FirstSpot® Guide

Date : February 13, 2018
Version : 8.1

PatronSoft

FirstSpot® Guide

Copyright © 2002-2018 PATRONSOFT LIMITED
All rights reserved.

Every effort has been made to ensure the accuracy of this guide. PATRONSOFT LIMITED makes no warranties with respect to this documentation and disclaims any implied warranties. In no event shall PATRONSOFT LIMITED be liable to you or any other person or entity for any indirect, incidental or consequential damages in connection with the use of this guide or FirstSpot®.

This documentation is subject to change without notice.

FirstSpot is a registered trademark of PATRONSOFT LIMITED. All other trademarks and registered trademarks are the property of their respective owners.

Table of Contents

1. Terminologies

Access Minutes (i.e. timeleft, also called air time credit in the past) - When the user is online, FirstSpot will keep decrementing this value. When this value reaches zero, the user account will be frozen until this value is increased again.

Administrator - The “superuser” (user with the highest authority) of FirstSpot administration

Authentication Server - the FirstSpot component that serves login page and other web page to the client device. It also handles username/password lookup and other authentication services.

Captive Portal - the technology FirstSpot utilizes for authenticating users. The term Captive Portal (sometimes also known as “catch and release”) comes from the fact that it forces unauthenticated users to a web portal (“capture” the users and redirect them to a “portal”). Also, known as web-based authentication.

Client Device (or Client PC) - term to describe the client side machine in a Wi-Fi Hotspot or visitor-based network. Normally a Notebook PC, PDA or Internet-enabled mobile phone in a Wi-Fi Hotspot. Can be a normal Desktop PC in a MTU (Multi-Tenant Units) or Enterprise Intranet environment.

Configuration Manager - web-based tools to configure FirstSpot (Windows shortcut located in the FirstSpot program group).

Dispatcher - the lightweight FirstSpot process that dispatches the client device request to Authentication Server.

Exception free website - A FirstSpot feature that allows some web site to be “free” (i.e. without forced login page). Note that FirstSpot makes patronsoft.com a free web site by default.

FirstHop driver - Part of the FirstSpot program. Technically, FirstHop driver is a proprietary Windows-based NDIS intermediate driver (tied to the Visitor Network Interface only). It provides crucial service to the rest of the FirstSpot program to maintain session data, redirect web page and provide security control.

InfoBox - The browser pop-up that generated by FirstSpot after the end-user logins (you can also get open InfoBox using Instant Keyword “infobox”). It contains a logout button as well as other login information.

Instant Keywords™ - the FirstSpot technology that allow a Client PC to enter a keyword such as “logout” in the web browser to perform a certain pre-defined action. Note that the client PC needs to use FirstSpot DHCP Server to take advantage of this feature.

Internet Network Interface - formerly called Public Network Interface, the network interface card (NIC) that connects to the public Internet side.

ODBC datasource - source of data and the connection information needed to access that data. You can define the ODBC datasource through ODBC Data Source Administrator.

Operator - created by FirstSpot Administrator, this account will have partial administrative rights

Passive Login - for this type of username, the client device does not need to go through the web-based authentication page. Instead, FirstSpot will let the client device log in automatically when the first time it accesses the Internet.

Plan - a reusable template to help FirstSpot administrator or operator to create a group of users with the same attributes.

Prepaid card - a card or slip that contains the login information so that the Hotspot operator can pass to the end-users. FirstSpot supports prepaid card printout through the QuickAdd and Bulk Account feature.

RADIUS - stands for Remote Authentication Dial-In User Service. RADIUS is the most common standard for providing AAA (Authentication, Authorization and Accounting) services. In a Hotspot environment, FirstSpot will act as a RADIUS client (in RADIUS terminology, NAS or Network Access Server). Normally, you should only use RADIUS Authentication Mode if you have another NAS that needs to share the same RADIUS server with FirstSpot.

Session Handling - the method which FirstSpot uses to identify client device. IP-based session handling will use IP address to identify the client device while MAC-based session handling will use MAC address.

Shopping Cart - the interface to buy paid access using credit card. Administrator can change the rates and behavior of the Shopping Cart in the Configuration Manager.

SSID - an unique identifier to differentiate one WLAN from another.

Visitor Network - the term to describe the network that is used mainly by visitor or guest. Visitor network is most common in airport, hotel, or conference hall. Sometimes also known as Wi-Fi Hotspots.

Visitor Network Interface - formerly called Private Network Interface, the network interface card (NIC) that connects to the Wi-Fi Hotspot or visitor network side.

WLAN Access Point (WLAN AP) - A wireless LAN transceiver or "base station" that can connect a wired LAN to one or many WLAN devices.

2. Running FirstSpot® for the first time

FirstSpot installation is designed to be simple to use (refer to readme.rtf for issues about installation). Keep in mind that you need to put FirstSpot between the Internet connection and the Wi-Fi Hotspot (see the chapter Network Topologies of FirstSpot®). After the installation, you can test FirstSpot in the following ways:

i) Test (without Internet connection and even WLAN Access Point, and with only 1 physical network adapter) - To achieve this, connect a second PC (i.e. client PC) to FirstSpot's Visitor Network Interface (see Terminologies chapter) with a crossover cable. For Internet Network Interface, you can use the "virtual" adapter Microsoft Loopback Adapter as the Internet Network Interface if you have only one physical Network adapter in the computer that installed FirstSpot. If you use a physical adapter for Internet Network Interface, make sure it is plugged in before starting FirstSpot. Then do the following steps:

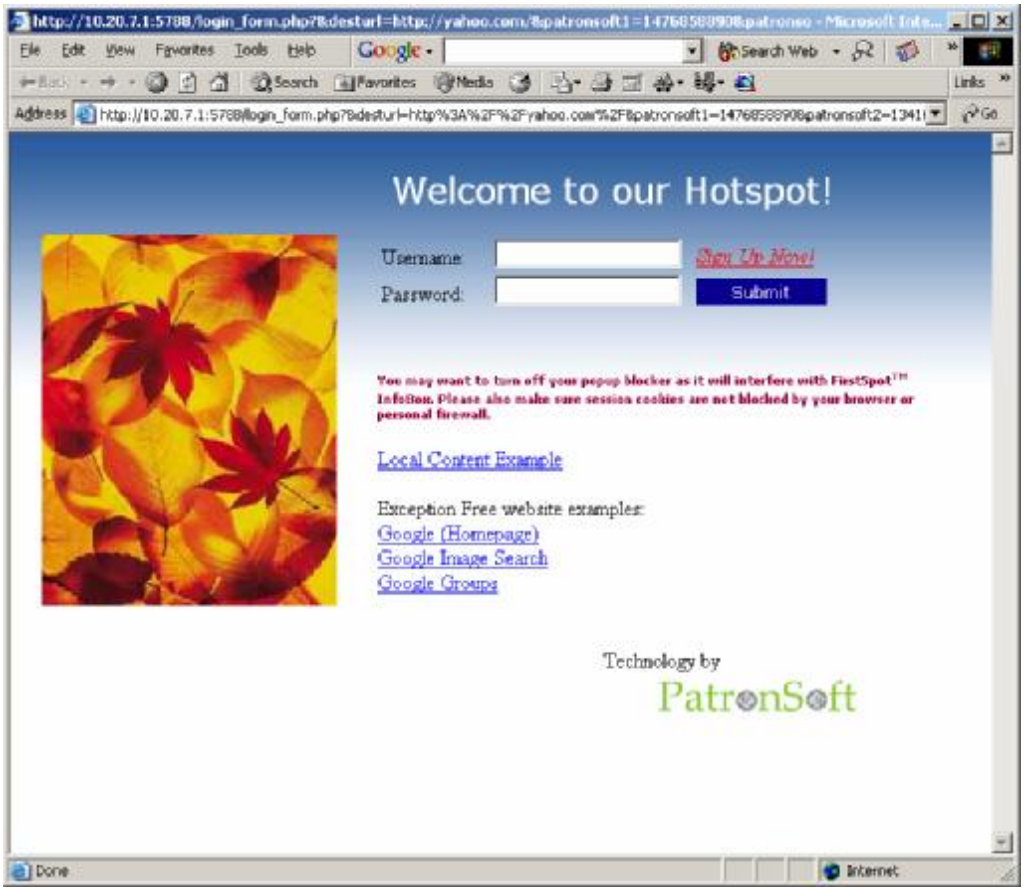
a. Start your client PC first since FirstSpot needs to detect a connection in the Visitor Network Interface.
(Note that even if you somehow force FirstSpot to start, it may not function correctly. Keep in mind that in the real deployment situation, the Visitor Network Connection will almost certain to have a connection first since it should connect to a switch or a AP instead of a PC via crossover cable.)

b. Start FirstSpot through the web-based Configuration Manager. (The shortcut is in your FirstSpot program group, username is "firstspot" and password is "password").

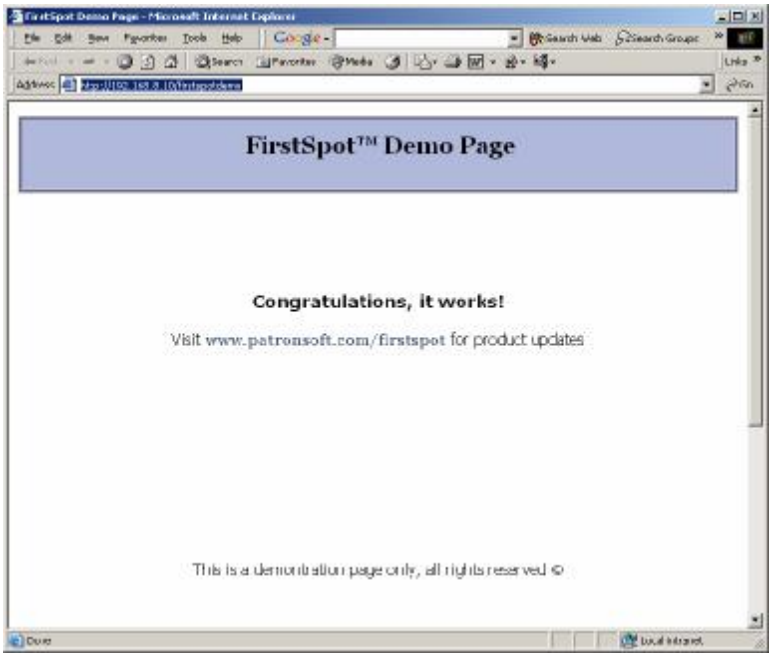
After you start FirstSpot successfully (you should see the word "STARTED"), you need to obtain a new IP address for the client PC. (Make sure you set the TCP/IP setting to “Obtain an IP address automatically” in the client PC)

For Windows client, issue commands:
ipconfig/release
ipconfig/renew

c. Launch the web browser in the client PC. Type http://internetnic_ip where “internetnic_ip" is the IP address of the Internet Network Interface.



d. Enter username as “sample” and password as “password”, you should be able to login and after a short delay, see the below screen:



ii) Normal – For more in-depth testing, in additional to i) above, you need to setup the Internet connection and WLAN Access Point. For Internet connection, FirstSpot can be placed behind NAT, or connect directly to the Internet (either DHCP or fixed IP). *For a WLAN Access Point with router feature (e.g. Linksys BEFW11S4), the WAN port should be unused (i.e. router is not used). For a "vanilla" WLAN Access Point (e.g. Netgear ME102), just connect the Access Point to FirstSpot Visitor Network Interface via a crossover cable or a switch.* Also, please disable DHCP Server within the WLAN Access Point since FirstSpot will handle it (again refer to the diagram in the Network Topologies of FirstSpot® chapter). As FirstSpot already provides access control in the Wi-Fi Hotspot and usually you want maximum usage in the Hotspot, normally you would disable WEP as well.

