Checkbox with Ticket Manager

Checkbox Setup and Admin Guide

Your Check Box and Ticket Manager System is designed to be simple to set up and use. To make set up as easy as possible, please take a moment to completely read through these instructions before you begin.

Setup Guide

Installing..... 3
Locating the equipment..... 3
Connecting the equipment..... 3
Optional external Antenna..... 3
Using Ticket Manager..... 4
Setting up Guest Access..... 4
Access Tickets..... 4
Credit Card Module..... 4
Free Access..... 4
Creating Tickets..... 5
Credit Card Module..... 6
Free Access..... 7
Customizing your Welcome..... 7
Administering Clients..... 8
Active Clients..... 8
All Clients..... 8
Accessing Your Hotspot..... 8
Outside The Hotspot But Inside Your Network..... 9
From The Internet..... 9
Network Setup..... 10
Internet..... 10
Local..... 11
Wireless..... 11
Current Configuration..... 11
Time & Tickets..... 11
Uploading Graphics..... 12
Connection Scenarios..... 13
Signal Strength..... 14
Mesh Nodes..... 16
Mesh Node Installation..... 17
User Guides..... 18
Warranties and Service..... 19

Installing Checkbox

Locating the equipment

Locate Checkbox in an area that is close to where your customers will be using the network. Wireless access points have a range similar to cordless telephones; in an open area they typically work from 300' to 1000', but walls and other devices can cause interference and shorten the range. By using mesh repeaters or an optional external antenna the range can be increased significantly. The access point can be mounted on a wall, set on a counter or a shelf, or placed inside a drop ceiling with the antennas pointed through the ceiling into the area below. Keep in mind that Checkbox will need access to electricity as well as a connection to your Internet Service Provider (ISP). If you ordered your Checkbox in a weatherproof enclosure your unit may look different from the diagram below.

Connecting the equipment *(Refer to the picture)*

Checkbox will connect to your cable, DSL, or local area network using a Cat5 network cable. (It looks like a telephone cord with fat plugs on each end). Depending upon your particular DSL or Cable modem the jack may be marked "LAN", "PC", "Host" or something else. In any event there will most likely be only one jack on the Cable or DSL modem that the plug fits into.

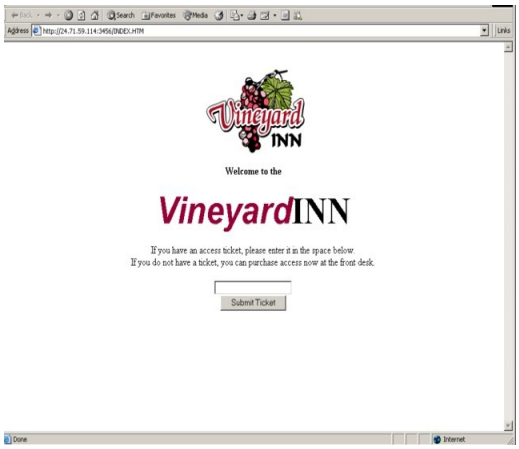
Optional external Antenna

Checkbox uses two short "rubber ducky" style antennas and can achieve a range of 300' to 1000' depending upon conditions. Using an optional external antenna the range can be extended. If you have purchased an optional external antenna it will connect to one of the antenna connectors on the unit. You may use either connector. When mounting an external antenna outdoors there are a few factors to keep in mind:

- Choose an area that is relatively high and free of obstacles.
- Choose an area where you will be able to mount the Checkbox nearby in a dry safe area (you do not want to use more than 4' of antenna cable between the antenna and the Checkbox as the signal will deteriorate rapidly).
- Choose an area where there will be power and you can run a cable to your Internet connection.
- Choose an area that is clear of power lines and other hazards.
- Do not locate the Checkbox antenna within 4 feet of a satellite dish or other antennas — they may cause interference to each other.
- You do not need to choose an area where you can regularly get to the Checkbox, as all administration work is done through a web browser.
- External antennas can be mounted to a mast, clamped to a vent pipe, mounted on a chimney or mounted to the side of a building using a bracket.

Using Ticket Manager to Create and Manage Tickets

Ticket Manager is the system you use to create and print tickets for your users. Ticket Manager also allows you to view users on the system (Active Clients), view tickets not yet used, and to delete tickets from the system. Ticket Manager is accessed through a web browser on your computer, and can be accessed from inside the Hotspot or from outside the Hotspot from anywhere on the Internet. To learn how to access the system from outside the Hotspot see the *Accessing Your Hotspot* section in this guide.



This is an example welcome screen your guests will see when they first log on to your Hotspot. From here they are prompted to enter a ticket before they can connect to the Internet. Of course you do not have tickets since you have not yet created them! To access the Ticket Manager screen, in the address bar enter the following: http://192.168.17.1:3456/admin

This will bring up a logon window asking you for a user name and password. The system has no user name or password as it is shipped. You may set a password inside the management screens. To logon now just hit <Enter> or <OK>

Once you have successfully logged on to Ticket Manager you will see the Checkbox Administration Screen.

Setting up Guest Access

There are three ways your guests can access the system; using Access Tickets, using Credit Cards and PayPal, and using Free Access.

Access Tickets allow you to create and distribute tickets to your guests that allow them an amount of time online that you determine. These tickets can be good for an amount of time ranging from 15 minutes to one year. You can give these tickets away or sell them.

With the **Credit Card Module** you can accept credit cards automatically through the welcome page. The credit Card Module uses the PayPal system to clear the transactions and deposit the funds into your account, and allows you to set the pricing and duration. With the Credit Card Module ***you do not need to be present to hand out tickets*** - great for unattended locations such as marinas and public spaces.

The **Free Access** System allows you to give your guests free access two different ways; You can allow free access once per period, for example 15 minutes free every day, or 1 day free per year. This is great for a coffee shop or restaurant that wants to advertise free Internet access but prevent guests from taking up a table for hours upon hours. The guests will still get your welcome screen when they first log on, and if they qualify for free access (if they have not had free access already in the predefined period) then they will be invited to try the access for free. Once the free period has expired the guest will be required to enter a valid ticket number or credit card (if you have the optional Credit Card Module) and the free option button will not be displayed.

