

C2Home[®] System User's Manual


C2 Home & Office Inc
 P.O. Box 5162
 Hazlet, NJ, 07730
www.c2home.com

Email: Custserve@c2home.com

C2Home[®] Server – US Patent Nov 2002
 C2Home[®] is a registered trademark with the US Patent
 and Trademark Office.
 Copyright 2001 C2Home & Office Inc.

Table of Contents

INTRODUCTION	3
GETTING STARTED:	3
PARTS INCLUDED	3
HARDWARE INSTALLATION	4
CM11A TO SERIAL PORT	4
SOFTWARE INSTALLATION	4
LOADING THE C2HOME® SERVER ON A WINDOWS (WIN95,98,NT, ME) PC.....	4
TO RUN THE C2HOME® SOFTWARE	5
INITIALIZING THE SOFTWARE	6
INITIALIZING BASE PROPERTIES.....	7
VIDEO CONFIGURATION	9
VIDEO VIA HTML.....	10
X.10 DEVICE LABELS	10
SETTING ALARM AND ALARM EVENT PROPERTIES	12
<i>Property Layout</i>	13
<i>Adding Stencils</i>	14
SECURITY CONFIGURATION.....	15
KEY MANAGEMENT FOR SECURE COMMUNICATIONS	16
PATROL WATCH DUTY SHIFT ASSIGNMENTS.....	16
TIMED EVENTS	17
COMMUNICATION OPTIONS.....	18
<i>Option 1 Dial up Direct</i>	18
<i>Option 2 Dial up Server-ISP, Remote Access Fixed</i>	18
<i>Option 3 Fixed Remote – Fixed Sever Connection</i>	18
NORMAL OPERATION	19
EXTENDED VIEW OF COMMAND CONSOLE	19
VERIFYING PROPER OPERATION	19
<i>Video Window</i>	20
<i>View Log</i>	20
<i>Base Watch</i>	20
REMOTE ACCESS	21
PHONE AND PDA ACCESS	24
TROUBLESHOOTING	25
GLOSSARY	27
APPENDIX A: HOUSE DEVICE LABELS WORKSHEET:	29
APPENDIX B: PLANNING SECURITY OPERATIONS	31
APPENDIX C: IP ROUTING TUTORIAL	34
<i>Steps for configuring a Windows PC for IP Networking</i>	34
MICROSOFT DIAL UP SERVER – (REQUIRES MICROSOFT DIAL UP SERVER –DUS – MS FREWARE).....	35
APPENDIX C: JRE CONFIGURATION	39

APPENDIX D: NEAT TRICKS (IF YOU DON'T KNOW THEM ALREADY)39

Introduction

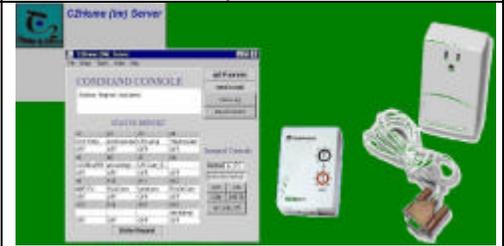
Congratulations on your purchase of the C2Home® system – the system which turns your PC into a Command and Control Base station analogous to the C2 system used by Defense organizations throughout the world!

The C2Home® System is the collection of Hardware and Software used to implement home monitoring and control. The software is the C2Home Server application. Hardware includes the user's computer, X.10 interface, X.10 modules, Video Cameras and any other items the user adds based on her/his strategy for implementing home security and automation.

This manual is provided to provide general guidelines for setting up the C2Home® Server for the most basic configuration options. The C2Home® Server was designed to be intuitive in it's setup, so growth of the user's home network into more complex configurations should be easy. In addition - to aid the user in implementing a custom home security and automation solution the appendix of this document provides examples and an analytical approach to an integrated and effective home security system.

Getting Started:

Parts Included

C2Home® Server Kit	C2Home® Starter Kit	C2Home® Starter Kit with Video
<p>This kit assumes the user already has, or will separately obtain - the peripherals necessary to fully implement a C2Home® System for Local or remote access to X.10 devices, video, alarms via internet technologies (HTML, WML, SSL, etc). The server Includes integrated tools for property layout. Just load it on your PC and you're ready to go!</p>	<p>This kit includes the C2Home Server Software and the CM11A computer interface and an X.10 lamp module to allow even the non-technical commanders the ability to get started setting up the C2Home environment for both local and remote use.</p> <p>The kit comes ready-to-go right out of the box in a matter of a few minutes. In the event of a problem troubleshooting guides are provided to address the most frequently occurring difficulties.</p> <p>Kit Includes: C2Home® Server CM11A computer Interface X.10 base lamp dimmer module</p>	<p>This kit includes the C2Home® Server Software, CM11A computer interface and lamp module to allow users of a more advanced skill level the ability to set up the C2Home® environment for both local and remote use, and also the Intel Pro Cam USB camera providing a video source for integration into the base station environment.</p> <p>Kit Includes: C2Home® Server CM11A computer Interface X.10 base lamp module PC Camera (USB based)</p>
		

Hardware Installation

Before the C2Home® Server is started the CM11A device, any video capture card, and Ethernet or other PC interfaces should be physically connected to the PC. This section is provided to aid the user in understanding how to make the connections and configuration necessary to get the C2Home® Server up and running in a snap.

NOTE: If you intend to use the C2Home® Server without any CM11A (or similar device), configure the Base Properties - CM11A type to "None" and exit and restart the software. If this step is not taken the C2Home® Server will perform sluggishly as it awaits a response from a CM11 module that is not present.

CM11A to Serial Port



CM11A Computer Interface

Attach the CM11A device to the serial port of your PC. If you already use this serial port for another purpose other than C2Home – make sure that you have stopped that application. If you fail to stop applications making use of the serial port they will not allow C2Home software to bind to the serial port. If you have several serial ports available, go into SETUP-Base Properties to select the available serial port for use with the C2Home Server.

In order to verify that things are working correctly, we recommend you start with a single X.10 device – such as a Lamp Module (with a lamp attached) –plugged directly to the outlet right on the CM11A. This eliminates all other variables such as wireless network variables or power line noise. Use a small screwdriver on the rotary switches located on the Lamp Module to select the proper house code (“A”) and device code (“1”). It might be a good idea to just leave it at device code A1 to start.

Once the basic functionality has been verified (as instructed in the sections of the manual to follow) you should follow all manufacturers instructions for activating other X.10 compatible devices. Ensure that all are on the same housecode, but no two have the same unit code.

Software Installation

Loading the C2Home® Server on a Windows (Win95,98,NT, ME) PC

IMPORTANT NOTE: Because the C2Home® Server requires the JAVA Runtime Environment, during installation users are given an option to load the JRE. This may be accomplished by **performing the complete C2Home® Server Installation and selecting “yes” when prompted to make a decision regarding installation of the JRE. Otherwise it is assumed the JRE has been loaded before the C2Home Server is installed. In any case C2Home installation will automatically overwrite some files in the JRE directory to ensure the C2Home Server is configured properly. Advanced users preferring to manage the JRE**

independent from the C2Home installation may refer to the appendix for information regarding specific configuration information.

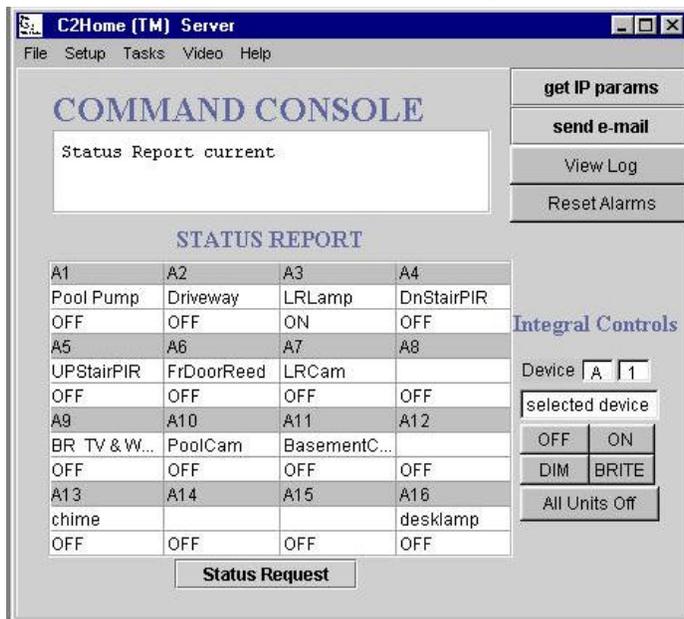
- 1) Place the C2Home® Server CD in CD Drive
 - Once the C2Home® CD has been placed into your CD drive, the installation program should automatically begin to run. System pauses for a minute or so are not uncommon, so please be patient.
 - Intro Screen Should Appear (Ft Irwin)
 - Welcome Screen Appears (Background is C2Home Server Setup)
- 2) Click the button "**NEXT>**"
- 3) The **Software License Agreement** appears (Please read and understand this). Click on the "yes" button only if you agree to the terms.
- 4) **Enter User Information**
 - Name
 - Company
 - Serial Number (located on the jacket of your C2Home Software CDROM disk)
- 5) Choose **Destination Location**. We recommend you choose the default location "C:\c2home". Only advanced users confident that they can manage all paths should select one other than the default.
- 6) Select **Setup Type** Unless instructed by C2H&O to choose another Setup - we recommend you choose typical
- 7) Select **Program Folder**. We recommend you choose C2 Home & Office
- 8) Setup Complete. Message Appears to inform you that you may be required to install the Java Runtime Environment before this software will run properly.
 - IMPORTANT NOTE:** If JAVA is required you must load the JRE and then reload the C2Home Server to ensure the JRE is configured properly for the C2Home Server. This may require loading the JRE and then ejecting the CD, and reinserting to restart the C2Home Server Software Installation Procedure.
- 9) Once Setup is complete you should be able to drag the **C2WIN Icon** from the program group to your desktop for easy access each time you wish to start the C2Home Server. As with any application invocation, you can also paste this icon into the startup portion of the windows-programs-startup menu.

