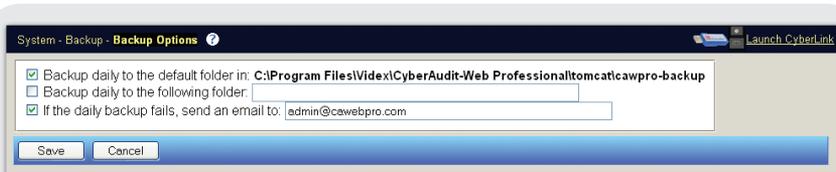


The Archive/Restore Page

When events are archived, the data is moved into different tables in the database. The entries for events, status, and the journal of changes can no longer be viewed through the user interface. If a date older than the last archive date is selected, data will be restored from the archive tables.

Backup Options

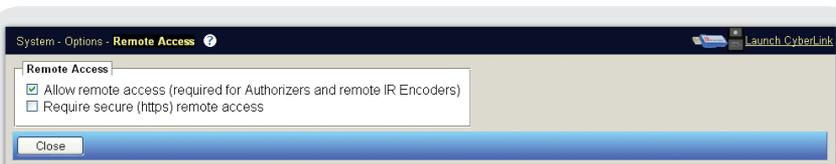
The *Backup Options* page, accessed by clicking the *Backup Options* link on the *Options by Category* page, contains options for automatic daily backup of the database and the placement of the files.



The Backup Options Page

Remote Access

The *Remote Access* page, accessed by clicking the *Remote Access* link on the *Options by Category* page, contains options for allowing the CyberAudit-Web Professional software to be accessed from computers other than the one on which it is installed.



The Remote Access Page

If Authorizers or IR Encoders (other than one attached to the host computer) will be used with the system, the remote access feature must be enabled. If these communicators will not be used, but remote administrator access is desired, enable the option. Use of this feature requires knowledge of general networking and familiarity with any firewall software running on the host computer or the network.

With local access, there is typically no need for a secure connection. For remote access, however, selecting the *Require secure (https) remote access* option is recommended. This will encrypt all network transmissions used with the system to protect against eavesdropping and “man-in-the-middle” attacks.

Re-Keying All Locks

If system passwords have been compromised or the vase Grand Master is lost, the locks in the system should be “re-keyed.” After changing the password, all locks in the system must be updated. Systems created using a Grand Master as the source of the access codes must designate that Grand Master as lost in order to re-key the system. For systems created with manual passwords, clicking on the *Re-key all locks* link on the *Options by Category* page brings up the *Re-key All Locks* page, where a new access password may be set.

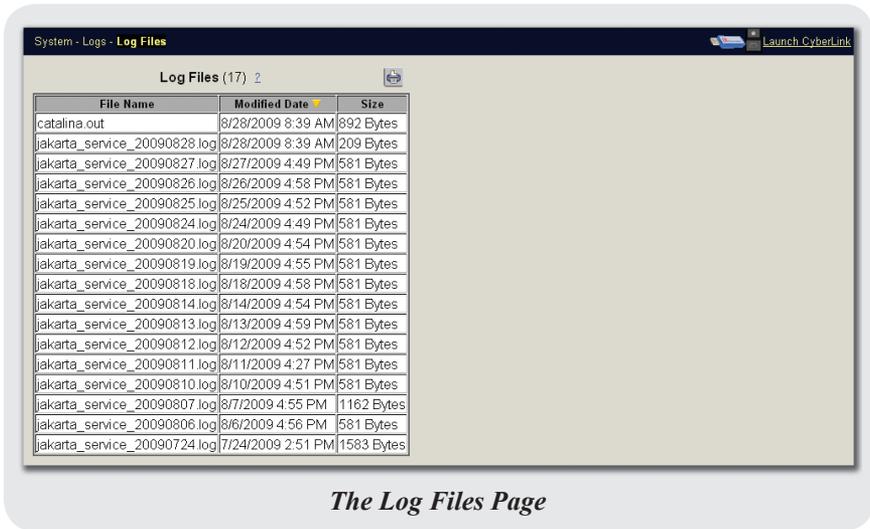


The screenshot shows a web interface titled "Locks - Re-key All Locks". It features two input fields: "New Lock Password:" and "Verify:". Below these fields is a yellow warning box with the text: "Warning: Changing the lock password will result in change icons for all locks and keys in the system." At the bottom of the form is a blue "Close" button.

The Re-key All Locks Page

System Logs

The *Log Files* page, accessed by selecting the *Logs* option from the *System* menu, displays the list of log files which have been created by the system.



Clicking in one of the table cells displays the operations pop-up menu for log files. Selecting the *Download* option allows the file to be saved to a specific location or opened with a text editor. Selecting the *Open* option will display the file as plain text in a new browser window. The *Delete* option will remove the log file from the system.

Note: Files from the current day cannot be removed.



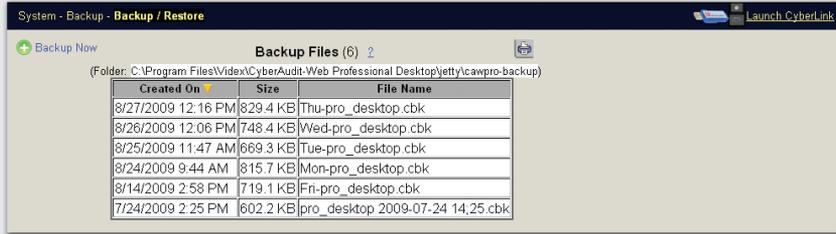
The screenshot shows a table titled "Log Files (17)". The table has three columns: "File Name", "Modified Date", and "Size". A context menu is open over the first "jakarta_service" row, showing options: "Download", "Open", and "Delete".

File Name	Modified Date	Size
catalina.out	8/28/2009 8:39 AM	892 Bytes
jakarta_service	8/2009 8:39 AM	209 Bytes
jakarta_service	8/2009 4:49 PM	581 Bytes
jakarta_service	8/2009 4:58 PM	581 Bytes
jakarta_service	20090825 log18/25/2009 4:52 PM	581 Bytes

The Log Files Operations Pop-Up Menu

System Backup and Restore

The *Backup/Restore* page, accessed by selecting the *Backup* option from the *System* menu, is used to create backups or to restore the system to a previous state from a backup file.



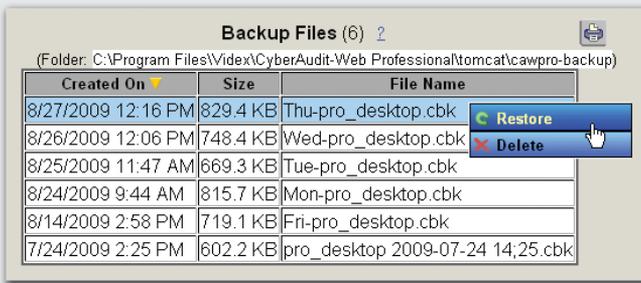
The screenshot shows the "System - Backup - Backup / Restore" page. It features a "Backup Now" button and a table titled "Backup Files (6)". The table lists backup files with columns for "Created On", "Size", and "File Name".

Created On	Size	File Name
8/27/2009 12:16 PM	829.4 KB	Thu-pro_desktop.cbk
8/26/2009 12:06 PM	748.4 KB	Wed-pro_desktop.cbk
8/25/2009 11:47 AM	669.3 KB	Tue-pro_desktop.cbk
8/24/2009 9:44 AM	815.7 KB	Mon-pro_desktop.cbk
8/14/2009 2:58 PM	719.1 KB	Fri-pro_desktop.cbk
7/24/2009 2:25 PM	602.2 KB	pro_desktop_2009-07-24 14:25.cbk

The Backup / Restore Page

By default, a daily backup is performed automatically by the system. These files are named following the convention “*ddd-pro_desktop.cbk*”, where “*ddd*” is the first three letters of the current day of the week. Files of the same name are automatically overwritten. Manually created backup files will not be overwritten. Note that backup options may be specified on the *Backup Options* page, described earlier in this chapter.

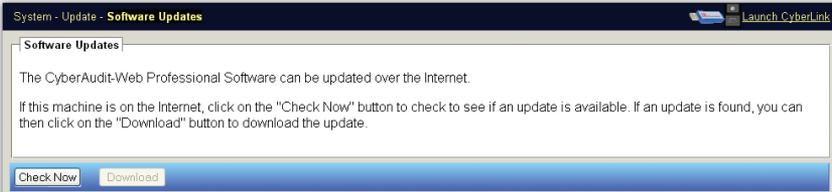
Clicking in a table cell displays the operations pop-up menu for backup files. Select the *Restore* option to restore the system to the state of the selected backup file. Select the *Delete* option to remove the selected backup file from the system.



The Backup Files Operations Pop-Up Menu

Software Updates

The *Software Updates* page, accessed by selecting the *Update* option from the *System* menu, allows the administrator to check for updates to the CyberAudit-Web Professional application.

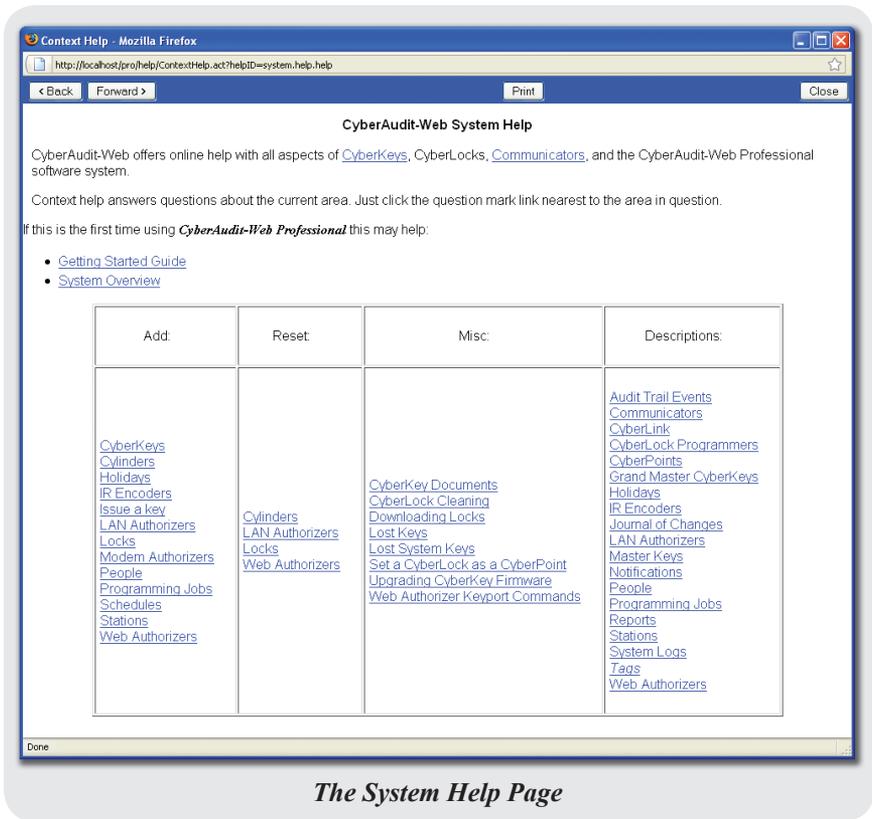


The Software Updates Page

Updates for CyberKey firmware are available directly from CyberAudit-Web. See the instructions in the “*Upgrading Key Firmware*” section of the next chapter.

System Help

In addition to the context help which appears on most pages within CyberAudit-Web Professional, there is a collection of help topics on the *System Help* page, accessed by selecting the *Help* option from the *System* menu.



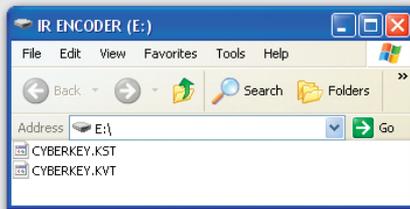
CyberLink

The *CyberLink* application controls the IR Encoder and USB Station devices. To use one of these communicators with CyberAudit-Web, the CyberLink application must be launched on a computer with an available USB port. The Java™ Web Start Launcher application (part of the J2SE Runtime Environment) is required. CyberLink requires Windows XP or later for correct operation on a PC. Macs require OS X 10.4.11 or greater. CyberAudit-Web must be running for CyberLink to launch.

Installing and Using CyberLink

To install the *CyberLink* application, follow these steps:

1. Plug an IR Encoder or USB Station into an available USB port on the computer with which it is to be used. If a window similar to the following appears, close it and return to CyberAudit-Web.

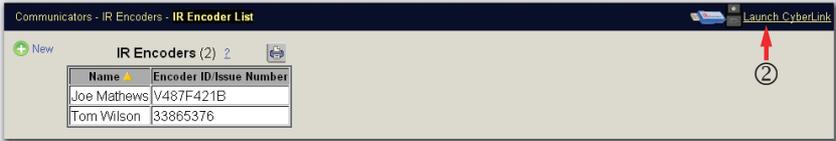


The IR Encoder Window

(Continues on next page . . .)

(. . . continued from previous page)

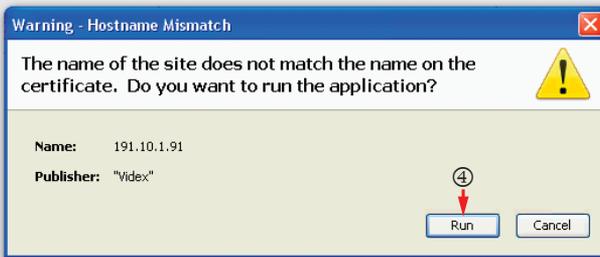
2. Click on the icons of the IR Encoder and USB Station or the *Launch CyberLink* link from any page within CyberAudit-Web Professional.



3. If asked what to do with the linked file, choose to open it with *Java(TM) Web Start Launcher*.



4. Continue past any warning dialogs that may appear.



(Continues on next page . . .)

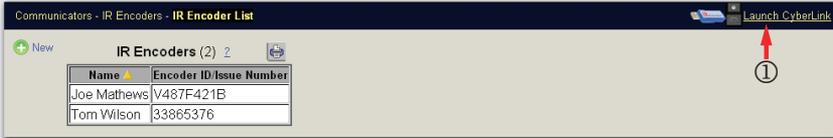
(. . . continued from previous page)

5. Wait while the CyberLink application starts up. The program will search for an IR Encoder or USB Station connected to a USB port, then connect to the CyberAudit-Web server to check for application updates. Installation is complete when the following message is displayed.



The CyberLink Application Window - Installation Complete

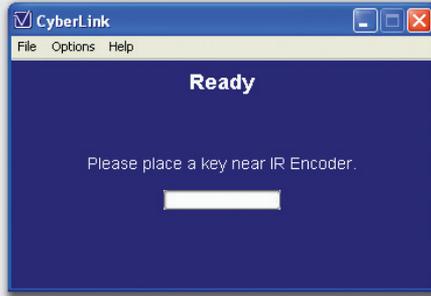
To use the *CyberLink* application, follow these steps:



1. If the application isn't already open, click on the icons of the IR Encoder and USB Station or the *Launch CyberLink* link from any page within CyberAudit-Web Professional.
2. Wait for the application to load and display the "Ready" page.

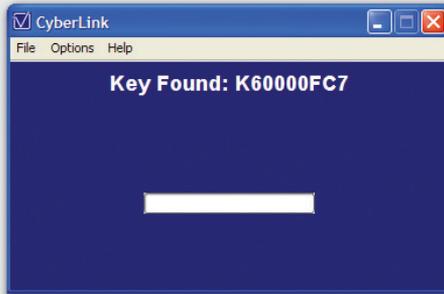
(Continues on next page . . .)

(... continued from previous page)

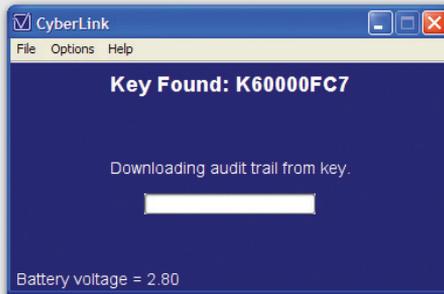


The CyberLink Application Window - Ready for Use

3. Place an infrared CyberKey near the IR Encoder with the LED of the key aligned with the end of the IR Encoder, or plug any key into the USB Station. The following sequence will occur:



The application detects the key.



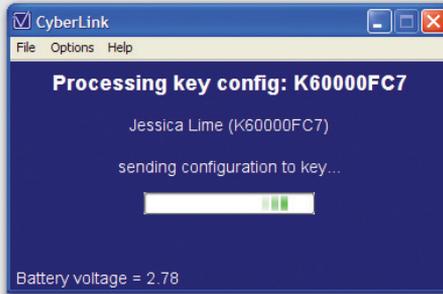
The application downloads events from the key.

(Continues on next page ...)

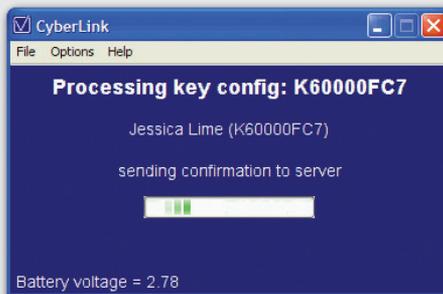
(. . . continued from previous page)



The application sends the key ID to the server and receives the appropriate configuration file.



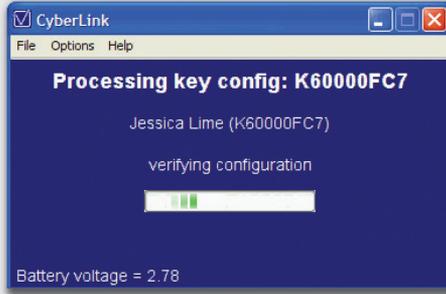
The application sends the configuration file to the key.



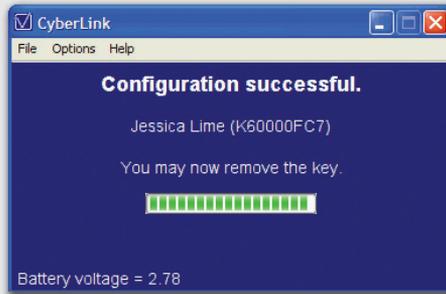
The application notifies the server that the new configuration was transferred to the key.

(Continues on next page . . .)

(... continued from previous page)



The application asks the key to verify the configuration it received.

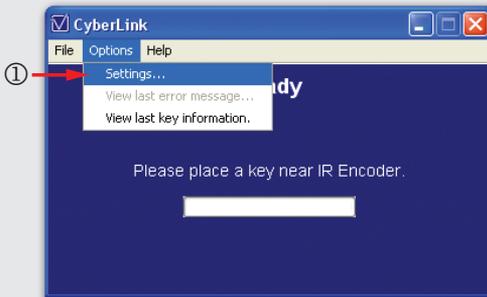


The application indicates success or gives an error message.

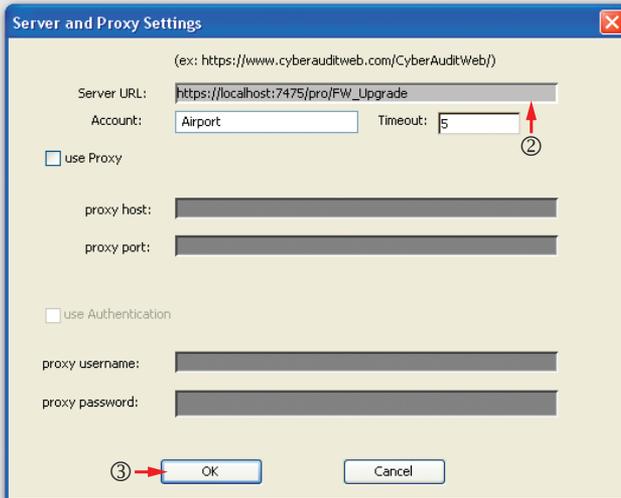
Upgrading Key Firmware

Newer models of CyberKeys have internal software which may be updated from CyberAudit-Web Professional. Each CyberAudit-Web update contains the latest available firmware for CyberKeys. Key models which can be updated include CyberKey Rechargeable, CyberKey Plus, and CyberKey Blue.