The system will ***automatically generate the appropriate buttons and boxes*** on your welcome screen; If you have not created any tickets and have enabled free access and credit cards, then the system will not display a box to enter access tickets. If you have not enabled credit card payments or free access and have created tickets then only the ticket box will be displayed on your welcome screen. If you have not enabled free access or printed tickets and have enabled credit cards then only the credit card buttons will be displayed.

The following is an example of a customer login screen with all the access options enabled:

- To activate the submit ticket button, you just need to generate some tickets.
- To activate the Credit card activation buttons, you need to setup your business PayPal account and set some charges into the appropriate fields.
- To activate the free trial button you only need to define how much free trial time and over what period you allow a trial to run.

If any particular access method is not activated, then that access method will not be shown to your users.

***Note:** If you disable all access methods, the only way for customers to gain access through your Hotspot is through the administration panel and manually activating a specific client through the All Clients menu.*

Creating Tickets

Click on Access Controls from the menu at the top to begin creating tickets for your users. The system will automatically take you to the Ticket Generation page.

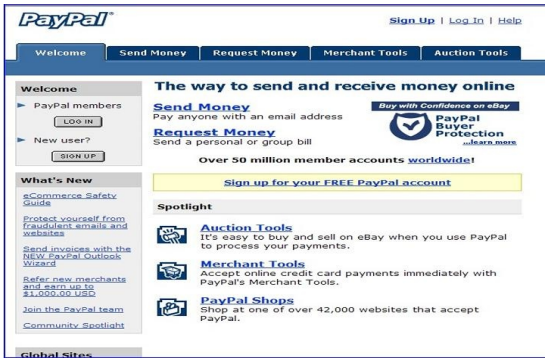
Select the usage duration of the tickets you wish to generate and their expiry date (shelf life) and then click on the "Create Tickets" button.

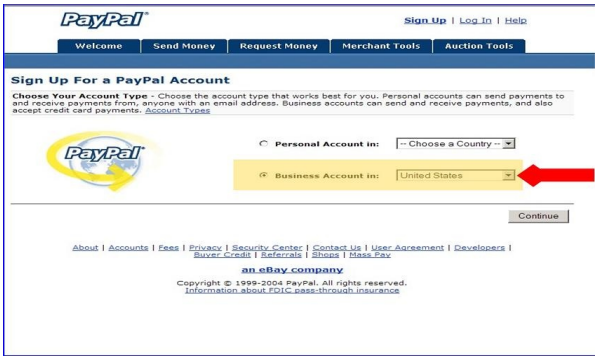
Shelf Life refers to how long the ticket is good sitting in the drawer until it expires. If you print a stack of tickets each good for 7 days of access with a Shelf Life of 1 year and they are not used the system will delete them from the ticket database 1 year after their creation. If a customer activates that ticket 363 days after it is created they will still get a full 7 days of access. If however they try to activate it 370 days after it is created the ticket will not be recognized by the system. Shelf Life is particularly handy for promotional events, for example; "today only free 30 minutes access with each purchase". Users can not save up these promotional tickets as you can set their Shelf Life to 1 day for this event. You can create ticket sets with different **Shelf Life** and **Access Time**.

Using the Credit Card Module

If you wish to use the credit card module first you must configure your credit card account and then you can set up your pricing and access times.

First you will need to set up a ***Business Account*** with PayPal if you do not already have one. Go to www.PayPal.com to set up a new account. (If you already have an existing business account with PayPal you can skip this section. If you have an existing personal account you will need to upgrade to a business account).

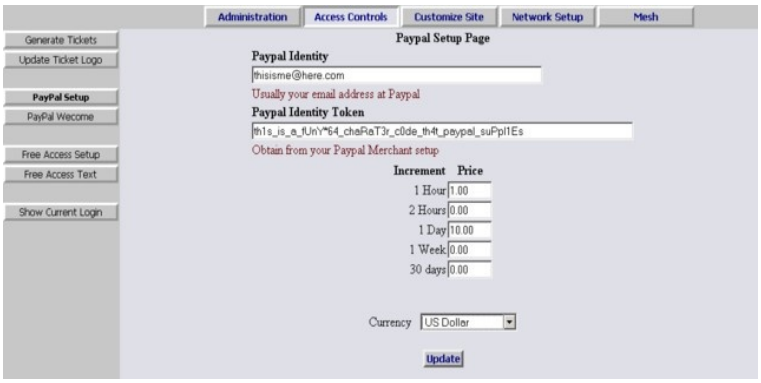




Make sure you specify a Business Account when setting up your PayPal Account!

After you have finished setting up your Business Account with PayPal you will receive an **identity token**. This token will look like a long string of random numbers and characters. This string is the unique identifier that PayPal will use to identify you and your system to their servers to properly authorize the charge and credit your account. It is ***very important that you copy this string carefully*** (using copy and paste) in the next step. We strongly suggest that you copy this string into a blank document and store it for safekeeping.

Once you have completed setting up your PayPal account and have copied your identity token, open the administration page on your Checkbox System and go to the PayPal Setup Option on the menu.



In the box marked PayPal Identity enter your PayPal ID (typically your email address).

In the PayPal Identity Token box paste your PayPal Identity Token.

Set your prices, and leave as zero's any time increments that you do not wish to offer. Press the Update button when done.

It would be a good idea at this point to run some sample charges through the system. You can refund those charges when you are done testing by using the PayPal merchant tools in your PayPal Account Management Screen.

