

CyberKey[®] Authorizer[™]

Handbook

vCom Software
Version 2.0



Videx Limited Warranty on Access 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 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.

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 or loss of life. Videx is not liable for the cost of labor to remove or replace products, or for the cost of transportation to 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.

Customer Support Policy

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

Phone: (541) 758-0521

Fax: (541) 752-5285

E-Mail: support@videx.com

If it has been determined that a product is to be returned after contacting Technical Support, please carefully pack the product and send it prepaid and adequately insured to Videx, Inc., 1105 NE Circle Blvd., Corvallis, OR 97330 USA, together with your purchase receipt or other proof of the date of original purchase. It would be helpful if you include a note detailing the problem.



FCC Statement: This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Copyright Notice:

This manual is copyrighted. All rights are reserved. This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent, in writing, from Videx, Inc.

Copyright © 2003 by Videx, Inc.

Videx, Inc., 1105 NE Circle Blvd., Corvallis, Oregon 97330
Phone (541) 758-0521 Fax (541) 752-5285
sales@videx.com
support@videx.com
www.videx.com

Authorizer™ is a trademark of Videx, Inc., and CyberAudit®, CyberLock®, CyberKey®, and Videx® are registered trademarks of Videx, Inc. All other trademarks are properties of their respective owners. Patent pending.

Part# MN-VAL-00

GCO# 1802

Table of Contents

Introduction.....	1
Glossary	5
Software Installation	7
Hardware Setup and Installation.....	9
Using vCom	17
Using Keyports	19
Software Reference.....	21
Troubleshooting	27
General Reference.....	29
Contacting Videx	45
Index	47

Thank you for purchasing CyberKey Authorizer, the remote management system for CyberKeys.

The CyberKey Authorizer provides convenient key control and management for both users and administrators of CyberLock installations. An Authorizer installation, comprised of the Authorizer unit and one or two Keyports, acts as a remote CyberKey Station which can download audit data from CyberKeys and Programmers, update CyberKey configurations, and renew key expiration.

The Authorizer is a TCP/IP network appliance which uses a fixed IP address and connects to the network via RJ-45 ports and standard Ethernet cables. Authorizer units come in network-only and network with modem versions. The Authorizer can be configured to use the modem to dial the host computer within specified time frames to transmit data collected from and to receive updates for CyberKeys. If the Authorizer will not be a part of the Local Area Network (LAN) when installed in its permanent location, the modem version of the unit is required. Alternatively, even if the Authorizer will be connected to the CyberAudit software via LAN, the modem can still provide a link to the host computer by dialing out if LAN communications are disrupted.

As an extra measure of security for CyberKeys, an optional four- to eight-digit PIN can be assigned that must be entered at the Keyport before new configuration information can be uploaded to the key.

System Requirements:

- Authorizer unit
- Keyport units (up to two)
- Power transformer for Authorizer unit
- Ethernet crossover cable (for direct connection between PC and Authorizer unit)
- Ethernet straight-through cables (for connecting with a hub, switch or router between PC and Authorizer unit and for connecting Keyport module to Authorizer unit)
- Standard telephone cable (for use with modem version of Authorizer)
- 6-32 x 1/4" tamper screws (4)
- 6-32 x 3/4" pan-head screws (2)
- Keyport mounting plate
- Keyport mounting gasket
- Drive head for tamper screws
- Single outlet box (1 per Keyport)
- Functioning CyberAudit database
- Network Interface Card (one card required for each computer if CyberAudit and vCom are installed on separate computers)
- PC modem (for use with modem version of Authorizer)
- vCom CD-ROM
- IT or networking manager

vCom Requirements:

- PC running Windows NT, 2000 or XP
- Minimum of 256MB RAM, 512MB recommended
- Pentium 4 or higher processor or equivalent
- Minimum of 1GB free hard disk space, 2GB recommended

Periodically throughout this manual, the following three icons appear:



This icon indicates a tip that may make a task easier.



This icon indicates some additional information on the subject.



This icon indicates a caution or warning. Careful attention should be paid to surrounding information when one of these icons appears.

Glossary

The following is a list of terms used throughout this manual and their definitions.

Authorizer -

Though a CyberKey Authorizer installation is really comprised of an Authorizer Hub (the black control unit) and one or two Keyports, *Authorizer* will hereafter be used to designate only the control unit for the sake of clarity.

Ethernet -

Ethernet is a type of network. For the purpose of this manual, *Ethernet* shall refer to a network that connects devices through CAT5 cables and RJ-45 ports.

Hub -

A hub is a network device that provides several RJ-45 ports for connection to multiple Ethernet devices.

Keypoint -

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

Local Area Network (LAN) -

A LAN is a set of devices which communicate with each other to transmit data. For the purpose of this manual, *LAN* shall refer to those devices connected to each other by Ethernet cables.

Modem -

A modem is a hardware device which transmits and receives data via telephone systems. For the purpose of this manual, *modem* shall refer to devices which are connected to telephone systems through standard phone cables and RJ-11 ports.

Network Interface Card (NIC) -

A Network Interface Card is a hardware device which serves as a go-between for a PC and Ethernet devices. A NIC can be either internal or external.

Router -

A router is a network device similar to a switch that provides RJ-45 ports for connection to multiple Ethernet devices and can bridge two unlike networks.

Switch -

A switch, like a hub, is a network device that provides RJ-45 ports for connection to multiple Ethernet devices, but is more efficient at network addressing and packet transfer.

vCom -

The vCom software drives communication with the Authorizer and synchronizes data and configurations with the CyberAudit database.

Software Installation

Follow these steps to install the vCom software. VCom does not have to be installed on the same computer on which the CyberAudit software is installed, provided that the CyberAudit database is accessible via a LAN connection.

1. Insert the vCom Ver. 2.0 CD-ROM into the computer's CD-ROM drive. The vCom Setup program should start automatically. If it doesn't, run "*setup.exe*" from the CD-ROM.
2. Follow the setup prompts as they appear onscreen. It is recommended that the default selections be used. VCom must be installed in a separate folder from CyberAudit and CyberCom if residing on the same computer.
3. Restart the computer to complete the installation. Please contact VIDEX Technical Support with any questions or concerns regarding the installation.