To upgrade CyberKey firmware, follow these steps:



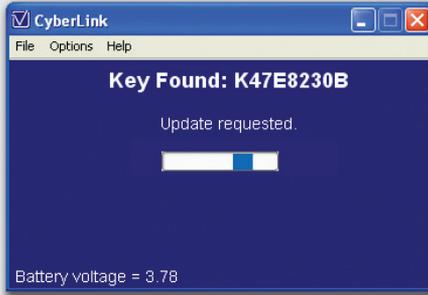
1. Choose *Settings...* from the *Options* menu to show the *Server and Proxy Settings* window.



(Continues on next page . . .)

(... continued from previous page)

2. Append “/FW_Upgrade” to the end of the server URL.
3. Click the *OK* button.



4. Present the key to be upgraded to the application.

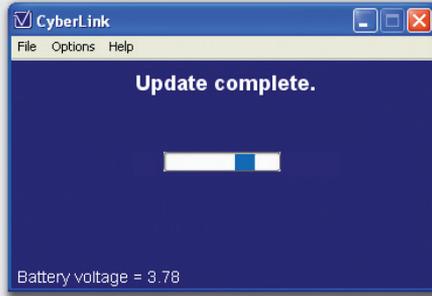


5. Select a firmware version to install from the pull-down menu. Normally, this will be the highest available number.
6. Click the *Proceed* button. CyberLink will transfer the firmware to the key.



(Continues on next page . . .)

(. . . continued from previous page)



7. Reset the server URL in the *Server and Proxy Settings* window (remove the “/FW_Upgrade”) in order to resume normal CyberLink operation.

Operations Reference

This chapter contains step-by-step procedure listings for performing actions within CyberAudit-Web Professional.

Access Matrix Operations

To set a schedule in the Access Matrix, follow these steps:

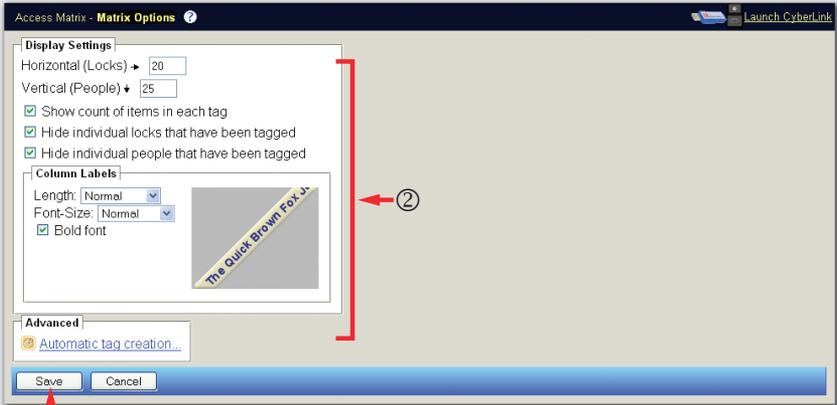


1. Click on the *Access Matrix* menu header.
2. Locate the desired person and lock (or applicable tags), using filters if necessary.
3. Click in the matrix cell where the two intersect.
4. Select a schedule to apply from the drop-down list.

To set Access Matrix options, follow these steps:



1. Select *Options* from the *Access Matrix* menu.



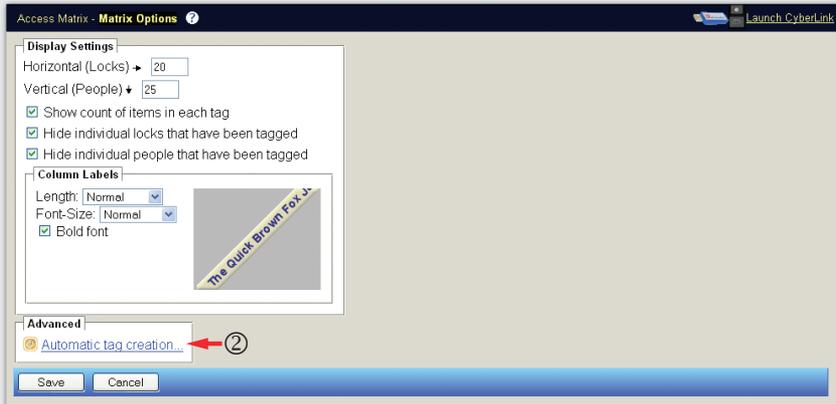
2. Set options as desired.

3. Click the *Save* button.

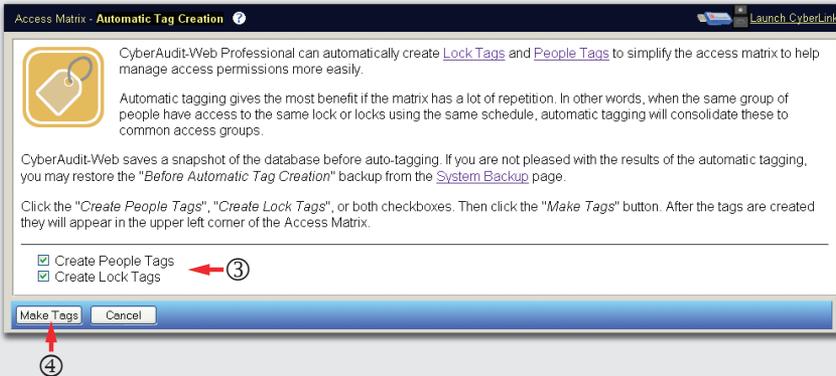
To automatically create tags, follow these steps:



1. Select *Options* from the *Access Matrix* menu.



2. Click the *Automatic tag creation* link.



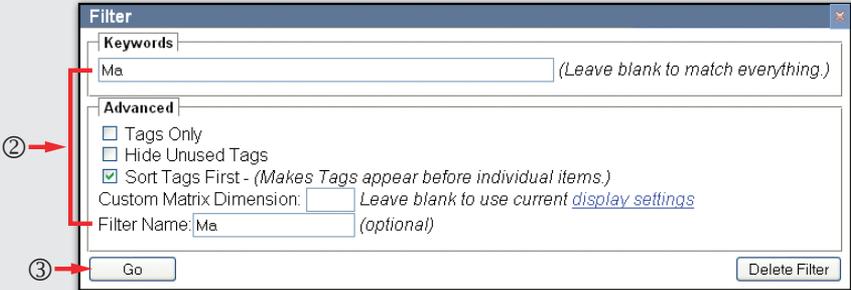
3. Select the type(s) of tags to create.

4. Click the *Make Tags* button.

To filter the Access Matrix, follow these steps:



1. Select *New Filter* from the drop-down filter list.



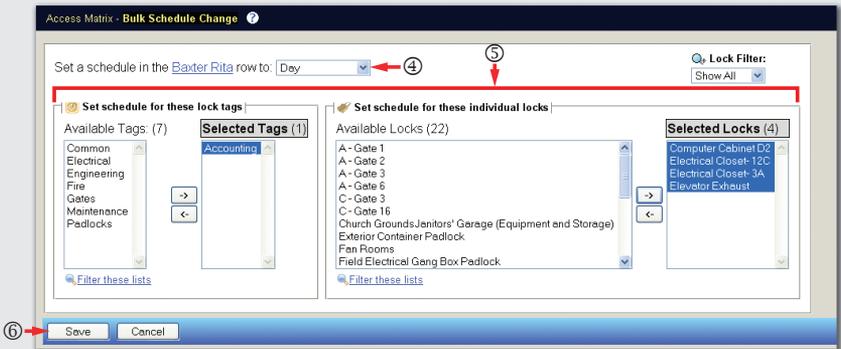
2. Set filter options as desired.

3. Click the *Go* button.

To change a person or tag's schedule for multiple locks, follow these steps:



1. Click on the *Access Matrix* menu header.
2. Click the desired person or tag name.
3. Select the *Bulk Schedule Change* option.

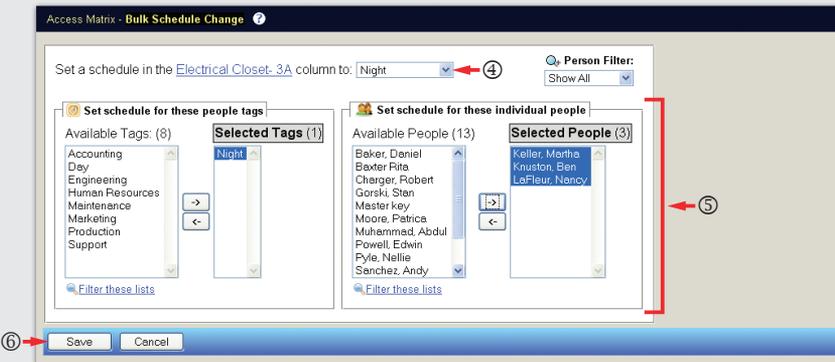


4. Select the schedule to apply from the drop-down list.
5. Use the item choosers to select the locks and tags to which the schedule should be applied.
6. Click the *Save* button.

To change a lock or tag's schedule for multiple people, follow these steps:

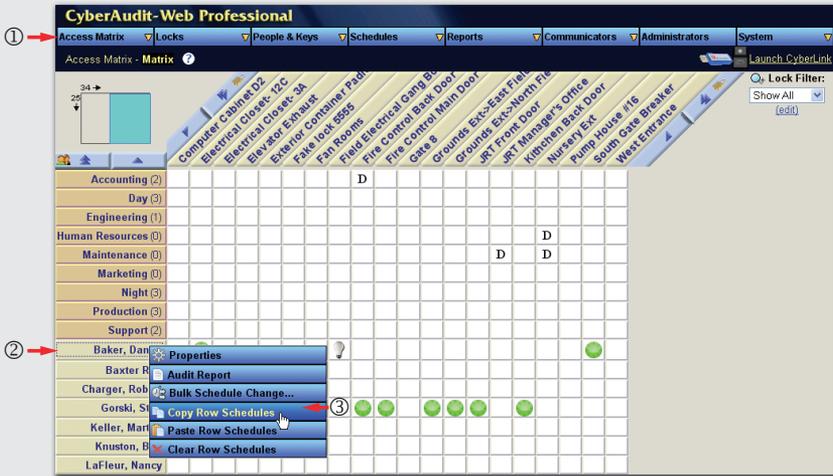


1. Click on the *Access Matrix* menu header.
2. Click the desired lock or tag name.
3. Select the *Bulk Schedule Change* option.



4. Select the schedule to apply from the drop-down list.
5. Use the item choosers to select the people and tags to which the schedule should be applied.
6. Click the *Save* button.

To copy schedules from one person or tag to another, follow these steps:



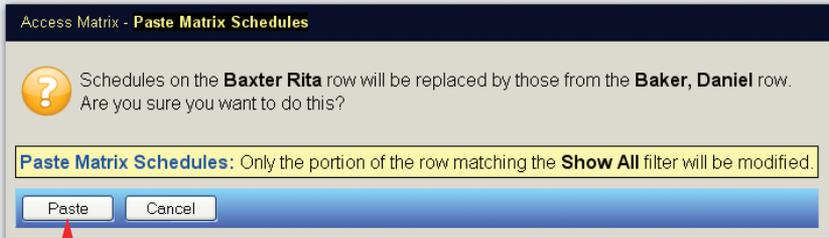
1. Click on the *Access Matrix* menu header.
2. Click the name of the person or tag to copy schedules from.
3. Select the *Copy Row Schedules* option.



4. Click the name of the person or tag to whom the schedules should be assigned.
5. Select the *Paste Row Schedules* option.

(Continues on next page . . .)

(. . . continued from previous page)



⑥

6. Click the *Paste* button to confirm the operation.

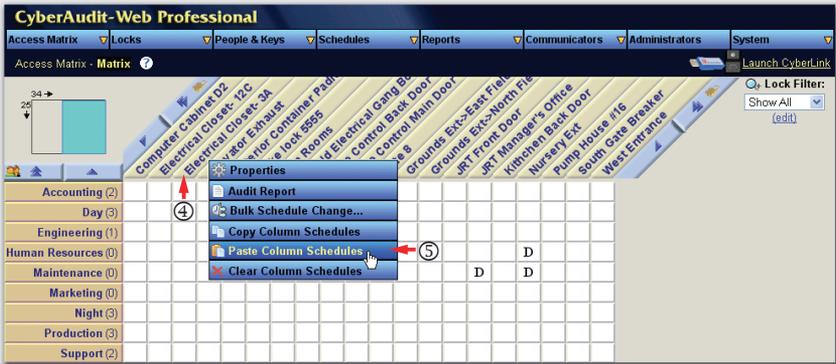
To copy schedules from one lock or tag to another, follow these steps:



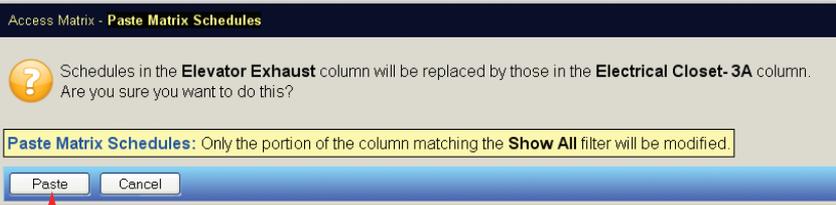
1. Click on the *Access Matrix* menu header.
2. Click the name of the lock or tag to copy schedules from.
3. Select the *Copy Column Schedules* option.

(Continues on next page . . .)

(... continued from previous page)



4. Click the name of the lock or tag to which the schedules should be assigned.
5. Select the *Paste Column Schedules* option.



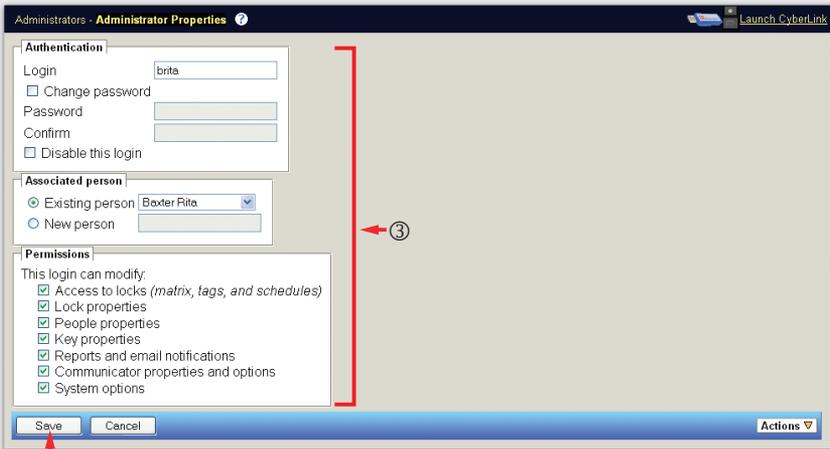
6. Click the *Paste* button to confirm the operation.

Administrators Operations

To create a new administrator, follow these steps:



1. Click on the *Administrators* menu header.
2. Click the *New* link.

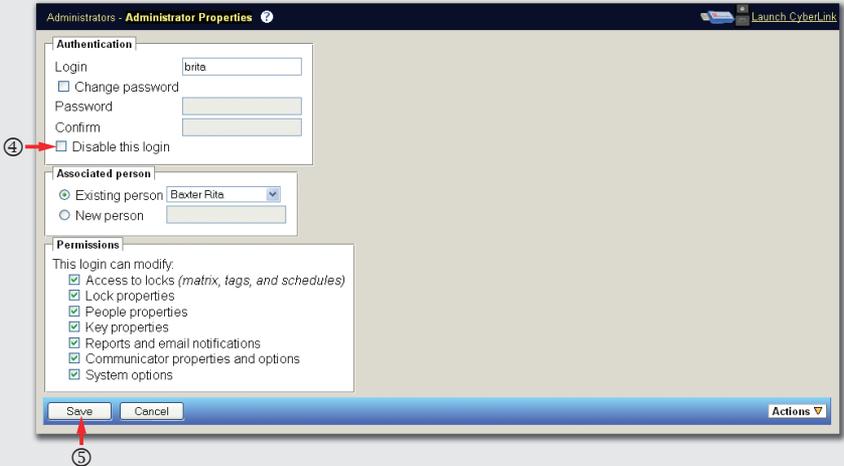


3. Specify properties for the new administrator.
4. Click the *Save* button.

To disable an administrator login, follow these steps:



1. Click on the *Administrators* menu header.
2. Click on the login name to be disabled.
3. Select the *Properties* option.



4. Select the *Disable this login* option.
5. Click the *Save* button.

Communicators Operations

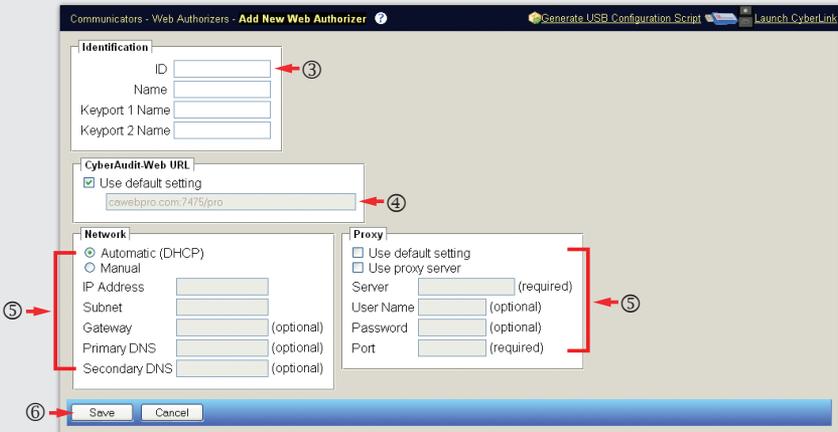
To add a Web Authorizer, follow these steps:



1. Select the *Web Authorizers* option from the *Communicators* menu.



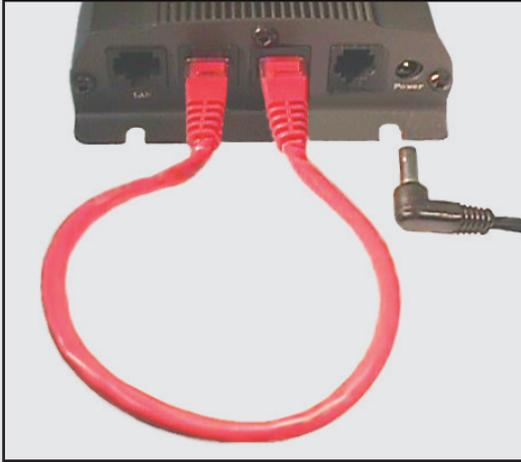
2. Click the *New* link.



3. Enter the ID of the Authorizer (found on the label on the bottom of the unit). The name fields are optional.
4. Verify that the URL or IP address of the CyberAudit-Web server is correct.
5. Configure the network and proxy settings, if needed.
6. Click the *Save* button.