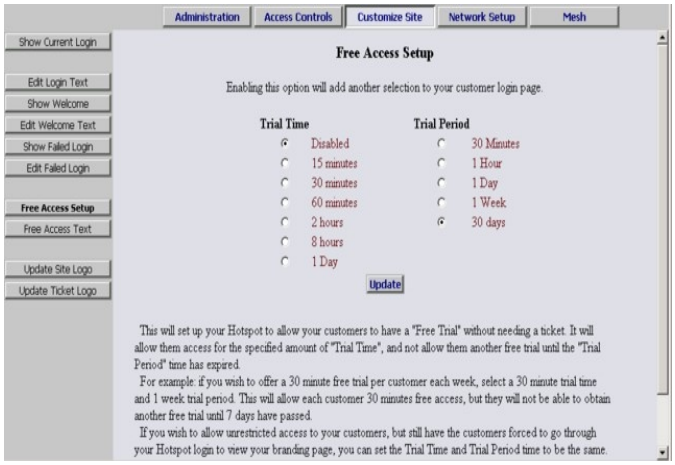
Please Note: *This software is provided to process credit card transactions securely through PayPal utilizing PayPal's systems. Checkbox Hotspots is not affiliated with PayPal and does not offer support for managing PayPal merchant accounts.*

Free Access

The Free Access System allows you to give your guests free access two different ways:

You can allow free access once per period, for example 15 minutes free every day, or 1 day free per year. This is great for a coffee shop or restaurant that wants to advertise free Internet access but prevent guests from taking up a table for hours upon hours. The guests will still get your welcome screen when they first log on, and if they qualify for free access (if they have not had free access already in the predefined period) then they will be invited to try the access for free. Once the free period has expired the guest will be required to enter a valid ticket number or credit card (if you have the optional Credit Card Module) and the free option will not be displayed.

If you wish to allow unrestricted access to your customers, but still have the customers view your site welcome page, you can set the Trial Time and Trial Period time to be the same. For example; by setting the Trial Time and Trial Period both to 60 minutes, your clients will see the site welcome page every hour.



To enable Free Access, select Access Controls in the top menu and then Free Access Setup on the left hand menu. Select the Trial Time, how much time you want to allow them on the system, and then select the Trial Period, the amount of time that must elapse before they get a new free trial.

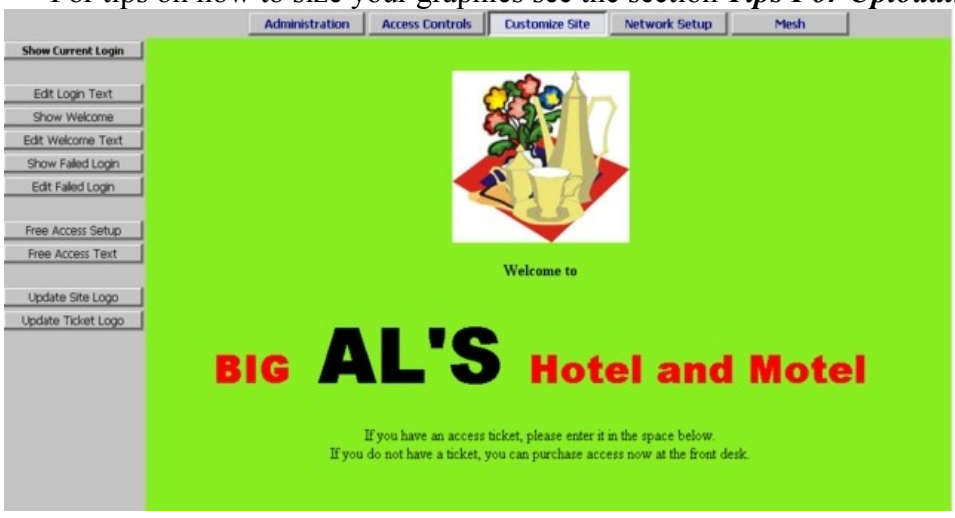
You may also customize the message your users see by selecting “Free Access Text” on the left hand menu and editing the message.

Customizing your Welcome Screen

As you add access methods the system will add the appropriate buttons and boxes to your welcome screen. You can customize the look of your welcome screen by uploading a picture or logo in .JPG format.

To upload an image click on **Customize Site** in the top menu and then select **Upload Site Logo** on the menu on the left hand side of the administration screen. You may also select the options to change the welcome messages and change the ticket graphics as well.

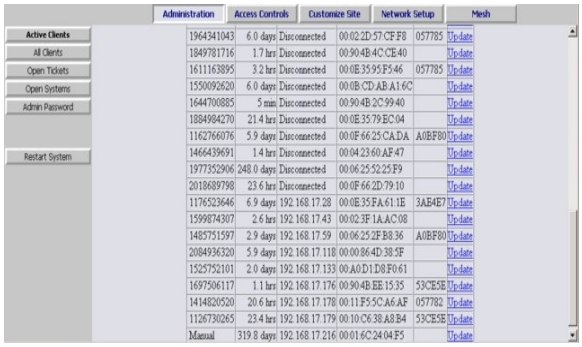
For tips on how to size your graphics see the section ***Tips For Uploading Graphics***.



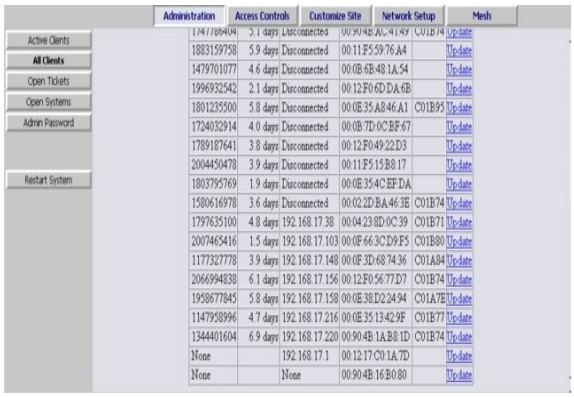
You can review the results with the various “show” options on the left menu. They will be shown within the main frame in the admin panels, although your customers will see this frame as their “whole window”.

Administering Active Clients

Under normal circumstances guests will get online, use their time and then automatically be logged off the system without any manual intervention from your or your staff. However there is an option to manually adjust a guest's remaining time, delete a guest from the system, and manually add a guest.



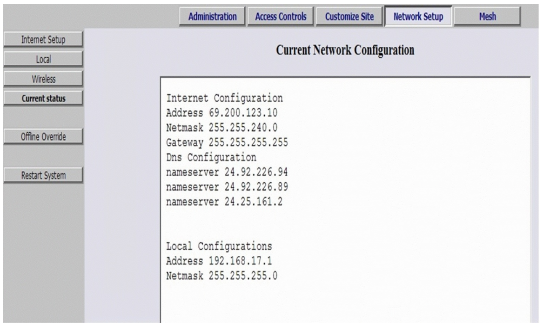
By selecting Administration in the top menu and then Active Clients on the left hand menu you will see a list of all client computers currently ticketed. Client computers are listed by their MAC address, a unique electronic serial number assigned to each network adapter. You can see their time remaining and whether or not they are online. By clicking on **Update** to the right of each client line you can manually change the remaining time or delete the client from the system.