After you setup the Internet connection and WLAN Access Point correctly, start FirstSpot through the web-based Configuration Manager. Then do the following steps:

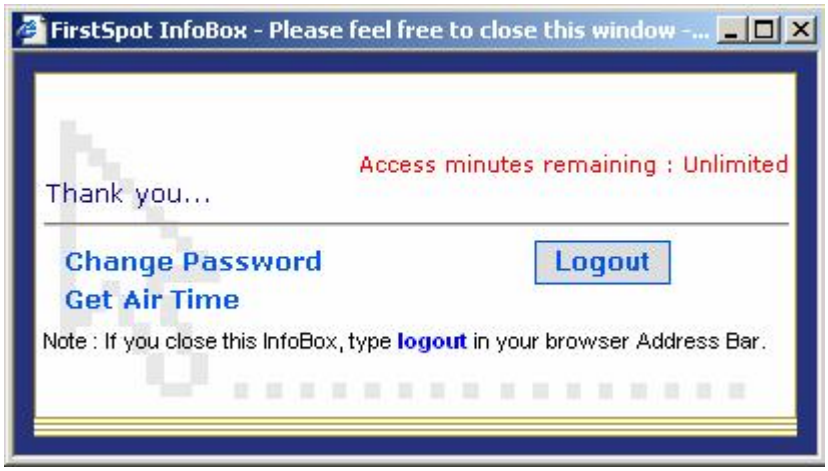
a. Connect to the WLAN from the client device. In most cases, you will scan for the available WLAN and then connect to the network you want (the network is identified by the SSID). Please refer to the document of your WLAN device for details about connecting to WLAN.
b. Launch your web browser. Go to any valid web site (that is not defined as exception free websites. Check out Configuration Manager for details). You should see the login page. Note that you can also reach the login page using the URL http://10.20.7.1:5788 (a.k.a. http://private_ip:auth_server_port), though accessing a valid web site is still the preferred way to bring up the

login page.

c. Enter username as “sample” and password as “password”. You should be able to surf the Internet now.

d. There are 2 ways to logout :

i) Click the Logout button in the FirstSpot InfoBox:



ii) If you close the above InfoBox, you can take advantage of FirstSpot unique *Instant Keywords* feature (refer to the Instant Keywords session in the chapter “Parameters in the Configuration Manager” for details). Type the keyword “logout” (or “logout.firstspot.org” if you have difficulty) in the browser, you will be logged out immediately.

3. Parameters in the Configuration Manager

Access Control:
IP Block list - you can specify the IP list that you want to block a specific group of client PC to access. *For those users that you want to limit their access, make sure you select Yes in "Apply IP Block List" option when you create users.* This option is useful when hotspot and enterprise internal network share the same Internet access. E.g. You can use this feature to block the internal network (i.e. Intranet) access right for guest login.

Port Filtering (White List) - When enabled, FirstSpot will only allow the traffic in the specified ports to go through. Note that this setting applies to client pass-through as well. For example, if you only want to allow web access in your Hotspot, you need to add TCP port 80 (http) and 443 (https). *Note that you must add port 80 to this white list; otherwise, the client PC won't be able to see the FirstSpot login page.*

URL Tracking - When enabled, FirstSpot will monitor the specified ports and will record the details of the outgoing Internet traffic from the client PC in the file urldata_[timestamp].csv under FirstSpot\log directory (note that FirstSpot will move the old files to FirstSpot\log\archive directory during startup). Note that if the URL is visited several times with the same destination port within the "Tracking Interval", FirstSpot will only record as one visit.

Web Filtering - When enabled, FirstSpot will filter web traffic (http, port 80) based on the entries that administrator enter. This feature support wildcard (*) when specifying domain names.

As a option, FirstSpot supports Shalla's Blacklists. Currently, the administrator needs to download, unzip and copy the blacklist files to FirstSpot\blacklists directory manually,

Announcement:
FirstSpot Announcement gives administrator the ability to push text message to the client PC via the InfoBox. Due to the nature of web browser, the client will only get the message when the InfoBox refreshes. One usage example is for the café owner to announce promotion to their customers.

Authentication server:
Authentication server port – the port number of the authentication server.

Maximum number of failed login attempts allowed - The parameter specifies the number of consecutive failed attempts allowed before FirstSpot disables that particular account. Only

FirstSpot administrator or operator can re-enable the account if it is disabled

SSL-enabled login pages - make login pages SSL-enabled

Use 3rd-party SSL certificates - By default, FirstSpot comes with its own self-signed SSL certificate. Alternatively, you can switch to use 3rd-party SSL certificate (e.g. VeriSign, GoDaddy)

* Refer to Chapter 5 : Other Deployment Issues for more detailed discussion on SSL

Show IP or domain name in login page URL - Starting from v6, by default FirstSpot login page URL will use domain name firstspot.org instead of IP. This should ease 3rd-party SSL certificate application process as most 3rd party certificate providers offer certificate signed by domain name only.

Redirect unauthenticated access for port 80 & 443 only - By default, only if client visits port 80 (http) or port 443 (https) initially, FirstSpot will redirect him to the login page. Administrator can change this behavior so that FirstSpot will redirect client to the login page for all other ports. Note that this change might incur significant overhead to the system (e.g. there are lots of non-web traffic) so administrator should monitor the situation closely.

Authentication Mode - Specified whether to use ODBC or RADIUS Authentication Mode. For detailed settings for each option, see the blue description below:

ODBC

File DSN location (.dsn file) – the location of the .dsn file (which stores the connection information to the ODBC datasource). FirstSpot comes bundled with a dBase datasource (i.e. .dbf).

Login option - FirstSpot supports the following login options : Username & Password, Scratch Code, Anonymous Option and Anonymous Option with Shared Secret.

- For Username & Password, user will need to login using username and password.
- For Scratch Code, user will only need to input the scratch code for login. Note that this mode does not provide self signing-up and password changing for users.
- For Anonymous Option, user will not need to input anything. Instead, he will be greeted by an anonymous login page (which the administrator can put disclaimer or advertisement in it, for example) with a button. After the user clicks the button, he can proceed to surf the Internet as usual.
- For Anonymous Option with Shared Secret, user needs to enter a shared secret in

the anonymous login page. Note that the idle timeout will still apply (for both Anonymous Option and Anonymous Option with Shared Secret) and the user will see the anonymous login page again if he is idle for a while.

- Through Social Network - user can gain access if he logins to Social Network like Facebook. Refer to the Social Network category for more details.

Note that for Anonymous Option with Shared Secret, FirstSpot supports the concept of "multiple logins" using the same Shared Secret (Alternatively, you can also use "Multiple Logins" user attribute in the Username/Password or Scratch Code mode). Also, administrator can define a limited set of user attributes (e.g. data transfer tracking, bandwidth throttling) for all the users that login using a particular Shared Secret.

Enable Scenario 2 - select this option if you want to configure FirstSpot as Scenario 2 (Distributed Network Topology). Refer to chapter 4 for more information.

Clear site message table - This table is used for communication between different FirstSpot instances under Scenario 2. In an unlikely event that this table is corrupted, administrator can use this feature to reset the table. Please make sure all instances of FirstSpot is shutdown before clearing this table.

RADIUS

RADIUS Server IP - the IP address of the RADIUS server

RADIUS Server Authentication Port - the UDP port number used for Authentication in the RADIUS Server

RADIUS Server Accounting Port - the UDP port number used for Accounting in the RADIUS Server

RADIUS Shared Secret - the shared secret between RADIUS server and RADIUS client (i.e. FirstSpot)

FirstSpot Vendor ID - FirstSpot vendor ID for RADIUS server to identify FirstSpot RADIUS packet

NAS Identifier Name for FirstSpot - Identifier for RADIUS server to identify FirstSpot NAS (Network Access Server). This information is stored within the RADIUS packet.

FirstSpot NAS IP Address (Blank=Visitor Network Interface IP) - IP address of FirstSpot NAS. This information is stored within the RADIUS packet. Note that the RADIUS server

may choose to ignore this information.

RADIUS server failover - If FirstSpot fails to contact the primary RADIUS sever, FirstSpot can trigger a failover mechanism and contact the second RADIUS server. You need to enter the above RADIUS server information again for the second RADIUS server.

File DSN for local temp data (.dsn) - In RADIUS Authentication Mode, FirstSpot will need to store some temporary data locally in an ODBC datasource This parameter specifies the File DSN for this datasource. Normally, you don't need to modify this parameter.

RADIUS ACCOUNTING -
Acc_Start : If selected, FirstSpot will send an accounting start packet when the user is logged in. Accounting start packet is a standard RADIUS accounting packet to start the accounting progress.

Acc_Stop: If selected, FirstSpot will send an accounting stop packet when the user is logged out. Accounting stop packet is a standard RADIUS accounting packet to stop the accounting progress.

Acc_FSLogin: If selected, FirstSpot will send a custom accounting start packet when the user is logged in. This packet is a custom packet for those who cannot use the standard accounting start packet in RADIUS server.