To reset a network Authorizer, follow these steps:

1. Connect an Ethernet cable between the *Keyport1* and *Keyport2* ports on the Authorizer.



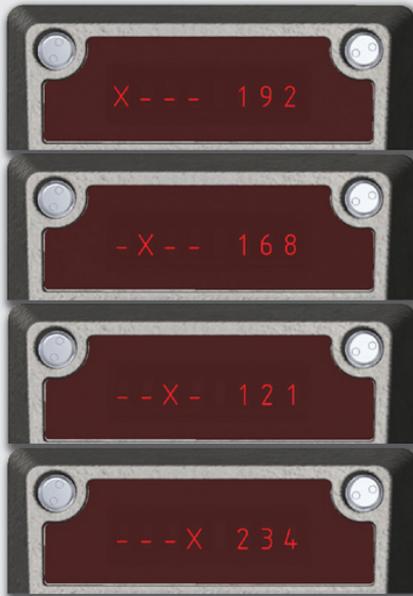
2. Disconnect the power cable, wait a few seconds, and reconnect the power.
3. The reset process is complete when the LEDs for *Keyport1* and *Keyport2* blink rapidly. The Authorizer may then be connected as normal.

To configure the CyberAudit-Web IP address from a Web Authorizer Keypoint, follow these steps:

1. Unless it is brand new, reset the Authorizer.
2. Enter 999 on the Keypoint and press the “#” key.

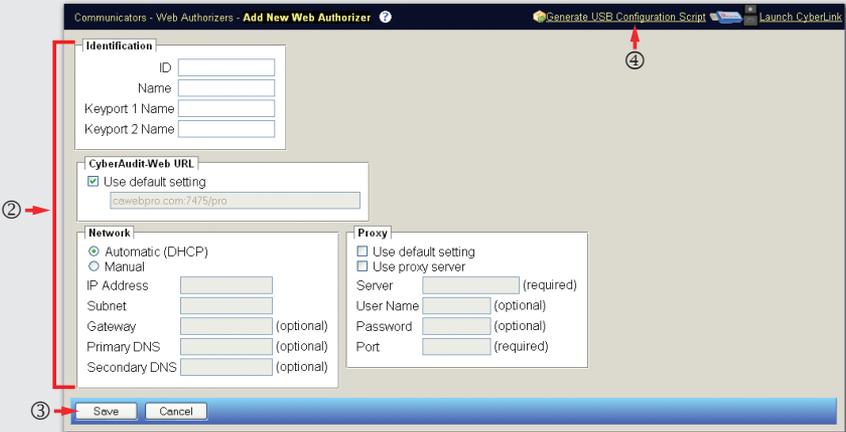


3. The 'X' indicates the octet of the IP address being edited, and 000 indicates the current value. Enter a new value and press the “#” key, or enter 999 and press the “#” key to keep the current value. Octets with only one or two digits may be entered without leading zeroes.
4. Enter values for the remaining octets, then cycle through the complete IP address by entering 999 for each octet, verifying that each was set correctly.



5. Enter 000 and press the “#” key to exit the IP address configuration mode.

To configure a Web Authorizer using a USB flash drive, follow these steps:



1. Select the desired Authorizer from the list and go to the *Properties* page.
2. Set properties for the Authorizer as needed.
3. Click the *Save* button.
4. Click the *Generate USB Configuration Script* link.



5. Save the generated file onto a USB flash drive. Check the drive contents to ensure that the latest *.tar.gz* file exists, without an appended version number.

(Continues on next page . . .)

(... continued from previous page)



5. Insert the flash drive into one of the Authorizer's USB ports, using an extension if necessary.
6. Unplug the power cable from the Authorizer, wait three seconds, then reconnect the cable.
7. Remove the flash drive when both status lights on the Authorizer cease flashing in unison.

To add a LAN Authorizer, follow these steps:

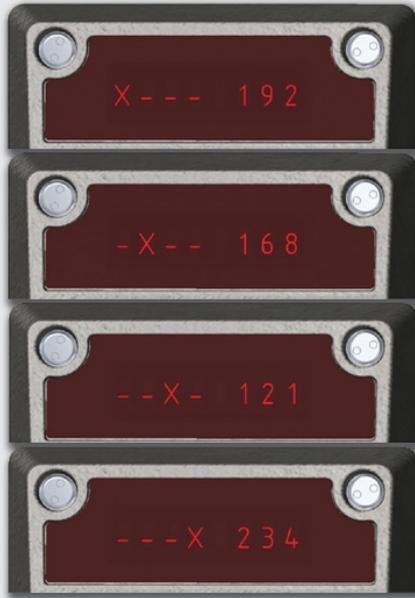
1. Enter 999 on the Keypoint and press the “#” key.



2. The 'X' indicates the octet of the IP address being edited, and 192 indicates the current value. Enter a new value and press the “#” key, or enter 999 and press the “#” key to keep the current value. Octets with only one or two digits may be entered without leading zeroes.
3. Enter values for the remaining octets, then cycle through the complete IP address by entering 999 for each octet, verifying that each was set correctly.

(Continues on next page ...)

(... continued from previous page)



4. Enter 000 and press the “#” key to exit the IP address configuration mode.



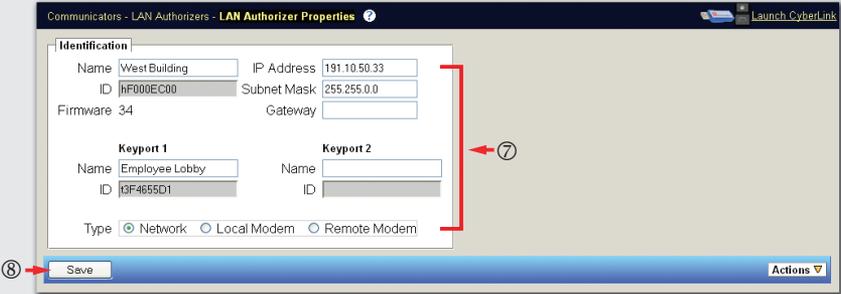
5. In CyberAudit-Web, select *LAN Authorizers* from the *Communicators* menu.



6. Click the *New* link.

(Continues on next page...)

(... continued from previous page)

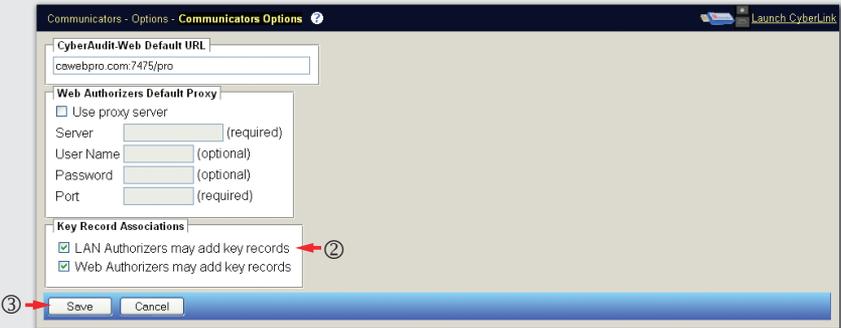


- 7. Set network properties for the Authorizer as needed.
- 8. Click the *Save* button.

To assign keys to a LAN Authorizer, follow these steps:



- 1. Select *Options* from the *Communicators* menu.



- 2. Ensure that the *LAN Authorizers may add key records* option is selected.
- 3. Click the *Save* button.

(Continues on next page ...)

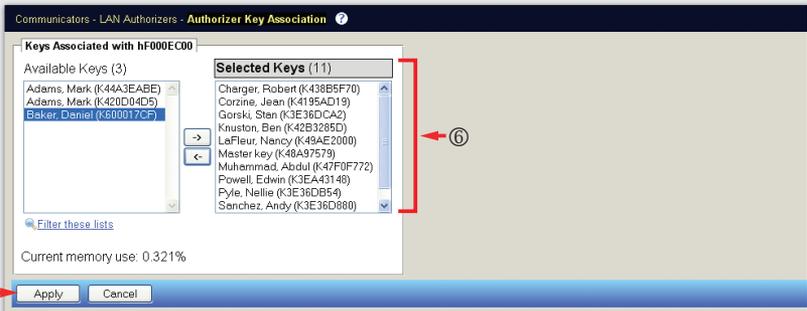
(... continued from previous page)



4. Select *LAN Authorizers* from the *Communicators* menu.



5. Click the desired Authorizer's table row and select *Keys* from the operations pop-up menu.



6. Use the item chooser to select the keys to assign to the Authorizer.

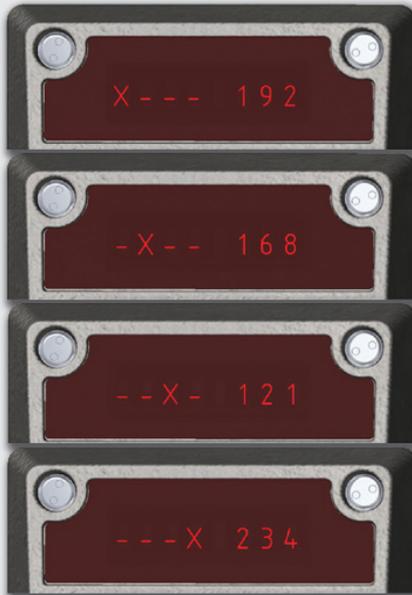
7. Click the *Apply* button.

To add a local modem Authorizer, follow these steps:

1. Enter 999 on the Keypoint and press the “#” key.



2. The 'X' indicates the octet of the IP address being edited, and 192 indicates the current value. Enter a new value and press the “#” key, or enter 999 and press the “#” key to keep the current value. Octets with only one or two digits may be entered without leading zeroes.
3. Enter values for the remaining octets, then cycle through the complete IP address by entering 999 for each octet, verifying that each was set correctly.



4. Enter 000 and press the “#” key to exit the IP address configuration mode.

(Continues on next page . . .)

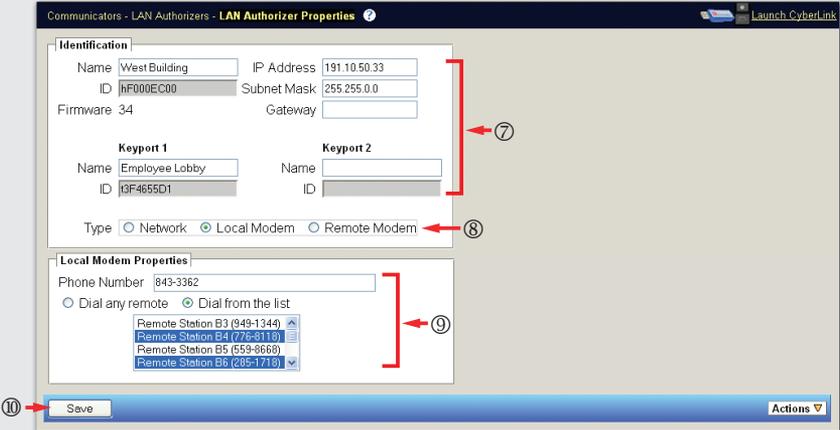
(... continued from previous page)



5. In CyberAudit-Web, select *LAN Authorizers* from the *Communicators* menu.



6. Click the *New* link.



- 7. Set network properties for the Authorizer as needed.
- 8. Select *Local Modem* as the Authorizer type.
- 9. Set the phone number and remote Authorizer dial list.
- 10. Click the *Save* button.

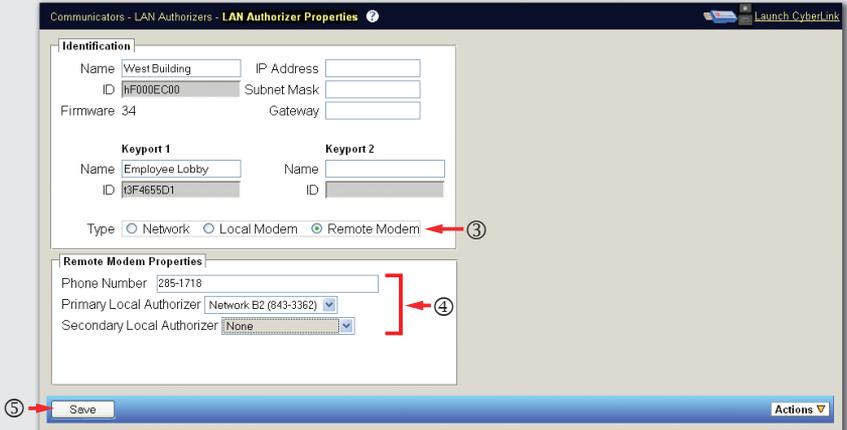
To add a remote modem Authorizer, follow these steps:



1. In CyberAudit-Web, select *LAN Authorizers* from the *Communicators* menu.



2. Click the *New* link.



3. Select *Remote Modem* as the Authorizer type.

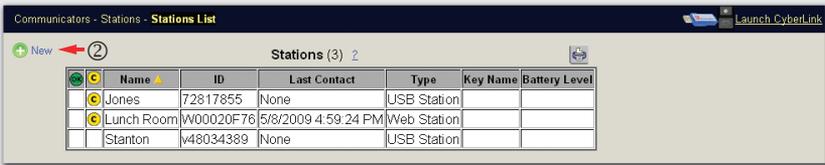
4. Set the phone number and select a primary (and optional secondary) local Authorizer to dial.

5. Click the *Save* button.

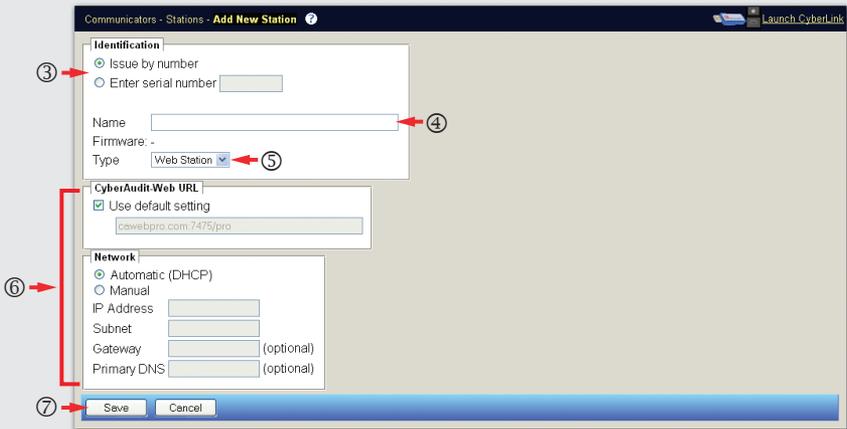
To add a new USB or Web Station, follow these steps:



1. Select *Stations* from the *Communicators* menu.



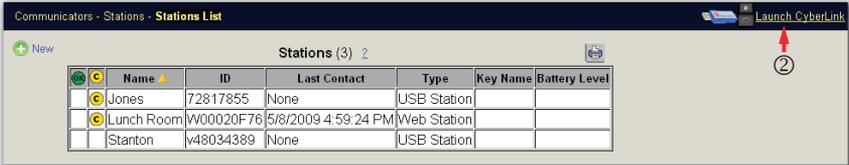
2. Click the *New* link.



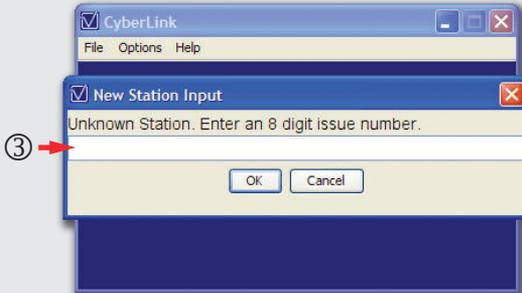
3. Select an issue method, entering the serial number if known.
4. Enter a name for the Station.
5. Select the Station type.
6. (*Web Stations only*) Specify network settings as needed.
7. Click the *Save* button.

To prepare a newly added USB or Web Station for first use, follow these steps:

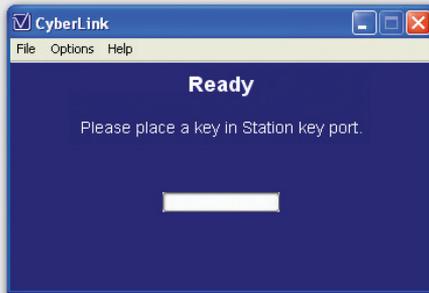
1. Connect the Station to the computer using a USB cable.



2. Click the *Launch CyberLink* link.



3. If the Station was added using an issue number, enter it when prompted by CyberLink.

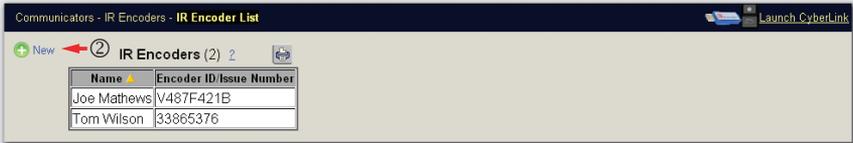


4. After CyberLink updates the Station and the ⓐ icon clears on the *Stations List* page in CyberAudit-Web, the Station will be ready to communicate with keys. It may then be disconnected from USB and connected to its power and Ethernet cables. When it makes contact with the server, its green *Ready* LED will light and the green ⓐ icon will appear on the *Stations List* page.

To add an IR Encoder to the system, follow these steps:



1. Select *IR Encoders* from the *Communicators* menu.



2. Click the *New* link.



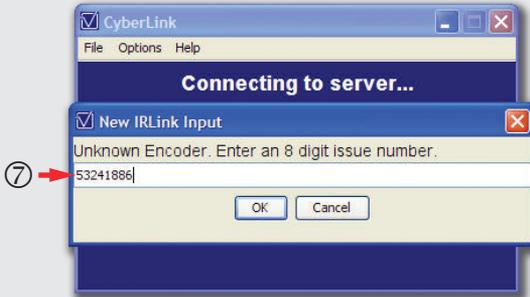
- 3. Select an issue method, entering the serial number if known.
- 4. Enter a name for the IR Encoder.
- 5. Click the *Save* button.



6. Connect the IR Encoder to the computer and click the *Launch CyberLink* link.

(Continues on next page . . .)

(... continued from previous page)



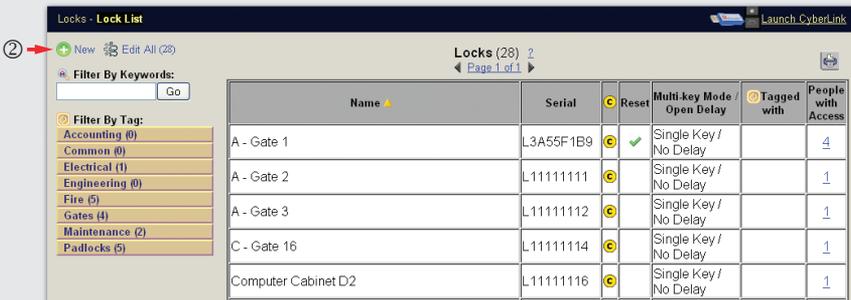
7. If the IR Encoder was added using an issue number, enter it when prompted by CyberLink.

Locks Operations

Note: The CyberLock Location Sheet may be found as a PDF file on the CyberAudit-Web Professional Installation Disc.

To manually add a new lock, follow these steps:

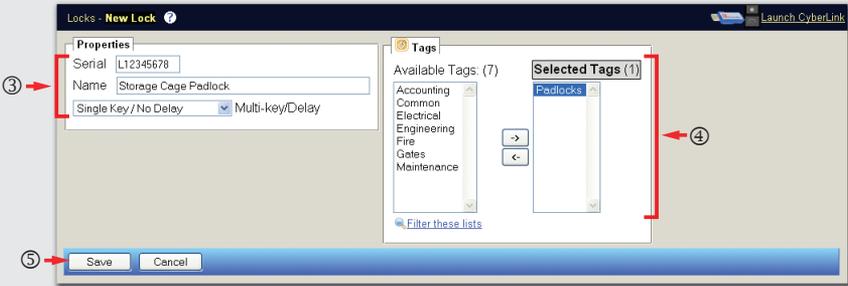
1. Click the header for the *Locks* menu.