To run the C2Home® Software

If the installation executed properly you should have an **icon with the C2Home®** logo on your desktop. You should be able start up the C2home Server by clicking on this icon. If the Icon doesn't show up on your desktop, or doesn't work properly you can start the software with the following command line (dos or Windows-Start-Run): **C:\c2home\guiserver\c2run.**

The appearance of the initial GUI for the C2Home server may be somewhat delayed (up to 30 seconds) depending on the speed of your PC and the number of applications competing with C2Home Server for CPU resources.

Note that if you already have a web server running such as MSN personal webserver or NT based Webserver these will prevent binding of the C2Home Server to the local host IP address. These non-C2Home Web Servers must be halted, or you must configure the C2Home Server HTTP port to something other than the default (port 80) before the C2Home Server is started if you intend to use C2Home for remote access.



Initializing the Software

Setting up the C2Home® software requires multistep process listed here and then described in detail later in this document.

1. Initialize all user configurable properties and layout the property using the integrated C2Home Layout tools.
2. The C2Home server may not operate properly until you have set the server properties properly for your base station and/or set the server operating options.
3. Verify the full functionality of the C2Home server locally, to the extent you wish to employ the features offered by this application
4. Use integrated tools to verify the remote access functionality locally. To access using a browser on local machine you can use Http:\127.0.0.1, or localhost or a legitimate IP address from a remote machine if you have been assigned one for any reason. You should be able to access using a PDA (palm, smartpone, etc) via Http:\\ipaddress"index.wml. Of course you can also access with domain name if you have actually registered one. (we are anticipating most running this software will be on dial up or dynamically configured internet connections and for this reason will not have legitimate domain names.)
5. Initialize all applications intending to feed data products to the C2home Server for consolidation and reporting. For example, as a Video source we recommend the Intel Pro Cam – Load only the Create and Share package. AutoSnap path must be changed to C:\c2home\GUIServer\payload. Save as a single file with the Intel default name AutoSnap.jpg.

Initializing BASE Properties

NOTE: values set might not become effective until the next time your C2Home® Server is started. To be safe you should always restart the server when you have reset any base properties.

Base Properties must be set to ensure proper operation of the entire C2Home® software application. The CM11A module should be put in place before the software is started. If the CM11A module is not in place or the serial port is not properly configured an error condition will result. The serial port cannot be shared with any other application. If you normally use your serial port for another application, such as a Palm hot Sync, you must shutdown this application before invoking the C2Home Server.

Base Properties

Setup E-Mail Reports and Alarms

Alert Addressee: watcher@pager.net

e-mail Originator: you@email.com

Mail Host (SMTP): smtp.email.com

ISP Call time: Sat 07:35:00 Example: Mon 21:15:00

Daily Time: 07:12:00 Note: 24 hour Clock

hourly: 00:00 Default to email alarms

Server Config

X.10 Serial Port: COM1 Default House Code: A

stat timeout: 20

Verbose Serial Port: client timeout: 20

Path to External Video Server: c:\c2home

Browser Invocation: c:\windows\Explorer.exe

Catalyst URL: www.c2home.com **Store Values**

To set Base properties - Once the C2Home Server software has been started - click on setup. Select "Base Properties". You should be presented with a dialog box to set the options.

Base Properties include two groups of configuration parameters to be set:

- **Setup E-mail Reports and Alarms** –provides the server with the information necessary send reports to you remotely. This must be configured properly for reporting to work.
- **Server Config** – Many of these configuration parameters are critical to the basic operation of the server.

You should make your decisions and set the server base properties as follows.

Alert Addressee – This should be configured to contain the e-mail address to which you intend to report alarms

E-mail Originator- This must contain a legitimate e-mail source of e-mails registered with the corresponding SMTP mail host in the next field below.

Mail Host (SMTP) – This would be the SMTP host name or IP address as supplied to you from your e-mail supplier or ISP (these usually take the form: SMTPserver@something.com).

ISP Call Time – This would be the time at which you wish your C2Home server to e-mail a single situation report to the alert addressee identified above. **Note that the form for this and all reporting times are specified in military time (24hour clock). For those customers more accustomed to conventional am-pm clock, this simply means all hours after noon are added to the number 12.**

Daily time– This would be the time at which you wish your C2Home server report in and e-mail situation report. **Daily.** If you do not wish to receive daily reports, a bogus value such as XX:XX:XX will prevent daily reports.

Hourly This would be the time at which you wish your C2Home server report in and e-mail situation report **hourly.** If you do not wish to receive hourly reports, a bogus value such as XX:XX will prevent hourly reports.

Default to email alarms– Check this box if you wish that the initial state of the server whenever the software is started is to send emails for all alarms and reports. (the state of the server can also be set temporarily in the extended view of the Command Console, but this will revert back to the default state when the software is restarted)

X.10 Serial Port – This field is asking the user to specify which COM port will have the X.10 based CM11A module attached. Typically this is either **COM1** or **COM2**. It may be easiest to try both if you don't know (one at a time).

Default house code – This is a single capital letter which must be selected by the user **A** thru **P** representing the default house code to be monitored whenever the C2Home software is restarted. The monitored housecode can be changed temporarily in the Command Console extended view, but this will revert back to the default state whenever the software is restarted.

Stat Timeout– Non – HTTP Server Sockets are a resource to be managed. If these go unused for a period of time it may indicate a communications malfunction. This particular timeout is for the status applet. If no action is seen on this socket for the timeout period the server will release the socket, allowing it to be used for another connection. If the status applet keepalive has been invoked and remains active, this socket remains open indefinitely. Applets do not default to HTTP communications. TCP ports will timeout after a user specified interval to ensure that the port is not locked up in a user

Client Timeout – This particular timeout is for all client device control applets. If no action is seen on this socket for the timeout period the server will release the socket, allowing it to be used for another connection.

HTTP Port - conventionally port 80 is used for HTTP transactions. However, if you prefer another port this is user configurable. Use of a port other than 80 may enhance security, but may also prevent access from remote browsers thru a proxy server or firewall.

Verbose Serial Port – This is a check box allowing the user to determine if the log or dos screen should report detailed information regarding raw data received on the serial port, or remote requests. Verbose mode may be important for determining who may have been trying to remotely access your C2home Server as all requests for login are logged by user's internet ID (typically IP address). Checking this option chooses that all serial port bytes are written to the parent shell screen. This may come in handy for troubleshooting or to determine if responses are appropriate. This was originally a development tool, but seemed handy for general purpose use, and so was made available for the consumer product.

Path to External video server – For those who wish to use another web server, such as an axis web cam as a video server, this would be the path required to retrieve video as demanded at the command console.

Browser Invocation—this field is meant to capture the command line required to invoke your browser. This is only used in the Command Console extended view to invoke the applets for modular control and status. The default is the typical command line used with Internet Explorer. The Netscape equivalent is very similar. You should verify this at a dos or windows command line before you assume it's correct

Catalyst URL– This field is very simply the URL to be used to kickoff an internet connection. This is mainly for use with dial-up connections to the ISP. Whenever an event occurs requiring access to the Internet, this URL will be called to initiate the dial connection. While we at C2Home & Office enjoy watching the site counter increase with each hit, we ask that you find a more suitable URL to use than the default.

Max Log Days - This is the maximum days for which the C2Home server will actively log all events. (Old logs are automatically stored to a backup file identified in the log file). To optimize performance, computer resources are optimized with a minimum value. If verbose serial port is not selected logs can be substantially older, as in that case fewer events are being logged.

Finally, after completing your data entry for base properties you must store these values or they will not be effective. In addition you should note that the values set might not become effective until the next time your C2Home Server is started. To be safe you should always restart the server when you have reset any base properties.

VIDEO CONFIGURATION

Initializing Local video Capture

Once connected to your PC, the camera or video capture device should be autodetected by Windows. Direct windows to use the driver that comes with your video capture device. You may have to reboot windows before this becomes effective. Normally the device driver is provided by the manufacturer on a disk with your video capture device when purchased. If you don't have the proper device driver available, the C2Home Server CD may have a compatible device driver in the drivers directory. It is also very likely the manufacturer or another party has the required device driver available thru a website. Simply search by model number via any common search engine.

When the C2Home Server is started for the first time, local video capture will not be configured to operate properly. To configure video properly from the Command Console go into **SETUP – VIDEO CAPTURE PROPERTIES**.

The C2Home Server should detect all available compatible video capture devices currently configured (including device drivers). If another application is accessing the capture device - shut down the application. To make the C2Home Server aware of the video capture device go to **Setup->Video Cap. Props -> new capture -> detect devices**. Wait a few seconds for a video device to be detected. Then close out both the **Media Device Detect** and **Video Config** dialogs. When you reopen **Setup->Video Cap. Props** the drop down list of device names should include the capture device. Select this new device and check the box marked **Video Capture**. Make sure to store the values. When you restart the C2home Server the Video Capture should be visible in the streaming video frame.

Click in the small square next to Video Capture causing a check to appear in the checkbox. Now click to the right of the **DEVICENAME** drop down box to select from the list of video capture devices. Choices for other parameters such as height and width may or may not be selectable depending on the device driver provided. If no choices are available you should leave these at the defaults. Now store these values for them to become

effective. You should now close the C2Home Server. These will become effective the next time the C2Home Server is started. NOTE: Video capture may take up to 20 seconds to complete when starting the C2Home Software. In order to ensure this capture occurs properly do not advance past the C2Home introductory screen, but rather wait for the screen to advance to the Command Console on it's own.