Acc_FSLogout: If selected, FirstSpot will send a custom accounting stop packet when the user is logged out. This packet is a custom packet for those who cannot use the standard accounting stop packet in RADIUS server.

Acc_FSWriteLog: If selected, FirstSpot will send a custom packet when the user is logged out. This custom packet is used to notify RADIUS server to create a user log.

Acc_FSLogin (Blank=217), Acc_FSLogout (Blank=218), Acc_FSWriteLog (Blank=219) - you can change the value of the Accounting Custom Attributes here. Note that you need to add the corresponding Accounting Custom Attributes in your RADIUS Server.

* Refer to Chapter 9 : Setting up RADIUS server for the details on the configuration of RADIUS server

Display "Sign Up Now" link in the login page - Option for showing the "Sign Up Now" link in the login page. Note that this "Sign Up Now" link will lead to several options including Self Sign-up, Free Access and SMS Sign-up.

After clicking "Sign Up Now" link, display - After clicking the “Sign Up Now”, FirstSpot has 3 ways to for end users to sign up :

i) Self Sign-up
Initial access minutes for self sign-up users - For self sign-up users, FirstSpot will assign the initial access minutes for them. A value of 0 means that users need to increase the access minutes via credit card immediately before they can access the Internet.

Self sign-up Plan - this option allows administrator to define initial user attributes when user self sign-up. Note that if this parameter is set, the above “Initial access minutes for self sign-up users” will be ignored.

Self sign-up Redirect option - allows administrator to configure which page to redirect the user to after self sign-up.

Enforce restriction on self sign-up accounts - enforce limitation on self sign-up (see the next parameter)

Time elapsed before the same machine can sign up again - FirstSpot can limit the frequency of a particular client PC can self sign-up. Note that FirstSpot will use either MAC or IP to identify the client machine (depends on the Session Handling setting)

ii) Free Access : FirstSpot supports initial free access without the need to create the user account (either through Self Sign-up or created by administrator). FirstSpot will create a special user which the username is the client MAC address with the Free Access user attribute set to Yes.

Free Access Plan - the Plan specified here is used to initialize the special Free Access users (for each Free Access session). Note that the Free Access user attribute will be set to Yes regardless of the Plan setting.

Availability of a new Free Access session (One-off/Daily/X mins after start time of previous session) - specify when to reset Free Access user. FirstSpot will re-apply the Free Access Plan to the Free Access user if the criteria is met. For One-off case, there won’t be any reset for any particular user. So for each client device only the initial access right (i.e. one session only) specified in the above Free Access Plan is available (unless the administrator manually change the user attributes afterwards).

Daily reset time to offer new Free Access session (hh:mm) - If Daily is selected, need to specific the daily reset time here. FirstSpot will reset the Free Access user right using the

above Free Access Plan (i.e. a new Free Access session) for the same client device if he login after the daily reset time.

Waiting time before offering a new Free Access session - If X mins after start time of previous session is selected, FirstSpot will reset the Free Access user right using the above Free Access Plan (i.e. a new Free Access session) x minutes after the previous login for the same client device.

iii) SMS Sign-up : FirstSpot will collect the mobile phone number from the end users. FirstSpot will then send a Scratch Code to that mobile phone number via SMS. Note that FirstSpot will assume hotspot operator has access to an SMS email gateway (see below).

SMTP server - the SMTP email server for delivering email to the SMS email gateway

SMTP Port Number (Default 25 if empty) - you can change the SMTP port if it is not using the default port 25

SMS email gateway - specify the SMS email gateway here. This gateway needs to perform the email-to-SMS conversion. You need to enter the SMS email gateway's suffix here (we assume the prefix to be the mobile number).

Email from - specify the from field within the email

Current Scratch Code being delivered - FirstSpot will deliver Scratch Code using SMS in "ascending order". FirstSpot will automatically will use the first available Scratch Code if this option is not specified. FirstSpot administrator can also change/reset the current Scratch Code here.

Enable password offloading - Feature to replace the default encrypt_pwd.exe encryption mechanism. One of the usage of this feature is to keep the password in sync with other user directory. You can insert the same username/password of other directory to the FirstSpot ODBC user table by changing the default FirstSpot encryption mechanism. Note that for this feature to work correctly, the command line program that replaces encrypt_pwd.exe must output the encrypted password "only" to standard output (without any additional text. Try to run encrypt_pwd.exe to mimic the behavior).

Path & filename for password offloading - the location of the password offloading program

Bulk Accounts:

Interface to create a large number of accounts

Enable slip printing - Administrator can enable prepaid card (i.e. slip) printing here. Note that the slip preview interface will show all the accounts that are just created, and the administrator can either print or save the slip in the popup window.

Client Filter:
Black List - this is useful for administrator to block offending client PC. For example, you can block a client PC that tries to gain unauthorized access to FirstSpot or monopolizes the bandwidth.

Client pass-through - you can specify the MAC or IP address of the client PC that FirstSpot will let its traffic to pass-through without login. Note that global bandwidth throttling does apply to pass-through client device. But client pass-through will NOT work with Per User Bandwidth Throttling. You need to use "use MAC as username" or "Passive Login" instead.

(Whether you specify IP or MAC in the above parameters depends on your Session Handling setting.)

Configuration Manager:
Username – the username of the Configuration Manager login. Default is “firstspot”.

Password – the password of the Configuration Manager login. Default is “password”.

Allow configuration manager access from Visitor Network (i.e. Wi-Fi Hotspot) - By default, FirstSpot Configuration Manager can only be accessed locally. By selecting this option, one can also access the Configuration Manager from the Hotspot side (the network that is connected to the Visitor Network Interface). Note that this has security implication and is usually reserved for testing only.

Allow configuration manager access from the Internet Network - Similar to the setting above. Allow administrator to access Configuration Manager from the Internet Network Interface.

Operator accounts - you can define operator accounts (in addition to the Administrator account, which is really the account with the highest authority). You can assign each operator account to be able to access specific category(s) within Configuration Manager. E.g. you can create an operator “operater1” to be able to access the “Administration” and “Users” categories only.

Credit Card:
Please refer to chapter “Credit Card Support”.

DHCP:
FirstSpot DHCP server will assign and recycle IP address dynamically and automatically. Keep in mind that if session handling is IP-based, the IP address of the client device need to remain unchanged during one session. This is handled correctly by the FirstSpot DHCP Server.

FirstSpot DHCP server determines the IP address range based on the Visitor Network Interface IP and subnet mask settings. E.g. (based on default Visitor Network Interface IP and subnet mask) the range will be 10.20.7.2->10.20.7.254. For the case of Multiple Network Segments (see Scenario 3 in the Network Topologies of FirstSpot® chapter), it is determined by the Router IP and Subnet Mask value within your Multiple Network Segments settings. Note that the largest subnet mask we support is 255.255.0.0 which is around 65535 IPs.

Excluded IP Address - FirstSpot DHCP Server will not hand out that particular IP if it is specified in the “Excluded IP Address” list. For example, this feature is useful if you want to exclude the IP addresses of WLAN APs so that FirstSpot DHCP server won’t hand out conflicting IP addresses.

Allocate IP only when IP-MAC mapping is defined (Excluded IP table will be ignored.) - By default, FirstSpot DHCP server will allocate an IP randomly if it is not defined in the IP-MAC mapping. When this option is selected, FirstSpot will only respond to a DHCP IP request if the IP-MAC mapping is defined. In other words, no IP will be handed out if the IP-MAC mapping is not there.

Static DHCP listing file location - location of the file that stores the IP-to-MAC mapping.

Lease time for DHCP Client - let you change the lease time for the IP handed out by the DHCP server

Preferred DNS server IP for the Visitor Network, Alternate DNS server IP for the Visitor Network - let you override the DNS settings handed out by the DHCP server. The default is to use FirstSpot Visitor Network Interface IP (i.e. FirstSpot DNS server). Note that you if you don’t use FirstSpot DNS server, you will lose the ability to use Instant Keywords.

Note 1: If you use IP-based session handling and disable FirstSpot DHCP server,

- → your DHCP server needs to hand out the same IP address to a particular client device within one session to avoid client device being asked to re-authenticate.
- → the idle timeout value in FirstSpot should be small (e.g. 2 minutes). For example, if the client changes IP (release and renew) and tries to re-login using the same username, either he waits for the 2 minutes so that FirstSpot timeout his account, or he explicitly logout first using "Instant Keyword" features.
- → the DHCP IP "recycle" time needed to be greater than the FirstSpot idle time. For example, if client A release an IP and client B gets the same IP before client A's username logout (by idle time out), client B can steal client A access right and surf the Internet. In other words, client B should not get client A IP address (i.e. IP recycle time) before client A username timeout (i.e. FirstSpot idle time)

Note 2: FirstSpot DHCP server supports DHCP relay. In Scenario 3 (see the Network Topologies of FirstSpot® chapter), the router must enable the DHCP relay function in order for FirstSpot DHCP Server to assign IP to the client device correctly.

Dispatcher (Main):
Dispatcher service listen port – the port number that dispatcher service listen to.

Connection idle timeout (minutes) – number of minutes that a user can idle (i.e. no network traffic) before FirstSpot will disconnect that particular user

Maximum time limit per session (No limit if empty) - maximum number of minutes per login session. This feature is useful when the administrator wants to force client device to re-login every once in a while. This parameter will work for all Login Options (see Authentication Server -> Login Options)

Maximum number of concurrent users (No limit if empty) - to limit the maximum number of concurrent users. Administrator can use this feature for sizing or troubleshooting purpose. Note that Passive Login user does not count under this parameter.

Visitor Network Interface IP - (formerly called Private Network Interface) the IP address that Visitor Network Interface. Normally, it is set to a private IP address such as 10.20.7.1 . Please note that you should NOT change the IP for the network interface card directly in Windows. Also, the visitor network IP address space (for local network segment) delivered by FirstSpot DHCP server is derived from this value.

Visitor Network subnet mask - the subnet mask of the above IP address

Client Isolation - this feature will prevent client PC from seeing each other in Windows “My

Network Places" or "Network folder". Note that this feature requires FirstSpot DHCP server to be enabled (default) and you cannot use third-party DHCP server.

Internet Network Interface IP - (formerly called Public Network Interface) this IP address needed to be configured in Windows directly before starting FirstSpot. FirstSpot will query the Internet Network Interface to obtain this IP address.