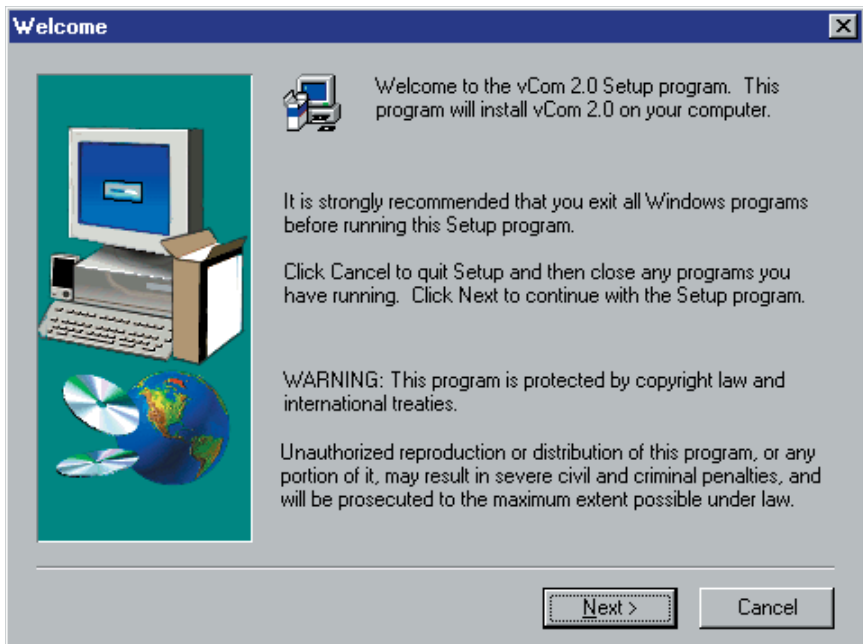


Figure 1: Setup Welcome Screen

Hardware setup:

Before vCom can communicate with an Authorizer, the Authorizer must first be added to the CyberAudit database it will be used with. It is recommended that the following steps be completed before the Authorizer unit is installed in its permanent physical location.



If installing additional Authorizers after initial setup has been completed, shut down vCom before adding new Authorizers.



To ensure correct IP addressing, it is *strongly* recommended that Authorizer setup be turned over to an IT or networking manager, or that they at least be present at the time of setup. Changing TCP/IP settings is not trivial!

The host computer (the computer on which CyberAudit is installed) must have a Network Interface Card (NIC) or external Ethernet Adapter installed and functioning. The Microsoft TCP/IP protocol must also be installed for the network adapter. Internal adapters are preferred to external adapters for functionality. If vCom and the CyberAudit database do not reside on the same computer, the database must be accessible across a Local Area Network (LAN) connection and the computer on which vCom resides must have read/write access to the database.

Connect the Authorizer unit to the host computer. Use a crossover Ethernet cable if connecting directly to the computer or straight-through Ethernet cables if connecting the Authorizer and computer through an intermediary hub, switch, or router. The Ethernet cable should be connected to the *LAN* port of the Authorizer.

Configure the host computer's TCP/IP settings so that it can communicate with the default Authorizer setup IP address of **192.168.192.192**. Once this address can be successfully pinged, the Authorizer can be added to the CyberAudit database.

Open CyberAudit and click the *Authorizers* button on the main screen to access the Authorizers window.



Figure 2: *CyberAudit Main Window*

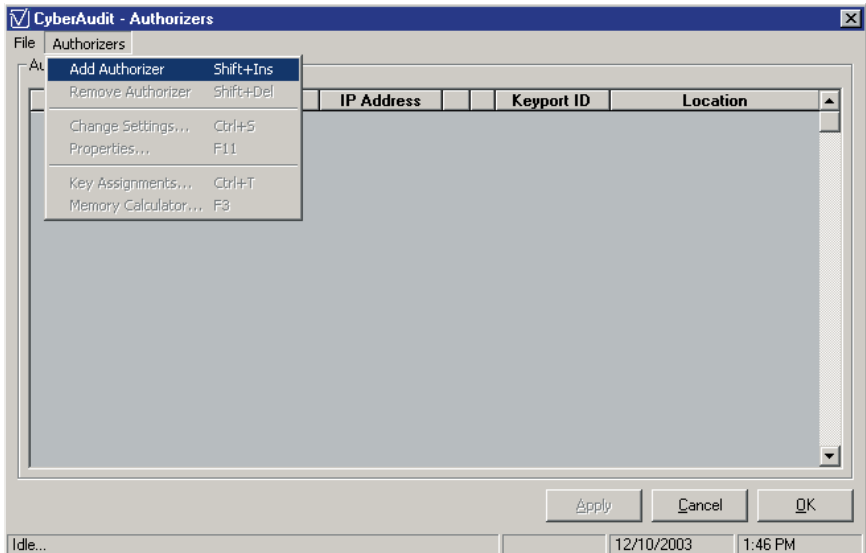


Figure 3: *CyberAudit Authorizers Window*

Select *Add Authorizer* from the Authorizers pull-down menu or use the keyboard shortcut *Shift + Ins*. The Add Authorizer window will appear.

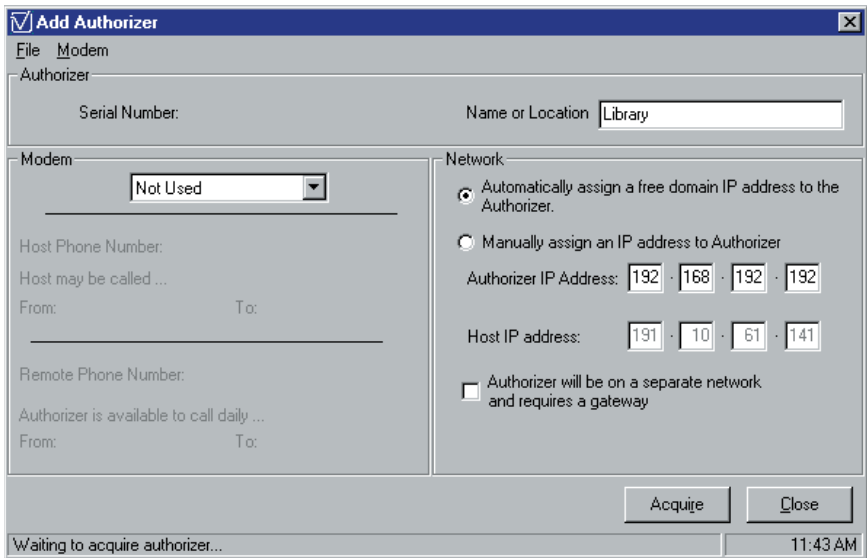


Figure 4: CyberAudit Add Authorizer Window

In the *Name or Location* field, type a logical name for the Authorizer. This name will appear in the Authorizers window.

To have CyberAudit select an unused IP address within the default range of **192.168.192.xxx** (a Class C standard range for small network appliances) and assign it to the Authorizer, click the topmost circle in the *Network* section of the window. To manually specify an IP address to assign to the Authorizer, click the lower of the two circles. If the Authorizer will be connected via LAN, but on a separate subnet, check the box labeled *Authorizer will be on a separate network and requires a gateway*. A new form area will appear to enter the gateway IP address into.

After having selected options and entered any necessary IP address information, click the *Acquire* button. CyberAudit will attempt to communicate with the Authorizer and assign it a permanent IP address. If successful, the message in the status bar at the bottom of the window will change from “Waiting to acquire authorizer...” to “Authorizer found and address set to <new IP address>.” The *Acquire* button will then become the *Update* button.

Any changes made to the configuration of the Authorizer after it has been acquired must be applied by clicking the *Update* button. If the *Close* button is clicked before updating the Authorizer with the changes, the changes will not be applied.

If the Authorizer being added to the system contains a modem, the modem must be enabled. This is done by selecting *Enabled* from the pull-down menu in the *Modem* section of the Add Authorizer window.