Local Video Capture is periodically saved to the hard drive with the file specified as "Grabfile Name:" in the **Video Capture Properties** at the interval specified by "GRAB INT (S) in the **Video Capture Properties** screen.

Once you have completed the setup screen for local video capture you must press the "STORE" button and restart the C2Home Server before the video capture device is assessable by your C2Home Software.

Video via HTML

As mentioned above, Local Video Capture is periodically saved to the hard drive with the file specified as "Grabfile Name:" in the Video Capture Properties at the interval specified by "GRAB INT (S) in the Video Capture Properties screen.

This file along with any other image file accessible by the C2Home Server is accessible once configured within the **SETUP- HTML Video Sources**. This also enables this video source to have event driven frames archived. Configure Source Properties by first creating a name to use to label this source (e.g. Garage, Pool, etc)

To add a new HTML source to the environment select "ADD NEW" from the dropdown list. Within the field labeled "Source label" type a unique name for the video source such as "bedroom" or "Pool". If the video source is from a device with multiple integrated video cameras (such as an Axis Cam Server) choose the family option and indicated the number of cameras for this path. Then specify the path to the video source such as "http:\\10.0.1.135\\largesize" or if you have edited the hosts table or have a domain name resolver you can use names such as "http\\guesthouse\\front yard" .

Finally, you must store this configuration by selecting the "Accept" button. This new video source becomes immediately available in your layout tool and can be viewed with the "HTML Video Sources" or "video applet component activator as part of your Command Console. Once the floor layout has been updated to include this video source you will be able to view the video remotely with any Java compatible web browser

X.10 Device Labels

Current Device Labels	
1 Pool Pump	9 BR TV
2 DrivewayLt	10 Cam 2 sw
3 LroomLt	11 Cam 3 sw
4 Sprinkler	12 Cam 4 sw
5 Office PIR	13
6 DoorReed	14
7 Cam 1 Sw	15
8	16 OfficeLamp

Store Values

This panel allows the user to specify unique names for the devices on the monitored housecode. Each name will be stored and become the default used whenever the software is restarted. These labels will appear on the Command Console device table after the first status report is received and displayed.

Setting ALARM and ALARM EVENT Properties

The screenshot shows a window titled "Alarm and Alarm Event Properties". It contains five rows, each representing an alarm event. Each row has the following fields:

- AlarmEvent 1:** Response Command: [A] [7] [ON]; Message: [No Message set]; VID GRAB: [] []; Flash Behavior: count [1], Interval(s) [1].
- AlarmEvent 2:** Response Command: [A] [13] [ON]; Message: [No Message set]; VID GRAB: [] []; Flash Behavior: count [1], Interval(s) [1].
- AlarmEvent 3:** Response Command: [A] [13] [ON]; Message: [No Message set]; VID GRAB: [] []; Flash Behavior: count [1], Interval(s) [1].
- AlarmEvent 4:** Response Command: [A] [13] [ON]; Message: [No Message set]; VID GRAB: [] []; Flash Behavior: count [1], Interval(s) [1].
- AlarmEvent 5:** Response Command: [A] [13] [ON]; Message: [No Message set]; VID GRAB: [] []; Flash Behavior: count [1], Interval(s) [1].

Additional controls on the right side include "Disarm Alarms" and "Disarm Alarms Event" (with a dropdown set to [A] [1]), "Restore Defaults", and "Store Values".

This configuration panel allows users to configure the server to recognize action on certain events as being alarms, and also allows the user to specify the way the server should respond to alarms. The user has the option to specify the response as either a device state response and/or a Video frame capture. State responses also have the option to specify a flash response. Flash responses are cyclical on/off responses for the duration and repetition specified at the bottom left on this panel.

Shown are the configuration fields for five events (currently C2Home supports only five event based events)

Alarm Events This data field should be configured to identify by house code and device code the device for which any related event should be considered an alarm

Response Command This data field should be configured to identify by house code, device code and command (ON, OFF or DIM) to be used as a response to the alarm identified

Message – This data field should be configured to include the message to be sent to remote users and recorded in the log when the corresponding alarm occurs

Vid Grab–. Selecting any option other than “none” here configures the response to include a frame grabbed from the camera specified. This frame can then be viewed as the “**Previous History**” in either the Video panel on the base station or in a video applet viewed remotely.

FLASH – A check in the flash check box turns on the Flash response for the associated alarm response.

Flash Behavior allows you to set the response as a repetitive response with a user configurable repetition rate (interval) and user specified number of times. When a event triggers such an alarm response the chosen device response will cycle on and off at the interval chosen, and repeat the number of times chosen.

Disable Alarm This option allows the user to specify a special X.10 address which when triggered by a remote control (such as a wireless remote control) will serve to disable the current patrol watch shift. (see Patrol Watch). Repeating this action again will serve to once again toggle the patrol watch back in service again. This "Disable Alarm" code feature is ideally used to prevent alarms from triggering when entering a house .

Property Layout

Perimeter Map Designer

Stencils Background Edit

Background C:\c2home\GUIserver\payload\1st_Floor.jpg

1st Floor View

CONTROL TYPE

- No Link
- X.10 Basic!
- X.10 Dimmer
- X.10 PIR Sense
- X.10 Timed Dev
- Camera

OUTPUT MAP

- basement
- 1st Floor
- 2nd Floor
- 3rd Floor
- user define

SAVE MAP

default.html

Default.jpg save image

1. Start the Layout service. To do this use a mouse click on the top bar of the Command Console chose **Setup – Layout** This should invoke the **Perimeter Map Designer**
2. Once the Map Designer Appears chose floor to be worked (basement through third floor allowed) Here you should first select which floor level you wish to design. The default floor when the map designer is opened is the 1st floor - a good place to start .
3. Chose background to be used. If you chose old background the existing background along with the icons already placed on this old background will be used. Alternatively users may choose to make use of a new user specified JPEG or GIF as the background image. You may choose to import a background created in another tool such as Paintbrush (must be either a JPEG or GIF file, recommended to be 4 inches by 4 inches (This dimension only applies as a reference value, such images can be displayed at any chosen size). The first time the floor layout is used a default background is presented with the a square box and a floor name as shown in the diagram.
4. To import the background, choose “**Load User Defined**”. A file finder dialog box should appear to assist you in locating the image file you wish to use as a background. Once you have chosen the file to use, press the “OPEN” button on the dialog and wait a few seconds for the background to appear.
5. Add features to the background image we have provided some stencils. These are in the Stencils, drawing tools. Features with no device associated with them should be chosen with the “Control Type” option specifying “No Link” Otherwise the tool will try and associate a hyperlink with the object drawn. You can always undo mistakes with the Edit Undo function.
6. Devices such as cameras or X.10 devices should be identified by clicking in the small circle on the right of the screen next to the device type. Click once at the beginning position and again at the end position. This creates a box to be used to position the object.
7. Chose the component to be placed. This is done by first selecting the desired stencil. Stencils are groups of component icons. As a stencil is chosen the group of components appears on the buttons to the right of the map layout.
8. After a stencil is chosen, and individual component should be chosen. This is done by simply clicking on one of the component buttons to the right.
9. Identify the component type. Users must select the component type (X.10 or video). If the user just wants to place a shape with no HTML action behind it – the option “none” should be chosen.
10. Click once in the upper left hand corner of the position where the component should be placed. Then release the mouse. As you move the mouse down and to the right you should see a black box growing. This is to show the size of the component after it is placed. Once the box is to the desired size, click the mouse again to lock in on the component position. Once the mouse is released again the component should appear. If the component is to be an X.10 component or a camera - Immediately a dialog box should pop up allowing the designer to specify the component identify. X.10 devices should a house code, device code and a label for status reporting purposes.
11. If a mistake has been made the user has the option of selecting Edit – Undo to reverse the last component placed.
12. After the design of a single floor is complete, each floor image should be saved and then each HTML map should be saved. This is done by clicking on the **save image** button, and then the **save map** button (in that order). It is not necessary to change either the image name nor the map name. The names of each will be auto generated to labels recognized by the C2Home Server.

Adding Stencils

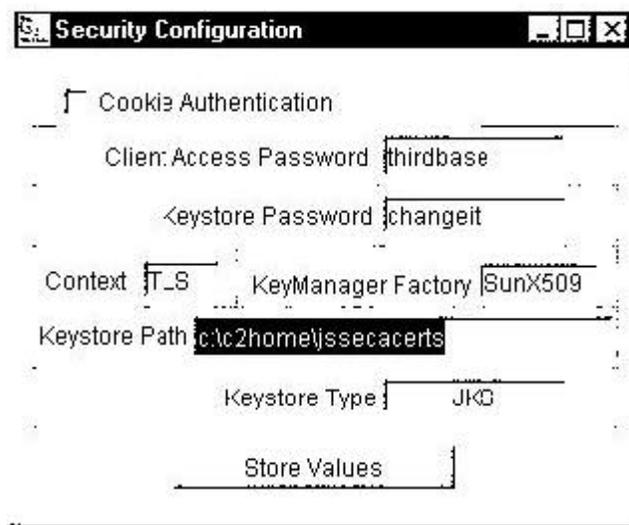
Users may import stencils directly independently created or created by a manufacturer. These are simply GIF files stored in the \C2home\GUIServer\user directory. These gif files should be renamed –“control1.gif” thru “control9.gif” (all lower case, case sensitive). Many manufactures such as X.10 have webpages with Gif or JPEG files containing images of their products - which can be saved directly

to the users base station hard drive for this purpose. While viewing such images in a browser such as IE or Netscape - just right click on the image and specify the path and name of the file.