2. Click the *New* link.

(Continues on next page ...)

(. . . continued from previous page)



3. Set properties for the new lock as needed.
4. If desired, associate the lock with tags using the item chooser.
5. Click the *Save* button.

To add locks using a Grand Master, follow these steps:

1. Configure the Grand Master using CyberLink and an IR Encoder or a USB or Web Station.



2. Place one serial number label for each lock on the cylinder itself, and another on the CyberLock Location Sheet.
3. Write the location where the lock will be installed next to the serial number label on the CyberLock Location Sheet.
4. Touch the Grand Master to each lock.
5. Update the Grand Master using CyberLink and an IR Encoder or a USB or Web Station to download the lock serial numbers to the database.

(Continues on next page . . .)

(... continued from previous page)

6. Locate each newly added lock on the CyberAudit-Web *Locks* page and set the properties as needed. For example, make the name match the location entered on the sheet.

To add locks using a CyberLock Programmer, follow these steps:



1. Place one serial number label for each lock on the cylinder itself, and another on the CyberLock Location Sheet.
2. Write the location where the lock will be installed next to the serial number label on the CyberLock Location Sheet.
3. Touch each lock with the Programmer.
4. Update the Programmer using CyberLink and an IR Encoder or a USB or Web Station to download the lock serial numbers to the database.
5. Locate each newly added lock in the *Locks List* and set the properties as needed. For example, edit the lock name to match the location entered on the CyberLock Location Sheet.
6. Create a programming job which contains the newly added locks. Note the job number.
7. Update the Programmer again, entering the job number created in the previous step.
8. Touch each lock with the Programmer to transfer the configurations.
9. Update the Programmer a final time, and the icons will be cleared on the *Locks List* page.

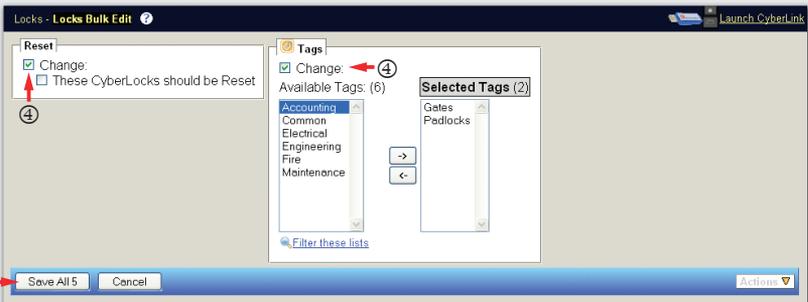
To edit lock properties in bulk, follow these steps:

1. Click the header for the *Locks* menu.



2. Use the filters to display only those locks to which the bulk edit should be applied.

3. Click the *Edit All* link.



4. Select the *Change* option for each frame of settings to be modified and specify the changes as needed.

5. Click the *Save All* button.

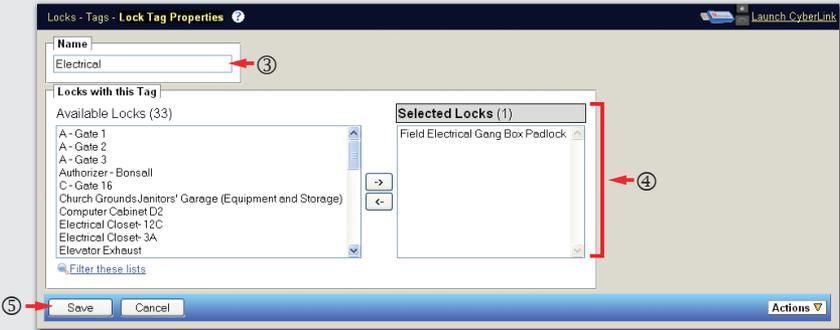
To add a lock tag, follow these steps:



1. Select *Tags* from the *Locks* menu.



2. Click the *New* link.



3. Give the tag a descriptive name.

4. Use the item chooser to select or remove locks from the tag.

5. Click the *Save* button.

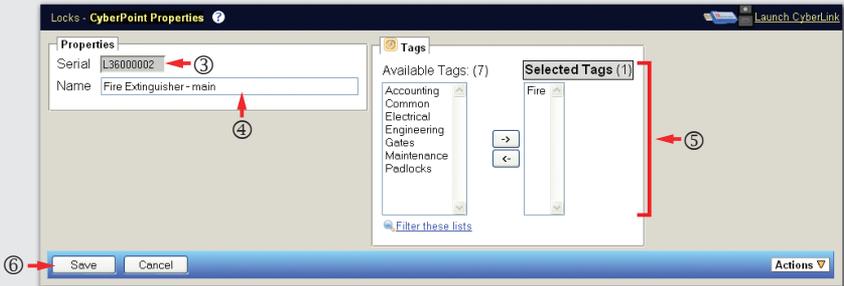
To add a CyberPoint, follow these steps:



1. Select *CyberPoints* from the *Locks* menu.



2. Click the *New* link.

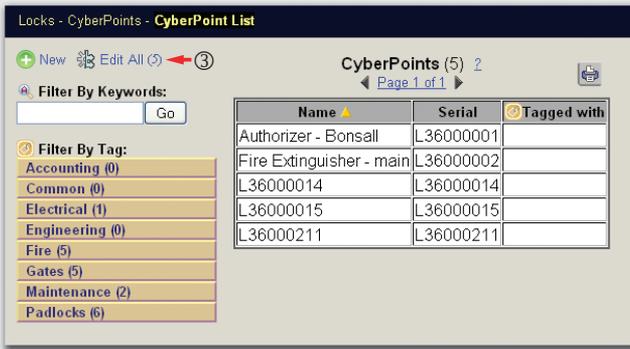


3. Enter the serial number of the CyberPoint.
4. Enter a descriptive name for the CyberPoint.
5. Assign lock tags as needed.
6. Click the *Save* button.

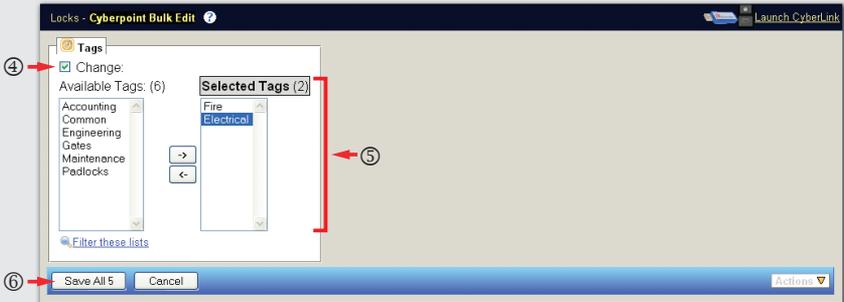
To edit CyberPoint properties in bulk, follow these steps:



1. Select *CyberPoints* from the *Locks* menu.
2. Use the filters to display only those locks to which the bulk edit should be applied.



3. Click the *Edit All* link.



4. Select the *Change* box to enable the item chooser.
5. Use the item chooser to apply lock tags to the CyberPoints.
6. Click the *Save* button.

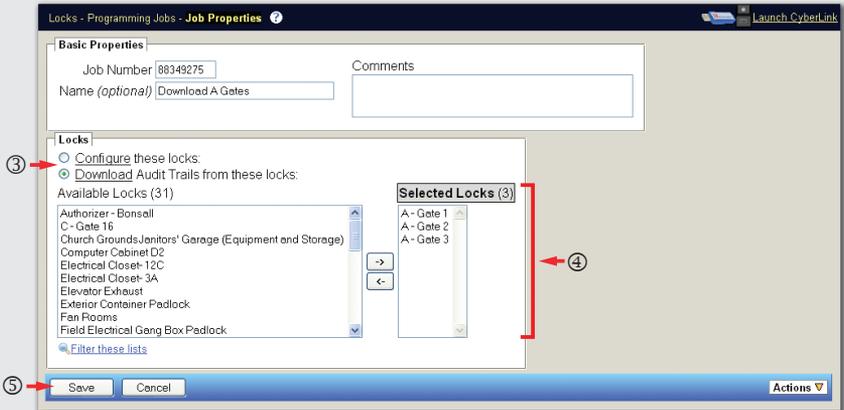
To add a programming job, follow these steps:



1. Select *Programming Jobs* from the *Locks* menu.



2. Click the *New* link.



3. Select the programming job type.

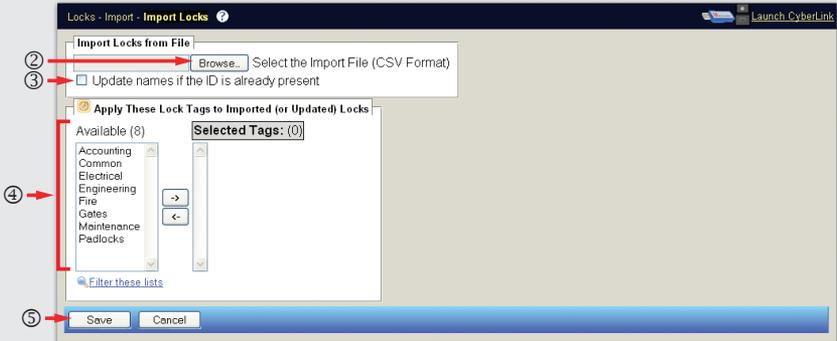
4. Use the item chooser to select locks to include in the job.

5. Click the *Save* button.

To import locks and CyberPoints, follow these steps:



1. Select *Import* from the *Locks* menu.

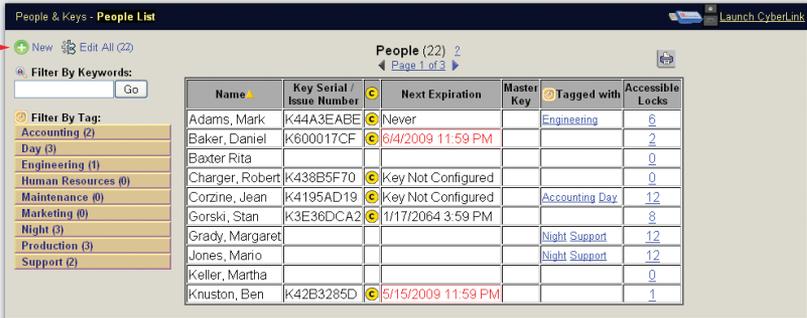


2. Click the *Browse* button to select an import file.
3. Select the *Update names if the ID is already present* box if names should be updated from the file when a lock ID already exists in the system.
4. Use the item chooser to apply lock tags to the locks being imported from the file.
5. Click the *Save* button.

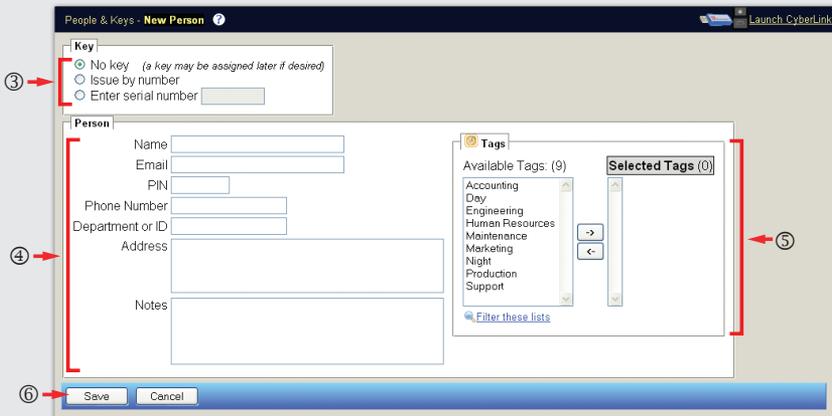
People & Keys Operations

To manually add people to the system, follow these steps:

1. Click the *People & Keys* menu header.



2. Click the *New* link.



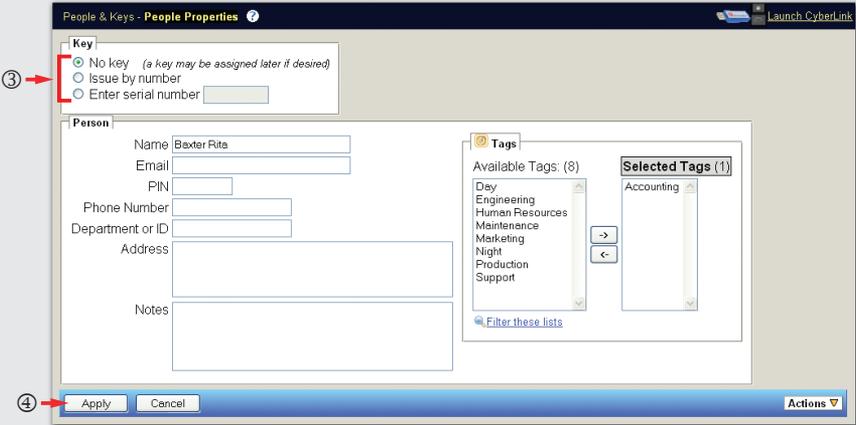
3. Select an option for issuing a key to the new person.
4. Specify details for the person.
5. Use the item chooser to associate tags with the person as needed.
6. Click the *Save* button. If an option other than *No key* is selected in the *Key* frame, the *Save* button changes to the *Apply* button.

To issue a key to a person, follow these steps:

1. Click the *People & Keys* menu header.



2. To add a person and issue a key at the same time, click the *New* link. To assign a key to an existing person, click on the person's row and select the *Properties* option from the operations pop-up menu.

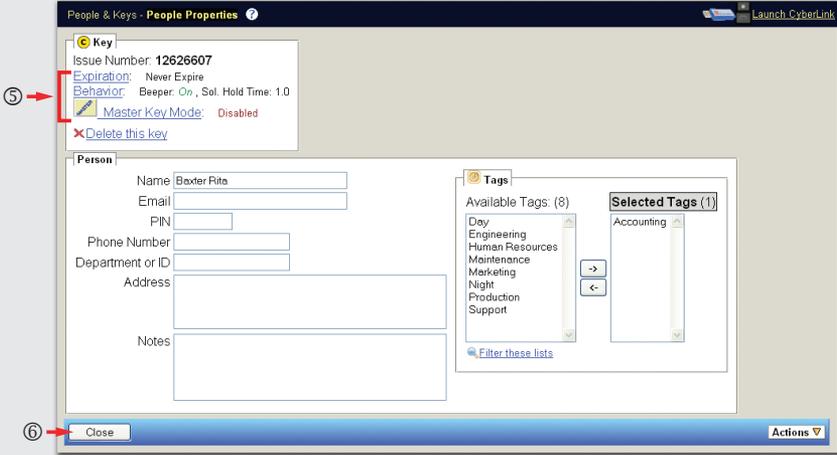


3. Select the *Issue by number* option in the *Key* frame, or manually enter the serial number of the key. Using an issue number allows the person to be given any available CyberKey. The key will be programmed when presented to an Authorizer or CyberLink along with the issue number.

4. Click the *Apply* button.

(Continues on next page . . .)

(... continued from previous page)



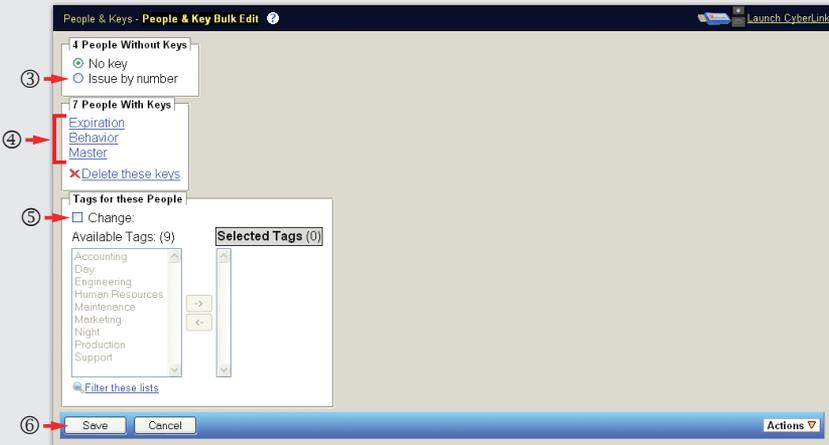
5. Set options for the new key as needed.
6. Click the *Close* button.
7. Update the key to clear the icon.

To edit properties of people and keys in bulk, follow these steps:

1. Click the *People & Keys* menu header.



2. Use filters to narrow the list of people to edit, then click the *Edit All* link.



3. To issue keys to the selected people who don't have one, select the *Issue by number* option.

4. Set options for people with keys as needed.

5. Select the *Change* option to enable the item chooser and apply tags to the selected people as needed.

6. Click the *Save* button.

To delete people in bulk, follow these steps:

1. Click the *People & Keys* menu header.

2. Use filters to narrow the list of people to edit, then click the *Edit All* link.

3. Select *Delete All* from the *Actions* button pop-up menu.

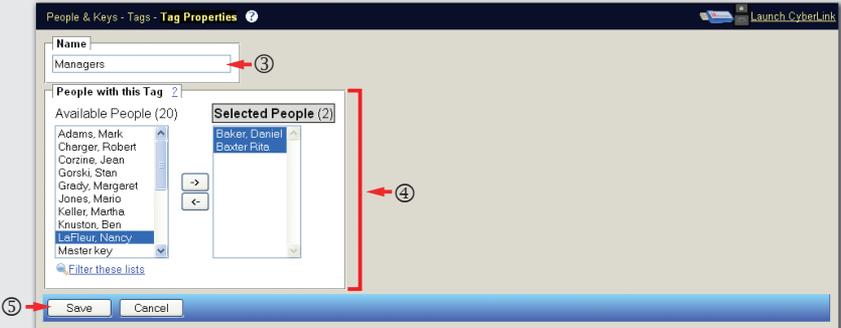
To add a new people tag, follow these steps:



1. Select *Tags* from the *People & Keys* menu.



2. Click the *New* link.



3. Give the tag a descriptive name.

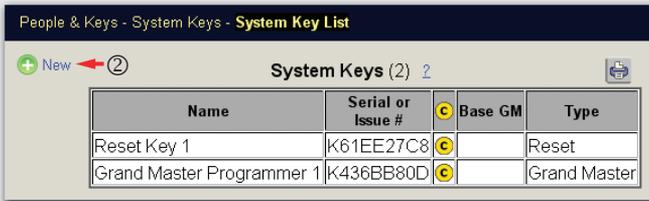
4. Use the item chooser to include people in the tag.