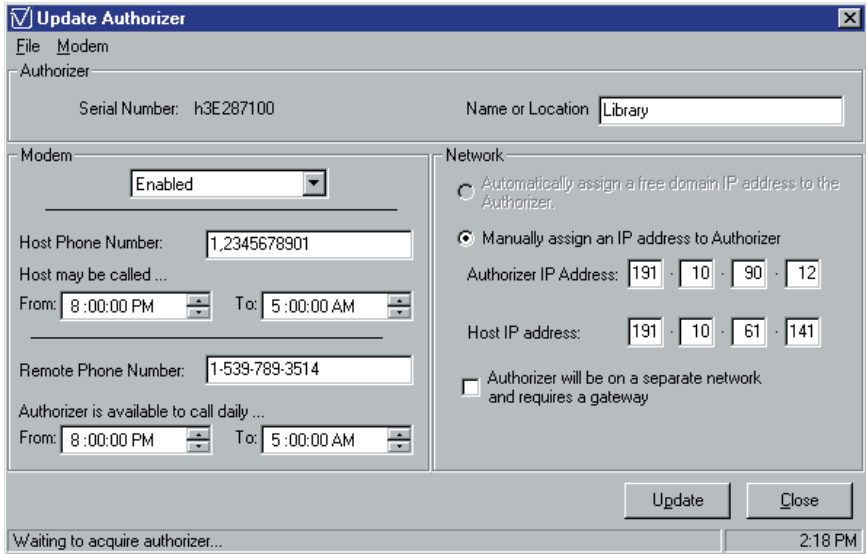


Figure 5: CyberAudit Update Authorizer Window

On occasion, such as when an unknown key is inserted into a Keypoint or when its memory is full, it may be necessary for the Authorizer to initiate a modem call to the host computer. Enter the telephone number of the line the host computer is connected to in the *Host Phone Number* field. See the General Reference section of this manual for a listing of valid control characters that can be used to format the dial string. Enter the phone number of the line the Authorizer will be connected to at its permanent physical location in the field labeled *Remote Phone Number*. As either or both the Authorizer or host computer may be connected to phone lines that are in use at certain times for other purposes, the times a call may be initiated can be restricted by adjusting the time frames in the *Host may be called...* and *Authorizer is available to call daily...* fields.



If the Add Authorizer window has already been closed, the same set of options (less *Acquire*, which becomes *Update*) is available via the Update Authorizer window. To access the Update Authorizer window, select *Change Settings...* from the *Authorizers* menu of the Authorizers window or use the keyboard shortcut *Ctrl + S*.

To specify modem wait times and country of operation for the Authorizer modem, select Configure from the Modem menu. This will bring up the Hub Modem Configuration window.

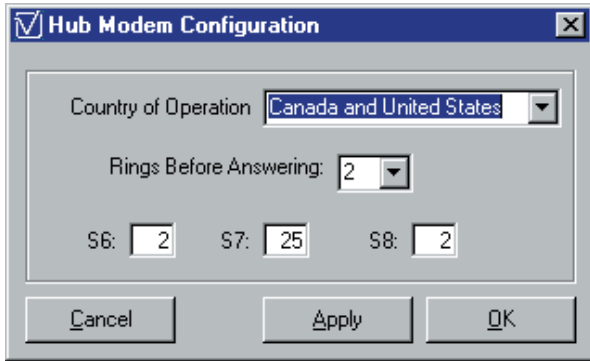


Figure 6: CyberAudit Hub Modem Configuration Window

Select the country of operation and number of rings before answering from the respective pull-down lists. The value specified in *S6* designates the number of seconds the modem will wait for dial tone detection. *S7* is the number of seconds the modem will wait for carrier detection before sending “No Answer.” *S8* specifies the number of seconds the modem will pause when it encounters a comma in the dial string. Click Apply to commit the changes without exiting or OK to save the changes and return to the preceding window. Clicking Cancel will return to the preceding window without effecting any changes.

After all options have been set, click the Uppdate button before exiting the Add or Update Authorizer window to apply the changes.



A modem Authorizer will answer a phone line at any time. It is recommended that a dedicated line be used with modem Authorizers in order to avoid conflict with other devices. If an Authorizer shares a phone line with another device, such as a fax machine or telephone answering device, the other device must first be turned off before the vCom software can update the Authorizer. Conversely, other devices will not be able to perform their duties unless they have been set to answer the line before the Authorizer.

Upon exiting back to the CyberAudit Authorizers window, the newly acquired Authorizer will be listed under the *Authorizers and Keyports* section.

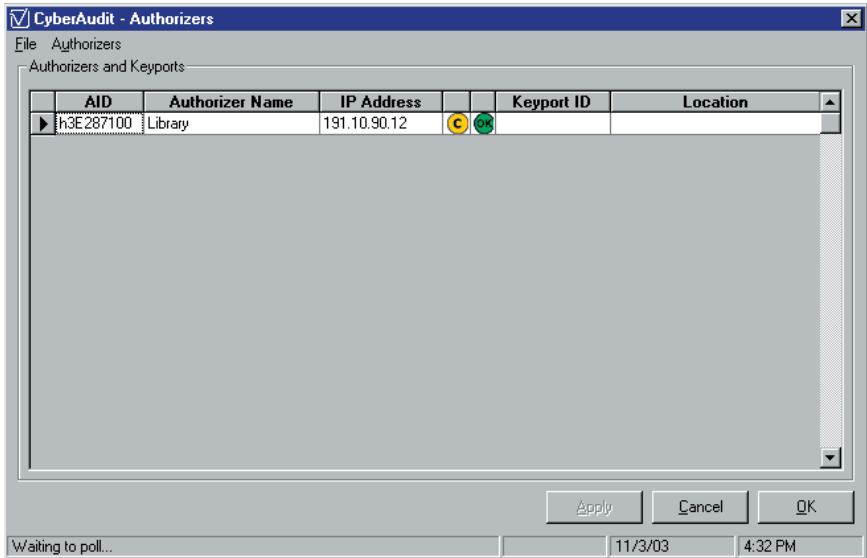


Figure 7: CyberAudit Authorizers Window - New Authorizer Added

A yellow **C** icon will be displayed any time that changes are pending for the selected Authorizer. The changes will be uploaded to the Authorizer during the next communications session. If a green **OK** icon is displayed, it means that CyberAudit can currently see the Authorizer (on the LAN, for instance). This does not mean that CyberAudit is currently communicating with the Authorizer, but merely that it is aware of a connection to the Authorizer. Unless the Authorizer is connected via LAN to the same subnet as the host computer, this icon will rarely be displayed in CyberAudit.

Hardware Installation:

At this point, the new Authorizer is ready to be installed in its permanent physical location. Mount the unit to an indoor wall in a protected area.

If the Authorizer will be directly connected to the computer on which vCom is installed, plug a crossover Ethernet cable into the *LAN* port. If the Authorizer will be connected via LAN with an intermediary hub, switch or router, plug a straight-through Ethernet cable into the *LAN* port. Connect a straight-through Ethernet cable for each Keypoint to be used to *KeyPort1* or *KeyPort2*. If using the Authorizer modem, connect a standard phone line cable to the *Modem* port. Connect the power jack of the supplied transformer to the *Power* port and plug the transformer into a wall outlet or an Uninterruptible Power Supply (UPS). As with all computer-related equipment, the use of some form of surge protection is recommended.