Security Configuration

This panel allows the user to configure measures to ensure the privacy and confidentiality of remote sessions with the base station. Client access password and cookie authentication are applicable to both normal HTTP access, while all other fields pertain to configuration for HTTPS access (SSL). The default values provided are sufficient to operate the SSL server without further configuration, but as a minimum users should change the client access password from the default. Note that cookies are not used for WML access to the base.

Cookie Authentication – This is a check box allowing the user to select whether or not cookie based



authentication is to be used. Cookie based authentication requires that the user after logging in, to automatically store a cookie provided to their browser (a common browser configuration option). After that point access to any additional screens requires that the cookie be in served up with the request. This all occurs transparent to the user. This prevents malevolent remote users from bypassing the login screen and going right to the HTML pages served up for command and control. If you are sure you are not susceptible to attack, cookies might be an inconvenience, in that they deny direct access to all C2Home products remotely without a legitimate login and password.

Client access Password - - This is a mandatory field for remote access This field contains the user selected password to be used for remote access via a browser. This is used to prevent remote access by those who do not know the password.

Keystore Password – This is required for SSL access (HTTPS). If you have derived a legitimate key and stored it properly in a keystore, the keystore should be password protected.

Keystore Path This too is required for SSL access (HTTPS). If you have derived a legitimate key and stored it properly in a keystore, you should explicitly define the path to obtain the keystore in this data field

To fully understand how the C2Home Server can be configured to utilize a key please refer to the section of this document entitled “Key Management for Secure Communications”.

Key Management for Secure Communications

The default configuration of the C2Home Server is sufficient to run SSL, but limits the degree to which security may be personalized to make use of any unique encryption key. To reduce risk of exposure of information critical to the most secure versions of the C2Home Server application, this section will only be provided upon request by the user to the following e-mail address: Custserve@c2home.com

Patrol Watch Duty Shift Assignments

The screenshot shows a configuration window titled "Patrol Watch Assignments". It is divided into four sections: Shift 1, Shift 2, Shift 3, and Default. Each section has a "begin shift" and "end shift" field (each with a dropdown for "XX" and a "00" field), a "day(s)" dropdown menu (set to "MTWTF"), and an "e-mail alarms" checkbox. To the right of each shift section is a list of "Event based events" (event resp 1 through event resp 5) with checkboxes. In the Shift 2 section, all five event response checkboxes are checked. In the Shift 3 section, the "begin shift" dropdown is set to "XX" and the "end shift" dropdown is set to "XX". In the Default section, all five event response checkboxes are checked. At the bottom of the window is a "Store Values" button.

Patrol watch personalities were created to try to mimic behavior of manned patrol shifts. The user sets the policy for any of three shifts, and selects the start time and stop time for that shift.

Event responses for each shift correspond to the events and event responses configured in ALARM and ALARM EVENT Properties. Selecting an event response by checking event response 1 directs this shift when on duty to observe this alarm and respond as prescribed in the alarm response configuration. You determine when each shift is on duty by assigning the begin shift time and the end shift time values. The default configuration is in effect when no other shifts are active.

Rules:

- Only one shift should be expected to be on duty at any point in time. (No overlaps in duty). Overlaps will result in the most recent shift scheduled to begin overriding the previously active shift.

Timed Events

X.10 Timed Events:						
1	A	3	ON	20	30	00
2	A	3	OFF	22	00	10
3	A	7	OFF	13	00	15
4	A	1	OFF	17	45	20
5	A	9	ON	05	30	30
6	A	9	OFF	08	00	40
7	A	9	OFF	23	30	00
8	A	16	ON	20	15	00

HTML Video Timed Camgrab Events:						
9	VID GRAB			XX	00	00
				Interval(s):	1	count 1
10	VID GRAB			XX	00	00
				Interval(s):	1	count 1
11	VID GRAB			XX	00	00
				Interval(s):	1	count 1
12	VID GRAB			XX	00	00
				Interval(s):	1	count 1

Restore Defaults

Store Values

This panel allows the user to configure up to twelve different timed events (eight X.10 and four video snapshot (camgrab) events). All can be specified with split second precision. Each event should specify this device (house code, device code) desired state (ON, OFF, Dim, Bri) and the time at which the event should occur in hours minutes and seconds. Keep in mind that this time is specified in Military time (24 hour clock). Each device event command is actually attempted twice to improve upon the normal reliability of X.10 device response. If the interface is busy or some other extenuating circumstance is preventing device response, the software will try again a half second later.

The Camgrab events must specify which of the configured html video sources should be used to capture the image. HTML video sources must be previously configured in the **Setup-HTML Video Sources** panel to be selectable for in the drop down lists provided for **VID GRAB**.

Communication Options

Option 1 Dial up Direct

The basic strategy for this connection is to have the MS Dial-Up Server configured and standing by waiting for a compatible client to dial in. IP Addresses must be on the same subnet, but neither have to be public IP addresses. DUS allows password protection.

Option 2 Dial up Server-ISP, Remote Access Fixed

Here the Remote server is dialing into the Internet as needed, but the remote connection is fixed. This is common when the remote user is on an office LAN. Very little has to be done at the remote site to make this work. The base station connection can get by with a dial up Internet connection as long as it is set to remember the password. The email sent due to a timed report, timed event, or event-based event, contains the dynamically assigned ip address. The remote user has but to simply enter this IP address into the browser URL field, click return and the base server should respond as long as the connection is open. This time for the connection to remain open is configurable in MSIE. We recommend 20 minutes as a security precaution. Continuously open dials up connections are not stable and can also occasionally be detected by nefarious agents.

Option 3 Fixed Remote – Fixed Sever Connection

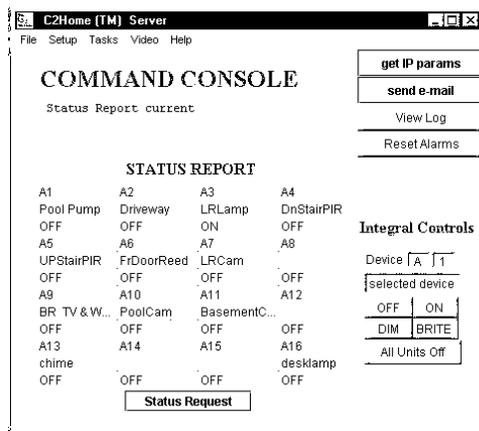
This is the easiest and most reliable connection to work with. This will also usually yield the best performance as most fixed connections are of a higher speed. Here the user can use the emails received to determine the IP address, or simply click once on the “get IP address” button on the Command Console. This only has to be done once. If DHCP is being employed on the fixed connection their may be a lease period after which this information will be refreshed.

NORMAL OPERATION

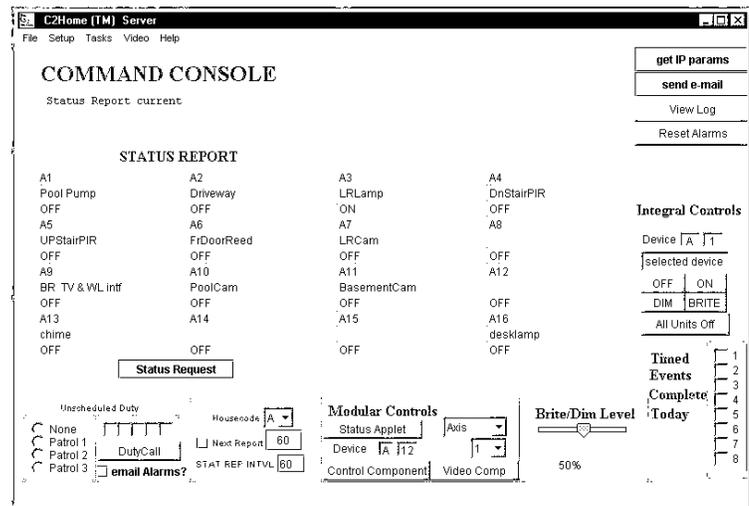
To use command console to control devices, place the mouse over device position on the table of devices and click. This selects the device. Then control the device using on, off, dim, or bright. The dim level can be set with the slide bar displayed in the extended view of the command console

Extended View of Command Console

Selecting view extended presents a longer screen for the command console. The bottom of this longer screen provides controls to be used to instantaneously adjust fundamental properties of the server. These include selection of the patrol watch, e-mail, server update rate, dim/bright level, and additional controls to invoke applets for component controls. These applet-based controls are identical to the controls to be used for remote access, and can be used to verify local operation before depending on remote access.



Normal View



Extended View

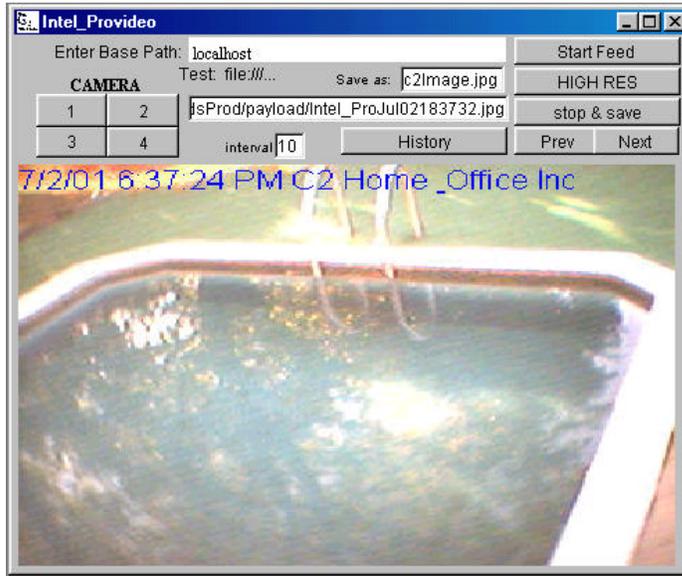
Verifying Proper Operation

On the command console there a number of options are provided to enable the performance of remote components before you try to access the server with a real browser

- **Send e-mail** can be used to simulate the response your C2Home Server might have to an alarm. When you press this button, if an Internet connection does not already exist, your C2Home server will initiate an Internet connection and send a test e-mail to the address you specified in your base properties setup. This test email will include the status.
- **Get IP Params** while you have the Internet connection in place you may wish to verify that the Internet address detection mechanism is working properly. This verifies that the mechanisms put in place to detect the current host Internet connection are working properly. Once this button is pressed the Command Console should display the current internet IP Address(es) assignment. If this does not

work properly, it is not possible for e-mails generated to include the correct assignment. This is especially important for users relying on dial-in connections to an ISP for e-mailing reports.