5. Click the *Save* button.

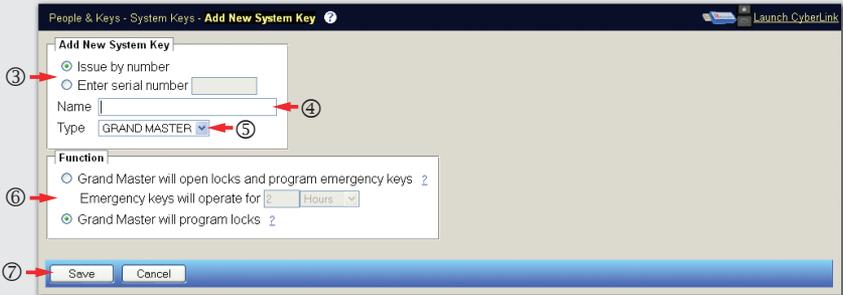
To add a new system key, follow these steps:



1. Select *System Keys* from the *People & Keys* menu.



2. Click the *New* link.



3. Select an issue method for the new system key.

4. Give the key a descriptive name.

5. Select the system key type - *Grand Master* or *Reset*.

6. If adding a *Grand Master* key, select its function.

7. Click the *Save* button.

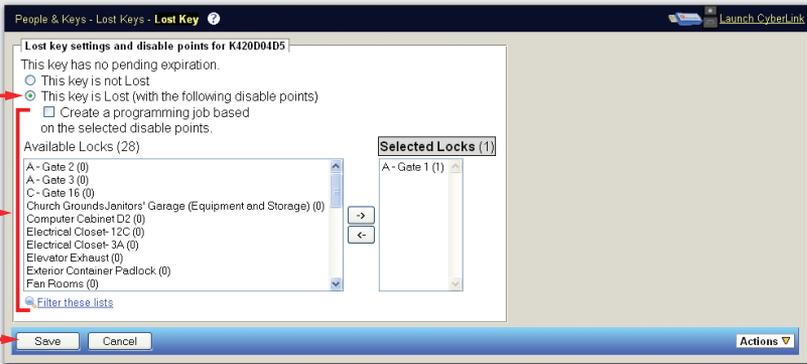
To disable a lost system key, follow these steps:



1. Select *System Keys* from the *People & Keys* menu.



2. Click in the lost key's row in the *System Keys* table and select *Lost* from the operations pop-up menu.



3. Select the *This key is Lost (with the following disable points)* option.
4. Select the option to create a programming job and use the item chooser to specify locks as disabling points for the key.
5. Click the *Save* button.

(Continues on next page . . .)

(. . . continued from previous page)

6. Configure a Programmer or Grand Master using the created programming job number.
7. Touch the locks chosen as disable points with the Programmer or Grand Master. The lost system key will then be disabled if it touches one of these locks.
8. Download the Grand Master or Programmer and confirm that all  icons have been cleared.

To replace a base Grand Master, follow these steps:



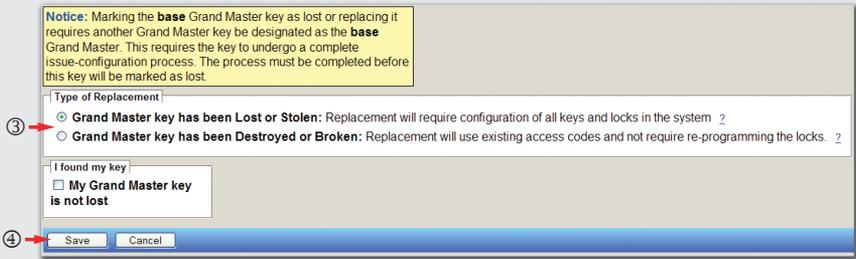
1. Select *System Keys* from the *People & Keys* menu.



2. Click in the base Grand Master's row in the *System Keys* table and select *Lost* from the operations pop-up menu.

(Continues on next page . . .)

(... continued from previous page)



3. Specify whether the Grand Master has been lost or stolen, or simply destroyed or broken.
4. Click the *Save* button.

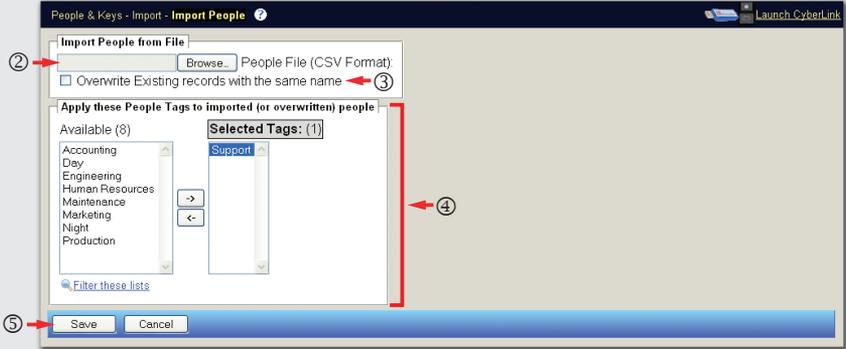
Important: The **Base** Grand Master key has been designated lost. Please present a new Grand Master key to the application.

5. Present a new Grand Master to the system.

To import people, follow these steps:



1. Select *Import* from the *People & Keys* menu.



(Continues on next page ...)

(... continued from previous page)

2. Type or browse to the location of the CSV file.
3. Specify whether or not existing records should be overwritten.
4. Use the item chooser to apply tags to the imported people.
5. Click the *Save* button.

To give a key master access, follow these steps:

Note: *Allow Master Keys* must be checked on the *Key Options* page in order to give master key access.

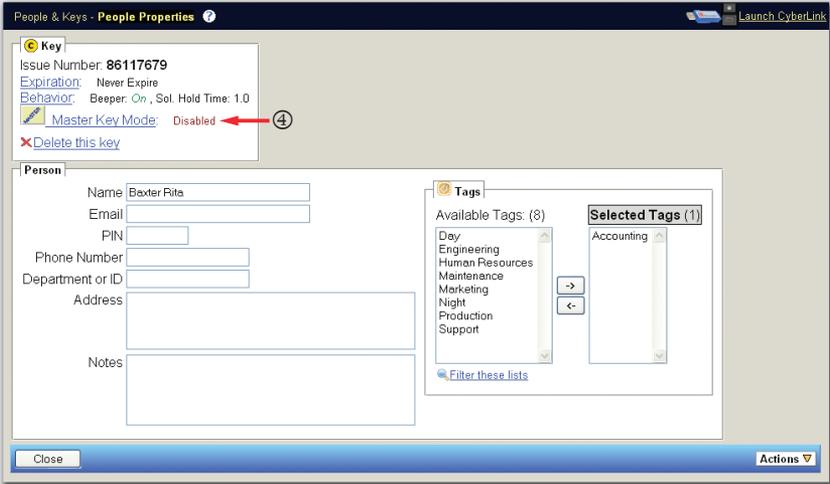
1. Click the *People & Keys* menu header.



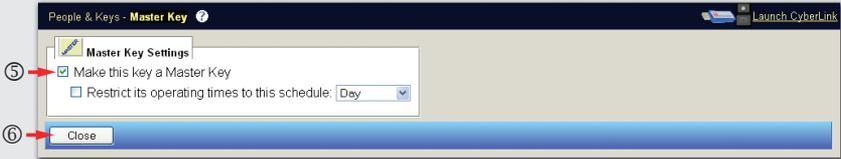
2. Click in the table row of the person who will keep the master key and select the *Properties* option from the operations pop-up menu.
3. Issue a key to the person, if they don't already have one.

(Continues on next page . . .)

(... continued from previous page)



4. Click the *Master Key Mode* link in the *Key* frame.



5. Select the *Make this key a Master Key* option and a schedule by which to restrict the master key, if desired.

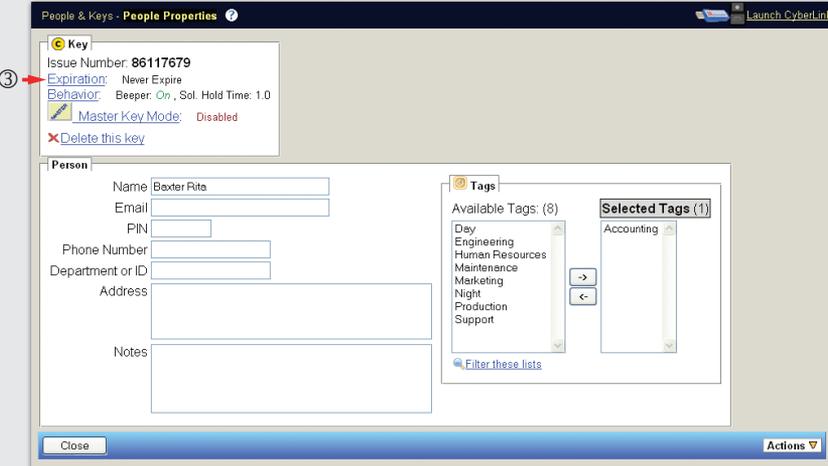
6. Click the *Close* button.

To edit key expiration, follow these steps:

1. Click the *People & Keys* menu header.



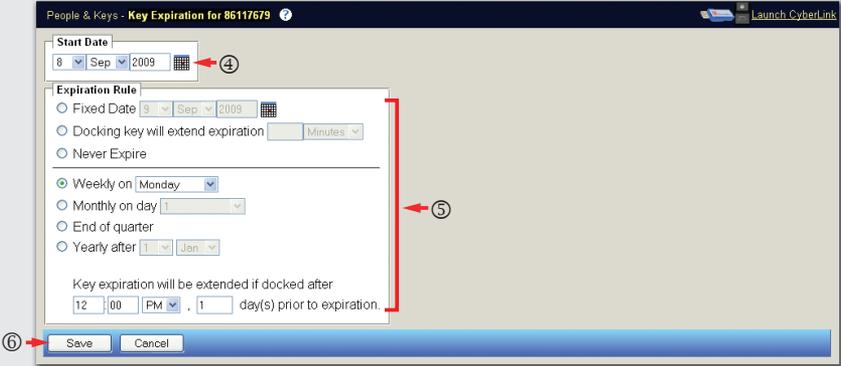
2. Click in the table row containing the key to edit and select *Properties* from the operations pop-up menu.



3. Click the *Expiration* link in the *Key* frame.

(Continues on next page . . .)

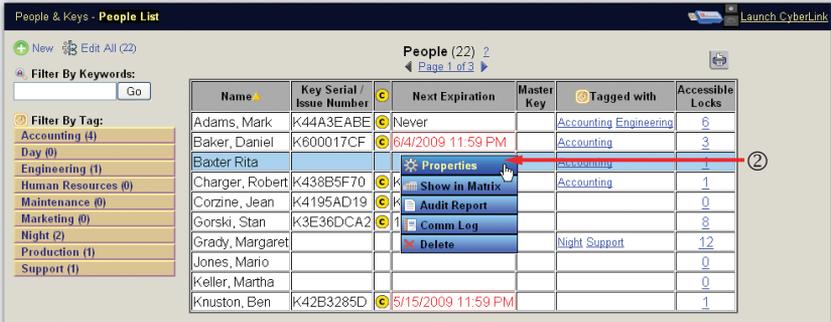
(... continued from previous page)



4. Select a start date for the key, if desired.
5. Select the desired expiration rule.
6. Click the *Save* button.

To configure a key to download events from a lock, follow these steps:

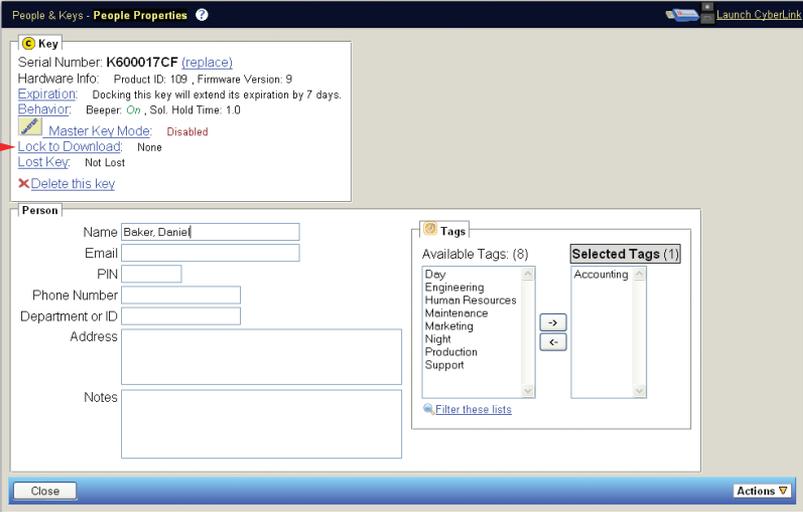
1. Click the *People & Keys* menu header.



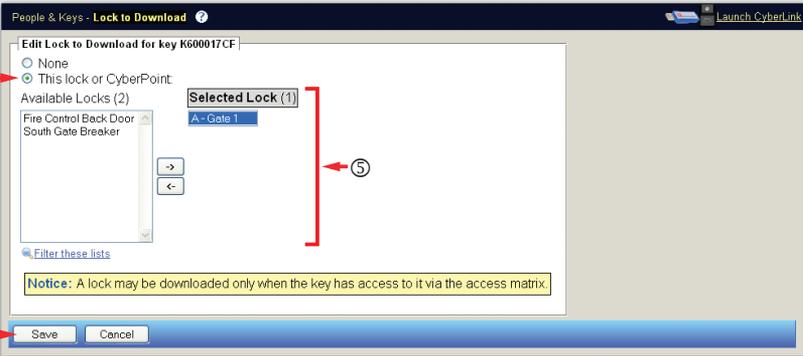
2. Click in the table row containing the key to edit and select *Properties* from the operations pop-up menu.

(Continues on next page ...)

(... continued from previous page)



3. Click the *Lock to Download* link in the *Key* frame.



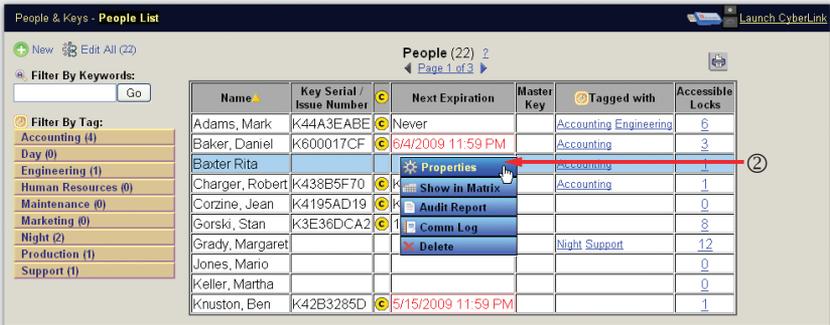
4. Select the *This lock or CyberPoint* option.

5. Use the item chooser to select the lock to download.

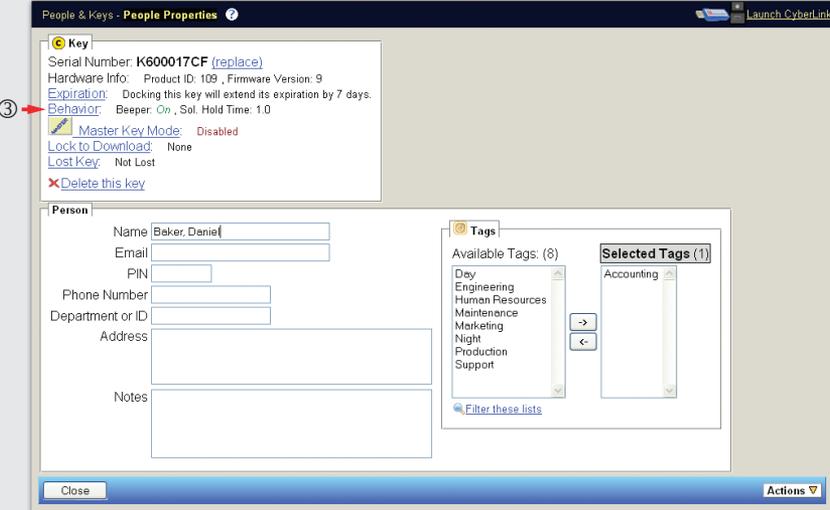
6. Click the *Save* button.

To change a key's behavior settings, follow these steps:

1. Click the *People & Keys* menu header.



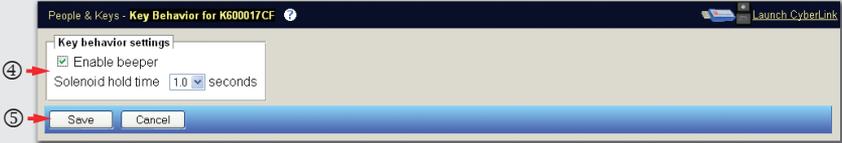
2. Click in the table row containing the key to edit and select *Properties* from the operations pop-up menu.



3. Click the *Behavior* link in the *Key* frame.

(Continues on next page . . .)

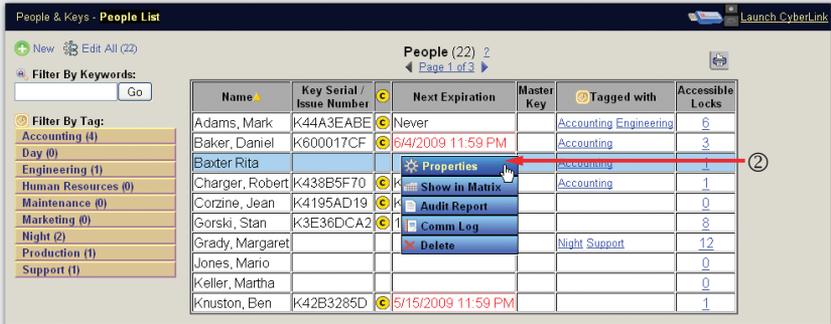
(... continued from previous page)



4. Specify behavior settings for the key as desired.
5. Click the *Save* button.
6. Update the key for the settings to take effect.

To replace a key, follow these steps:

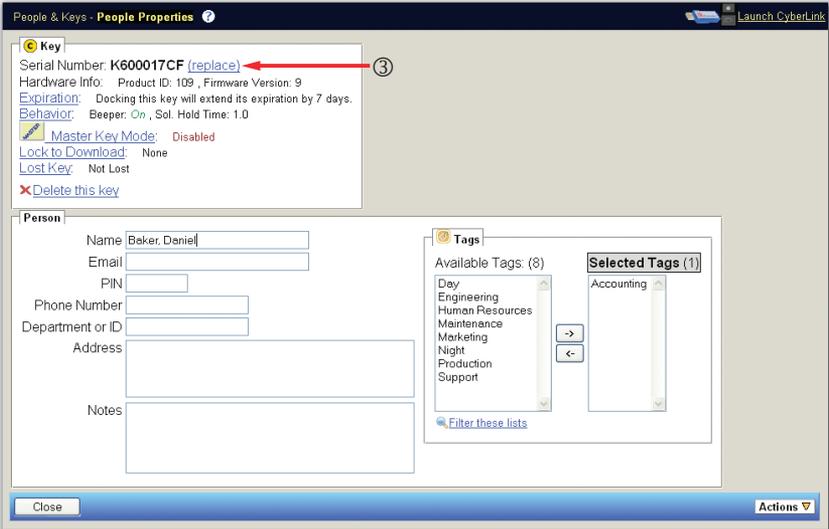
1. Click the *People & Keys* menu header.



2. Click in the table row containing the key to edit and select *Properties* from the operations pop-up menu.

(Continues on next page . . .)