Use proxy for port 80 (http) connection - FirstSpot supports web proxy for port 80 traffic. For some cases (e.g. in some countries), the only way to access a web is through a web proxy. FirstSpot can be configured to forward all port 80 requests to a web proxy. Note that FirstSpot assumes the port 80 traffic type is http.

Bandwidth Throttling (global setting) - to limit (i.e. throttle) the bandwidth consumed by users. This is used to prevent any particular user to monopolize the bandwidth (which will affect other users' performance). FirstSpot will use this global setting unless it is overridden by user (or shared secret) bandwidth throttling setting. *Please note that there will be some variations on the actual bandwidth the client device gets and this value is an approximation only (Please use NetMeter as a measuring tool).* Also, the minimum custom bandwidth throttling value should be 2.

Flexible Bandwidth Throttling - a special bandwidth throttling mode that only enable when the total upload or download bandwidth utilization has reached a certain limit. The purpose of this mode is that a quiet system will give bandwidth throttling users plenty of bandwidth, but when a system gets busy bandwidth throttling is enforced so that no one will monopolize the bandwidth. Note this setting will apply to all users that enable bandwidth throttling (whether by the above global setting or through the per-user bandwidth throttling setting).

Download Data Transfer (Global Setting), Upload Data Transfer (Global Setting) - When enabled, FirstSpot will track the total data transfer in one login session. FirstSpot will use this global setting unless it is overridden by user (or shared secret) data transfer counting setting.

When to reset data transfer counters of all users (global setting) - specify the interval that FirstSpot resetABW.exe will reset the data transfer counter to zero. Note that you need use Windows "Scheduled Tasks" to run resetABW.exe at midnight (12am) everyday. FirstSpot resetABW.exe program will reset the data transfer counter according to the setting here. FirstSpot will reset both download and upload data transfer.

Path & filename for post-startup batch file - Specify a batch file that FirstSpot will run as the last step of FirstSpot startup sequence. Usually used to change IP or Routing setting. The format should be "[drive]:\[path]\[filename]"

SMTP Roaming - this feature allows client device to send email regardless of its SMTP setting. For example, if a client device's SMTP setting is configured as the corporate Intranet SMTP server (which cannot be accessed in Hotspot), he needs to change the SMTP setting in order to send email. By enabling this feature, FirstSpot will forward all the outgoing mails (through port 25) to the ISP SMTP server instead.

ISP SMTP server - specified your ISP SMTP server domain name or IP address.

ISP SMTP server requires authentication - you can specify the username and password here if your ISP SMTP server requires login

SMTP Port Number (Default 25 if empty) - By default, SMTP server will receive email from port 25 (and then push the email to recipients' SMTP). Some SMTP server will allow email from other port (e.g. 26) in order to bypass restriction in the Internet access. This parameter will allow administrator take advantage of this kind of SMTP server.

Maximum Recipients Per Mail (Default 50 if empty) - the maximum total number of recipients in the to, cc and bcc fields per email

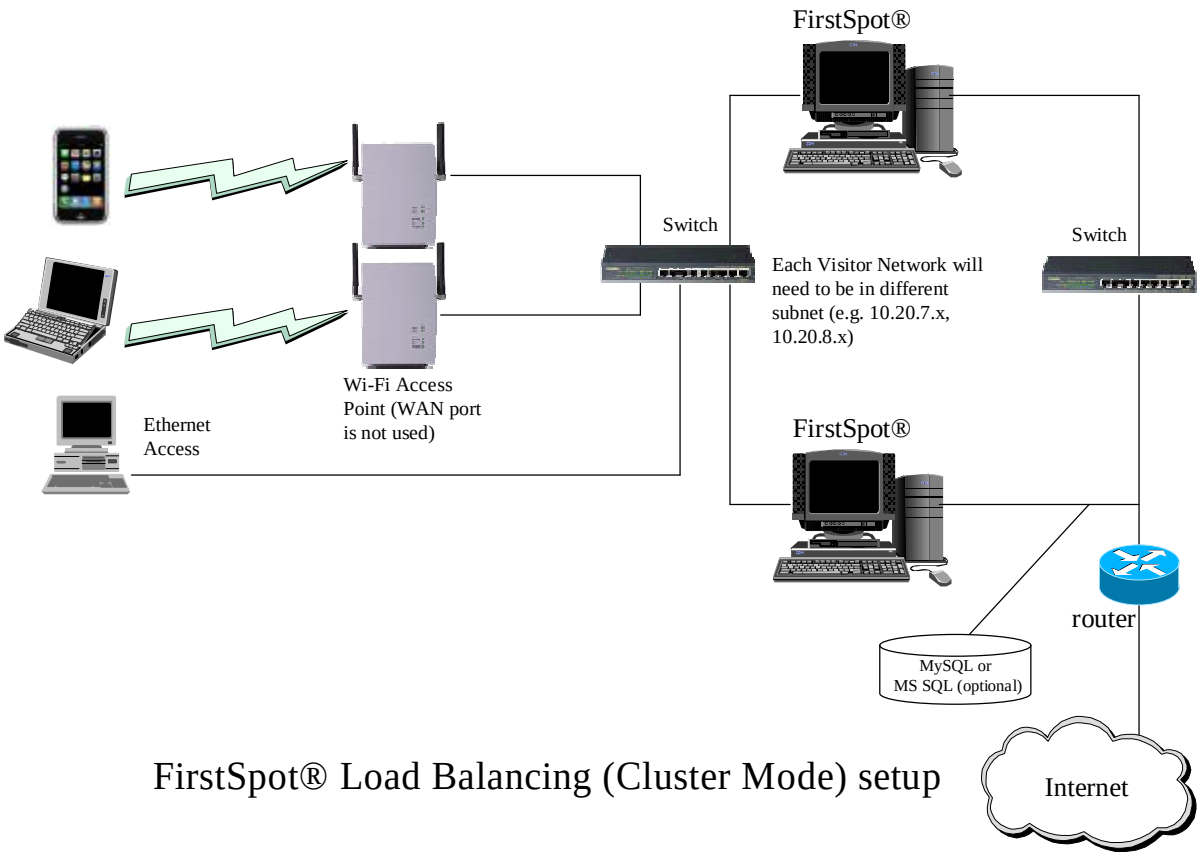
Maximum Mail Size in MB (Default 2MB if empty) - the per email size limitation (including attachment)

Send Mail Frequency Cycle (in second, default 60 if empty) - FirstSpot will queue up the emails and set them in batch. This parameter defines the time interval that FirstSpot will wake up to send the pending emails.

Email Report:
Configure the tool fsEmailReporting.exe that will email report periodically. Administrator needs to enter the correct setting in the Configuration Manager UI, and then put the program fsEmailReporting.exe in Windows Task Scheduler (run a midnight daily). The program fsEmailReporting.exe will email the reports according to your setting here.

Exception free websites:
To define the Exception free websites (see Chapter 5 : Other Deployment Issues for details)

Failover/Load Balancing:



FirstSpot® Load Balancing (Cluster Mode) setup

FirstSpot Load Balancing (Cluster Mode) is an easy-to-setup clustering feature which allow several FirstSpot to share the load of the incoming traffic automatically. This is also a Failover feature for new incoming devices. For existing devices that are already on the Visitor Network, they need to renew the IP either by disabling/enabling Wi-Fi network or restarting the devices. In this mode, the same device will always get priority response from the same FirstSpot DHCP server (unless one of them is down), so it won't keep switching DHCP and thereby switch FirstSpot. Architecturally, each FirstSpot DHCP server within the cluster is active and there is no heartbeat connection among different FirstSpot servers.

Share FirstSpot User Table - External MySQL or MS SQL datasource is needed if you want share FirstSpot user table (refer to Chapter 8 : Using External Datasource as User Database). This setting is optional and each FirstSpot can use its own the default datasource instead (e.g. Anonymous Option).

Number of FirstSpot Machine in the Visitor Network - the total number of the FirstSpot in the whole cluster.

Machine ID - make sure each FirstSpot within cluster has its own unique ID. For example, if “Number of FirstSpot Machine in the Visitor Network” is 2, make sure one FirstSpot is set

to 1, and the other is set to 2. This number is used to evenly randomize the DHCP server response according to the device.

Initial DHCP response delay time - In the ideal situation if all the FirstSpot machines within the cluster has similar CPU power, different devices will get IP from different DHCP server. If all the devices (need use more devices to test) keep getting the IP from the same DHCP server, try to increase from the default value to anything up to 2000ms.

Clear Load Balancing message table - This table is used for communication between different FirstSpot instances. In an unlikely event that this table is corrupted, administrator can use this feature to reset the table. Please make sure all instances of FirstSpot is shutdown before clearing this table.

Several points to note about Load Balancing (Cluster Mode):
1) Using FirstSpot machines with similar CPU power is recommended
2) Only MAC-based Session Handling is supported
3) You need to configure each FirstSpot with unique, non-overlapping Visitor Network side IP (e.g. 10.20.7.x, 10.20.8.x)
4) RADIUS Authentication Mode are not supported
5) “Enable Scenario 2” under Authentication Server is disabled if Load Balancing (Cluster Mode) is selected

In-browser Message:
The technology that inserts message to client active browsing section. This feature is useful for delivering message to the client, especially when he has difficulty viewing the InfoBox popup.

Instant Keywords™:
There is no way to prevent the user accidentally closing InfoBox (as the browser does not allow that kind of control). If an user accidentally closes the FirstSpot InfoBox (the window that contains the logout button), he can type the Instant Keyword “logout” in his browser to bring up the logout screen (See the chapter “Running FirstSpot® for the first time” for the screenshot).

For client device that does not support DNS domain suffix (e.g. some version of PocketPC), you may need to type “logout.firstspot.org” instead. Note that FirstSpot DHCP server will give the DNS domain suffix “firstspot.org” to the client device.

Note that if the original login browser is not yet closed, FirstSpot will remember the login

setting and it will skip the step of asking you the username/password (e.g. if you type “logout”, you will be logged out immediately instead of being asked by FirstSpot for the username/password).

FirstSpot has several pre-defined Instant Keywords. You can also add your own customized Instant Keywords in the Configuration Manager.

Also, Instant Keywords will not work for the user that is configured with the “use MAC/IP as username” option.

Default DNS suffix - The setting allows administrator to change the default DNS suffix “firstspot.org” to other domain name (e.g. yourdomain.com). Note that this DNS suffix is necessary for “Instant Keywords” feature to function correctly. Note that the domain name you specify should not respond to any sub-domain requests (e.g. mail.yourdomain.com, abc.yourdomain.com), otherwise it will conflict with Microsoft Windows Network Sharing.