- **Modular Controls**, part of the extended view of the Command Console, can be used to verify the operation of Applets and the ability of applets to communicate with the base station server. Note that cookies really have to be turned off for this to work properly (being that there are no log in prompts to get the initial cookie assigned).



Video Window

In addition to basic web cam access, the C2Home® Server provides the ability to see archived JPEGs remotely, such as snaps grabbed when particular events occur. C2Home® provides the ability to use a browser to control the cameras remotely and SSL to ensure privacy. *Do you know who's intercepting your webcam video now?* Selecting video from the command console presents a number of video options. Axis, Ispy, Intelpro Each relies on other configuration settings to view the video presented.

View Log

Clicking on the View Log button of the command console will initiate the log screen to appear. Depending on the size of your log file and speed of your computer this may take several seconds. Slower computers should clear out the log regularly by clicking on the Restart Log button inside the view log dialog.

The log presented will not be automatically updated with events as they occur. If you wish to see events that have occurred since the time the view log screen was presented you may click on the Load button within the view log screen.

Base Watch

Clicking on the **BaseWatch** Button will direct your **C2Home Server** to take a snapshot of your desktop and put this up in the space of your entire display screen. While in this mode anytime the keyboard or mouse are used an alarm response is triggered. The alarm triggered will always be the first alarm of those listed in the SETUP Alarm Response dialog. Note that this feature will function without the use of any X.10 devices. You can use this feature to take a snapshot of whomever may be at your PC, and also log every key that is pressed to determine what they have been doing. Note that if the desired response includes

taking a snapshot, a html video source must be configured and selected at the response to Alarm number 1.

Remote Access

The C2Home Server may only be access remotely via an internet browser. To verify that this means of accessing the C2Home Server is functioning properly, you should access the base server using a browser on the server using the following URL `http://127.0.0.1`, or `http://localhost`, or the legitimate host IP address (if the server has been assigned one) as follows: `http://<hostipaddress>`. A legitimate IP address assignment and proper routing between the server and clients are necessary for remote access to the server from the clients.

Similarly, to access home base from a remote location via any standard browser, the URL entered in your browser should be derived using the following formula:

`http://<homebase>`

Where `<homebase>` is most likely the IP Address provided to you in a emailed report. If the home base connection is a fixed IP connection the IP Address will always be the same. You can also access with domain name if you have actually registered one. Most users running C2Home software won't have legitimate domain names.

Remote Login

The first screen presented when remote access works properly should appear as shown. To proceed enter your login name and password as configured at the base station. (if you haven't reconfigured it - the

C2Home Server - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Stop Refresh Home Search Favorites Media Histo

Address `http://localhost`

C2HomeServer Login:

Username

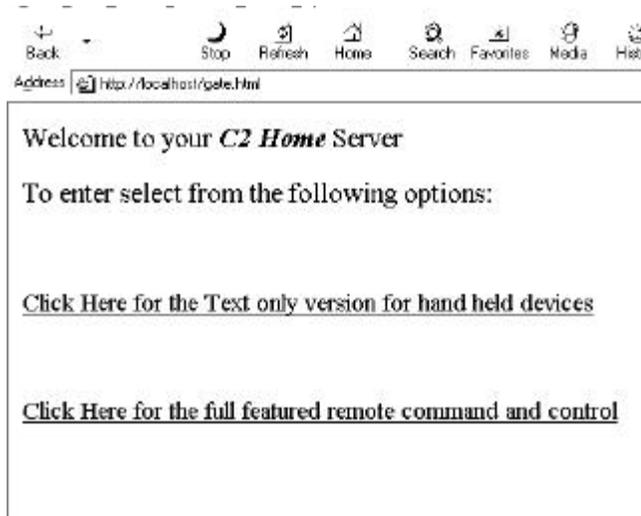
Password

Submit Reset

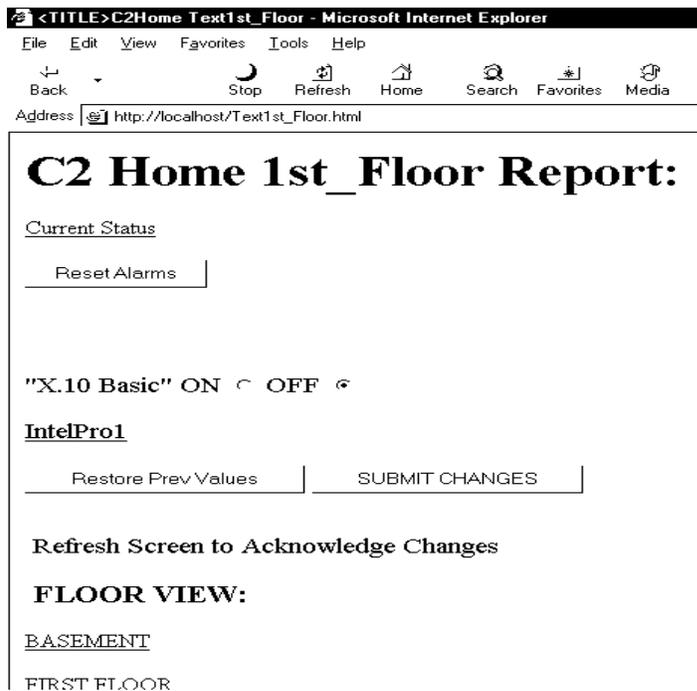
[palmtop version](#)

Copyright: C2Home & Office Inc. 2000

default password is "thirdbase").



If the login is successful, you should be at the "gate.html" screen. This is the point where you choose if you want simple "HTML text" screens or the full featured Java applet screens. The text based screens are ideal for primitive browsers, such as those which do not run Java.



To see video or other video control in a separate window hold down shift key while selecting the camera or device icon.



Phone and PDA Access



Users are able to access the C2Home® Server with handheld devices while on the go. These allow not only reports of status, and a view of event logs, but also remote control of X.10 devices. *This really comes in handy if you forgot to turn on the sprinkler or the pool before you left home.*

Remote access via a WML enabled browser is very similar to access via a normal desktop browser, the only difference being the addition of a few letters to the URL to specify the desire to utilize WML.

To access home base from a remote location via a WML enabled browser, the URL entered in your WML browser should be derived using the following formula:

<http://<homebase>\index.wml>

Where <homebase> is most likely the IP Address provided to you in the emailed report to you. If the home base connection is a fixed IP connection the IP Address will always be the same.

In other words, you would use the same URL normally used to access home base on a full size browser, plus the addition of the "index.wml" term to specify that you desire to access home base via a wml.

Troubleshooting

Symptom	Problem	Solution
After loading the C2Home Server, Icon appears on desktop, but nothing happens when double clicked.	Possible corrupt file, or file not copied correctly.	Try reloading software. New JRE load may be unnecessary if not corrupted. As last resort, possibly use DOS prompt command "C2Run" to see java run in a terminal mode. Error message may be indication of missing or corrupt file. If you tried to use your own instance of the JRE, environment may not be correct for this application.
C2Home® Server will not run on the version of Java (JRE) I have running on my host.		The C2Home Server was compiled with JDK1.3. You must have JDK1.3 or a newer version to ensure operation. If you are using your own version of the JRE you should delete the java.exe and javaw.exe files in the GUIserver directory, and ensure that you have defined paths to your own JRE. If you are intending to work with a configuration other than the default provided with the C2Home® Server it is very likely that any problems you have will be related to paths.
Direct Video Capture not visible on from the base station console	Another application may be accessing your video capture device or the C2Home Server is not yet aware of the video capture device.	If another application is accessing the capture device - shut down the application and restart the C2Home Server. If the C2Home Server is not yet aware of the video capture device go to Setup->Video Cap. Props -> new capture -> detect devices. Wait a few seconds for a video device to be detected. Then close out Video Cap Props and re-open it. The drop down list of device names should include the capture device. Select the device and check the box marked video capture- The make sure to store the values. When you restart the C2home Server the Video Capture should be visible in the streaming video frame.
Error Message : Main Class GUI not found	Application file has either not installed correctly or is corrupt	Re-install C2 Home Server.
Web Cam Video Shows corrupted image		Reboot of webcam application. Perhaps use MS Scheduler to reboot all applications regularly to ensure reliability.
C2Home shows mail going out, but mail is never received.	Mail service provider is erroneous.	Complain to ISP or Mail service provider or perhaps get a new mail provider
Com port not available	Driver for Com Port is either occupied or stuck in an erroneous state	May require you access MSWIN98 control panel, systems, and remove driver. Then do autodetect to reinstall the comm port driver. (warning: This may require that you have your WIN98 installation disk handy)
Status not reporting properly on	X.10 problems between	Reinitiate wireless interface module (upplug

Symptom	Problem	Solution
command console	CM11A module and the wireless interface	and plug-in), set all units off.
Intermittent X.10 Response	Possible noise power lines	Electric Motors running on power lines in the proximity of any device may inhibit performance. (Electric Motors create exorbitant electrical noise not only on power lines but also as radiated RF)
Command Console invocation of status applet or control applets are not responding	Browser invocation line in the base properties is not set	When first loading C2Home Software make sure you save all properties (Setup properties) at least once. Ensure the line indicated in the base properties for browser invocation is appropriate for your browser. You can test this on a DOS command line by duplicating the line and ensuring it starts your browser.
Command console will not activate applet based components properly. Gives login screen or browser doesn't open		Cookies must be turned off for component simulator to work properly. Also base properties must have proper browser invocation command line.
Command Console device status table does not populate		This make take a minute after startup if there are a number of commands queued up within the CM-11A buffer. If this fails completely it is most likely a hung serial port. Ensure all applications using serial port have been halted before C2Home Server is started. Reboot may be required if port is held in a hung state. Wrong Serial Port may also be assigned. Setup-Basic properties allows selection of proper serial port.
No response on Command Console applet view for a component control or video	Not yet configured	The applet for a particular component is not necessarily in existence until you have done a property layout. This creates the applet. Once the applet has been created it should be accessible in both the remote view and Command Console component viewer.
java.security.NoSuchAlgorithmException: Algorithm TLS not available		java.security file is missing or does not reflect the proper security provider (10/99 version is too old)
C2Home® Server performance is sluggish.	No CM11A device attached to the serial port	If you intend to use the C2Home® Server without any CM11A (or similar device), configure the Base Properties - CM11A type to "None" and exit and restart the software.
		The timer may not work properly until you go to the properties screen, fill in times for the timed events, and save the file. Then restart the program. If you check in the checkbox for the next interval it should show the counter counting down.