By selecting All Clients on the left hand menu you will see not only clients with tickets but also those clients that have connected with the Hotspot system but who have not entered a ticket, credit card or free access. (Although these clients have been recognized by the system, they have not been allowed onto the Internet yet, or have been on the Internet and their time has expired.) Here you can manually give them time.

Accessing Your System Outside The Hotspot But Inside Your Network

If you have your Checkbox and Ticket Manager system connected to your company network you can access the Checkbox Administration Screens from any PC on your network, even if these PC's are not connected through the Checkbox system. In order to access your Checkbox and Ticket Manager system from your company network you will need to know the WAN IP address assigned to the Checkbox and Ticket Manager server by your network.



If you have access to Checkbox through a wireless client you can find this address in the Checkbox Administration Screen by clicking on Network Setup in the top menu and Current Status on the left hand menu. On the second line you will see a listing for "Address". This is the IP address assigned by your Internet Service Provider (ISP), or your internal router, to our system.

Once you have determined the IP address assigned to your Checkbox by your network you can access it by entering the IP address in the address bar of your web browser with **http://** in front of the IP address and **:3456/admin** after the address. For example, if the IP address assigned by your network to the Checkbox and Ticket Manager server was 10.0.0.21 then you would enter **http://**10.0.0.21**:3456/admin**.

This will bring up a password login box just as it would if you were connected from inside the Hotspot, and all administrative functions are accessible.

Accessing Your System From The Internet

In order to access your Checkbox and Ticket Manager system from the Internet, you need to know the IP address assigned to you by your Internet service provider. An IP address is a unique number much like a telephone number that identifies a unique machine on the Internet. No two IP addresses can be the same on the Internet. Most Internet Service Providers (ISP) use dynamic IP addresses which may change periodically, in order to conserve the pool of available IP addresses. Some ISP's will provide a static (non-changing) IP address upon request, and may charge for this service. If you intend to regularly administer your system from off site through the Internet it will be easier if you have a static IP address.

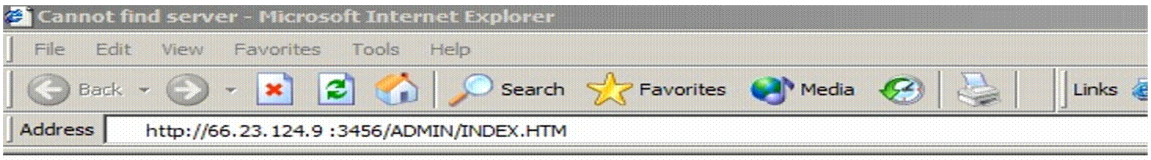
Your ISP may need to know the MAC address of your Checkbox and Ticket Manager server. The MAC address is a unique hardware ID that your ISP will use to tie your Checkbox and Ticket Manager server to the static IP address. You will find the MAC address listed on the bottom of the server itself. (If your server has been mounted in an external enclosure the MAC address label will be missing - contact Checkbox Hotspots support for help in determining your system's MAC address)

If your Checkbox and Ticket Manager server is connected to your cable or DSL modem through a router, you will need to enable static routing, DMZ, or virtual servers through your router. Please refer to your router manufacturer's instructions for details on how to enable static routing or virtual servers.

If you have obtained the static IP address from your ISP you will probably have to reboot your cable or DSL modem, and once that is done you will also need to reboot your Checkbox and Ticket Manager

server. Upon reboot your Checkbox and Ticket Manager server should automatically see its new static IP address.

To access Checkbox and Ticket Manager server through the Internet you will enter the IP address assigned by your ISP in the address bar of your web browser with **http://** in front of the address and **:3456/admin** after the address. For example, if the static IP address for the Checkbox and Ticket Manager server was 66.23.124.9 then you would enter **http://**66.23.124.9**:3456/admin**



This will then bring up a password login box just it would if you were connected from inside the Hotspot, and all administrative functions are accessible.

Network Setup

You probably will not need to make any changes in the network setup of your Checkbox system as most Internet Service Providers use DHCP, Dynamic Host Configuration Protocol, to tell the devices connected to their network what address and other parameters to use.

If your Internet Service Provider uses PPPOE or static IP addresses, or if you are connecting Checkbox to an internal company network you may need to set some network parameters manually.

To Enter Network Setup click on Network Setup on the top menu. The Network Setup Page will appear. Enter the parameters as provided by your Internet Service Provider or network administrator. After you have entered the parameters press update and then **Restart** the **System** with the menu item on the left.

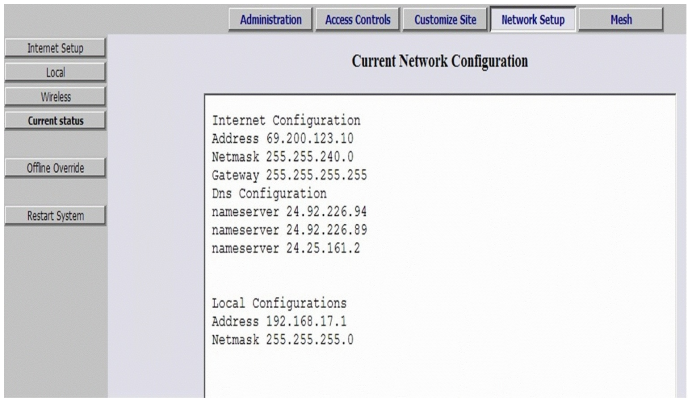
Local Address

Local Address refers to the IP addresses the Checkbox system assigns to users on the system. By default this address is in the 192.168.17.xxx range. This setting should not need to be changed under most circumstances. If there is a need to change this address range, select Local from the menu on the right hand side and enter the new address in here, press update and **Restart** the **System**. Important: If you are using mesh repeaters ***allow 10 minutes after restart*** for the mesh repeaters to rediscover the master. During this period **Do Not** make any other system changes (i.e. SSID or channel) or you run the risk of the mesh nodes becoming "lost" for an extended period of time.