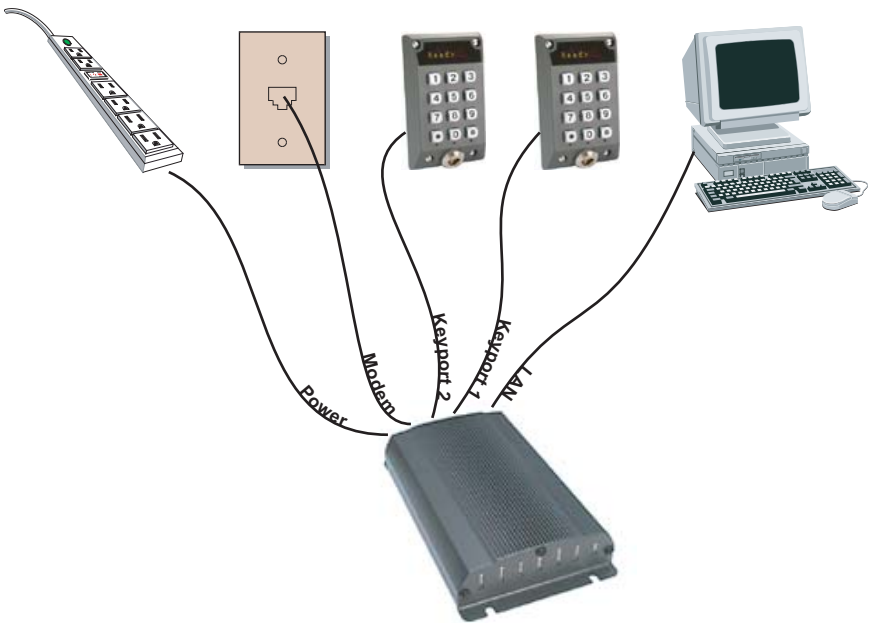


Figure 8: Authorizer Connections

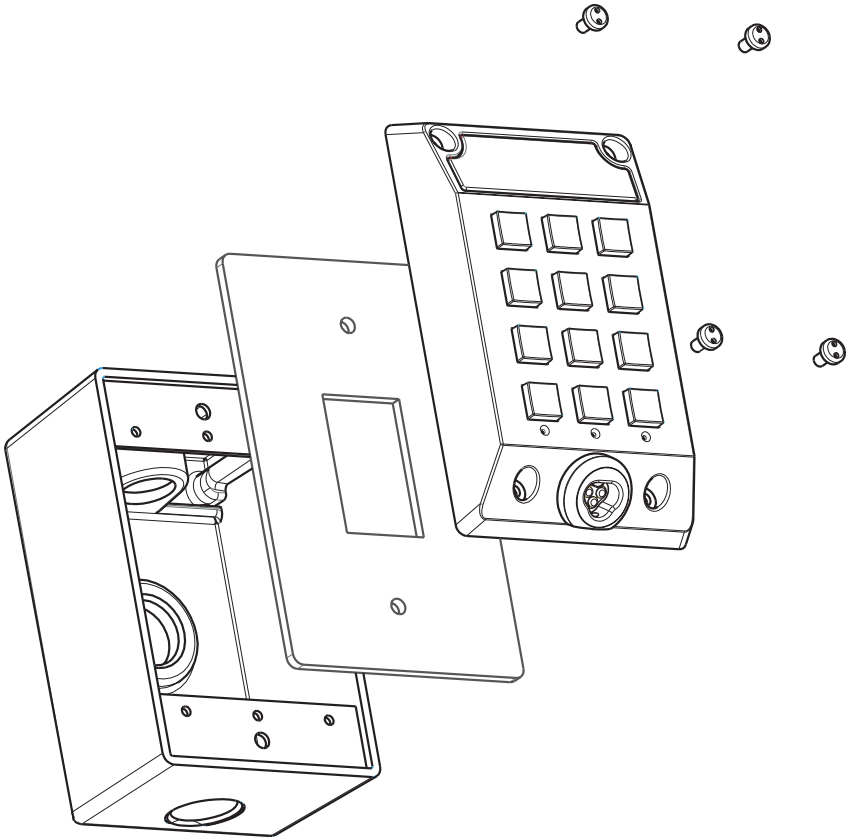



Figure 9: Keyport Assembly

To complete installation of the Keyport(s), thread the free end of the Ethernet cable through a single outlet box and mount box in the installation location. For outdoor installations, a waterproof box is recommended. Feed the Ethernet cable through the Keyport mounting plate and screw the plate to the outlet box using the provided 6-32 x 3/4" pan head screws. Pull the cable through the mounting gasket, then insert the RJ-45 connector into the jack on the back side of the Keyport. Situate the mounting gasket over the plate and align the Keyport unit over the outlet box. Secure the Keyport to the box using the four provided tamper screws.

VCom is responsible for synchronizing data in Authorizer units with the CyberAudit database. Though Authorizers are able to function independently without vCom running, they will not be able to receive updates or transmit data without it. It is desirable to have vCom running a majority of the time.

Start the vCom software by double-clicking the  icon that was placed on the desktop during installation or by selecting the vCom entry from *Start* → *Programs* → *CyberAudit*. The first time vCom is run, it will prompt for a CyberAudit database if it cannot find the one CyberAudit currently points to. Select the file the Authorizer was added to in the Hardware Setup section. If the current CyberAudit database is not the one to which the Authorizer was added, select the correct database by choosing *Open Database* from the *File* menu.

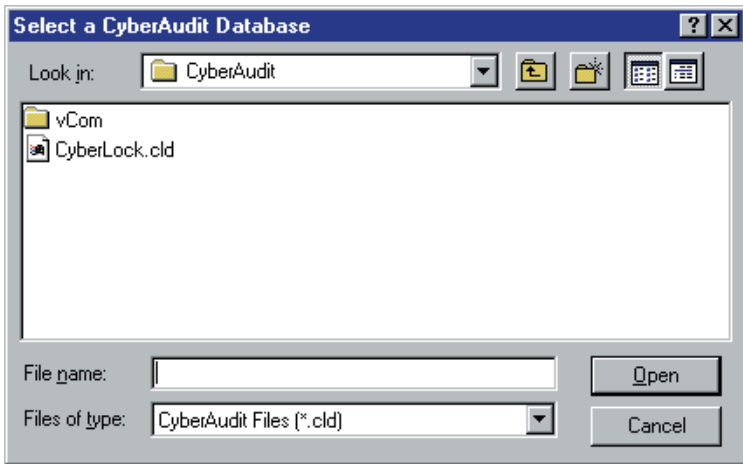


Figure 10: *Specifying Database File for Authorizer Use*

If any of the Authorizers in the database are configured for modem use, vCom will automatically display the Modem Settings window the first time it is started. This window is used for configuring the modem connected to the computer on which vCom is installed. This local modem will be used to interface with the modems in the Authorizer units. The Modem Settings window can be accessed in the future by selecting *Configure* from the *Modem* sub-menu, found under the *Settings* menu.