Glossary

Applet	Java programs which are specially encapsulated to run within a web browser environment.
C2	Command and Control – a term universally employed by militaries of the world to describe the function performed by commanders at all echelons to actively direct subordinate activities based on collected intelligence and disciplined decision making.
Cable	The cable industry has experienced dynamic changes over the last few years. Traditionally, cable companies offered only video services. Today, cable companies are broadband companies offering video digital and analog, high speed Internet access, and local telephony. These new services will help boost cable industry revenue by as much as 67% over the next five years. Adding to this fuel is the consolidation of the industry..
DSL	Digital subscriber line (DSL) technologies leverage ordinary twisted copper pair telephone wires to deliver broadband data connectivity. DSL is revolutionary not only because it offers an inexpensive substitute for existing fractional T1 and T1 customers, but because it creates a tremendous opportunity for small and medium sized businesses to migrate to broadband connections that make new services and Internet applications possible.
PIR	Passive Infra Red - Sensor – detectors which employ detection of radiant heat energy as light in the Infra Red region of the electromagnetic spectrum.
USB	Universal Serial Bus a now commonplace serial interface on personal computers (esp. IBM or Apple)
X.10	a communication protocol widely accepted as an industry standard for communication between devices via AC power lines within a single facility. X 10 communicate between transmitters and receivers by sending and receiving signals over the AC power line wiring. These signals involve short RF bursts, which represent digital information.
Internet	It is a worldwide network of interconnected computers, "containing" protocols for accessing the Web, email, Telnet, newsgroups, etc. There are about 60,000 independent, interconnected networks that comprise the Internet. The Net is the set and the World Wide Web is just one of many subsets.
ISP	Internet Service Provider – Used by many households to access the Internet via either dial up or broadband connections. And ISP has a high-speed connection directly to the Internet. They "sublet" access to the general population, who cannot afford or maintain such connections on their own. You connect to the ISP, who in turn connects you to the Internet through its own connection.
Server	A computer that stores Web site files and "serves" them to clients requesting them
Client	A computer system that asks another computer to do something for it. Your computer is a client when it asks a server to send it a Web page.
Browser	a software program that interprets and arranges (based on coded programming instructions, such as HTML) all the hypermedia elements (text, sound, images) contained on a Web page. Note that different browsers (Internet Explorer and Netscape Navigator, to name just two) may interpret and render identical HTML code in different ways
SOHO	Short for: Small Office/Home Office. Used to identify people who work from home or small home based businesses
PDA	the abbreviation for Personal Digital Assistant , a handheld computer that can be connected to desktop computers to upload and download information. (i.e. handheld, Palm top, etc), also now embedded in Smart Phones.
WAP	Wireless Access Protocol used in smart phones for data formatting and exchange.
URL	an acronym for Uniform Resource Locator , describes the address (e.g., www.c2home.com) and method of reaching a file (e.g., http) on the Internet. Today most people use "URL" and "domain name" interchangeably. URLs, in their complete form, usually take this form: protocol://host.domainname/directory/filename.filetype
WML	Wireless Markup Language _ analogous to HTML used with common PC based browsers, WML

	is the de facto standard for browsers in handheld devices.
--	--

Appendix A: House Device Labels Worksheet:

For your convenience this worksheet is provided to help keep track of current device assignments. Photocopy this worksheet and use it as a record of your current device assignments. If your copier allows, perhaps you can make a miniature copy, and keep it in your wallet. Laminated versions will last longer. Keep in mind that you might not want this to fall into the wrong hands.

Sample Version:

C2Home® Devices deployed.			
House Code: B .			
Device 1	Device 2	Device 3	Device 4
Label: Pool Pump	Label:Driveway PIR	Label: LR Lamp	Label:
Device 5	Device 6	Device 7	Device 8
Label:Office PIR	Label:SideDoor PIR	Label: LR Cam SW	Label:
Device 9	Device 10	Device 11	Device 12
Label:MBR TV	Label:	Label:	Label:
Device 13	Device 14	Device 15	Device 16
Label: Chime Alert OTHER NOTES:	Label:	Label:	Label:

C2Home® Devices deployed.			
House Code: . . .			
Device 1	Device 2	Device 3	Device 4
Label:	Label:	Label:	Label:
Device 5	Device 6	Device 7	Device 8
Label:	Label:	Label:	Label:
Device 9	Device 10	Device 11	Device 12
Label:	Label:	Label:	Label:
Device 13	Device 14	Device 15	Device 16
Label:	Label:	Label:	Label:
OTHER NOTES:			

C2Home® Devices deployed.			
House Code: . . .			
Device 1	Device 2	Device 3	Device 4
Label:	Label:	Label:	Label:
Device 5	Device 6	Device 7	Device 8
Label:	Label:	Label:	Label:
Device 9	Device 10	Device 11	Device 12
Label:	Label:	Label:	Label:
Device 13	Device 14	Device 15	Device 16
Label:	Label:	Label:	Label:
OTHER NOTES:			

APPENDIX B: Planning Security Operations

- **Mission - Protect**

While the C2Home system has capabilities to support Command and Control operations beyond those limited to security operations, security is certainly a component of C2 which should be taken most seriously. The purpose of a security system, in general, should be to serve to provide some level of protection for the element of concern. The element of concern can generally be assumed to be persons and/or property. While security systems can frequently help in recovering damages, this should be considered a secondary objective to be sought once sufficient assurance is in place to ensure that the elements of concern are no longer at risk.

The C2Home Server, and the collection of hardware and systems making up your automated home security system, should not be considered the complete end-to-end security solution. Rather C2Home should be considered an augmentation to the system you currently have in place. For example: Your current security apparatus may just include windows, door locks, and your own senses detecting possible threats, combined with your response involving telephone and the police. C2Home can take the burden off your senses and the pressures to detect signals, process these and filter threats, and respond by taking measures to alert private or public authorities to respond.

C2Home can be viewed as a tool for security enhancement. The effectiveness of the C2Home system as a security system, and any security system for that matter, is directly dependant on the quality of the planning that goes into to implementing the system. As with any effective tool, preventive maintenance is important to ensure reliable operation.

- **Strategy : Risk Assessment, Threat Detection, Response Tactics**

- **Risk assessment**

Developing a strategy for enhanced home security must begin with a reasonable assessment of current risks. Users should deliberate on the risks and vulnerabilities. Be as honest as you can about why you feel you need home security. List these risks on a piece of paper and address each individually.

Characterize risks (e.g. internal vs. External, Animal vs. Human, etc). Use observations: either automated, or directly observed evidence to try and determine the nature of the offending element. Newspaper stories, footprints in the dirt, tooth marks on the garbage containers. Be resourceful in learning about the nature of the risks. Look for behavior patterns which might aid in threat detection.

Develop judgement regarding true risk credibility. (C2 Home and Office is not looking to drive customers into sanitariums with paranoia. This is bad for business for a variety of reasons. We ask that you immediately rule out the possibility of detecting space aliens, big foot, etc using C2Home as these elements are known to have effective countermeasures;)) C2 Home and Office does not recommend use of the C2Home System for simply spying on neighbors or family for the sake of entertainment, as this represents an invasion of privacy. As with any tool, C2Home should be used responsibly.

Possible Risks to be targeted may include known criminal or other offending elements. Neighborhood gangs, (note methods used as these tend to be repeated). Malevolent neighbors (we all want good neighbors, unfortunately not all neighbors are good citizens). Animals raiding the property. Other foreseeable risks may include those of house fire or flood.

Of course specific risks may be unforeseeable. For these a more general approach to detection and response may be in order based on an assessment of probabilities. For example, if you live near a heavily wooded area there are probably a number of more general assumptions you should make concerning your risks. Perhaps the general assumption is that any animal may find it's way out of the woods. You may wish to characterize this unknown as simply warm-blooded and carnivorous, dangerous to persons and property, and devise threat detection and response sufficient for the entire set of local animal life.

Domains with particularly valuable elements, or numerous risks, or both - may wish to employ continuous monitoring. C2Home provides the capability for real time monitoring, archiving, detection of events, and programmed responses.

Risk assessment should be a reiterative process. Risk assessments should be repeated regularly - especially as new information is received regarding old risks or new risks are perceived.

- **Threat Detection**

Develop a plan for dealing each individual risk based on the risk characterization. This begins with developing a means of detecting when a previously perceived risk may be undergoing realization (Threat Detection). Detection of the threat within sufficient time to respond before damage is inflicted should be of paramount importance.