Wireless

Your Checkbox system, like most data wireless access points, announces its presence by broadcasting its SSID. This SSID is a name that your guests will see when their laptops connect to the Checkbox system. By default this name is **hotspot**, which lets the guests know they have found a public Hotspot. If you wish to change the SSID select wireless from the menu on the right hand side of the Network Setup Menu. Enter in the new name and press update. Important: If you are using mesh repeaters ***allow 10 minutes after update*** for the mesh repeaters to reconfigure their SSID. During this period **Do Not** make any other system changes (i.e. Local Address or channel) or you run the risk of the mesh nodes becoming "lost" for an extended period of time.

Current Network Configuration



On the network setup menu selecting Current Status on the left hand menu brings up a window that shows the current network configuration. This screen will show you the parameters of the network the Checkbox is connected to, including its IP address, as well as the network address that the Checkbox is providing to clients.

A Note About Time & Tickets

Your Checkbox system sets its internal clock from a time server on the Internet. The first time the unit powers up, or after it has been unplugged, it will attempt to connect to one of many time servers on the Internet to set its clock, including the date and year. Since tickets are time and date sensitive if the system does not know what time it is it can not determine if a ticket is still valid.

If the system can not set its clock for some reason (i.e. your Internet connection is not set up or your Internet service provider is down) it will not generate tickets or allow users on the system. Users will receive a screen that lets them know that the system is temporarily unavailable. You will still be able to access the administrative pages.

Note: *If you must access the Internet through your hotspot before it has obtained the proper time, you can temporarily override this behaviour with the* **Offline Override** *menu item under the* **Network Setup** *page. Example usage may be if you need to "register" your hotspot with your ISP before they activate your hotspot for Internet access.*

Tips for Uploading Graphics

Ticket Manager provides the option to upload a graphic for the welcome page and a different graphic that prints out on the tickets. For best results these graphics should not be too large, either in pixels or file size.

Pixels refers to the number of dots in a picture, these dots make up the picture itself. If a picture is described as 200 x 400 pixels, the picture is 200 dots wide by 400 dots tall. If the pixel count is too big then the picture may not fit on the page or it may push other elements of the page off the screen. It is important to remember that not all screens are the same size! It may look fine on your screen but may not fit on somebody else's screen! The standard minimum screen size for computers 640 x 480.

File size refers to the amount of data used to record the picture information. Too little data and the picture looks course, blurry or grainy. Too much information and the picture takes too much space on the hard drive and takes too long to download.

So what is the "right" size? For the welcome screen logo generally an image that is no bigger than 640 pixels wide and 240 pixels tall works best. You can make them less wide or less tall. As for file size, somewhere between 20Kb and 100Kb is about right.

For the logo on your ticket, an image that is 110 pixels tall by 200 pixels wide is ideal, with a file size around 20 kb.

There are many tools you can use to resize your graphic, including Adobe Photoshop, Microsoft Picture It and a shareware tool called Irfanview (http://www.irfanview.com). Whichever tool you use, make sure to save your graphic in a .jpg format (most universally accepted by browsers).

An example Welcome screen logo.

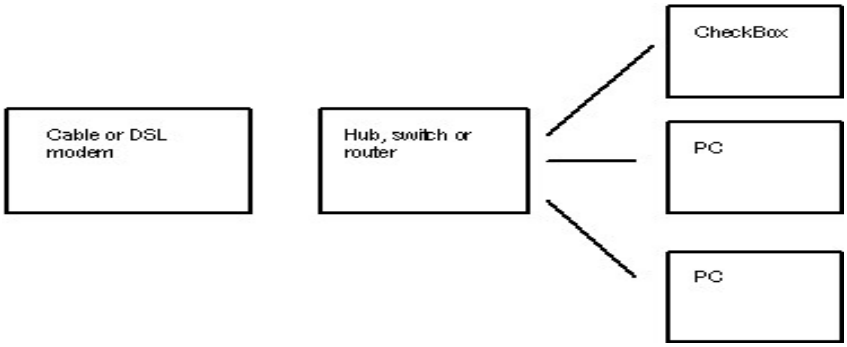
An example Ticket logo.

Alternate Connection Scenarios

The best way to connect your Checkbox System is directly to your DSL or cable modem. You may also connect it through a switch or hub to the DSL or cable modem (*see figure 1*). You can also connect it through another router to the DSL or cable modem but this may prevent the Checkbox Hotspots Support Server from being able to connect to your unit to provide support and updates.

If you wish to connect your Checkbox through another router to the DSL or Cable modem and you would like to access your system from the Internet or receive support you will need to enable "Port Forwarding" to your Checkbox for port 3456, or place the Checkbox in the router's "DMZ" (De-militarized Zone). Please check with your router's documentation for instructions on how to do that.

Figure 1



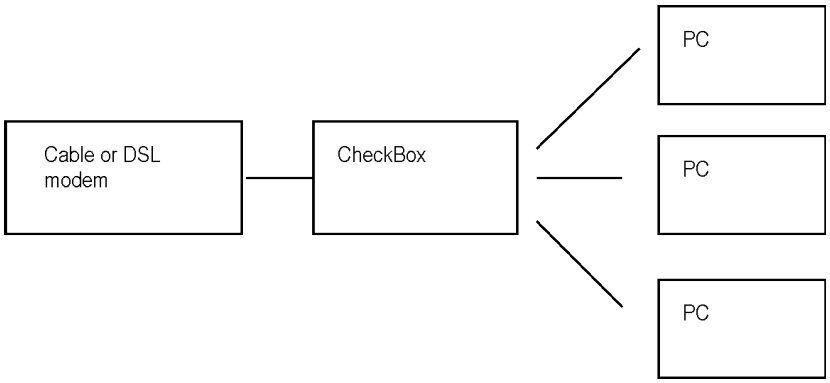
The best way to connect your Checkbox System is directly to your DSL or cable modem. You may also connect it through a switch or hub to the DSL or cable modem (as shown in figure 1). You can also connect it through another router to the DSL or cable modem but this may prevent the Checkbox Hotspots Support Server from being able to connect to your unit to provide support and updates.

If you do wish to connect your Checkbox through another router to the DSL or Cable modem and you would like to access your system from the Internet or receive support you will need to enable "Port Forwarding" or place the Checkbox in the router's "DMZ" (De-militarized Zone). Please check with your router's documentation for instructions on how to do that.