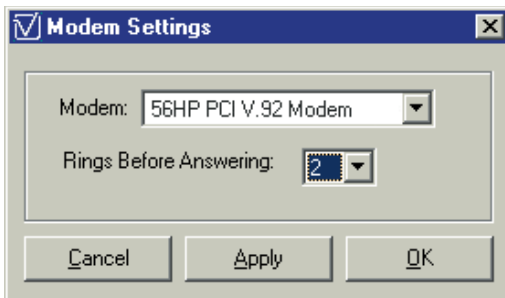


Figure 11: *Modem Settings Window*

While vCom is running, it periodically contacts all the Authorizers connected via LAN to verify the connection and to update them with new configuration information. Authorizers configured to be contacted via modem are treated as a separate group. The length of time between communications sessions can be specified in the vCom Settings window. This window is accessed by selecting vCom from the Settings menu.

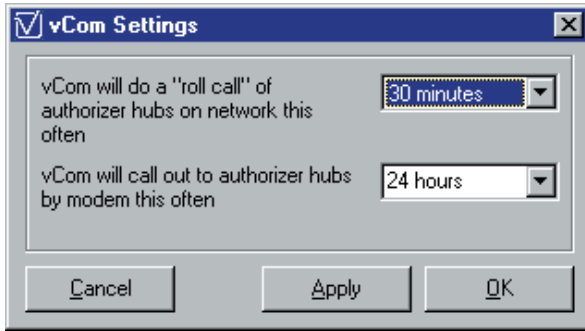


Figure 12: vCom Settings Window

All operations carried out by vCom are automatic and require no user interaction after all settings have been established. However, the system administrator should occasionally check to be sure that the software is running and contacting Authorizers normally. It may also be necessary to disable the software at certain times, such as during a system backup. To temporarily stop vCom from communicating with Authorizers, select *Suspend* from the Settings menu. When ready to continue with communications, select *Resume*. (For information on shutting down vCom automatically, see the General Reference section entitled *Scheduling a Daily Shutdown of vCom*.)

To view general information about specific Authorizer units, select an Authorizer from the list and choose *Properties* from the Authorizer menu or use the keyboard shortcut *F11*. This will bring up the Authorizer Properties window.

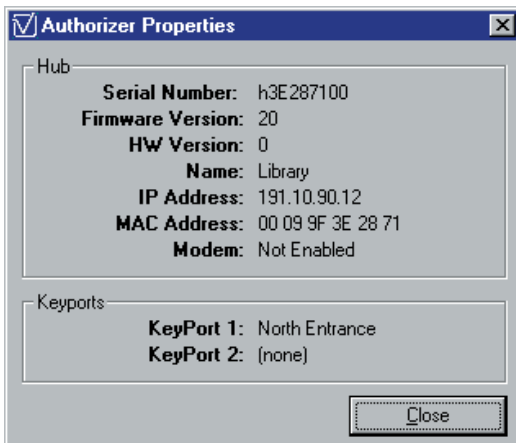


Figure 13: Authorizer Properties Window

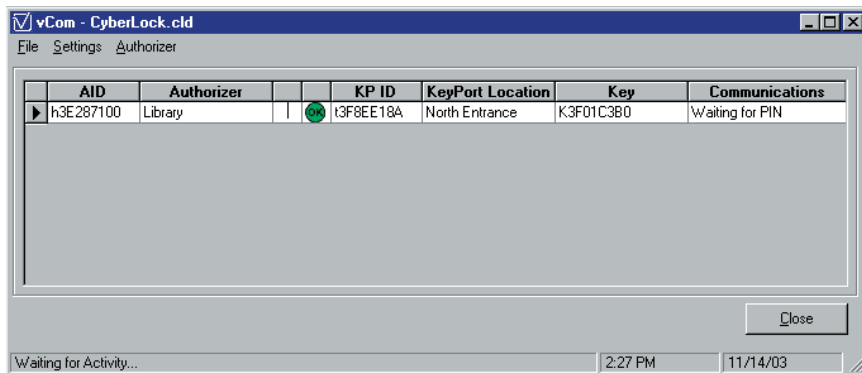
To download audit data from a CyberKey at a Keypoint, simply insert the key into the receptacle below the 12-button keypad. If the Authorizer is connected via LAN, the Authorizer will immediately initiate communications with vCom and transfer the data from the key. Otherwise, the data is stored in the Authorizer's memory until the next communications session.

Authorizers maintain a list of CyberKeys that they are able to update. For instructions on how to configure CyberKeys for use with Authorizers, refer to the *CyberAudit Version 2.0 Instruction manual*.

If a key in the Authorizer's list is inserted into a Keypoint, the Authorizer will clear the events from the key's memory after downloading them. If the presented key is not in the Authorizer's list, the Authorizer will attempt to contact vCom and the Keypoint will display the message "LINKUP HOST." If the Authorizer is connected via LAN, vCom will immediately be able to store the key data in the CyberAudit database and clear the events from the key's memory. If the Authorizer is connected via modem and is within its specified timeframe, it will attempt to call out to the computer on which vCom resides. If the Authorizer is not within its specified timeframe, it will timeout and the Keypoint will display "COMMFAIL." The key events will be downloaded and stored in the Authorizer's memory, but will not be cleared from the key itself. The Authorizer will then transmit the key events to vCom at the next communications session.

Keypoints can also be used to download audit data from CyberLocks. To do so, first configure a CyberLock Programmer using CyberAudit, then insert it into either a CyberKey Station or a Keypoint to upload the configuration. (Note: the new configuration will not be immediately available at a Keypoint if the Authorizer is connected via modem and has not yet been updated by vCom.) Next, contact the lock to download. After collecting the audit data from the lock, insert the Programmer into the Keypoint to send it to the CyberAudit database. The Keypoint will display the message "PROGRAMR" and the Authorizer will immediately initiate communications with the vCom computer in order to send the audit data to the CyberAudit database, as described above.

For added security, a 4- to 8-digit PIN can be assigned to CyberKeys through the CyberAudit software. When the key is inserted into the Keypoint, the PIN must be provided before the key can be updated. The Keypoint will display "PIN#" and wait for the correct PIN to be entered. Enter the PIN and then press the '#' key to submit. The '*' key functions like the Backspace key on a keyboard. Once the correct PIN has been entered, the Authorizer will upload any pending configuration changes to the key. When it has finished, the Keypoint will display "KEYREADY."

vCom Main Window:**Figure 14: *vCom Main Window***

The vCom main window allows the user to select a CyberAudit database to interact with, to specify contact intervals for Authorizers, to change local modem settings, and to view general information about Authorizers.

The File menu:**Figure 15: *File Menu***

The File menu provides options for selecting a CyberAudit database file to use and for exiting the program.

Open Database - This option will bring up a dialogue box allowing the user to specify a CyberAudit database file for vCom to interact with.

Exit - This option will exit the vCom software.

The Settings menu:



Figure 16: Settings Menu

The Settings menu allows the user to change local modem and vCom program settings, and to suspend or resume program functions.

Modem → Configure - This option will bring up the Modem Settings window, where the user can change local modem settings.

vCom - This option will bring up the vCom Settings window, where Authorizer contact intervals can be specified.