Multiple Network Segments:
This setting allows FirstSpot administrator to setup multiple network segments within the visitor-based network (see scenario 3 in the Network Topologies of FirstSpot® chapter). The information provided in this setting will enable FirstSpot to setup return-path routing and DHCP server correctly. Below is the explanation of each field:

Router IP - This is the IP address of the router within the network segments. This setting is used by the FirstSpot DHCP Server to make sure it delivers the right setting to the client device.

Subnet Mask - This is the subnet mask of the corresponding Router IP.

Gateway (for return-path) - This is the gateway IP that facing FirstSpot Visitor Network Interface. This setting is used to setup return path to the corresponding network segment (via the corresponding router). The Gateway IP needed to be accessible from Visitor Network Interface (i.e. you can ping the Gateway IP from the Visitor Network Interface)

Enable Redirect File (TPL format) - let you specify the greeting page for each network segment. If this option is not checked, all network segments will use the same greeting page.

Redirect File (TPL format) - Filename of the targeted redirect template file (.tpl, full path is not required). The file should be placed under FirstSpot\authserv\template directory. You can use the file login_form_body.tpl (for Username & Password or Scratch Code) or alogin_form_body.tpl (for Anonymous Option) as a base template for this redirect TPL file.

NAT:
Network Address Translation (NAT) - Configure the NAT feature within FirstSpot. Note that if NAT is disabled, you have to add a return route correctly in your next-hop router. For example:

Client PC → FirstSpot → Router (add the return route here) -> Internet

** client PC IP - 10.20.7.x*
Visitor Network Interface IP - 10.20.7.1
Internet Network Interface IP - 192.168.0.4

Disabling NAT will reveal the client IP (i.e. 10.20.7.x) to the router. When the returning traffic arrives from the Internet, your router need to know where the packet should send to. You need to inform your router that all returning traffic which is destined to 10.20.7.x should be forwarded 192.168.0.4. Using the above example, the return route will be:

10.20.7.0, 255.255.255.0, 192.168.0.4

Note that for forward traffic, it is determined by "default gateway" so there is no need to do anything in your network (whether NAT is enabled or not). Also, if your NAT is on (default setting), there is no need to set the return route in the router as all client traffic will be looked as if it is coming from 192.168.0.4 from the router point of view. In that case the router will know where to send the return traffic to (since it belongs to the same subnet, it will just use ARP).

Real IP Address Mapping - Used when NAT is enabled. The Real IP Address Mapping feature gives administrator the ability to map a real IP to a private IP address (in FirstSpot hotspot side of the network). It allows an external user to reach the FirstSpot hotspot internal user from the outside via a real IP address. The administrator needs to define the pool of available real IP address in advance. Once the client PC logs in correctly and that particular FirstSpot username is enabled for “Real IP Address Mapping”, FirstSpot will automatically map one of real IP address to the private IP of that client PC. Administrator needs make sure:

1) there is enough IP in the Real IP pool. FirstSpot will recycle the IP once the user logs out. Still, you might want to give some slack if the Real IP utilization is approaching the limit.
2) if there is another NAT router/firewall between FirstSpot and the Internet, you need to configure the router (e.g. using DMZ) so that all the real IPs are pointing to FirstSpot Internet Network Interface. Again, FirstSpot will only map the real IP to the client PC after login.

Port Forwarding - When NAT is enabled, the Port Forwarding allows administrator to open a port so that an external user can access a visitor/private IP address (in FirstSpot hotspot side of the network) via the Internet Network Interface IP. The feature is port-level so the visitor/private IP is only accessible through the port specified. As an example, this feature can let administrator access a device (e.g. Webcam) from the Internet.

ProxyARP - ProxyARP is a protocol that exposes the client PC IP in the Visitor Network Interface side so that it is visible from the Internet Network Interface side. In FirstSpot case, it is used to simplify the network setup when NAT is *disabled*. Under normal circumstances, when NAT is disabled, a return route has to be set up so that the router in the next hop knows the fact that it needs to forward the network packets that are destined to the client PC to FirstSpot's Internet Network Interface. When ProxyARP is enabled, the return route is no longer necessary and FirstSpot will handle everything automatically. Note that administrator needs to define the ProxyARP IP range in advance for the client PC. Also, the IP range must be in the same subnet as the Internet Network Interface IP.

Plans:
You can define usage plan here (see the Chapter 1: Terminologies on the definition of Plans). Note that there is no linkage between the Plan and user attributes once the user account is created or shopping cart items is being purchased.

Session Handling:
By default, FirstSpot uses MAC-based session handling. In other words, MAC address is used as a way to identify the client devices. The MAC-based session handling is a more secure setting. If there are router(s) between the hotspot network segment and FirstSpot machine, MAC address is not visible from FirstSpot. Alternatively, IP-based session handling should be used instead.

Shopping Cart:
You can customize Shopping Cart here (see Chapter 1 : Terminologies for the definition).

Starting from v7, administrator can define Shopping Cart Items directly here instead of using Plan (i.e. v6 or earlier, legacy mode). The Shopping Cart Items are a subset of user attributes. FirstSpot only includes the items (user attributes) that are make sense for user to purchase. Also, instead of relying on Shopping Cart purchase to apply user attributes, the administrator needs to initialize the user attributes correctly.

Redirect to shopping cart when user fails to login - when a certain resource of an user

account is used up (e.g. data transfer quota, access minutes) or the account is suspended, FirstSpot will redirect the user to the shopping cart (so that he can buy more access). The administrator can disable this redirection using this setting.

Social Network:
When login through Social Network is enabled, user can gain access to FirstSpot by logging in to a social network (e.g. Facebook). Note that FirstSpot will automatically create a FirstSpot user the first time he gains access to FirstSpot though social network.

Facebook

Your Facebook page ID - the Facebook page ID of page that the Like button will be shown in the FirstSpot captive portal (i.e. greeting) page.

Prevent user from logging in if user does not like your page - If the administrator select this option, the user also needs to “Like” the above Facebook page first before gaining Internet access. If the page is “unlike”, he needs to redo the “Like” action before he can gain access to FirstSpot.

Your Facebook app ID - this Facebook app needs to have user_likes permission. Facebook may require app developer to provide Privacy Policy URL before enabling this permission.

plan for Facebook user - the default FirstSpot user attributes for newly create user account.

Status:
For monitoring the current FirstSpot login status. Note that the IP address shown here is derived from FirstSpot DHCP Server for MAC-based session handling, and the MAC address shown here is derived from FirstSpot DHCP Server for IP-based session handling. If you are not using FirstSpot DHCP Server, the IP (in the case of using MAC-based session handling) or the MAC (in the case of using IP-based session handling) will not be shown.

FirstSpot administrator can also disconnect users (including anonymous login) here.

UI Customization:
Login page picture file - you can specify the picture of the login page (i.e. captive portal) here.

Redirect option - By default, FirstSpot will redirect the client PC to the original URL (i.e. the

URL it accesses before being redirected to the FirstSpot login page) after the user login successfully. You can change to a fixed URL page instead. For example, you can push the user to your promotion page or corporate web site after the user successfully login.

Redirect delay (in seconds) - After the client PC login successfully, the client will be redirected to page after a certain delay (default is 5 seconds). This parameter allows the administrator to change the delay time.

Show InfoBox - In some rare circumstances, the InfoBox windows may intervene with your browsing. You can disable the InfoBox here. Disabling InfoBox will not affect FirstSpot operation.

Logout automatically when Infobox is closed - When enabled, FirstSpot will disconnect the user if he closes the InfoBox. This is useful if you want to make sure the client see the message within the InfoBox. "Logout automatically when Infobox is closed" is not real time. So it is normal that administrator needs to wait for a while (e.g. 60 seconds) before client is disconnected.

Show the extra 'Buy more credit' button - you can enable/disable “Buy more credit” button within InfoBox here.

Enable user to change password - option to show the change password button in the InfoBox.

Enable disconnect reminder - When FirstSpot is about to disconnect an user (e.g. access minutes is about to used up), a reminder will appear in the InfoBox. Note that user can click anywhere in the InfoBox to close the reminder.

Remind user before disconnect (minutes) - the time interval that the disconnect reminder will appear before the actual disconnect happens.

Enforce character encoding - when enabled, FirstSpot will display the appropriate language (if available) based on the client device setting (i.e. Dynamic Multiple Languages Support). FirstSpot will select the appropriate language based on client device http header. If the best-match language file is not defined, FirstSpot will use default language instead.

You can only modify the content of the default language in FirstSpot Configuration Manager. For other language, you need to change the language file directly.

Several points to note:

1. *To change the end-users interface text, either you change it here in the UI category of Configuration Manager, or you can edit the custom_lang.php file directly.*
2. *To change the Configuration Manager interface text, you need to edit the custom_cmlang.php file directly.*

3. *The custom_lang.php and custom_cmlang.php act as an overlay that sit on top of lang.php and cmlang.php respectively. You should change the files custom_lang.php and custom_cmlang.php only. The file lang.php and cmlang.php contain the default text and we will be most likely adding new text when we upgrade FirstSpot. If you need to migrate/upgrade FirstSpot, you just need to copy your custom_lang.php and custom_cmlang.php files to the new FirstSpot directory. This way you can ensure that you don't overwrite the new default text.*
4. *As for Dynamic Multiple Languages Support, the new language file should follow the format of lang.php. Note that Dynamic Multiple Languages Support focuses on end-users interface only.*

Users:
You can configure individual user accounts here.

QuickAdd - a simple add user mechanism which administrator only needs to fill in username/password and select the appropriate Plan. After the user account is created, FirstSpot will display the Prepaid card printout in a separate browser window (which the administrator can then print it out).

Account is disabled - this is used to temporary disable an account without deleting it

Account is active - set the activation time. This is used as the starting point by the "After x Minutes/Hours/Days" condition (see the next parameter).

Restricted account - When restricted account option is set, if the access minutes or data transfer quota is used up, FirstSpot will not suspend the user account; instead, user can still have access on the Internet but with 'bandwidth throttling' set to global bandwidth throttling setting. Normally, you set the global bandwidth throttling value to a small value, so that the user speed will be slowed down after the above access minutes or data transfer quota is used up. When the account is in restricted state, the account will be back to normal state by adding access minutes or Download/Upload Quota through FirstSpot Configuration Manager User Section or by end-users purchasing through Shopping cart.