You may also connect wired PC's to the ports on the Checkbox (as shown in figure 2). These wired PC's may be used as public email stations, or you can use them in your office. These machines will need access tickets to connect to the Internet, so if you choose to use them in the office, and your employees need to access the Internet you will need to issue tickets for these machines (probably 30 day or 1 year tickets).

IMPORTANT - Please note! If you connect PCs as shown in figure 2 the wired and wireless PC's are on the same subnet—the PC's will be able to "see" each other . If you have your office PC's connected this way, make sure you have taken appropriate security measures.

Figure 2



Signal Strength, Power Levels and Antennas

Data communication between your guest's laptop and the Checkbox is a two-way affair. For a successful connection not only does a signal need to get from the Checkbox to the user's laptop, but they need to get a signal back to the Checkbox. Laptop wireless cards are not all created equal and few have an external antenna. Therefore it is not unusual for a guest to "see" a signal of a few bars, or "good" on their laptops but have a difficult time maintaining a connection. This is usually a case of the laptop seeing the signal from the Checkbox but the Checkbox not being able to see the Laptop.

Another issue wireless users often encounter is the "signal strength" meters displayed on their screens. These signal strength displays are an approximation of the signal strength averaged over a period of time and do not take into account signal noise, the interference inherit in every radio transmission. This can lead to users seeing a strong signal displayed, but still not being able to establish a connection.

Of course just the opposite can occur; sometimes users will see a weak signal but yet make a solid connection. Regardless of what the signal strength display reads the bottom line for the user is always this: Can they connect and is the connection fast enough?

One way to improve the range of the signal is by adding a long range antenna to your access point (the access point in this case is the Checkbox system). Long range antennas are rated in "dbi" and can sometimes help and sometimes can make the situation worse. While a standard antenna sends out radio waves equally in all directions like a balloon, long range antennas achieve greater range by changing the shape of the signal.

Instead of sending out the signal in a balloon shape some antennas flatten out the balloon into more of a donut, sending less of the signal straight up into the sky and more out towards the edges. These antennas can generally extend the usable range from 10% to 30%. However they can introduce two new problems; the case of the laptop seeing the Checkbox but the Checkbox not being able to see the laptop mentioned above, or a case where the "donut" is so flat that it shoots over the heads of the users, like a layer of fog traveling a few feet off of the ground. Generally if the property is flat, antennas with a gain of 6dbi or less are acceptable.

A second type of antenna re-shapes the signal even more, sending it in a pinpoint beam. These antennas can increase range ten-fold or more, however if the user is not in the direct path of the signal they will not be able to see it. Even if they are in the direct path if they are not able to send a signal back the full distance they will not be able to establish a connection. These high-gain point-to-point antennas are best used in pairs, one on each end of the path, and while not practical for laptops they are good for connecting buildings in remote locations or repeaters in areas not contiguous to other units.

There are other ways to improve the range of the signal for users. One way is to improve the sensitivity of the radio receiver at both ends. While we do not have control over the quality of the user's laptops we have made the receiver in the Checkbox very sensitive.

Another way to improve range is to increase transmit power. Again, since we do not have control over the quality of the user's laptops we cannot affect their transmit power, but we could boost ours. Checkbox uses the maximum legal power for unlicensed operation in the frequencies (channels) it occupies. There are some Hotspot companies that do use higher power, but that is a dangerous game. Unlicensed operation at higher power can result in the property owner being fined.

When you boost the transmit power on one end of the connection but not the other you also run into the problem of one side being able to see the signal from the other side but not being able to send a signal back.

Since laptops do not have good antennas and do not generally use the maximum output power they really benefit from having a high density signal. The best way to have a high density signal is by using multiple access points.

Determining the proper number of access points requires taking into consideration several factors:

- How great a distance do you need to cover?
- What are the surroundings? Are there walls or open spaces? Is the building made of wood, rebar reinforced concrete, or steel?
- Is there any interference in the area?

On a flat open field with no interference a signal can travel up to 1000'. When we start adding walls, other devices and users, that distance will begin to shrink.

For example, a hotel with two wings each 200 feet long and three floors per wing, made of rebar reinforced concrete, might need 5 units, one master and 4 mesh repeaters, to provide solid coverage. Another hotel, constructed of wood but with similar dimensions, may only need 3 units, one master and two repeaters to provide solid coverage.

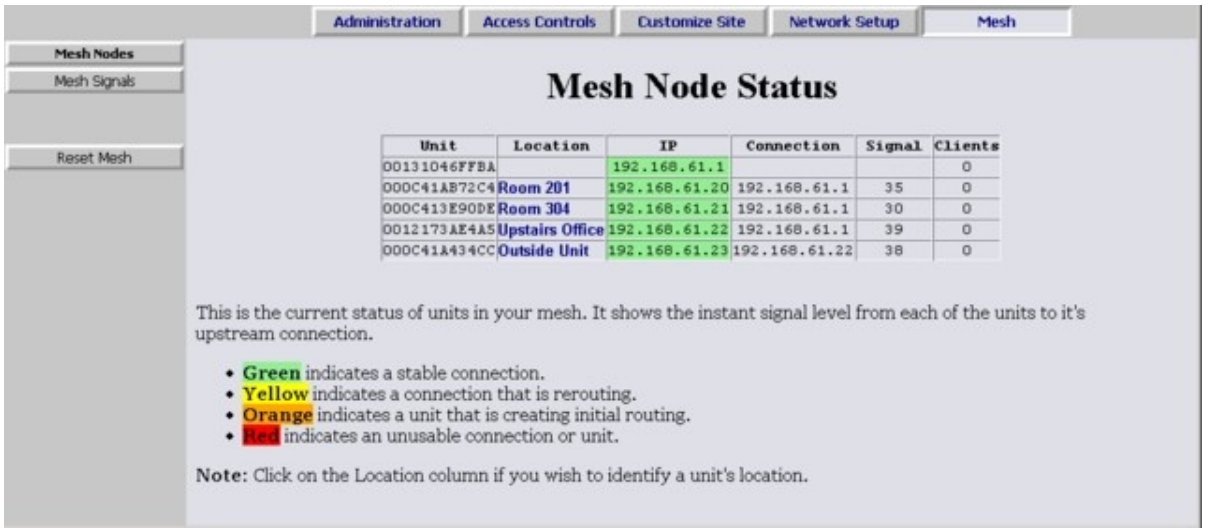
Another example would be a campground that is on an open flat field. To provide complete coverage however you need to penetrate the aluminum skin of the travel coaches which might require mesh repeaters spaced every 300 feet, so that no coach is more than 150 feet from a unit.