Suspend - This option will suspend vCom operations. No Authorizer communications can take place while vCom is suspended.

Resume - This option is only available if vCom has been suspended. Selecting this option will resume normal vCom operation and communications with Authorizers.

The Authorizer menu:



Figure 17: Authorizer Menu

The Authorizer menu allows the user to view general information on the currently selected Authorizer unit.

Properties (F11) - This option will bring up the Authorizer Properties window, which displays general information about the currently selected Authorizer.

Buttons:

Close - Exits the vCom software.

Modem Settings Window:

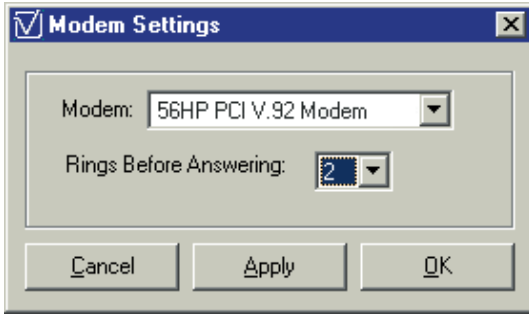


Figure 18: *Modem Settings Window*

The Modem Settings window allows the user to select a local modem (if more than one modem is installed) to be used for Authorizer communications, and to specify the number of rings before the local modem will answer an incoming call from an Authorizer unit.

Buttons:

Cancel - Returns to the vCom main window without effecting any changes.

Apply - Applies changes to settings without exiting the Modem Settings window.

OK - Applies changes to settings and returns to the vCom main window.

vCom Settings Window:

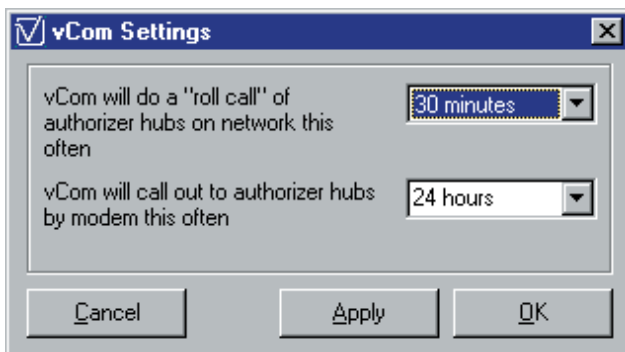


Figure 19: *vCom Settings Window*

The vCom Settings window allows the user to specify the interval at which vCom will check network connections to Authorizers or dial Authorizers via modem. VCom is still restricted by the setting in the CyberAudit Add/Update Authorizer window and will only initiate modem communications at the specified interval if it falls within the specified timeframe.

For example, if the interval is set at 1 hour, but modem communications are restricted to 2:00am - 5:00am, vCom will only contact the Authorizer a total of four times a day.

Buttons:

Cancel - Returns to the vCom main window without effecting any changes.

Apply - Applies changes to settings without exiting the vCom Settings window.

OK - Applies changes to settings and returns to the vCom main window.

Authorizer Properties Window:

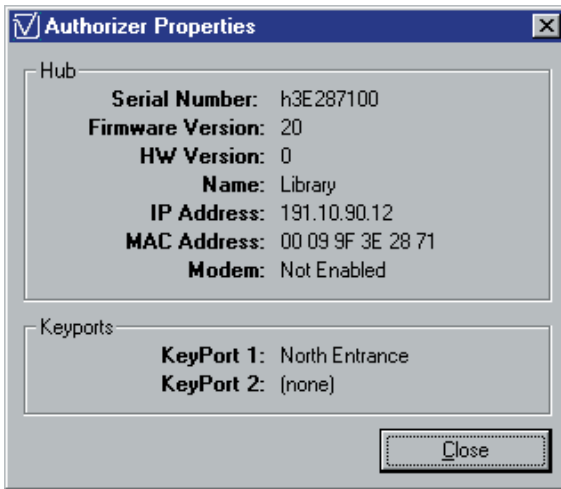


Figure 20: *Authorizer Properties Window*

The Authorizer Properties window displays general information about the selected Authorizer unit.


Buttons:

Close - Closes the Authorizer Properties window and returns to the vCom main window.


vCom Software Updates:

Updates to the vCom software may occasionally be made available for download from the Videx web site (<http://www.videx.com>).



Before running a software update, be sure to close vCom and make sure that all  icons have been resolved in CyberAudit for all keys, locks, and Authorizers in the database.

For LAN connected Authorizers:

If LAN communications between the Authorizer and the computer on which vCom is installed do not appear to be functioning properly, first make sure the vCom software is running. If it is, make sure that it is linking to the correct CyberAudit database. If it isn't, choose *Open Database* from the File menu and select the correct database. When vCom is linked to the correct database, does the green  icon display for the Authorizer in question? If not, does the Authorizer respond to a network ping? (Ask a networking or IT professional.)

If none of the previous suggestions resolve the communications issue, the problem is most likely in the hardware. Check the Ethernet cable. Is it the correct type (straight-through or crossover)? Is the cable longer than the maximum length of 250' (76.2m)? Try unplugging the Authorizer for a few seconds, then reapplying the power and waiting for the Authorizer to reboot. If communications are still not working, try connecting a correctly functioning Authorizer unit with the same cable(s), if one is available. (If no other Authorizer is available to substitute, ask a networking or IT professional to test the cable(s) with a cable tester.) If vCom cannot communicate with the known good Authorizer unit, the problem is the Ethernet cable(s). If the known good Authorizer is still able to function, return it to its original location and try resetting the non-functioning Authorizer. (See the General Reference section of this manual.) Once the Authorizer has been reset, remove it from the CyberAudit software and go through the setup process again. If vCom is still unable to communicate with the Authorizer after it has been reset and re-setup in CyberAudit, contact Videx Technical Support for further assistance.

For Authorizers connected via modem:

If communications with modem-connected Authorizers are not functioning properly, first make sure that vCom is running and is linked to the correct CyberAudit database. Look at the Keypoint to see if any messages are being displayed. Also check CyberAudit to make sure that no hours restrictions have been set for the Authorizer in question and that the host and remote phone numbers (including formatting and special characters) are correct. Try using the modem installed in the computer on which vCom is installed for another purpose, such as sending a fax or connecting to the Internet. (If more than one modem is installed, make sure vCom is configured to use the right one.) If the local modem does not function, but is correctly installed and using the correct drivers, check the phone line it is connected to for a dial tone. Also check for a dial tone on the line the Authorizer modem is connected to. Are other devices or people using the phone line during scheduled communications sessions? If there is a synchronization utility for a PDA (Palm, Handspring, etc.) installed on the vCom computer, make sure it is disabled. If communications are still not functioning after trying all previous suggestions, contact Videx Technical Support for further assistance.

If the Keypoint is not functioning correctly:

If vCom and the Authorizer unit appear to be communicating correctly, but the Keypoint does not appear to function correctly, or only displays the “WAIT” message when a CyberKey is inserted, first verify that a straight-through Ethernet cable is being used between the Authorizer and the Keypoint. If the correct cable type is being used, try substituting a known good straight-through cable for the first one. If the communications problem is not solved, try plugging the cable into another Keypoint, if one is available. Also, try unplugging the Authorizer for a few seconds, then reapplying the power and waiting for the Authorizer to reboot. If none of the previous suggestions correct the problem, contact Videx Technical Support for further assistance.