Conditions to suspend this account - you can specify several conditions to suspend an user account. You can combine several conditions, and the user account will be suspended when the first condition is met.

Bind to first login MAC address - By default (option No), FirstSpot username and scratch code can be access from different client (identify by MAC address). For each login, user can login using different machine. For option Yes, FirstSpot will record the client MAC for first login so all subsequent logins must be from the same machine. For option Yes (login once - set as Passive Login after first login), after first login, the user account will be converted to "Passive Login" so the same client machine can access the Internet without login.

Remove user(s) that has not login for certain period of time - the will delete all the inactive users in the user table. You can specify the inactive time period (in days) in the UI. Alternatively, we provide a command line program called removeUser.exe which will let administrator to perform periodic cleanup to the user table. You can run removeUser.exe in Windows Scheduled Tasks. The syntax is : removeUser.exe X (where X is the inactive time period in days). Note that this feature will not work under RADIUS Authentication Mode.

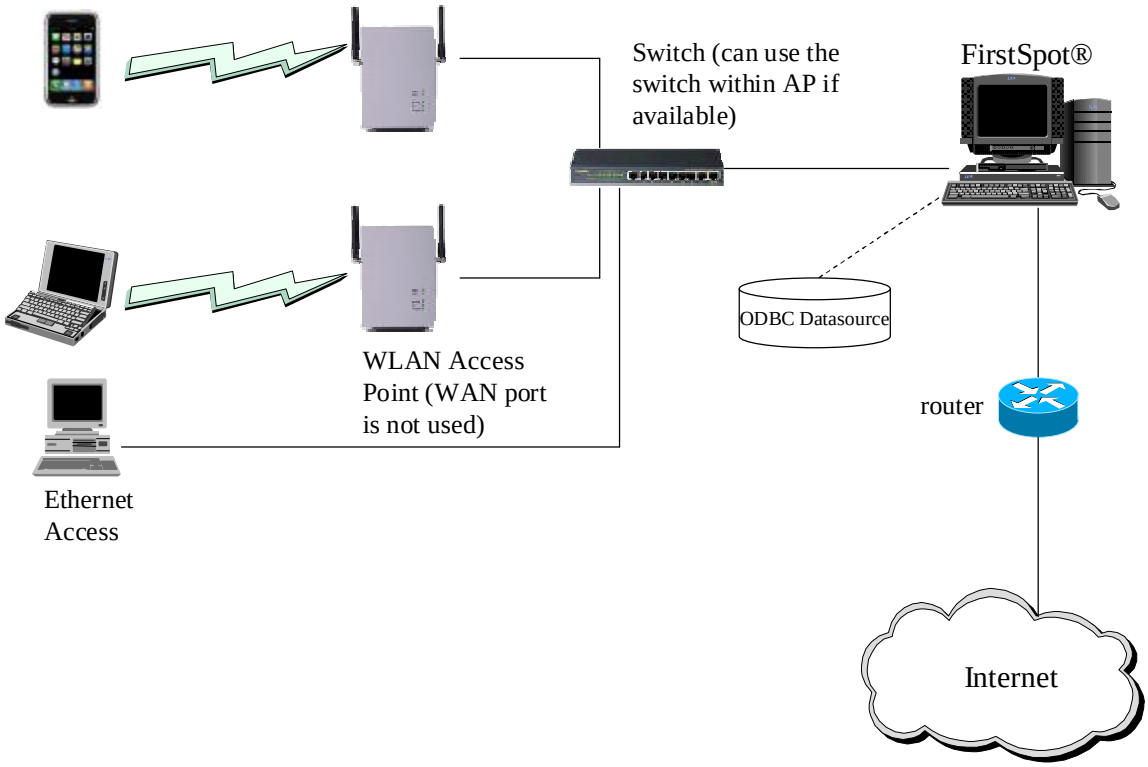
Reset data transfer counters of all users - reset the data transfer counters of all users to zero immediately.

4. Network Topologies of FirstSpot®

Scenario 1 (Simple Network Topology) - one network segment in the Hotspot

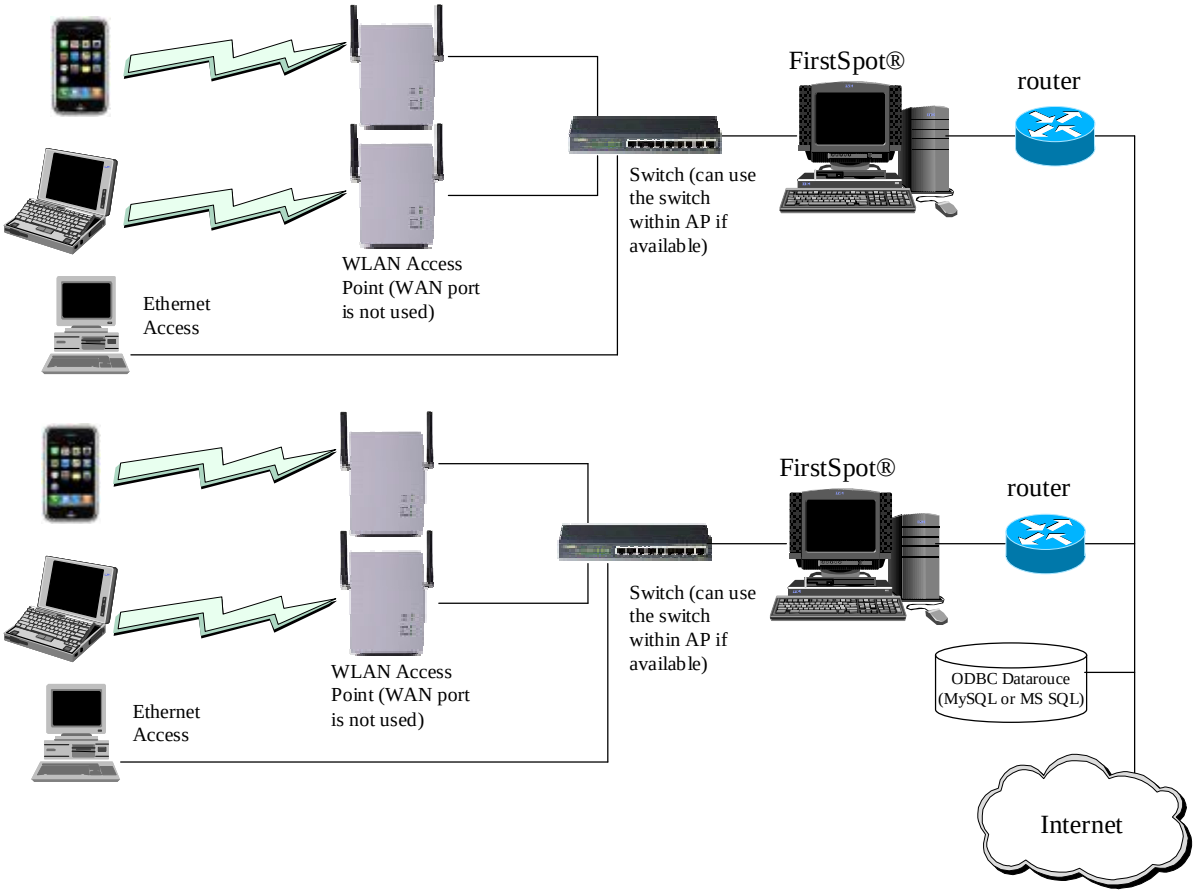
FirstSpot and the whole Wi-Fi Hotspot need to be on the same network segment. As there is only one network segment, MAC-based session handling should be used (see Session Handling parameter in the Configuration Manager).

FirstSpot can utilize either local or remote ODBC datasource. In this scenario, only one FirstSpot instance will connect to the ODBC datasource.



Scenario 2 (Distributed Network Topology) - multiple Hotspot sites with one FirstSpot per site

Starting from v6, several FirstSpot installations can share the same ODBC datasource. In this scenario, administrator needs to setup external MySQL or MS SQL Server datasource (refer to Chapter 8 : Using External Datasource as User Database for setup instructions). The MySQL or MS SQL can reside remotely (e.g. hosting). FirstSpot design guideline is that it will work with relative slow connection (200ms+ using "ping" test).



Several points about this scenario :

1. Please make sure "Enable Scenario 2" option is enabled under Authentication Server
2. Only MAC-based Session Handling will work (i.e. IP-based Session Handling is not supported)
3. Real IP Address Mapping will work. But note that if several FirstSpot servers are behind the same router (e.g. each floor of the building is using its own FirstSpot and they share the same ODBC datasource), make sure each FirstSpot has its own unique Real IP pool.
4. Multiple Network Segments, Failover/Load Balancing and Passive Login users will not work in this scenario.
5. The Status page within Configuration Manager will only show the users logged in the current FirstSpot
6. This scenario is available in both Standard and Advanced edition