(... continued from previous page)

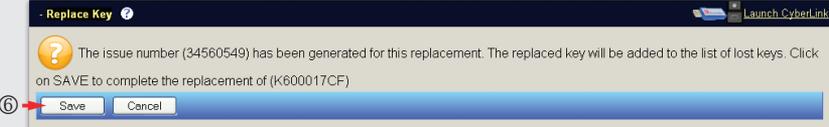


3. Click the *replace* link in the *Key* frame.



4. Select a method for adding the replacement key.

5. Click the *Save* button.



6. Click the *Save* button in the confirmation dialog to complete the replacement process.

7. Update the new key to configure it with the settings of the replaced key.

Reports Operations

To edit report properties, follow these steps:

1. Click on the *Reports* menu header.

Report Name ▲	Included People	Included Locks and CyberPoints	Included Events
All Key Holders	All	All	All
Denied Access	All	10	All
Engineering Ac	All	All	All
Maintenance A	All	All	All
Off Hours Early Morning	All	1	All
Off Hours Late Night	All	All	All

2. Click in the table row of the report to edit and select *Properties* from the operations pop-up menu.

Reports - Properties ? Launch CyberLink

Engineering Access (Rename)

Included People 11 Edit ← ③	Included Locks and CyberPoints All Edit ← ③	Included Events All Edit ← ③
---------------------------------------------------	-------------------------------------------------------------------	----------------------------------------------------

Date Filter

Date Any dates

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

Time of Day Any
[Edit](#) ← ③

Included Columns
Person, Key, Lock, Event, Date, Source, Download Date

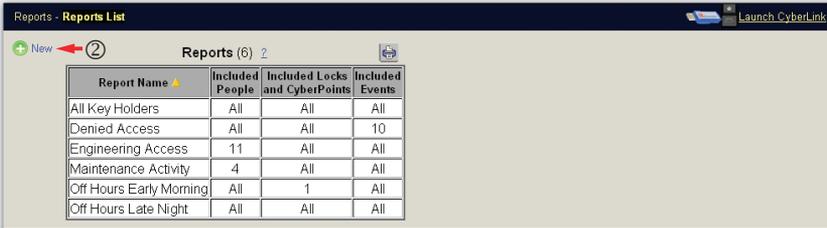
Sorting By Date (Descending)
[Edit](#) ← ③

Close Actions ▾

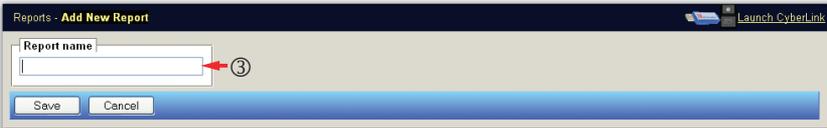
3. Click the *Edit* link in any of the frames to modify the associated report properties.

To add a report, follow these steps:

1. Click on the *Reports* menu header.

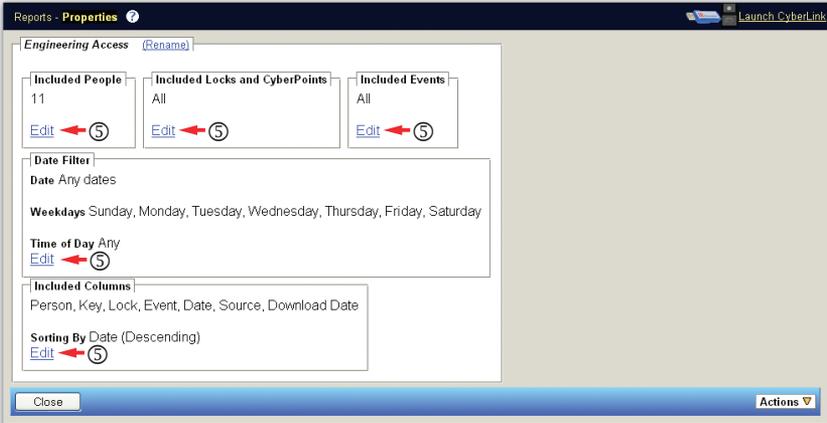


2. Click the *New* link.



3. Give the report a descriptive name.

4. Click the *Save* button.



5. Click the *Edit* link in any of the frames to specify the associated report properties and save each edit.

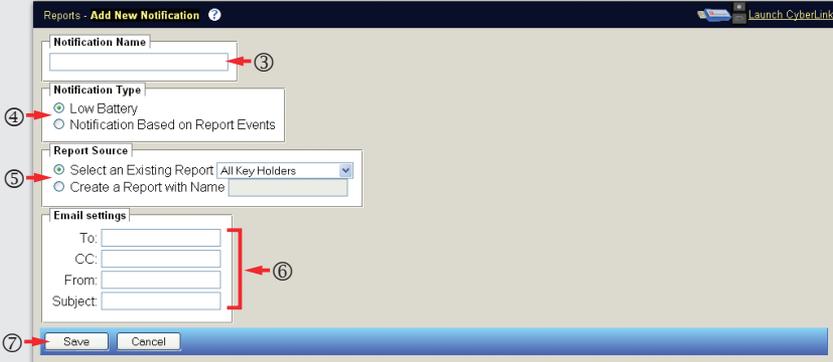
To add a notification, follow these steps:



1. Select *Notifications* from the *Reports* menu.



2. Click the *New* link.



3. Give the notification a descriptive name.

4. Choose the notification type.

5. Select a report source for the notification.

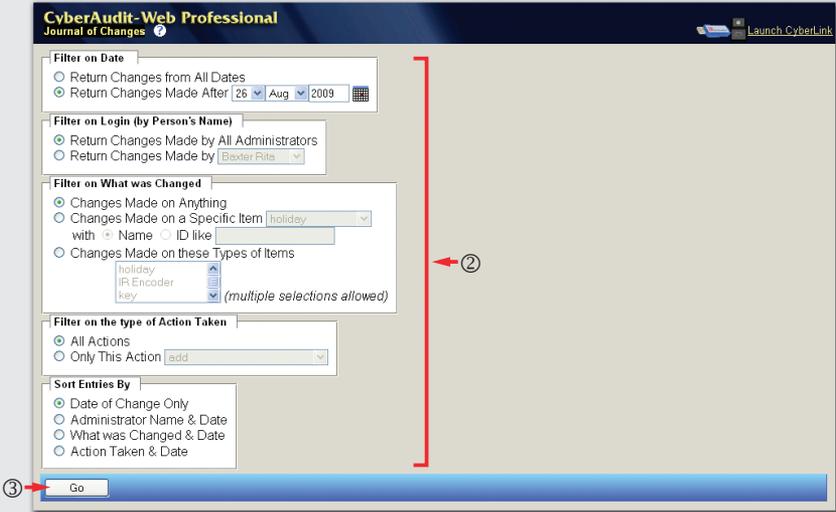
6. Specify parameters for the email which will be sent.

7. Click the *Save* button.

To view the journal of changes, follow these steps:



1. Select *Journal* from the *Reports* menu.

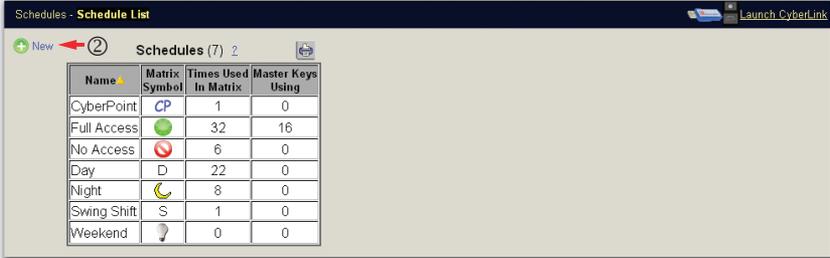


- 2. Specify filters and sorting as desired.
- 3. Click the *Go* button.

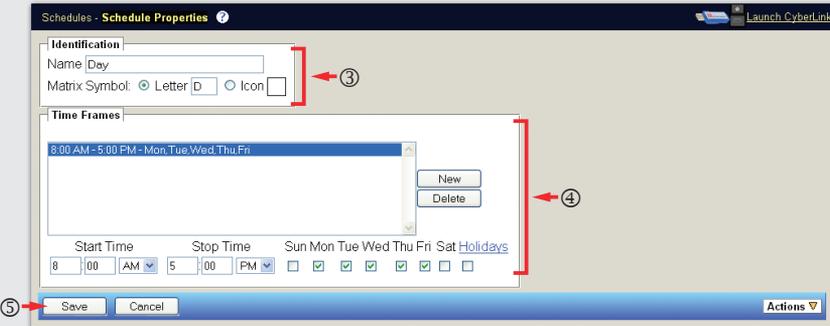
Schedules Operations

To create a new schedule, follow these steps:

1. Click the *Schedules* menu header.



2. Click the *New* link.

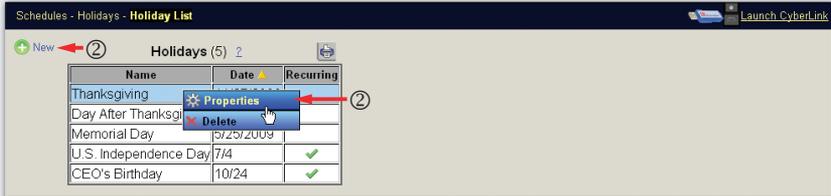


3. Give the schedule a descriptive name and choose a letter or icon to represent it in the Access Matrix.
4. Add time frames to allow access. If access will extend past midnight, split the time into one time frame that ends at midnight of the start day and a second that begins at midnight of the following day and ends when access should stop. CyberAudit-Web automatically translates times of 0:00 or 24:00 as the beginning of the following day.
5. Click the *Save* button.

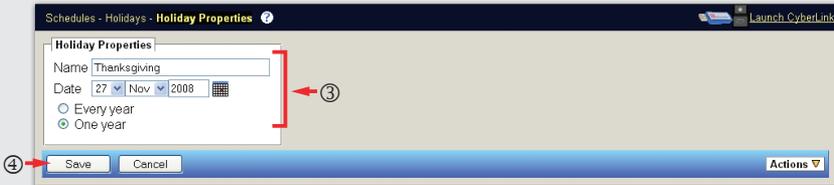
To add or edit a holiday, follow these steps:



1. Select *Holidays* from the *Schedules* menu.



2. To add a new holiday, click the *New* link. To edit an existing holiday click it in the table and select the *Properties* option from the operations pop-up menu.

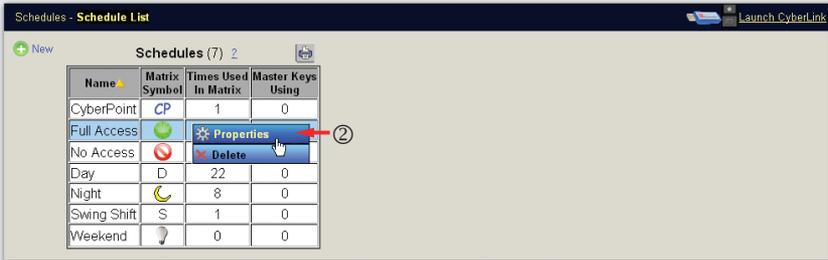


3. Specify the properties of the holiday as needed.

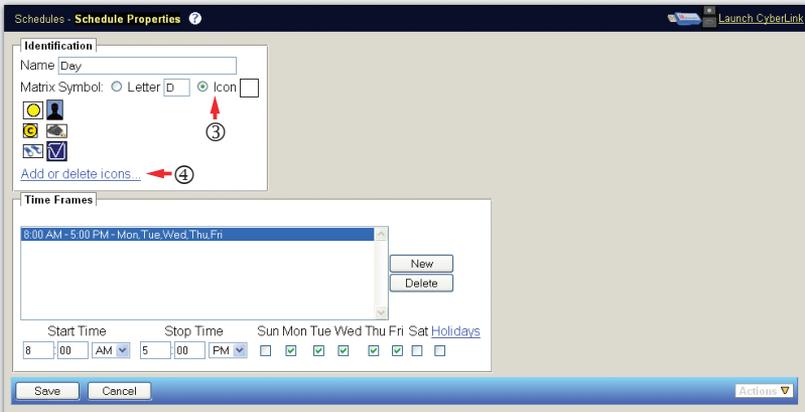
4. Click the *Save* button.

To add or delete schedule icons, follow these steps:

1. Click the *Schedules* menu header.



2. Click any row in the table and select *Properties* from the operations pop-up menu.

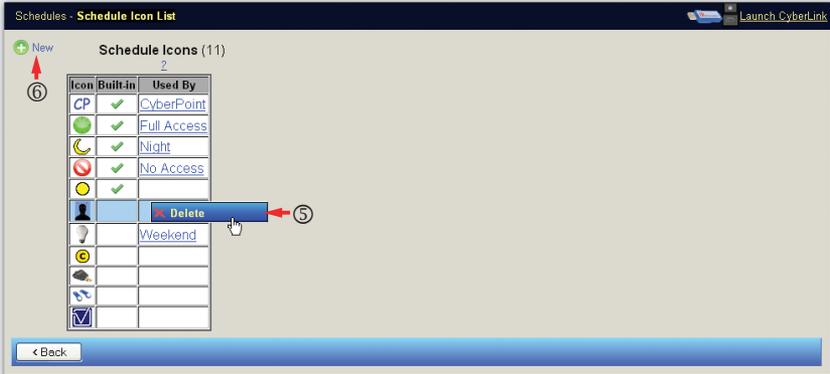


3. Select the *Icon* option in the *Identification* frame.

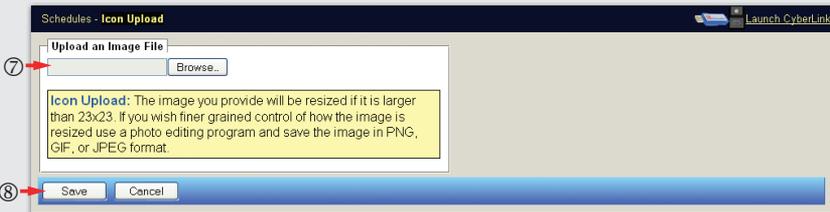
4. Click the *Add or delete icons* link.

(Continues on next page . . .)

(... continued from previous page)



5. Click the table row for any icon and select *Delete* from the operations pop-up menu to remove that icon.
6. Click the *New* link to add an icon.

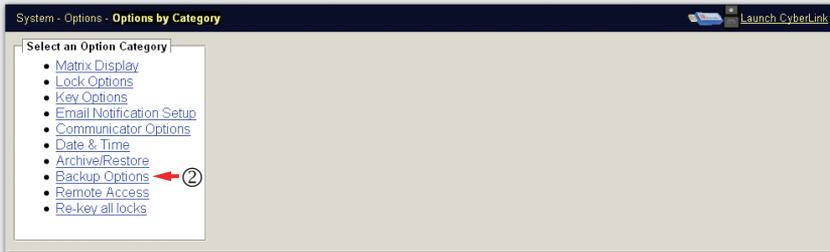


7. Type in or browse to the location of the icon file. CyberAudit-Web supports *.png*, *.gif*, and *.jpg* formats. Images larger than 23 x 23 pixels will be resized.
8. Click the *Save* button.

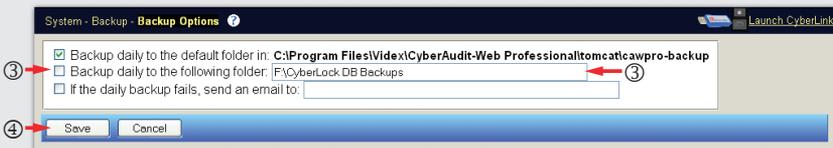
Database Backup and Restore Operations

To change the save location of automatic daily backups, follow these steps:

1. Click the *System* menu header.



2. Click the *Backup Options* link.



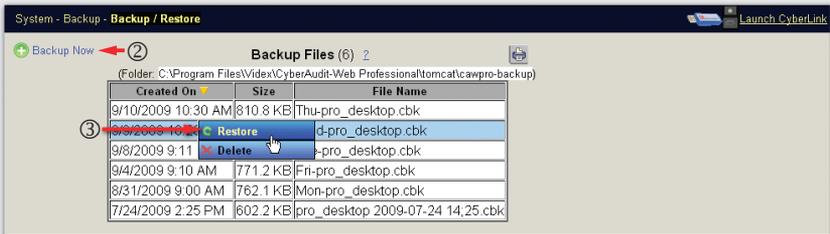
3. Select the *Backup daily to the following folder* option and specify a location. It is recommended to write backup files to a location other than the host computer, in case of hardware failure.

4. Click the *Save* button.

To perform a manual backup or restore of the database, follow these steps:



1. Select *Backup* from the *System* menu.



2. To perform a backup, click the *Backup Now* link.

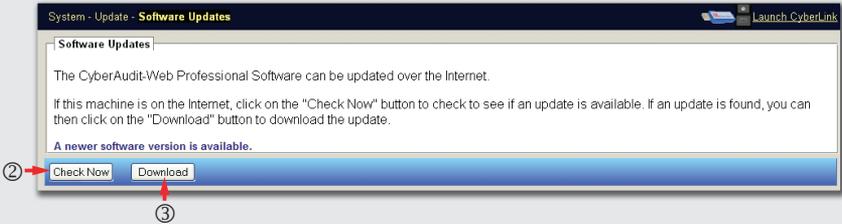
3. To restore a backup file, select *Restore* from the operations pop-up menu.

Miscellaneous Operations

To update the CyberAudit-Web Professional software, follow these steps:



1. Select *Update* from the *System* menu.



2. Click the *Check Now* button.

3. If an update is found, click the *Download* button.

4. Run the installer and follow the prompts.

To log in to CyberAudit-Web Professional, follow these steps:

1. Double-click on the  icon, located on the desktop (Windows) or in the Tomcat preferences pane (Macintosh.)



2. Enter an administrator login and password.
3. Click the *Log In* button.

Additional Information

This chapter contains information which isn't essential to understanding how to use CyberAudit-Web, but may be useful for understanding how it works.

Glossary of Terms

Access Code – An access code is an encrypted password that is programmed into locks and keys. A CyberKey must present one of these access codes to the CyberLock in order to gain access. CyberAudit-Web Professional uses two access codes in locks. The codes are either manually entered or come from a Grand Master CyberKey.

Access Matrix – The CyberAudit-Web Access Matrix displays people and CyberLocks in a grid format. Schedules are designated in the common square where a key and lock meet.

Administrator – Administrators are people with access to CyberAudit-Web, who may view audit trails and make changes to components in the system.

Archive – A set of Audit Trail records and Change Logs that have been removed from the visible sections of the database. Archived information can be restored to the database.

Audit Trail – The audit trail is the activity recorded by the CyberKey and the CyberLock. Each audit trail record typically contains information about an event that occurred within the lock or key. It also includes the date and time that the event happened. There are also Authorizer and IR Encoder audit trails. These show activity at the Keyports as well as network communication issues.

Authorizer – A device for updating CyberKeys and retrieving logs from CyberKeys. An Authorizer can interact with CyberKeys without a real-time connection to a database. CyberAudit automatically retrieves and sends information to Authorizers as needed.

See also: *LAN Authorizer* and *Web Authorizer*.

Brush – A stainless steel wire brush available from CyberLock vendors used for cleaning locks and keys. Instructions for cleaning locks are available from CyberAudit-Web’s context help.

Change Icon – This icon (🟡) is shown on most list and properties pages. It indicates that the settings of a lock, key, or Authorizer have changed in CyberAudit-Web but the item still needs to be updated.

Comm Log – A record of the communications an object has had with the database. For keys, this is when a communicator is contacted. For locks, this is when a lock is touched by either a CyberLock Programmer or Grand Master.

Communicators – Communicators are the devices by which CyberKeys and CyberLocks are downloaded and programmed. There are four categories of Communicators: Authorizers, IR Encoders, Programming Jobs, and Stations.

Configuration File – A special file that contains settings for a Web Authorizer. This file is saved to a USB flash drive and physically transferred to the Web Authorizer.

Control Key – A type of CyberKey that is used to install or remove interchangeable core cylinders. It has a special tip that engages the cylinder retention mechanism. Like a regular CyberKey, it must have permissions to open a lock. This is also called a core key or a change key.

CSV (Comma Separated Values) File – A text file in which each line represents one item, and fields describing that item are separated by commas. Most spreadsheet applications can export in this format. CyberAudit-Web uses this type of file to import people and locks.

CyberAudit-Web Professional – A web-based version of CyberAudit that is designed for medium size CyberLock installations of up to 500 keys and 500 locks. Videx also offers software for smaller and larger installations.