If vCom displays an error about the database being locked:

In rare instances, vCom may display an error message stating that the database is locked. This error typically occurs when network communications are interrupted or lost and database access has not been released. This type of error indicates that the database engine is having trouble maintaining a workable connection, and is best solved by installing and running vCom on the same computer on which the CyberAudit database resides.

Resetting Authorizer Units:

Sometimes, usually during setup, it may be necessary to reset an Authorizer unit. To do this, disconnect all cables from the Authorizer and attach a straight-through Ethernet cable between the RJ-45 ports labeled *KeyPort1* and *KeyPort2*, then reconnect the Power cable. The Authorizer will take a few moments to reset itself, and indicates a successful reset by rapidly flashing the *KyPort1* and *KyPort2* LEDs simultaneously. Disconnect the Ethernet cable and reattach the other cables in their correct locations.



Figure 21: *Authorizer Reset Configuration*

Straight-through vs. Crossover Ethernet Cables:

This section explains how to tell the difference between a straight-through and a crossover Ethernet cable.

Straight-through Cables:

With the brass contacts of the RJ-45 plug facing up and away, the individual wires of a straight-through Ethernet cable will be in the following order:

Pin	Wire Color(s)
1	White / Orange
2	Orange
3	White / Green
4	Blue
5	White / Blue
6	Green
7	White / Brown
8	Brown

Both ends of straight-through Ethernet cables are identical in wire order.

Crossover Cables:

With the brass contacts of the RJ-45 plug facing up and away, the wire order of one end of a crossover Ethernet cable will be identical to that of a straight-through cable and the wires of the other end will be in the following order:

Pin	Wire Color(s)
1	White / Green
2	Green
3	White / Orange
4	Blue
5	White / Blue
6	Orange
7	White / Brown
8	Brown

Authorizer Memory Capacity:

The percentage of memory used in the Authorizer unit varies based on the following factors: the total number of keys that have been assigned to the Authorizer, how many out of those keys are actually downloaded at the Authorizer, the average number of locks each key has access to, and how many events are downloaded from each key.

Here are some examples:

Number of Keys	Number of Key Downloads
1000 keys with \approx 250 locks ea.	15 key downloads of \approx 250 events ea.
950 keys with \approx 200 locks ea.	15 key downloads of \approx 1000 events ea.
550 keys with \approx 200 locks ea.	125 key downloads of \approx 1000 events ea.
500 keys with \approx 200 locks ea.	500 key downloads of \approx 250 events ea.
15 keys with \approx 200 locks ea.	1000 key downloads of \approx 250 events ea.

The CyberAudit software contains an Authorizer Memory Calculator, which can be used to calculate the approximate percentage of the total Authorizer memory being used, based on theoretical values used for input. For more information, please refer to the *CyberAudit Version 2.0 Instruction Manual*.

Authorizer Error Logs:

Anytime an error occurs with an Authorizer, an entry describing the error is written to a log that resides in the vCom directory. A separate text file is created for each Authorizer in the system that has an error. The filenames follow the format *<Authorizer ID>err.log*.



The Authorizer ID is the number indicated by the column *AID* in the vCom main window.

Scheduling a Daily Shutdown of vCom:

Certain system backup utilities will not function properly if vCom is running. If interruptions in automatic backups occur, specific shutdown and restart times can be assigned to vCom so that the backup may execute at its scheduled time. Specifying these times involves editing the Windows registry keys for vCom.



Improperly editing the Windows registry could cause damage to the operating system, resulting in an unusable computer! These steps should be performed ONLY by a System Administrator or Software Manager!

Using the built-in Windows program *Regedit*, navigate to the folder ***HKEY_CURRENT_USER\Software\VB and VBA Program Settings\VCom\Shutdown***. Select the *StopTime* key to specify the time at which vCom should shut itself down. The value given to the *EndStop* key specifies the end of the “blackout” period wherein vCom cannot be run and must be greater than the value of *StopTime*. Both 12- and 24-hour time formats are acceptable.

To automatically restart vCom after the automated system backup is expected to have finished, a scheduled task must be added for Windows to run at the desired time. To add the task, open the Windows Scheduled Task Wizard. When the wizard prompts for a program to run, click the *Browse...* button and navigate to the vCom directory. Select the program *StartvCom.exe*, then click the *Open* button and continue specifying options as prompted by the Wizard.

The following table lists the various messages that may appear on a Keypoint LED display and their meanings.

Keypoint Display Messages:

Message	Meaning
BAD PIN#	PIN entered does not match the PIN assigned to the key
CLOCK STOP	The clock in the Authorizer has stopped. This can occur if power is lost for more than 24 hours
COMMFAIL	Ethernet or modem communication failed
COMMFAIL PLSRETRY	Communication failed between the computer on which vCom is installed and the Keypoint
CONNECT	The Authorizer modem has established a connection with the modem in the vCom computer
DIAL MODEM	The Authorizer is dialing the vCom computer and waiting for a connection to be made
FAILCOMM	Communication failed between vCom and CyberKey
HANGUP MODEM	Modem communications are complete and the Authorizer has issued a hangup command
HUB BUSY WAIT	The Authorizer is busy with internal processes
HUBREADY	The Authorizer has finished rebooting and is ready
INIT MODEM	The Authorizer is initializing the modem at startup
KEYPAD DISABLED	Communications are in progress between vCom and the Authorizer
KEY FAIL	Communication failed between Authorizer and Keypoint
KEYREADY	Communications with the CyberKey are complete
LINE BUSY	The vCom computer's phone line is busy
LINKUP HOST	The Authorizer is contacting vCom, usually because an unknown CyberKey has been inserted into the Keypoint
LOADING KEY	The vCom computer has finished lookup and begun processing the CyberKey
LOWBATT	The battery in the CyberKey needs to be replaced
NO ANSWER	The vCom computer did not answer within the time specified in the Hub Modem Settings window
NO CARRIER	The modem connection has been terminated
NO DIAL TONE	No dial tone on the line when trying to dial out
PIN#	A PIN is required for the current CyberKey

(Continued on following page...)

Message	Meaning
PLS WAIT	The vCom computer is busy with internal processes
PROGRAMR	A Programmer is in the Keyport. The vCom computer will be immediately contacted to download the information contained in the Programmer
READY	The Keyport is ready for use; the Authorizer is offline
READING	The vCom computer is downloading audit data from the key and storing it in the CyberAudit database
READY *	The Keyport is ready for use; the Authorizer is online
REBOOT HUB	Initial message shown after Authorizer has been reset
RING	The Authorizer modem has detected a ring on the line
UNKNOWN KEY	The CyberKey was not found in the database
WAIT	The Authorizer is busy with internal processes
WRITING	The vCom computer is reading the configuration from the CyberAudit database and programming the key
WRONG PW	The Authorizer and key database identifiers don't match

The following table lists the LEDs found on the Authorizer unit and what each indicates.