An endless number of sensors are available for threat detection. Sensors are available to detect anything you can imagine, and more are being developed every day. Electric and/or Magnetic Field sensors (including light –an electromagnetic field), weight, heat, wind, moisture, sound, movement, etc. Sensitivities are varied. It's important to have sufficient knowledge of the threats to target the threat with the right sensor.

It may also be necessary to examine extenuating factors which may prevent detection. Many PIR sensors, for example, are not capable of detecting body heat at certain ambient temperatures. Electromagnetic Fields are severely reflected when attempting to permeate conductors (such as foil insulation). Many CCD cameras are bleached out by direct light. Study the environment in which you wish to employ a sensor. Proper sensor selection and positioning may be critical to effective threat detection.

Sensor installation should also be discrete where desired. At times it may be effective to place sensors (such as cameras) in plain view to thwart offensive activities, other times hidden sensors should be considered.

- **Formulate response (tactics)**

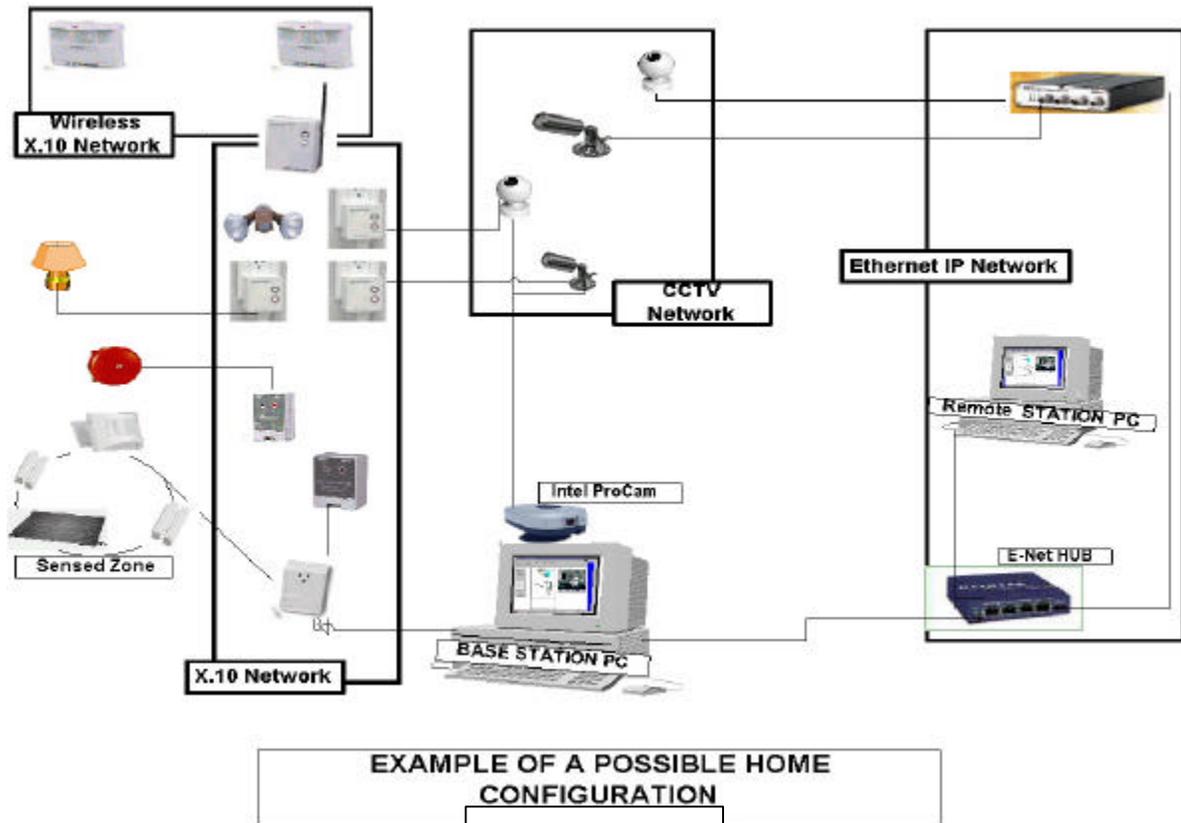
Tactics should include a determination of the plan for responding to detected activities.

These can be planned. Some responses may be fully automated. Some may require evidence gathered by the C2Home server to directly confront offenders or perhaps use legal leverage to seek relief. Responses, in general, depend on the nature of the threat and the advantage gained through the use of a security system. The following is a list of common tactics used to mitigate threats.

- **Eliminate the Element of Surprise** Security systems can be used to provide an advance warning not otherwise known regarding the existence of a threat. The response in this case should involve employing this advantage to timely action to mitigate the threat. Perhaps you wish to see who is at the door before you open it. The response may be to refrain from opening the door, escape thru another exit, or call for relief. Early knowledge of a fire or Carbon Monoxide vapors provides the opportunity for evasive action.
- **Eliminate the Element of Anonymity.** Simply detecting and identifying the offender, and confronting with evidence may be sufficient to halt the threat. Occasionally a spot light on nocturnal invaders is sufficient to thwart the invasion., or perhaps an audible alarm is sufficient. Offenders dumping garbage illegally or trespassing can many times be stopped using this tactic.
- **Eliminate the Element of Arrogance.** Some offenders may not care that you have knowledge of the offense. Direct confrontation is not usually recommended in this situation as it can lead to escalation. Countermeasures in this situation may involve overpowering the offender thru the use of formal or informal alliances. Good citizens can usually consider the local law enforcement an ally. In this case you may choose to simply collect sufficient data to take measures involving larger responses such as legal relief. For smaller offenses,

evidence collected can be used in combination with peer pressure to embarrass the offender into ceasing a pattern of offensive behavior.

- **Eliminate the Element of Deception.** Offenders may have given cause to suspect their motivations or behaviors. Without an effective security system the offender has the advantage of deception. A countermeasure to this advantage is advanced surveillance. Babysitters or other guardians of your children should not feel entitled to privacy beyond the normal bounds of personal privacy. Protecting defenseless children from possibly predatory or abusive guardians should be a consideration in many cases. C2Home believes strongly in empowering parents to protect the sake of children. Along the same lines, and considered invasion of privacy by some, we believe children have no right while under a parents watch to destroy their lives. Feel free to use C2 Home & Office products to any extent possible to prevent children from doing drugs or engaging in any otherwise self-destructive behavior.
- **IFF (Identification Friend or Foe)**
You may at some time plan on entering your house. You should put measures in place to somehow manage alarms and responses so that they are either not active during low risk periods, or they can distinguish high risk intruders from low risk intruders. Similarly, accessing the controls used to configure such features should require authentication. Screen Savers or password protection on boot up can easily be configured as a first level of protection from intrusions.



Appendix C: IP Routing Tutorial

(see RFC 1180 and RFC 790 at <http://sunsite.dk/RFC/rfc/rfc1180.html> for more detailed tutorial on IP routing)

Steps for configuring a Windows PC for IP Networking

STATIC IP Configuration (usually employed for Home Ethernet networks)

Select the **Specify an IP address** option. Then type in your IP address, which was assigned to you by your provider. Next, fill in the **Subnet Mask** text area. This number will probably be **255.255.255.0**.

Dial Up IP Configuration (Dynamic Connection – frequently used with Dial-ISP connections)

Step 1: Verify that Dial-up Networking is Installed

- Press the START Button, select **Settings...**, then **Control Panel**. Double-click the **Add/Remove Programs** icon. Select the **Windows Setup** tab, then click on the **Communications** option and press **Details...** Make sure that the **Dial-up Networking** option is selected. If it is, go on to step 2. If it isn't, select it and click **OK**. Windows will attempt to install the needed drivers, so make sure you've got your installation disks or CD handy! Now that **Dial-up Networking** is installed, you can proceed to step 2.

Step 2: Verify that the Dial-up Adapter and TCP/IP Protocol are Installed

- Press the START button, select **Settings...**, then **Control Panel**. Double-click the **Network** icon. Make sure the **Configuration** tab is selected. Both **Dial-Up Adapter** and **TCP/IP** should be present (like in the picture), then you're ready to proceed to step 3.
- To add the **Dial-Up Adapter**, hit the **Add...** button, double-click **Adapter**, then scroll down the list until you can select **Microsoft**. Choose the **Dial-Up Adapter** and hit **OK**.
- If you need to install **TCP/IP**, hit the **Add...** button, double-click **Protocol**, then select **Microsoft**, then **TCP/IP**, and hit **OK**.
- Now your **Network** dialog box should contain both **Dial-Up Adapter** and **TCP/IP**. Select the adapter, click **Properties...**, **Bindings**, and make sure the **TCP/IP** box is checked. You're now ready to proceed to step 3.

Step 3: Configure your TCP/IP Protocol

- For this step, dial-up IP connections usually assume addresses are dynamically assigned (change each time you log on)?.
- Go to the **Control Panel** and double-click the **Network** icon.
- Click on the **TCP/IP** protocol (highlighted in the picture) and press the **Properties...** button. You should get the **TCP/IP Properties** box.
- There are six sections in this dialog box. We'll deal with them in order. In each case, you can click on the section title to get a picture of the dialog box with the correct options selected.
- **IP Address:** Select the **Obtain an IP address automatically** option

Microsoft Dial Up Server – (Requires Microsoft Dial Up Server –DUS – MS Freeware)

If you don't intend to access the C2Home base over the public internet, but would instead prefer to dial directly from a remote connection to the base station, Microsoft DUS can assist with this connection. This software once loaded on the base and configured performs the task of answering the phone when you try to dial in remotely. This supports the TCP/IP connections and supports fixed IP Address assignments. Note that this use of a fixed IP address assignment probably precludes you from accessing an ISP with this same modem. You may consider adding an additional modem, for a total of two: one for fixed IP DUS server dial-in connections and one dynamic IP to be used for dialing into ISP type connections. In this situation the first is used to accept incoming calls for point-to-point connections. The second modem is for the PC to send outgoing emails and alarms.