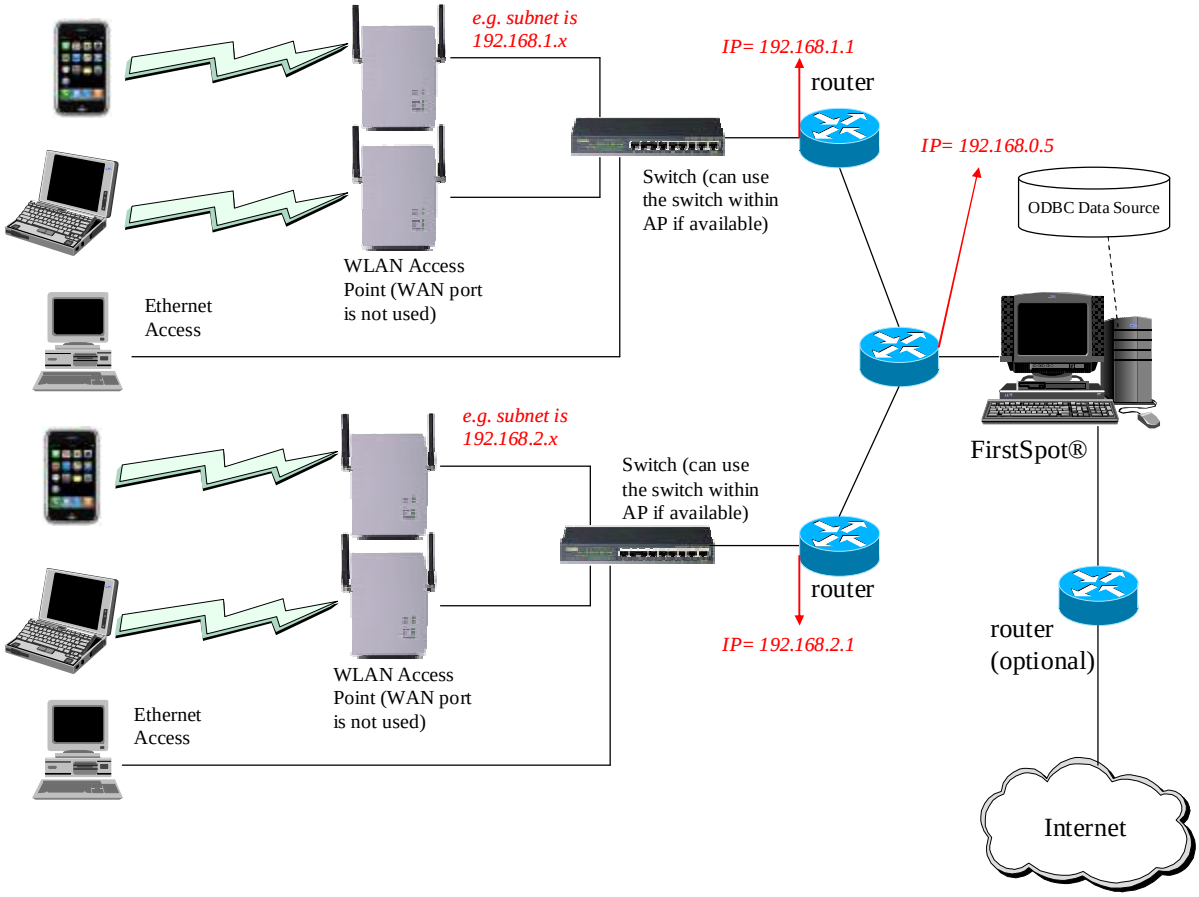
Scenario 3 (Centralized Network Topology) - multiple network segments with one centralized FirstSpot to serve all Hotspot sites

In this topology, there are routers between the Hotspots and FirstSpot. FirstSpot administrator needs to understand the followings:

1) Since the router makes the client PC's MAC address invisible from FirstSpot point of view, IP-based session handling must be used (see Session Handling parameter in the Configuration Manager for details). Also, you need to turn off NAT within your router, or otherwise it will hide the client PC's IP from FirstSpot point of view.
2) As IP-based session handling will be used, DHCP server must hand out the same IP address to a particular client device during one session to avoid client device being asked to re-authenticate. This is very important if you plan to use your own DHCP server (refer to DHCP parameter in the chapter "Parameters in the Configuration Manager" for details).
3) If you use FirstSpot DHCP Server, it will handle the above-mentioned session problem correctly. Keep in mind that you need to turn on "DHCP relay" in your routers. Also, note that FirstSpot only supports the router and DHCP relay belong to the same IP.
4) FirstSpot administrator needs to setup FirstSpot "Multiple Network Segments" section correctly. Using the example in the below diagram (see the red text), you need to add the following entries to the section:

Router IP	Subnet Mask	Gateway	Redirect File (TPL format)
192.168.1.1	255.255.255.0	192.168.0.5	(optional)
192.168.2.1	255.255.255.0	192.168.0.5	(optional)

** Assuming the Visitor Network Interface IP is 192.168.0.1 and subnet mask 255.255.255.0*



FirstSpot can utilize either local or remote ODBC datasource. In this scenario, only one FirstSpot instance will connect to the ODBC datasource.

5. Other Deployment Issues

Accounts creation (batch mode):
The easiest way is to write a SQL script to insert records into table “fsusr”. Note that you need to use the command line utility encrypt_pwd.exe to encrypt the password first before inserting into the table. Here are the field definitions:

Field	Definition	Example
user	username	testuser
pwd	encrypted password	a03af780c0f2959f26512a2cc8c2efb6
timeleft	access minutes (or air time) left for that particular account. This field can be used to enforce time limit for prepaid accounts. 0 represents no minutes left (i.e. cannot login). NULL represents there is no time limit for that particular account.	100
btul	Upload bandwidth throttling limit. 0 means there is no bandwidth throttling. NULL represents use global setting.	50
btdl	Download bandwidth throttling limit. 0 means there is no bandwidth throttling. NULL represents use global setting.	100
bwcount/bwcountUL/bwcountSha	0 means download/upload/total data transfer counting is disabled 1 means download/upload/total data transfer counting is enabled 2 means download/upload/total data transfer counting plus quota enforcement	1
bwquota/bwquotaUL/bwquotaSha	download/upload/total data transfer quota in KBytes (should only be specified if bwcount/bwcountUL/bwcountSha is 2)	10000 (~ 10MB)
startmod	NULL means Account is active “at the user's first login” 0 means Account is active “now” (must fill in sdate field) 1 means Account is active “at the user's first login” 2 means Account is active “at a specific date and time”	1
sdate	Account active time (should only be specified if startmod is 0 or 2)	Mon Nov 15 16:25:00 2004
bwrmethod	NULL means use data transfer counter global setting “disable” means FirstSpot will never reset data transfer counter “month” means FirstSpot will reset data transfer counter monthly “day” means FirstSpot will reset data transfer counter daily	disable

Field	Definition	Example
lastrbw	Last data transfer counter reset time (in ANSI C system format*)	1100150730
bwrperiod	For bwrmethod=month, reset every “bwrperiod” months For bwrmethod=day, reset every “bwrperiod” days	2
bwrdate	(For bwrmethod=month only) reset on day “bwrdate” of every “bwrperiod” month	7
status	NULL or 0 - account is enabled; 1 - account is disabled	NULL
edate	If “edate” is not NULL, FirstSpot will suspend this account at “edate”.	Mon Nov 15 16:25:00 2004
eminutes	A non-NULL value in this field represents the number of minutes (count from the time after the account has been activated) that this account is functional before it is being suspended, correspond to the “After x minutes” field in the UI)	120
logins	A non-NULL value in this field represents the number of logins which FirstSpot will allow before suspending this account	3
acl	Y - Apply IP Block List N or NULL - does not Apply IP Block List	Y
MACasUsr**	Y indicates this user uses MAC address as username (must put MAC in format xx-xx-xx-xx-xx-xx in username field) N or NULL means this user uses a normal username	Y
ReqSignUp***	Y indicates this user needs to fill in extra information form at the first login (only for administrator-created username) N or NULL means otherwise	Y
roption	NULL or 0 - recurring option is off, 1 - recurring option is on	1
rsdate	The start time of the recurring period (should only be specified if roption is 1)	09:00
redate	The end time of the recurring period (should only be specified if roption is 1)	17:00
weeksch	The day of the week which the account is active. It is stored using 7 binary digits with Sunday being the first digit. E.g. for active on Sun and Sat, the value is 65 (Hex:1000001) (should only be specified if roption is 1)	65
resetopt	0 - means the username is not a restricted account, 1 - means the username is a restricted account	1
auto_del	NULL or 0 - auto delete is disabled, 1 - auto delete is enabled	1

Field	Definition	Example
macmap	0 - Bind to first login MAC address is not enabled, 1 - Bind to first login MAC address is enabled, 2 - login once - set as Passive Login after first login	1
loginmac	If Bind to first login MAC address is enabled, this field will store the MAC at a particular user is tied to. Note that FirstSpot will set the MAC address automatically when the user login the first time (provided that Bind to first login MAC address is enabled). In case you want to set the MAC manually (which is not necessary), you can use the PHP function mac_address_translate (found in common_functions.php)	5510477070592
ipmap	0 - Real IP address mapping is disabled, 1 - Real IP address mapping is enabled	1
acctype	Null or 0 - “single login” username/password, 1 - “single login” Scratch Code, 3 - Multiple Logins for username/password, 4 - Multiple Logins for Scratch Code, 5 - Multiple Logins users spawned by FirstSpot during login (don’t set this explicitly)	3
max_logins	Maximum login limit for multiple logins userename. NULL or 0 means unlimited	5
all “reserved” fields****	For FirstSpot internal use	

* The number of seconds elapsed since midnight (00:00:00), January 1, 1970, coordinated universal time (UTC), according to the system clock.

** If MACasUsr is Y and Password is blank, this is known as Passive Login (see Chapter 1 : Terminologies). If you create or change a Passive Login user when FirstSpot is started, you need to run QueryPassiveLogin.exe to update FirstSpot.

*** signuptime - store the time when the user clicks submit button in Account Sign Up Form (for self sign-up) or Free Access Request Form (for Free Access)

signupmac - store the MAC of user that completes the Extra Information Form
signup01-10 - store the answer from user when the user completes the Extra Information Form

**** reserved1 field - A non-null value in this field indicates the user is logged on. This field for FirstSpot internal use.

The Shared Secret information is stored in the table “fssecret”. Below are the field definitions:

Field	Definition	Example
groupname	the unique identifier for the Shared Secret	Room1
secret	the actual Shared Secret itself	!secret1234
btul, btdl	Bandwidth throttling parameters. Refer to the definition for table fsusr in the previous section for details.	
bwcount, bwquota, bwcountUL, bwquotaUL, bwcountSha, bwquotaSha bwrmethod, lastrbw, bwrperiod, bwrdate	Bandwidth counting and quota parameters. The definition here is similar to the definition for table fsur. Note that data transfer for Shared Secret scenario includes the total data transfer for all users that connect using this particular Shared Secret	
all “reserved” fields	For FirstSpot internal use	

Session Logging:
To view the session information of users (e.g. for billing and tracking), make sure you turn on “Enable user session logging” parameter. You can then view the table fsusrlog (default table name) for the all the user session information. Each session (a session is terminated when the user logout, forced to timeout or FirstSpot is shut down) will have one record in the table.