If that hotel happens to be at the end of an airport runway with a radar system nearby or that campground has a cell tower in the middle of the property then interference from those devices may necessitate additional units to overcome the interference.

Mesh Nodes

You can extend the range of your system using Mesh Repeaters. These devices relay the data stream from your master unit further throughout your facility. Mesh Repeaters only need power, they do not need a wired network connection back to the master unit. Not only do Mesh Repeaters extend the wireless signal, they also provide wired ports to allow computers, printers, VoIP telephones and other ethernet devices to access the network.

Mesh units are completely self-configuring. As long as they can receive a signal from one of their peers or the master they will establish a connection amongst themselves and actively determine the best route back to their master unit. ***There are no parameters to set.***



Once your Mesh Repeaters are in place you can monitor their status by selecting Mesh Status on the top menu.

- The first column identifies the repeater unit by its MAC address.
- The second column is an editable field which you can use to identify the unit's location.
- The third column shows that unit's IP address.
- The fourth column shows the IP address of the unit from which this unit gets its connection, this address may be the master or another repeater if the units have daisy chained themselves.
- The fifth column shows the current signal strength of this unit to its downstream connection.
- The last column shows how many clients are using this repeater.

Mesh Node Installation

The Optional Mesh Repeater Node can extend the range of your Checkbox by relaying the signal from one area to the next. No wiring is needed from the repeater back to the master, the repeater connects wirelessly. The repeater will need power, and will need to be within range of the master unit (between 50’ and 500-1000’ depending on intervening construction) and will then extend the signal up to another 50-1000’, depending upon local conditions.

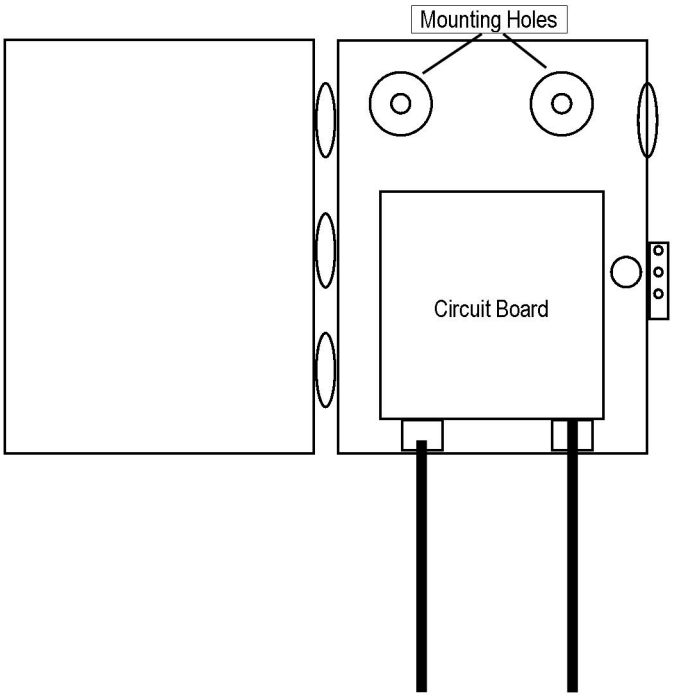
If your repeater is mounted in a weatherproof enclosure it will look like the unit illustrated below. Indoor repeaters look just like the master units, and can be placed on shelves or mounted on walls.

The Repeater System should be located in a high clear location, preferably at least 8 feet off of the ground. The repeater will need to be able to “see” the signal from the master; the repeater can usually receive a good signal at the fringe of where most laptops begin to lose signal if it is up high enough. Depending upon local conditions this distance may vary from a 50 feet to over a thousand feet.

The Outdoor Repeater System should be mounted with the antennas pointing down. Use the two mounting holes at the top of the box to bolt the unit to a wall or pole. Do not use the two lower holes; they are too close to the circuit board and you may damage the board trying to tighten screws down.

Once the outdoor unit has been mounted close the cover and secure with one of the included nylon ties. Make sure the antennas are extended straight down. In a high traffic area where the box is mounted within reach you may wish to use a small padlock.

Finally, apply power to the unit and allow up to 8 minutes for the unit to boot and find the master. The power adapter should be in a protected area. If you are connecting it to an outlet located outdoors use a suitable plug enclosure. These can be found at most hardware and home improvement stores.