CyberKey – An electronic key used to open CyberLock cylinders. CyberKeys contain three levels of intelligence:

- Encrypted access codes which provide security.
- Access privileges for the key holder.
- Audit trail records of up to 3900 events.

CyberKey Recharging Station – A standalone docking station (not connected to CyberAudit-Web) that charges one CyberKey Rechargeable at a time. It connects to a wall outlet using the standard Videx 12V DC, 300mA transformer.

CyberLink – A Java client application that connects an IR Encoder or USB Station to CyberAudit-Web.

CyberLock – An electronic version of an existing mechanical lock that provides access control and an audit trail for many types of lock hardware. No wiring is required. There are currently over 240 designs.

CyberLock Programmer – A type of a CyberKey that is designed to program information into locks, download the audit trails from locks or reset locks. It can program up to 1250 locks at a time. It can download 3 to 7 lock audit trails at a time. Unlike a CyberKey, Programmers will not open a lock.

CyberPoint – CyberPoints are electronic tags designed to serve as data checkpoints during security guard tours. CyberPoints have no editable settings and require no programming. When a programmed CyberKey touches a CyberPoint, the key beeps three times. CyberPoints may be added to CyberAudit-Web so that they can be downloaded for reporting purposes.

Delay – A waiting period required of keys before a lock will open. The CyberKey keeps track of the time and will beep to let the user know when the lock can be opened. Delays cannot be combined with multiple-key access. Master keys ignore the delay setting.

Disabling Point – A lock that has one or more keys in its lost key list. Keys in the list will be disabled upon contact. They will cease to work in any lock until reprogrammed as a non-lost key.

Emergency Key – A key that has been granted temporary access to all locks in the system by a configured Grand Master key. Temporary access time ranges include 1 to 64 minutes, 1 to 24 hours, or 1 to 127 days. Emergency keys are referenced under the *System Keys* section of the text.

Expiration – A date and/or time after which a CyberKey will stop working. It must then be reauthorized by an Authorizer, IR Encoder, or Station. An expiration can be a fixed date, fixed to a calendar period, or based on the re-authorization time.

Filter – A mechanism for finding specific records or limiting the amount of data shown on the screen. There are three categories of filters in CyberAudit-Web: *Access Matrix*, *Keyword*, and *Tag*.

Grand Master Key – A Grand Master key can program CyberLocks and CyberKeys. It can be configured to behave like a CyberLock Programmer. It also can be configured to create time limited “emergency” master keys.

See also: *CyberLock Programmer*

Holidays – Holidays are utilized as schedule exceptions in CyberAudit-Web. They do not have to be literal holidays – any day of the year can be designated as a holiday. The rules specified for holidays in a schedule time frame take priority over normal access. For example, if access is allowed on Wednesdays, but not on holidays, then the key will not be granted access on Wednesdays that are also holidays. The system can have up to 126 holidays. Holidays may be set as one-time or occurring every year.

Interchangeable Core – A type of lock cylinder that can be removed without disassembling the door hardware. Used to make mechanical re-keying easier. Interchangeable core CyberLocks never need to be removed since all CyberLocks can be electronically re-keyed. Videx has cylinders that are physically compatible with the Best and Schlage interchangeable cores. These are the CL-SF03 and CL-LF01 respectively.

IR Encoder – A custom USB to Infrared adapter made by Videx.

IR Encoders use the CyberLink software. Unlike a regular IR adapter, the IR Encoder shows up as a drive in the “My Computer” window.

Issue Number – An issue number is a unique, 8-digit number generated by the system that acts as a temporary placeholder for some item. Items that can be represented by issue numbers include CyberKeys, IR Encoders, and Stations. CyberKey issue numbers are linked to a user’s record. The user takes any CyberKey not already in the system and puts it into or near the communicator. When prompted, the user enters the issue number. When the number has been correctly entered, the CyberKey will be programmed according to the settings associated with the issue number. The key serial number will take the place of the issue number in the database.

Journal of Changes – Whenever a CyberAudit-Web administrator makes changes to the system, it is logged in the database. A journal may be viewed of all records or filtered records based on several categories. It includes what was changed, who changed it, and when the change was made.

Key Compatibility, Part Numbers – Currently, these CyberKey models are compatible with CyberAudit-Web: CK-U4, CK-U5, CK-IR6, CK-IR7, CK-RCG, CK-RXD, CK-P3, CK-P4 and CK-GM. Some CK-P2s and some CK-C1s are also compatible. Some features require IR keys or new firmware.

Keypoint – The Keypoint provides the user interface for the CyberKey Authorizer. It consists of a numeric keypad, an LED display, and a docking receptacle for CyberKeys.

Key Retaining Locks – Some CyberLocks will not release a key when they are in the open position. This ensures that users return the lock to the closed position.

Key Types, Hardware –

- CyberKey Plus
- Cellular CyberKey
- CyberKey Rechargeable
- CyberKey
- CyberLock Programmer
- Control Key

The CyberKey Plus, CyberKey Rechargeable, Cellular CyberKey and the Control Key can be configured into any of the types listed in the “*Key Types, Software*” entry.

Key Types, Software – User Key, Master Key, Reset Key and Lost Key. See individual entries. Physically, these are all standard CyberKeys.

LAN Authorizer – An Authorizer which connects to the CyberAudit-Web server via either an Ethernet network or a modem.

Lock List – A list of lock IDs paired with a schedule and stored in a CyberKey’s memory. It controls if and when a key may open a given lock. The lock list is programmed into the key with each communication. It may also contain additional information such as a lock to download or to locks to treat as CyberPoints.

Lock Programming Devices – CyberLock Programmers, USB Programmers, or Grand Master keys, if so configured. See individual entries.

Login – A login is an identifier and password given to an administrator to run the CyberAudit-Web software. Administrator logins have these properties:

- Login - A unique combination of 4 or more characters used to identify the person attempting to log in to CyberAudit-Web.
- Password - A secret combination of 4 or more characters used to validate the attempted login.
- Person - Each Administrator login must be linked to a personnel record in the CyberAudit-Web database.
- A set of permissions.

Lost Key – A CyberKey can be designated as lost in a CyberLock’s memory. A CyberLock will not allow access to a lost key even if that key believes it has permission to open the lock.

See also: *Disabling Point*.

Master Key – A software setting that allows a CyberKey access to all locks in the system. A master key has either full access or a restricted time range. Master keys can also have a list of locks for which they behave like a standard user key.

Master Key Schedule – A special schedule that restricts when a master key will function. It is essentially an on/off schedule for the key that is checked prior to any other operation.

Mortise – A type of cylinder often used in deadbolts. Videx makes 1 1/8” and 1 1/4” lengths, covered and uncovered.

Multi-Key Access – A lock with this setting requires more than one CyberKey to open it. Master keys ignore this setting.

Notification – a report sent by email. After a CyberKey is downloaded, the notification process scans the newly arrived data to determine if it matches the criteria of the report it is based on. If so, an email is generated.

Password – Text that is encrypted and provides security for a CyberLock installation. This text can be composed of letters and/or numbers. There are up to 3 types of passwords - system passwords, access passwords and login passwords. The system and access code passwords are the basis for the codes used by keys and locks but are not used to log in. Users do not enter these if a Grand Master was used during setup.

PIN – Personal Identification Number. A PIN can be assigned to a person for use in conjunction with an Authorizer, IR Encoder or Station to provide an additional level of security. The correct PIN must be entered before the user's key is re-authorized.

Position Box – The box found in the upper left of the Access Matrix page. Users may drag the teal box to change which section of the people and locks are shown.

Programming Job – Programming Jobs are a way by which CyberLocks can be configured, downloaded or reset by CyberAudit-Web. Each job is designated by a job number which is used to identify it to a CyberKey Authorizer or IR Encoder. Any Programmer can be assigned any programming job.

Reset Key – When a reset key touches a lock in the system, it clears the access codes and configurations from the lock, thereby resetting it to the original (unprogrammed) factory configuration. A reset key can be made from any standard CyberKey.

Schedule – A set of access times and rules. A standard schedule includes up to 7 access times.

Schedule, CyberPoint – This schedule will not open locks. Instead, the key treats the lock like a CyberPoint. It is commonly used for guard tours.

Schlage – A lock manufacturer. The Videx CL-6P1 and CL-6P3WR replace a Schlage 6-pin key-in-knob cylinder. The Videx CL-LF01 replaces the Schlage Interchangeable core.

SDK – The Software Development Kit allows all text and messages seen in the user interface to be translated into languages other than English.

Serial Cable, Videx – A custom cable that is used to update LAN Authorizer firmware. The Authorizer interface is a telephone jack connector (RJ-11). The PC interface is available in either 9-pin or 25-pin serial connectors. Pin-out specifications are available from Videx Technical Support.

System Keys – A special type of key used for specific tasks in a CyberLock system. CyberAudit-Web Professional version 1.1 has Grand Masters and reset keys. See the individual entries.

Tag - A free-form way to organize people and locks into logical categories. People and locks may have any number of tags. Access may then be granted by person to lock tag, lock to people tag, and/or people tag to lock tag.

Tamper Delay – A “tamper delay” is a wait period that a lock may require of keys before it will communicate. It may occur when the lock denies entry to a key. For each denied key touch, this delay is incremented; it should never exceed 20 seconds. The first authorized key to touch the lock will clear the delay time after the delay is served. After it gains access, subsequent authorized keys will be unaffected.

Time Frame – A definable time range having start and stop times and selectable days of the week, plus holidays. Time frames are a component of schedules.

USB Station – A communicator device which attaches to a computer’s USB port. It uses the CyberLink application to communicate with the CyberAudit-Web server, and can also be used as a charging station for rechargeable CyberKeys.

User Key – A general term describing a standard CyberKey that has not been programmed as a master key.

Web Authorizer – An Authorizer which uses DHCP to obtain an IP address and can communicate with the CyberAudit-Web server over the Internet, without requiring the special setup required with LAN Authorizers.

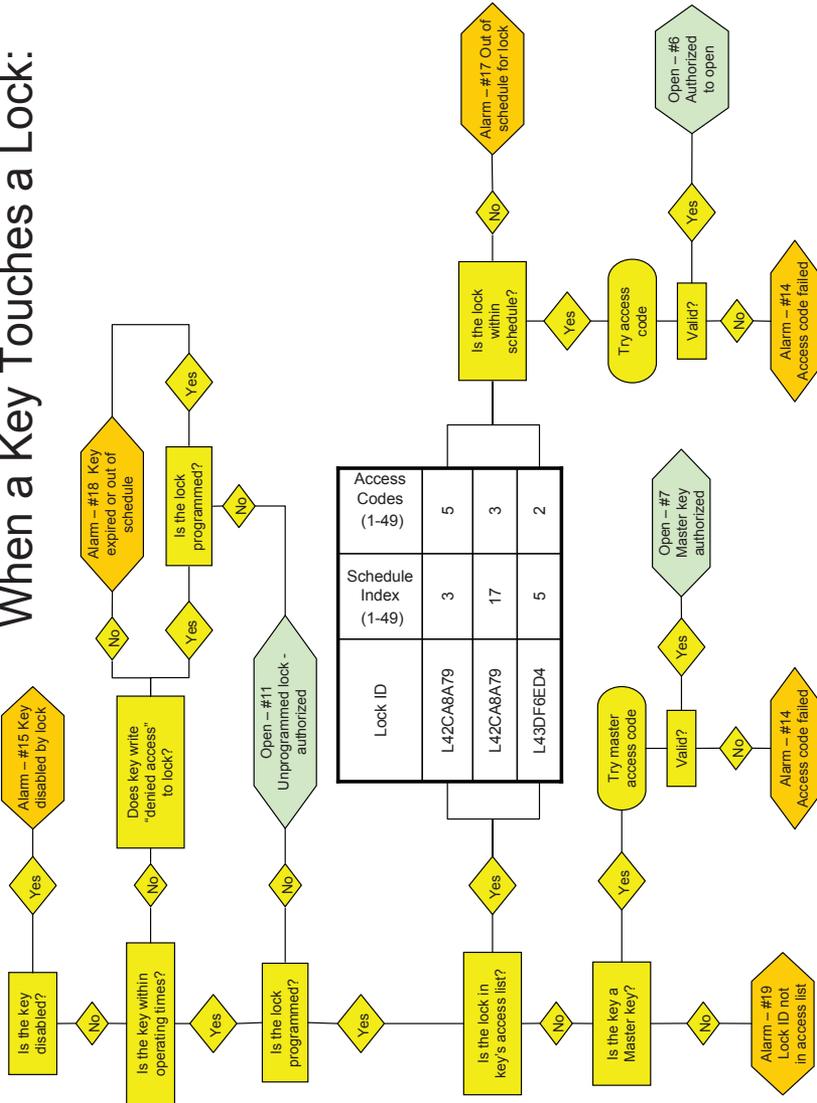
Web Station – A docking station for CyberKeys than can be used as a USB Station, or can be connected to a network using TCP/IP to communicate with the CyberAudit-Web server.

Yale – A lock manufacturer. The Videx CL-6P2 and CL-7P1 replace the Yale 6-pin and 7-pin key-in-knob cylinders, respectively.

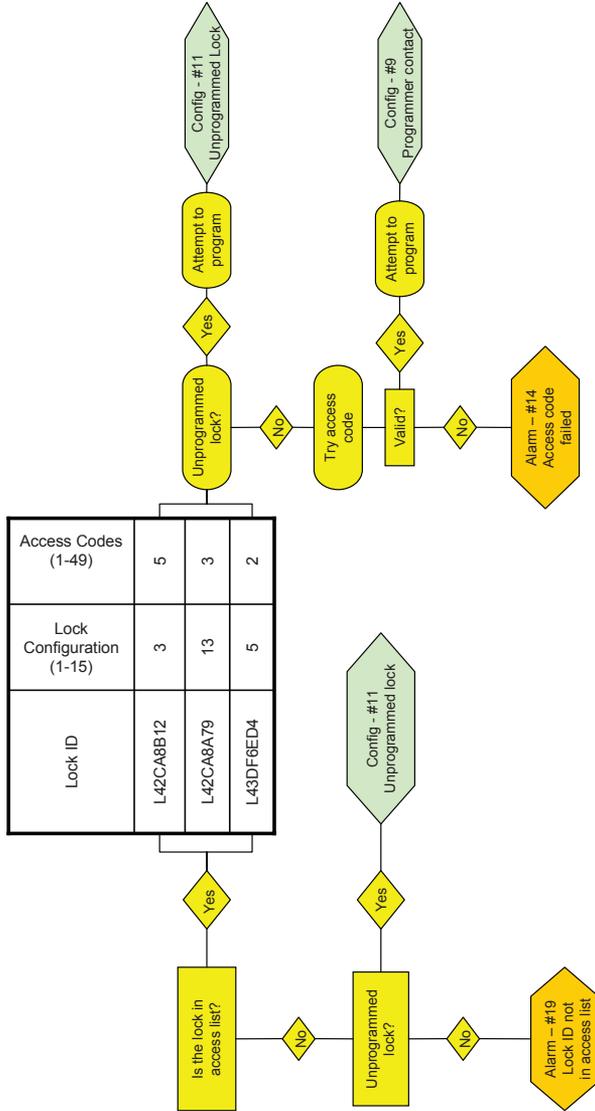
Lock Contact Diagrams

Note: Alarm numbers refer to the Audit Trail Event Descriptions, discussed later in this chapter.

When a Key Touches a Lock:



When a Programmer Touches a Lock:



CSV File Format Descriptions

For Importing Locks

Field	Required	Information
Lock ID	Yes	Starts with 'L', followed by 8 hexadecimal digits. Lower case letters in the ID will be promoted to upper case.
Lock Name	No	If left blank, the CyberLock or CyberPoint will be named with the ID. Names may be a maximum of 128 characters.

For Importing People

Field	Name	Max.	Details
1	Name	64	
2	Department ID	64	
3	External ID	255	This field is not displayed in CyberAudit-Web Professional and may be left empty.
4	Email Address	255	
5	Address	255	
6	Phone Number	64	
7	PIN	8	Must be a valid 4-8 digit number.
8	Notes	255	

Modem Control

The following is a table of control characters that may be entered in the dial string of modem Authorizers, in addition to the phone number:

Character	Meaning
*	The “star” digit (tone dialing only)
#	The “gate” digit (tone dialing only)
A-D	DTMF digits A, B, C and D. Some countries may prohibit the sending of these digits during dialing.
W	Wait for dial tone - the modem will wait for dial tone before dialing the following digits. If dial tone is not detected within 25 seconds (US) or 2 seconds (W-class), the modem will abort the rest of the sequence.
@	Wait for silence - the modem will wait for at least 5 seconds of silence in the call progress frequency band before continuing with the next dial string parameter. If the modem does not detect a period of 5 seconds of silence before 25 total seconds has elapsed, the modem will terminate the call attempt.
,	Dial pause - the modem will pause for 2 seconds before dialing the following digits.
()	Ignored - may be used to format the dial string.
-	Ignored - may be used to format the dial string.
<space>	Ignored - may be used to format the dial string.
All other	Invalid character - will be ignored.

Event Descriptions

Audit Trail Events from CyberKeys

- *CyberPoint Contact*: The key contacted a CyberPoint or contacted a lock using a CyberPoint schedule.
- *Software Reset*: The key was reset at the factory during manufacture or service. Lock column contains voltage data from battery and capacitor. Applies to CyberKeys manufactured after October 2008.
- *Low Battery*: The key discovered its battery voltage was below the threshold during one of its periodic reads or during a lock opening. Lock column contains voltage data from battery and capacitor. Applies to CyberKeys manufactured after October 2008.
- *Dead Battery*: The battery voltage dropped below operating voltage during one of its periodic reads or during a lock opening. Lock column contains voltage data from battery and capacitor. Applies to CyberKeys manufactured after October 2008.
- *E2 Access*: Failure to read memory. Applies to CyberKeys manufactured after October 2008.
- *Scheduled Battery Reading*: The key reads and records its battery level daily, after midnight local time. Lock column contains voltage data from battery and capacitor. Applies to CyberKeys manufactured after October 2008.
- *Write Event Failed*: Failure to write to memory. Applies to CyberKeys manufactured after October 2008.

Audit Trail Events

- *(-1) CyberPoint Contact:* The key contacted a CyberPoint, or contacted a CyberLock using a CyberPoint schedule.
- *(1) Power restored:* The battery was replaced in the key.
- *(2) Multikey access key 1:* The first key for multi-key access was accepted by the lock.
- *(3) Multikey access key 2:* The second key for multi-key access was accepted by the lock.
- *(4) Multikey access key 3:* The third key for multi-key access was accepted by the lock.
- *(5) Multikey access key 4:* The fourth key for multi-key access was accepted by the lock.
- *(6) Authorized to open:* *
- *(7) Master key authorized:* *
- *(8) Authorized to open (bypass multikey or delay):* The key bypassed a lock's multi-key or delayed opening setting, using the option in its schedule.
- *(9) Programmer or CyberPoint contact:* The lock was contacted by a CyberLock Programmer, or was contacted by a CyberKey using a CyberPoint schedule type.
- *(10) Lock reset attempted:* A reset key attempted to reset a CyberLock.
- *(11) Unprogrammed lock - authorized:* The key accessed an unconfigured CyberLock.
- *(12) No lock ID - authorized:* This event should never occur. It indicates that the lock was not set up with an ID. It cannot be programmed and will not function in a CyberAudit system.

(Continues on next page . . .)