Basic IP Routing

Routing in IP is based entirely upon the network number of the destination address. Each computer has a table of network numbers. For each network number, a gateway is listed. This is the gateway to be used to get to that network. Note that the gateway doesn't have to connect directly to the network. It just has to be the best place to go to get there.

A gateway is a system that connects a network with one or more other networks. Gateways are often normal computers that happen to have more than one network interface. For example, we have a Unix machine that has two different Ethernet interfaces. This machine can act as a gateway between those two networks. The software on that machine must be set up so that it will forward packets from one network to the other. If a machine on network 192.6.4 sends a packet to the gateway, and the packet is addressed to a machine on network 192.6.3, the gateway will forward the packet to the destination.

When a computer is to transmit a packet, the computer first examines the packet's leading information (a.k.a. header) to determine if the destination address is on the system's own local network. If so, the packet can be sent directly. Otherwise, the computer expects to find an entry for the network of which the destination address is a member – and the packet is sent to the gateway listed for that network entry.

The routing table of destination networks can get quite large. When no specific route is found for a packet the packet is sent to the default gateway. A default gateway can even be used when there are several gateways on a network.

The IP Address and Classes Hosts and networks

IP addressing is based on the concept of **hosts** and **networks**. A host is essentially anything on the network that is capable of receiving and transmitting IP packets on the network, such as a workstation or a router. It is not to be confused with a server: servers and client workstations are all IP hosts.

The **hosts** are connected together by one or more **networks**. The IP address of any host consists of its network address plus its own host address on the network. IP addressing, unlike, say, IPX addressing, uses one address containing both network and host address. How much of the address is used for the network portion and how much for the host portion varies from network to network.

IP addressing

An IP address is 32 bits wide, and as discussed, it is composed of two parts: the **network number**, and the **host number**. By convention, it is expressed as four decimal numbers separated by periods, such as "200.1.2.3" representing the decimal value of each of the four bytes. Valid addresses thus range from 0.0.0.0 to 255.255.255.255, a total of about 4.3 billion addresses.

There are 5 different address classes. You can determine which class any IP address is in by examining the first 4 bits of the IP address

Class	Prefix	Network Number	Host Number
A	0	Bits 0-7	Bits 8-31
B	10	Bits 1-15	Bits 16-31
C	110	Bits 2-24	Bits 25-31
E	1111	N/A	
D	1110	N/A	

The bits are labeled in network order, so that the first bit is bit 0 and the last is bit 31, reading from left to right. Class D addresses are reserved for multicasting. Class E addresses are reserved for future use. They should not be used for host addresses The range of network numbers and host

numbers may then be derived:

Class	Range of Net Numbers	Range of Host Numbers
A	0 to 126	0.0.1 to 255.255.254
B	128.0 to 191.255	0.1 to 255.254
C	192.0.0 to 254.255.255	1 to 254

Addresses beginning with **127** are reserved for loopback and for internal testing on a local machine and should never be used for addressing outside the host. [You can test this: you should always be able to ping **127.0.0.1**, which points to yourself]

A host number of all binary 1's indicates a directed broadcast over the specific network. For example, 200.1.2.255 would indicate a broadcast over the 200.1.2 network. If the host number is 0, it indicates "this host". If the network number is 0, it indicates "this network" [2]. All the reserved bits and reserved addresses severely reduce the available IP addresses from the 4.3 billion theoretical maximum. Most users connected to the Internet will be assigned addresses within Class C, as space is becoming very limited. This is the primary reason for the development of IPv6, which will have 128 bits of address space.

Subnetting an IP Network can be done for a variety of reasons, including organization, use of different physical media (such as Ethernet, FDDI, WAN, etc.), preservation of address space, and security. The most common reason is to control network traffic. In an Ethernet network, all nodes on a segment see all the packets transmitted by all the other nodes on that segment. Performance can be adversely affected under heavy traffic loads, due to collisions and the resulting retransmissions. A router is used to connect IP networks to minimize the amount of traffic each segment must receive.

Subnet Masking

Applying a subnet mask to an IP address allows you to identify the network and node parts of the address. Performing a bitwise logical AND operation between the IP address and the subnet mask results in the *Network Address* or *Number*.

For example, using a test IP address and the default Class B subnet mask, we get:

10001100.10110011.11110000.11001000	192.179.240.200	example Class B IP Address
11111111.11111111.00000000.00000000	255.255.000.000	Default Class B Subnet Mask
<hr style="width: 50%; margin-left: 0;"/>		
10001100.10110011.00000000.00000000	192.179.000.000	example Network Address

Default subnet masks:

- Class A** - 255.0.0.0 - 11111111.00000000.00000000.00000000
- Class B** - 255.255.0.0 - 11111111.11111111.00000000.00000000
- Class C** - 255.255.255.0 - 11111111.11111111.11111111.00000000

Private Subnets

There are three IP network addresses reserved for private networks. The addresses are **10.0.0.0/8**, **172.16.0.0/12**, and **192.168.0.0/16**. They can be used by anyone setting up internal IP networks, such as a lab or home LAN behind a NAT or proxy server or a router. It is always safe to use these because routers on the Internet will never forward packets coming from these addresses. These addresses are defined in [RFC 1918](#).

Direct vs. Indirect Routing

If the packet does not need to be forwarded, i.e. both the source and destination addresses have the same network number, direct routing is used.

Whereas, indirect routing is used **when the network numbers of the source and destination do not match**. This is the case where the packet must be forwarded by a node that knows how to reach the destination (a router).

A Unix command for adding a routing entry to any host "A" for the purpose of communicating with host "B" via a gateway "C is":

```
route add [destination_ip] [gateway] [metric]
```

Where the metric value is the number of hops to the destination. In this case,

```
route add 192.138.165.3 192.139.2.3 1
```

192.138.165. 3 is node B

192.139.2.3 is gateway node C

will tell A to use C as the gateway to reach B.

In most cases it is not necessary to manually add this routing entry. It would normally be sufficient to set up C as the default gateway for all other nodes on both networks. The default gateway is the IP address of the machine to send all packets to that are not destined to a node on the directly-connected network. The routing table in the default gateway will be set up to forward the packets properly, which will be discussed in detail later.

Static vs. Dynamic Routing

Static routing is performed using a preconfigured routing table which remains in effect indefinitely, unless it is changed manually by the user. This is the most basic form of routing, and it usually requires that all machines have statically configured addresses, and definitely requires that all machines remain on their respective networks. Otherwise, the user must manually alter the routing tables on one or more machines to reflect the change in network topology or addressing. Usually at least one static entry exists for the network interface, and is normally created automatically when the interface is configured.

Dynamic routing uses special routing information protocols to automatically update the routing table with routes known by peer routers. These protocols are grouped according to whether they are Interior Gateway Protocols (IGPs) or Exterior Gateway Protocols. Interior gateway protocols are used to distribute routing information inside of an Autonomous System (AS). An AS is a set of routers inside the domain administered by one authority. Examples of interior gateway protocols are OSPF and RIP. Exterior gateway protocols are used for inter-AS routing, so that each AS may be aware of how to reach others throughout the Internet. Examples of exterior gateway protocols are EGP and BGP. See RFC 1716 [11] for more information on IP router operations. In practice, **it is almost always better to use explicit static routing table entries rather than relying on dynamic routing.**

Appendix C: JRE Configuration

Installation of the C2home Server requires the JAVA Runtime Environment (at least version 1.3.1) be installed. Users with the JRE v1.3.1 already installed will have files overwritten as the C2Home Server autoinstallation proceeds to ensure that proper configuration of the JRE occurs. The files impacted are as follows (assuming C: drive):

- C:\Program Files\JavaSoft\JRE\1.3.1\lib> javax.comm.properties
- C:\Program Files\JavaSoft\JRE\1.3.1\lib\security>java.security
- C:\Program Files\JavaSoft\JRE\1.3.1\lib\security>cacerts
- C:\Program Files\JavaSoft\JRE\1.3.1\lib\security>java.policy
- C:\Program Files\JavaSoft\JRE\1.3.1\lib\ext>jcert.jar
- C:\Program Files\JavaSoft\JRE\1.3.1\lib\ext>jnet.jar
- C:\Program Files\JavaSoft\JRE\1.3.1\lib\ext>jsse.jar
- C:\Program Files\JavaSoft\JRE\1.3.1\lib\ext>jmf.jar

Appendix D: Neat Tricks (if you don't know them already)

- **Autostart C2Home with each boot of PC.** Delete all *.pwl files and drag c2home icon from desktop to start – programs-startup
- **Ping** - from start-run, type in the word "ping" followed by the host name or IP address you would like to verify connectivity. The reply will indicate if connectivity exists and the round trip time to receive an echo from the remote host.
- **Trace Route** - from start-run or any dos or command line prompt - in windows type the word `tracert` - followed by the host name or IP address you would like to verify connectivity. The reply will indicate the routers used to relay this packet and the time to echo an acknowledgement.
- **Hosts table (windows\hosts)** - there is a sample known as hosts.sam. This file contains a list of host you manually configure rather than rely on a domain server for automatic host lookup. This allows you to name hosts locally, rather than index hosts by ip address.
- **Alt –F4 to close browser**
- **Shift Click H-link to open in separate browser**
- **Improve performance by clearing out all *.tmp files and all *.chec files**
- **arp –s** (especially important for Axis products). From a dos prompt, this command allows you to map a MAC address to an IP address. Type `arp -s` with no parameters for further instructions.