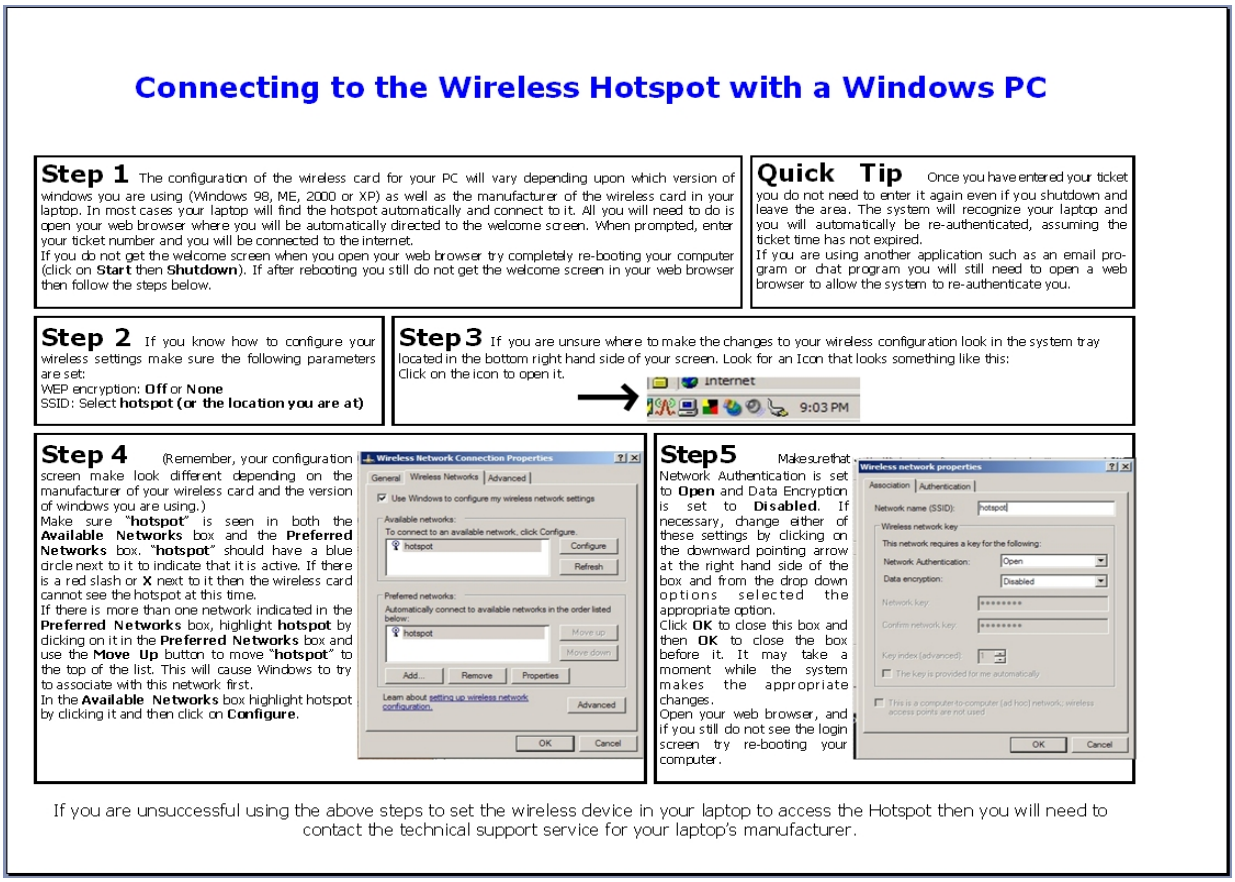
Tip:

When installing repeaters install the repeater closest to the master first and work your way outward. Have the master turned on and connected to the Internet and turn on each repeater as you install it.

When all of the repeaters are installed and powered up, disconnect the master from power for 30 seconds and then re-power the master. The repeaters will all reconfigure themselves to create the optimum mesh. This re-configuring may take up to 10 minutes to complete, depending upon the number of repeaters you have.

User Guides for Your Wireless Hotspot

Laminated User Guides



Connecting to the Wireless Hotspot with a Windows PC

Step 1 The configuration of the wireless card for your PC will vary depending upon which version of windows you are using (Windows 98, ME, 2000 or XP) as well as the manufacturer of the wireless card in your laptop. In most cases your laptop will find the hotspot automatically and connect to it. All you will need to do is open your web browser where you will be automatically directed to the welcome screen. When prompted, enter your ticket number and you will be connected to the internet.
If you do not get the welcome screen when you open your web browser try completely re-booting your computer (click on **Start** then **Shutdown**). If after rebooting you still do not get the welcome screen in your web browser then follow the steps below.

Quick Tip Once you have entered your ticket you do not need to enter it again even if you shutdown and leave the area. The system will recognize your laptop and you will automatically be re-authenticated, assuming the ticket time has not expired.
If you are using another application such as an email program or chat program you will still need to open a web browser to allow the system to re-authenticate you.

Step 2 If you know how to configure your wireless settings make sure the following parameters are set:
WEP encryption: **Off** or **None**
SSID: Select **hotspot (or the location you are at)**

Step 3 If you are unsure where to make the changes to your wireless configuration look in the system tray located in the bottom right hand side of your screen. Look for an Icon that looks something like this:
Click on the icon to open it.

Step 4 (Remember, your configuration screen make look different depending on the manufacturer of your wireless card and the version of windows you are using.)
Make sure "**hotspot**" is seen in both the **Available Networks** box and the **Preferred Networks** box. "**hotspot**" should have a blue circle next to it to indicate that it is active. If there is a red slash or **X** next to it then the wireless card cannot see the hotspot at this time.
If there is more than one network indicated in the **Preferred Networks** box, highlight **hotspot** by dicking on it in the **Preferred Networks** box and use the **Move Up** button to move "**hotspot**" to the top of the list. This will cause Windows to try to associate with this network first.
In the **Available Networks** box highlight hotspot by clicking it and then click on **Configure**.

Step5 Make sure that Network Authentication is set to **Open** and Data Encryption is set to **Disabled**. If necessary, change either of these settings by clicking on the downward pointing arrow at the right hand side of the box and from the drop down options selected the appropriate option.
Click **OK** to close this box and then **OK** to close the box before it. It may take a moment while the system makes the appropriate changes.
Open your web browser, and if you still do not see the login screen try re-booting your computer.

If you are unsuccessful using the above steps to set the wireless device in your laptop to access the Hotspot then you will need to contact the technical support service for your laptop's manufacturer.

The laminated guide helps users, who may not be familiar with their own laptops, connect to the Checkbox system. These guides are printed on high quality stock, laminated and designed to be used over and over again.

Customized user guides are available for an additional charge.

Warranties and Service

Your Suggestions are Welcome

This is the second generation of this product, and many of the added features, improvements and refinements have been made at the suggestion of our users. We absolutely welcome your feedback and suggestions.

Warranty and Service

We have worked hard to design the best possible system for you and your guests. We want you be completely satisfied with your system. If you are not completely satisfied please let us known and we will try to make it right. If you are still not satisfied you may return the system in its original condition within 30 days from the date of purchase for a full refund, less shipping.

This system includes a 1 year warranty from the date of purchase and 90 days of standard support. This warranty covers repair or replacement of the components of the system as we determine necessary. Standard support is for use by the site management and employees and is provided via telephone or email at our option delivered during standard business hours. Support does not include guest support, on-site visits, after hours calls, or assistance with network issues and items not related to this system. In no event shall Checkbox Hotspots be responsible for consequential damages due to the failure of this system or any of its components. We reserve the right to terminate support in the unlikely event of excessive, or abusive calls.

Legal disclaimer

Legal disclaimer – the simple version: Under *no* circumstances will Checkbox Hotspots liabilities exceed the original purchase price of the product. This is a network access device, and the purchaser alone is ultimately responsible for network and data security.