(. . . continued from previous page)

- (13) *Key in lock more than 1 minute -or- removed from lock:* By default, a record is made when a key is left in a lock for more than one minute. Keys in a system may be configured to report all “removed from lock” events. The setting affects the text for this event.
- (14) *Access code failed:* This event type occurs if a lock contains different access codes than expected by the database because it has been moved to or from another database. It also occurs if a lock has been updated with new access codes but the key has not, or if a lock does not contain the access code that a master key is programmed to use.
- (15) *Key disabled by lock:* The key was designated as “lost” and the lock was designated as a disabling point. When the key contacted the lock, the lock deactivated the key’s functionality.
- (16) *Hardware mismatch - access denied:* This event indicates hardware incompatibility between a lock and a key. Currently, there are no incompatible locks and keys.
- (17) *Out of schedule for lock:* The key contacted one of the locks in its access list outside of the time frames defined in the applied schedule.
- (18) *Key expired or out of schedule:* The key attempted to open a lock outside of its scheduled operating time or after it had expired.
- (19) *Lock ID not in access list:* The key has no permissions to access the lock.
- (20) *Clock stopped:* This event is recorded when power is supplied to a key that has been without it for one minute or more.
- (21) *Access count expended:* This event occurs when one-time access and fixed-use countdown schedules are used up. These are not available in CyberAudit-Web Professional.

Keypoint Messages Generated by LAN Authorizers

- *PIN#* - Key record in the Authorizer requires a PIN before key will be enabled.
- *WAIT* - The Keypoint is waiting for the Authorizer to respond.
- *KEY NOT FOUND* - This key does not have a key record in the Authorizer and the Authorizer does not have a designated host server to contact (the Authorizer has not been configured).
- *HUBREADY* - The Authorizer successfully completed a power-on reset.
- *REBOOT HUB* - The Authorizer is restarting after power-on.
- *READY* - The Authorizer is ready but it is not connected to a network device. This would be normal for a remote modem connection.
- *READY ** - The Authorizer is ready and connected to a network device.
- *KEYREADY* - The key has been programmed and is ready to use.
- *LOW BATT* - The Authorizer has determined that this key has a low battery.
- *BAD PIN#* - The PIN input does not match the expected PIN for the key.
- *WRONG PW* - The database identifier between the Authorizer and the key do not match.
- *KEY FAIL* - Keypoint was unable to communicate with the key.
- *COMMFAIL* - No response from the CAW server when Authorizer attempted to contact it.
- *LINKUP HOST* - The Authorizer is attempting to contact the CAW server. Typically this occurs to get information to program a key that is not in the Authorizer's memory.

(Continues on next page . . .)

(. . . continued from previous page)

- *HUB BUSY WAIT* - This message is displayed when the server has instructed the Authorizer to erase one of its databases, schedules, key records, holidays, etc.
- *KEYPAD DISABLED* - The server has temporarily disabled the Keypoint during an update. This temporarily prevents a key from being processed.
- *CLOCK STOP* - The Authorizer's clock has stopped, typically because of an extended power loss. It will continue to display this message when a key is inserted into the Keypoint until the server updates the Authorizer's clock.
- *KEY LOCKED* - The Authorizer has reached the number of times it will allow retrying a PIN number.
- *LOAD HUB FIRMWARE* - Displayed during the process of updating Authorizer firmware.
- *UPDATE BOOTLOAD* - Displayed during the process of updating Authorizer firmware.
- *SEC CODE* - The Authorizer is prompting for a security code.
- *BAD CODE* - The security code does not match the one the Authorizer is expecting.
- *DIAL MODEM* - Authorizer is attempting to connect with another Authorizer.
- *INIT MODEM* - Authorizer is loading the modem from its stored configuration.
- *HANGUP MODEM* - Authorizer is terminating its modem connection.
- *CONNECT* - Authorizer has established a modem connection with another Authorizer.
- *RING* - The Authorizer being called displays this message.
- *NO CARRIER* - Connection dropped by remote.
- *MODEM ERROR* - Internal error. Possible hardware or configuration problem.
- *NO DIAL TONE* - No phone line detected when attempting to dial out.

Keypoint Messages Generated by Web Authorizers

- *WAIT* - The Keypoint is waiting for the Web Authorizer to respond.
- *LOADING* - The Web Authorizer is loading software components from memory.
- *STARTING* - The Web Authorizer is starting software components, acquiring the network, and starting the application.
- *USB SCAN* - After starting the application, the Web Authorizer checks its USB ports for a USB flash drive and searches for a configuration file to load.
- *REMOVE USB* - If a USB flash drive is present after the scanning process is completed, the Web Authorizer will display this message until the USB flash drive is removed.
- *READY* - The Web Authorizer is ready, but has not yet synchronized with the CyberAudit-Web server.
- *READY ** - The Web Authorizer is ready and has successfully synchronized with the CyberAudit-Web server.
- *X__ 192* - The Web Authorizer is in IP address configuration mode. The placement of the *X* indicates the section of the IP address that is being edited.
- *INVALID#* - An invalid octet (a number greater than 255) was entered during IP address configuration.
- *NOSERVER* - The Web Authorizer has no information about how to contact the CyberAudit-Web server because it has not been configured yet.
- *CLEARING* - The inserted CyberKey is resetting the audit trail event counter and preparing to accept a configuration.
- *READING* - Data is being downloaded from the inserted CyberKey.
- *VERIFY* - The Web Authorizer is confirming the successful configuration of a key.
- *NOT VERIFIED* - The Web Authorizer was not able to verify that the key received the intended configuration.

(Continues on next page . . .)

(. . . continued from previous page)

- **BUSY** - The Web Authorizer is processing data received from the key or the server.
- **8 DIGITS** - An incorrect number of digits was entered for an issue number or job number (each must be 8 digits long).
- **WRONG KEY TYPE** - A different type of key than expected was inserted into the Keypoint.
- **KEY DENIED** - The inserted key may not be used with the mission number that was entered, either because the mission is unavailable or because the key cannot support the configuration. (CyberAudit-Web Enterprise only.)
- **KEY GONE** - The inserted key was removed from the Keypoint before communications were completed.
- **KEY COMMFAIL** - There was a communication failure between the key inserted in the Keypoint and the Web Authorizer.
- **MEMORY FULL** - The amount of available memory in the Web Authorizer has reached the minimum allowed. The Web Authorizer will no longer update keys.
- **INSERT KEY** - A 2-key input that requires the insertion of a CyberKey has been received.
- **ONLINE!** - The Web Authorizer successfully synchronized with CyberAudit-Web following the “22#” 2-key directive. See “2-Key Inputs for Web Authorizers,” later in this chapter.
- **SERVER COMMFAIL** - There either was no response from CyberAudit-Web when the Web Authorizer attempted to contact it, or the communications were interrupted.
- **SYNC...** - The Web Authorizer is attempting to synchronize with CyberAudit-Web. This will occur automatically every 30 seconds while the Web Authorizer is idle.
- **LOAD HUB FIRMWARE** - The Web Authorizer is in the process of updating its firmware.

(Continues on next page . . .)

(. . . continued from previous page)

- **SOFTWARE UPDATE** - The Web Authorizer is downloading an update from CyberAudit-Web.
- **UPDATE FAILED** - The download of an update from CyberAudit-Web failed.
- **UNKNOWN WEBAUTH** - The Web Authorizer contacted CyberAudit-Web, but the ID of the Authorizer was not recognized.
- **TIME OUT** - There was no response when the Web Authorizer attempted to contact CyberAudit-Web.
- **NO ROUTE** - The Web Authorizer is not able to reach CyberAudit-Web because it lacks the proper routing information.
- **CONNECT REFUSED** - The Web Authorizer was able to reach CyberAudit-Web, but CyberAudit-Web is not listening on the requested port.
- **SSL FAIL** - The Web Authorizer connected to CyberAudit-Web on the designated port, but was unable to establish the secure sockets layer.
- **DNS FAIL** - The Web Authorizer could not resolve the CyberAudit-Web domain name.
- **NET UNREACHABLE** - The Web Authorizer cannot establish a network connection. This happens if the network cable is unplugged. Allow up to 30 seconds for the Web Authorizer to re-establish a connection after the cable is plugged back in.
- **UNKNOWN NET ERR** - An unrecognized networking error occurred.
- **READ USB** - A USB drive was detected and is being read.
- **CONFIG APPLIED** - A configuration for the Authorizer was found and the changes have been made.
- **NO CONFIG** - A configuration for the Authorizer was not found on the USB drive.
- **NO USB** - No flash drive was found.

(Continues on next page . . .)

(. . . continued from previous page)

- **STARTING** - USB processing is complete and the startup process is continuing. This message is only displayed if a flash drive was found.
- **UPDATING** - No flash drive was found, but an auto update was detected and is being installed.
- **UPDATED!** - Displayed when the auto update has been successfully installed.

Keypoint Messages Generated by the Server

- **PLS WAIT** - A short period of time is expected after removing a key to allow the processing of the key's events from an Authorizer. The server will also display this message while issuing or missioning a key, or gathering status information.
- **COMMFAIL** - This message will be displayed by the server if an exceptional error occurred while the server programs a key.
- **LOOKUP** - The server is determining if the key is known to the system and if it should be issued, missioned, and/or dynamically programmed.
- **UNKNOWN KEY** - The server has not found the key ID in the database but has found the key's DB flag is set. This indicates that the key belongs to another database and should be rejected.
- **ISSUE#** - The server is prompting the user to input an issue number for this key.
- **ISSUE# OR MISSION#** - The server is prompting the user to input an issue number or a mission number for this key if missioning has been activated for the subsystem. (CyberAudit-Web Enterprise only.)
- **BAD ISSUE#** - The server has determined that the number input does not match any numbers in the system.

(Continues on next page . . .)

(... continued from previous page)

- **JOB# OR LOGIN#** - The server is prompting the user to input a job number or an administrator's login number for a programmer or Grand Master. (LOGIN# exists only in CyberAudit-Web Enterprise.)
- **BAD JOB#** - The server has determined that the number input does not match any JOB#s or LOGIN#s in the database.
- **PIN#** - If a PIN is required to program this key, the server will prompt with this message.
- **BAD PIN#** - The server has determined that the PIN input does not match the expected PIN for the key.
- **DISABLED** - The server has determined that this key has an active mission or is a deleted key. In both cases, CyberAudit-Web disables the key prior to re-issuing.
- **CLEARING** - The key is zeroing the audit trail events and preparing the key to accept a configuration.
- **READING** - The server will display this message while gathering information for programming this key.
- **WRITING** - This message is displayed while the key's new configuration is being written to it.
- **KEYREADY** - The key has been configured and is ready to use.
- **INSERT KEY** - The server will prompt with this message in response to a 2-digit input requesting an ID, (55#) battery voltage check, (66#) or next expiration (77#.) Applies to Web Authorizers only.
- **LOW BATT** - The server has determined that this key has a low battery.
- **NO READING** - The server can not read the battery voltage of this key.
- **DB FLAG ERROR** - The server was unable to check the database flag for this key.
- **OLD KEY REMOVE** - The server has determined that this key has firmware too old to be used by CyberAudit-Web.
- **KEY DISABLED** - The server has determined that this key was designated as lost and is now disabled.

2-Key Inputs for Web Authorizers

- 11# - Displays the Web Authorizer ID
- 22# - Directs the Web Authorizer to synchronize with CyberAudit-Web. If successful, the Keypoint will display “*ONLINE!*”
- 33# - Displays the current date and time from the Web Authorizer’s clock.
- 55# - Special function for displaying the ID of a CyberKey. The Keypoint will prompt “*INSERT KEY.*”
- 66# - Special function for displaying the battery voltage of a CyberKey. The Keypoint will prompt “*INSERT KEY.*”
- 77# - Special function for displaying the next expiration date and time of a CyberKey. The Keypoint will prompt “*INSERT KEY.*” If the key is not part of the same system as the Web Authorizer, the Keypoint will display “*UNKNOWN KEY.*”

CyberKey Support Information

To change the battery in a CyberKey with replaceable batteries, follow these steps:

1. Use a ball-point pen to depress the upper lobe of one of the latches which holds the battery cap in place.



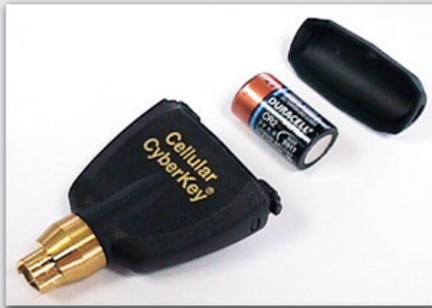
(Continues on next page . . .)

(... continued from previous page)

2. Lift the cap up, then toward the latch on the opposite side.



3. Replace the battery. Note the proper polarity.



4. Hook one side of the battery cap onto a latch, then snap the opposite end into place over the other latch.



Rechargeable CyberKey Flash Patterns

Event	Green LED	Red LED	Notes
Access Granted	Steady On	Off	LED remains on for duration of solenoid hold time or until key is removed from lock.
Access Denied - Expired or Out of Schedule	Off	Long flash once per second	
Key Expired	On for 1 second	3 flashes	Occurs after above pattern, if <i>“flash after expiration”</i> is set. Pattern repeats until key is updated or battery is drained.
Access Denied - No Permissions or Wrong Access Code	Off	Rapid flash	
Battery OK	One flash every 8 seconds	Off	
Battery Low	Off	One flash every 8 seconds	Occurs until key is placed in charger or battery is drained.
Battery Charging	Off	Short flash once per second	Occurs while in charger or idle in USB Station.

Event	Green LED	Red LED	Notes
Battery Charged	Short flash once per second	Off	Occurs while in charger or idle in USB Station.
Battery Dead	Off	Off	
Communications	Irregular flashing	Irregular flashing	
CyberPoint Contact	Steady On	Rapid flash	
Download Lock	Steady On with slight flicker	Steady On with slight flicker	
Resetting a Lock (As a Subsystem Reset Key)	Steady On	3 flashes	
Delay Instruction Received from Lock - Key in Lock	Steady On	3 flashes	
Delay Time Has Been Served - Key out of Lock	On for 1 second	3 flashes	Pattern continues for 3 to 5 minutes.
Key Left in Lock	Rapid flash	One flash after each minute	
Multi-Key Access	Steady On	Three flashes for each key after the first	
Key Disabled	On for 1 second	3 flashes	Pattern repeats until key is updated or battery is drained.

CyberKey Tones and Descriptions

Tone	Description	Applies to
An alarm (8 second siren).	Access denied – indicates the key does not have permission to open or program the lock. Download the key and refer to the resulting audit trail to view the specific cause.	CyberKeys, Programmers, Grand Masters
A single beep once every 8 seconds.	The battery has dropped below the low voltage threshold.	CyberKeys, Programmers, Grand Masters
A single beep once per minute until the key is removed from the lock.	The key has been left in a CyberLock for more than one minute. It will beep until the CyberKey is removed from the lock.	CyberKeys, Programmers, Grand Masters
A single beep followed by a delay, then a single beep every second for approximately five minutes, or until the CyberKey touches the lock. (Applies to CyberKeys made after July of 2005.)	The CyberKey has served the delay setting that was programmed into a CyberLock.	CyberKeys
A double beep for the first CyberKey, and a single beep for each CyberKey thereafter.	The CyberLock has been programmed using multiple-key access (2, 3, or 4 keys).	CyberKeys

Tone	Description	Applies to
A single beep once per second that does not stop after five minutes.	The CyberKey has expired.	CyberKeys
A quick buzz.	The CyberLock Programmer successfully read the serial number of a new or reset CyberLock.	Programmers
A buzz with no beeps.	The contacted CyberLock is unprogrammed.	CyberKeys configured to program locks, Programmers, Grand Masters
A buzz with 3 beeps.	A new configuration has been transmitted to a programmed CyberLock.	Programmers
A long buzz with no beeps.	The audit trail of a reset CyberLock has been downloaded by a CyberLock Programmer. - OR - The audit trail of a CyberLock has been downloaded by a User key or Grand Master with permissions to open a CyberLock.	CyberKeys configured to download locks, Programmers, Grand Masters
A long buzz with 3 beeps.	The audit trail of a programmed CyberLock has been successfully downloaded.	Programmers
A single beep.	Successful lock reset. (Applies to CyberKeys manufactured after December 6, 2004.)	CyberKeys configured as Reset Keys

Infrared Communication Sounds

Tone	Description
A rhythmic chirping.	Waiting for communication.
A high-pitched buzz.	Sending or receiving data.
A double beep.	Accepted a file.

Tips for Using a CyberKey

- Conduct a training session for CyberKey users. Let them try their key in a lock before it is installed.
- Insert the key straight into the lock, not at an angle.
- Press the key firmly into the lock before rotating away from the home position.
- When opening a lock, wait for a solid light on the key prior to turning. The lock should turn only if the light is on. You may hear or feel a click, depending on background noise.
- To prevent undue wear, do not use the key to pull open a door.
- Periodically inspect your key tip for wear. If it is worn, replace it with a new tip (Videx part number TIP-001, TIP-004, or TIP-006).
- When the battery in the key is running low, the key will emit a warning. For keys with beepers, this is a beep that sounds once every eight seconds, for a period of one minute. The battery should be replaced. For keys without beepers, this is a red flash once every eight seconds. The battery should be recharged.
- When changing the battery in a key with a replaceable battery, the operation must be completed within one minute. If it is not, the key may need to be updated to reset its clock.
- When updating a key in an Authorizer Keypoint, wait for the display to read “KEYREADY” before removing the key.

(Continues on next page . . .)

(... continued from previous page)

- The default solenoid retention time is one second. Some users may require more time to rotate the key. Consider increasing this value to two or three seconds. Note: Increasing the time will reduce the life of the battery.
- If a lock does not respond immediately to an authorized key, try holding it in the lock for up to twenty seconds to see if the lock will open. The lock may have been in “tamper delay” mode. Normal operation is restored when an authorized key opens it.
- If a key sirens or flashes an unauthorized pattern (see CyberKey Rechargeable Flash Patterns) when contacting a lock, it does not have authorization to open that lock. Try updating it. If this does not resolve the issue, please contact your system administrator.
- To ensure good electrical contact between keys and locks, it may be necessary to periodically clean contaminants from the tip of the key and the face of the lock. To clean locks and keys, refer to the CyberLock Contact Cleaning Instructions.

Warranty Information

Videx Limited Warranty on CyberLock Hardware

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 end user purchase. Videx, Inc. agrees to repair or, at our option, replace this product without charge if found to be defective during the warranty period.

This warranty does not cover damage or failures caused by products or services not supplied by Videx, Inc., or which result from abuse, attempted burglary, vandalism, misuse, neglect, mishandling, faulty installation, alteration, or modifications of the products supplied by Videx, Inc. This warranty does not cover exterior finish; i.e., color change due to weather, salt air, or chemicals. Only the weather-resistant CyberLock cylinders (CL-6P3WR & CL-OVLWR) are warranted for use in padlocks. Periodic cleaning of the face of the lock is recommended for dirty or outdoor installations.

Videx, Inc. liability hereunder is limited to the purchase price of the product. In no event shall the company be liable for any consequential, indirect, incidental, or special damages of any nature arising from the sale or use of this product, whether in contract, tort, strict liability, or otherwise. Videx, Inc. strongly recommends that this product not be installed in a location where installation could result in bodily injury, loss of life, or property losses that exceed \$10,000. Videx is not liable for the cost of labor to remove or replace locks, or for the cost of transportation to or from the job site.

No other warranty, either expressed or implied, is authorized by Videx, Inc. Videx, Inc. assumes no responsibility for any special or consequential damages resulting from the use of this product or arising out of any breach of warranty. **All expressed and implied warranties, including the warranties of the merchantability and fitness for a particular purpose, are limited to the warranty period set forth above.**

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



MN-CYA-08 • GCO2526