CyberKey Authorizer LED Indications:

LED	State	Indication
Link	On	The Authorizer is connected to a LAN
Active	On/Flashing	Network communications are active
KyPort2	On/Flashing	Communications with Keypoint 2 are active
KyPort1	On/Flashing	Communications with Keypoint 1 are active
Serial	On/Flashing	Serial communications are active - only used for firmware updates
Modem	On/Flashing	The Authorizer modem is currently in use
Power	On	The Authorizer is on and ready to operate

The following is a table of countries in which the modem version of the CyberKey Authorizer can be used:

Countries Available for Modem Use:

- Australia
- Austria
- Belgium
- Brazil
- Canada
- China
- Denmark
- Finland
- France
- Germany
- Greece
- India
- Indonesia
- Ireland
- Israel
- Italy
- Japan
- Korea
- Malaysia
- Mexico
- The Netherlands
- Norway
- Panama
- The Philippines
- Portugal
- Singapore
- South Africa
- Spain
- Sweden
- Switzerland
- Taiwan
- United Kingdom
- United States
- TBR21

This list continues to grow as new countries are added. If an Authorizer is intended for use in a country that is not on this list, please contact Videx Technical Support, as the country may have been added after the publication of this manual.

The following is a table of supported S registers that can be used to configure modems in CyberKey Authorizers:

Supported S Registers

Register	Function	Range	Units	Default
S0	Rings until Auto Answer	0 - 255	rings	2
S6	Wait time before blind dialing or dial tone	2 - 255	seconds	2
S7	Wait time for carrier, silence or dial tone	1 - 255	seconds	25
S8	Pause time for dial delay modifier	2 - 255	seconds	2

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

Valid Control Characters:

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 the time specified by S7 (US) or S6 (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 5 seconds of silence before the expiration of the call abort timer (S7), the modem will terminate the call attempt.
’	Dial pause - the modem will pause for the amount of time specified in S8 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.

Specifications:

Authorizer -

Physical:	Black powder-coated extruded aluminum
Dimensions:	1.42" H x 4.15" W x 7.12" L (3.60cm H x 10.54cm W x 18.08cm L)
Weight:	15.3 ounces (433.7g)
Operating Temperatures:	32° to 122°F (0° to 50°C) Indoor use only
Power Supply Adapter:	12v DC, 300mA
Transformers:	120v, 60Hz or 220v, 50Hz
Indicator Lights:	<i>Link, Activity, KyPort2, KyPort1, Serial, Modem, Power</i>
Ethernet Connection:	10baseT, 10Mbps, RJ-45 Maximum 250' (76.2m) length CAT 5 cable
Clock:	Real-time clock with 24 hour backup power
Memory:	2MB Flash
Regulatory Compliance:	FCC, CE

Modem version only:

Modem Connection:	PSTN, 2 wires, RJ-11
Data Transmission:	33,600bps
Auto Answer:	Yes
PTT:	FCC Part 68
EMI:	FCC Part 15, Class A

Keypoint -

Physical:	Black powder-coated cast aluminum with standard metal numeric keypad. Connects to single outlet electrical box. Weather-resistant
Dimensions:	0.98" H x 3.00" W x 4.75" L (2.49cm H x 7.62cm W x 12.07cm L)
Weight:	6.6 ounces (187.1g)
Operating Temperatures:	2° to 140°F (-17° to 60°C)
Power:	Supplied by Authorizer unit
Ethernet Connection:	10baseT, 10Mbps, RJ-45 Maximum 100' (30.48m) length CAT 5 cable
Display:	8 character LED
Keypad:	Standard 12-key numeric keypad

FCC Information:

(Applies to Authorizers with optional modem module)

FCC Compliance, Part 68

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the underside of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. If requested, this number must be provided to the telephone company.

The product is designed to be used on standard device telephone lines. It connects to the telephone line by means of a standard connection called the USOC RJ-11C.

Connection to telephone-company-provided coin service (central office implemented systems) is prohibited. Connection to party lines service is subject to state tariffs.

A plug and connector used to connect this equipment to the premises' wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular connector that is also compliant. See installation instructions for details.

The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXXX. The digits represented by ## are the REN without a decimal point (e.g., 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

If this equipment (AUTHORIZER) causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. However, if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

For repair or warranty information if trouble is experienced with this equipment (AUTHORIZER), please contact VIDEX, INC. at 541-758-0521. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

The modem contained in this product is not intended to be repaired by the customer.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission, or corporation commission for information.

If your facility has specially wired alarm equipment connected to the telephone line, ensure the installation of this product (AUTHORIZER) does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

Information needed in the United States:

The modem complies with Part 15 and Part 68 of the FCC Rules.

Ringer equivalence number:	0.5B
Telephone connection type:	USOC, RJ-11
Manufacturer:	VIDEX INC.
Product ID number:	US:AAAEQ##TXXX
Model Name/Number:	CyberKey Authorizer

FCC Compliance, Part 15

This equipment has been tested and found to comply with the limits for Class A digital devices, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his or her own expense.

Contacting Videx

Videx Technical Support representatives will be glad to answer any additional questions between 8:00 AM - 12:00 PM and 1:00 PM - 4:30 PM (Pacific), Monday through Friday.

Phone: (541) 758-0521
Fax: (541) 752-5285
E-mail: support@videx.com
Web: www.videx.com
Post: 1105 NE Circle Blvd.
Corvallis, OR 97330

A

Authorizer

Error logs	32
LED indications	36
Memory capacity	31
Modem	
Configuration	13
Control characters	39
Countries available for use	37
S Registers	38
Properties	
Viewing	18
Resetting	29
Specifications	40
System explanation	1
Troubleshooting	27
Using to download audit data from CyberLocks	19

E

Ethernet

Cables	
Crossover	30
Straight-through	30
Definition	5

F

FCC

Information	42–43
Statement	iii

H

Hardware

Installation	15–16
Setup	9–14
Specifications	40–42

Hub

Definition	5
------------------	---

I

Icon Explanations	3
Installation	
Software	7

K

Keypoint

Definition	5
Display messages	34–35
Specifications	41
Troubleshooting	28
Using	19

L

LAN

Definition	5
------------------	---

Local Area Network

Definition	5
------------------	---

M

Modem

Definition	5
------------------	---

Modem settings	38–39
----------------------	-------

N

Network Interface Card

Definition	5
------------------	---

NIC

Definition	5
------------------	---

R

Router

Definition	5
------------------	---

S

Software

Installation	7
--------------------	---

Updates	25
---------------	----

Support

Policy	ii
--------------	----

Switch

Definition	5
------------------	---

System Requirements.....	2
--------------------------	---

T

Technical Support

Contacting	45
------------------	----

V

vCom

Authorizer Properties window	24
Automatically shutting down and restarting	33
Definition	5
Installation. <i>See</i> Software installation	
Main window	21–22
Modem Settings window	23
Settings window	23–24
Troubleshooting	28
Using	17–18

Videx

Contacting	45
------------------	----

W

Warranty Information	ii
----------------------------	----



GCO # 1802 Part # MN-VAL-00