Exception Free Website:
FirstSpot administrator can define a list of web sites that users do not require login. When user accesses those web sites, he can access the sites directly without seeing the login page. You can specify the list of exception free websites in the Configuration Manager. You can also define the list of exception free websites in the files *AllowedHostsIps.txt* (for specifying in IP format) and *AllowedHostsKeywords.txt* (for specifying in host keywords format) if you want to manipulate the list in batch mode. Keep in mind that you should not change the list in both Configuration Manager and *AllowedHostsIps.txt/AllowedHostsKeywords.txt* simultaneously to avoid confusing FirstSpot. Also, you need to restart FirstSpot after making those changes. The advantage of specifying host (i.e. domain name) keywords format is that it allows you to specifying all the sub-domains for a particular domain. It is very difficult to get all the IP addresses of all the sub-domains. For example, if you want the user to freely access all Yahoo web sites (i.e. www.yahoo.com, uk.yahoo.com, hk.yahoo.com …), instead of building a list of IP addresses of all yahoo web sites (which is difficult if not impossible), just put in “yahoo.com” as allowed hosts keywords (i.e. Exception Free Domain Names).

Login (and other end-users) Pages Customization:
Note that you can change the text or picture under Configuration Manager -> UI Customization. For deeper customization, you can customize the login page files directly (see below).

Starting from FirstSpot v6, FirstSpot will use Smarty template engine for the end-users page (e.g. login page). Smarty is a PHP based web template system, which separate presentation (resides in .tpl file under FirstSpot\authserv\template directory) and logic (resides in .php files). Users are highly recommended to perform their own layout customization within tpl files and keep the PHP files unchanged. FirstSpot setup won't replace the tpl during the upgrade process (e.g. v6.0.x -> v6.0.x) to ensure that your customization is not overridden. Note that if you customize any php files, your changes might get overridden during upgrade if there is change (e.g. bug fix) for that php files. So you need to reapply your customization after the upgrade. For more information about Smarty, please refer to http://www.smarty.net.

When Anonymous mode is selected, login_select.php will redirect users to alogin_form.php. Otherwise, login_form.php will be brought up. Both login_form.php and alogin_form.php link to their corresponding template files login_form_body.tpl and alogin_form_body.tpl and obtain the layout content. Therefore, to change the look and feel of the login page, login_form_body.tpl or alogin_form_body.tpl is the file to start with.

Content in the template files purely controls the layout, which is free for modification. Therefore, it is very safe to play it with any HTML page editor without risking to mess up the login logic.

login_form_body.tpl
Essentially, apart from the cosmetic design, this file provides login_form.php with HTML layout content to post a form with the following information to the fs_login.php script which handles the authentication logic:

The following shows a simple example of HTML codes which can act as the username/password mode login page:

```
<html>
<body>
    <form name="loginForm" method="post">
        Username:
        <input type="input" name="username" value="">
        Password:
        <input type="password" name="password" value="">
        <input type="hidden" name="ok_url" value="redirect.php">
        <input type="hidden" name="cart_url" value="cart.php">
        <input type="hidden" name="fail_url" value="login_form.php">
```

```
        <input type="submit" value="login">
    </form>
</body>
</html>
```

The following shows a simple example of HTML codes which can act as the Scratch Code mode login page:

```
<html>
<body>
    <form name="loginForm" method="post">
        Scratch Code:
        <input type="input" name="username" value="">
        <input type="hidden" name="ok_url" value="redirect.php">
        <input type="hidden" name="cart_url" value="cart.php">
        <input type="hidden" name="fail_url" value="login_form.php">
        <input type="submit" value="login">
    </form>
</body>
</html>
```

The following shows a simple example of HTML codes which can act as the “Both Username/Password and Scratch Code together” mode login page:

```
<html>
<body>
    <form name="loginForm" method="post">
        Username:
        <input type="input" name="username" value="">
        Password:
        <input type="password" name="password" value="">
        <input type="hidden" name="ok_url" value="redirect.php">
        <input type="hidden" name="cart_url" value="cart.php">
        <input type="hidden" name="fail_url" value="login_form.php">
        <input type="submit" value="login">
    </form>
    <form name="loginForm" method="post">
        Scratch Code:
        <input type="input" name="username" value="">
        <input type="hidden" name="ok_url" value="redirect.php">
        <input type="hidden" name="cart_url" value="cart.php">
        <input type="hidden" name="fail_url" value="login_form.php">
        <input type="hidden" name="scratchCodeLogin" value="true">
        <input type="submit" value="login">
    </form>
</body>
</html>
```

alogin_form_body.tpl

You simply have to create an HTML form with a submit button and a hidden field. Then, alogin_form.php will post it to the fs_login.php script:

The following shows a simple example of HTML codes which can act as the Anonymous Option login page:

```
<html>
<body>
    <form name="loginForm" method="post">
        <input type="submit" value="login" name="anonymous_mode_button">
        <input type="hidden" name="ok_url" value="redirect.php">
        <input type="hidden" name="cart_url" value="alogin_form.php">
        <input type="hidden" name="fail_url" value="alogin_form.php">
    </form>
</body>
</html>
```

The following shows a simple example of HTML codes which can act as the Anonymous Option with Shared Secret (multiple logins) login page:

```
<html>
<body>
    <form name="loginForm" method="post">
        Shared Secret:
        <input type="password" name="secret_code" value="">
        <input type="submit" value="login" name="anonymous_mode_button">
        <input type="hidden" name="ok_url" value="redirect.php">
        <input type="hidden" name="cart_url" value="alogin_form.php">
        <input type="hidden" name="fail_url" value="alogin_form.php">
    </form>
</body>
</html>
```

Other points to note:

Shown below is the list of PHP files of those commonly used pages and their corresponding template files:

PHP File	Description	HTML Template File
login_form.php	Login page	login_form_body.tpl (PC and tablet), ip_login_form_body.tpl (smartphone)
alogin_form.php	Anonymous user login page	alogin_form_body.tpl
cart.php	Shopping cart	cart_body.tpl
chgpwd_form.php	Change password page	chgpwd_form_body.tpl
info.php	Infobox	info_body_normal.tpl
paypal_history.php	Instant payment history	paypal_history_body.tpl
signup_form.php	Self sign-up page	signup_form_body.tpl

In general, content in the template files (.tpl) is free for modification. However, some of the HTML codes need to be generated dynamically from the PHP files through the template engine. Those areas are marked with special tags (starting with “{%” and ending with “%}”) in the current template files. Users should pay attention whether they really require to modify or to delete those tags during their customization.

If users want to change the name of the template files, they also need to modify the .tpl filenames in the corresponding PHP files.

E.g.: If the new template file “new_login_form_body.tpl” is used instead of the existing “login_form_body.tpl”, search in login_form.php and replace the line

```
$smarty->display('login_form_body.tpl');
```

with

```
$smarty->display('new_login_form_body.tpl');
```

Upgrade/Migration issues:

FirstSpot can perform upgrade automatically if only the third digit of the version number has increased (e.g. v8.0.0 to v8.0.7). Note that FirstSpot will backup the files that needed to be upgraded before replacing them. If you have customized your original files (e.g. PHP files), you need to apply your customization again manually.

For case that needs to upgrade manually (i.e. v6 to v8, v7 to v8, v7.0.0 to v7.1.0) or migrate FirstSpot to another machine, you need perform the following steps:

1) export the relevant FirstSpot information (see below)
2) uninstall FirstSpot
3) install the new version of FirstSpot or install FirstSpot in another machine
4) import relevant FirstSpot information

There are several pieces of FirstSpot information that administrator may want to transfer:

1) user information - this includes username/password, Plan definition. You can export the table (i.e. fsusr, fsplan) in the Users tab within Configuration Manager.
2) FirstSpot configuration settings - you can take advantage of fsset.exe (a command line based FirstSpot Setting Export/Import Utility). The command "fsset export" will generate a file named "BackupConfig". You need to copy the file "BackupConfig" to the target dispatcher subdirectory before you run "fsset import". Note that fsset.exe will skip the following parameters and you need to deal with them manually:

- Authentication Server : File DSN location (.dsn file), Path & filename for password offloading
- DHCP : Static DHCP listing file location
- [misc] section of the config.ini file : _debug, _allow_private_disconnect, _allow_public_disconnect, _skip_nic_disable_enable

3) License file (license.key) - note the FirstSpot uninstall will delete the FirstSpot directory, so you might want to backup the license.key file and transfer it to the appropriate place.
4) The custom_lang.php and custom_cmlang.php files if you change the default text
5) Optional - User log, Credit card transaction log (in table ppal). You can also export the information in the Users tab within Configuration Manager

SSL-enabled login pages:
FirstSpot supports SSL protection of authentication pages so that all information submitted by end-users can be encrypted using 128/256-bit encryption.

This SSL feature may cause security alert from web browsers due to the self-signed nature of the SSL certificates generated by FirstSpot itself, instead of from a trusted agent/CA. However, you can purchase your own if you really want to eliminate that warning. That is a common challenge to those solutions where the SSL protection is on the visitor-side. More and more end-users are getting used to this warning though.

To use a SSL Certificate from a Trusted CA in FirstSpot to Protect the Login Pages, generally the steps are:
- generate a private key for the SSL certificate from the FirstSpot machine;
- generate a CSR (Certificate Signing Request) using that private key;
- send the CSR to your trusted CA for approval;
- receive the SSL cert from the CA and copy it to the FirstSpot machine;

Technically, here're the steps:
1. On the FirstSpot machine, open a command prompt

2. change directory to FirstSpot\www\Apache\bin directory

3. run this command:
openssl genrsa -out ..\conf\my-server.key 1024 (for 128 bit encryption)

or

openssl genrsa -out ..\conf\my-server.key 2048 (for 256 bit encryption)

which creates the private key (my-server.key) of 1024/2048 bits for the SSL cert, please back up this file; you need this to run SSL session in the future

4. run the following command:
openssl req -new -key ..\conf\my-server.key -out ..\conf\my-server.csr -config ..\conf\openssl.cnf

You will then be prompted to enter values for the distinguished name of the cert. The most important one is the value of Common Name, you should put in exactly the domain name (default : firstspot.org) you're planning to use for the *visitor* network interface of FirstSpot. If you're asked to provide values for 'extra' attributes, simply press the Enter key will do.

The command will generate a file called my-server.csr. When you purchase a SSL cert from a trusted CA, they will ask you to supply a CSR. What you need to do is simply open the my-server.csr file using a text editor and copy-and-paste the content inside onto their online form.

5. When the trusted CA send you the SSL cert of your server, please rename the cert to my-server.cert and copy it to the FirstSpot\www\Apache\conf directory

6. The trusted CA will also provide you the public cert of their own root CA; please rename that cert to ca.crt and copy it to the FirstSpot\www\Apache\conf directory as well

7. You will need these 3 files under the FirstSpot\www\Apache\conf directory:
my-server.key, my-server.cert, ca.crt

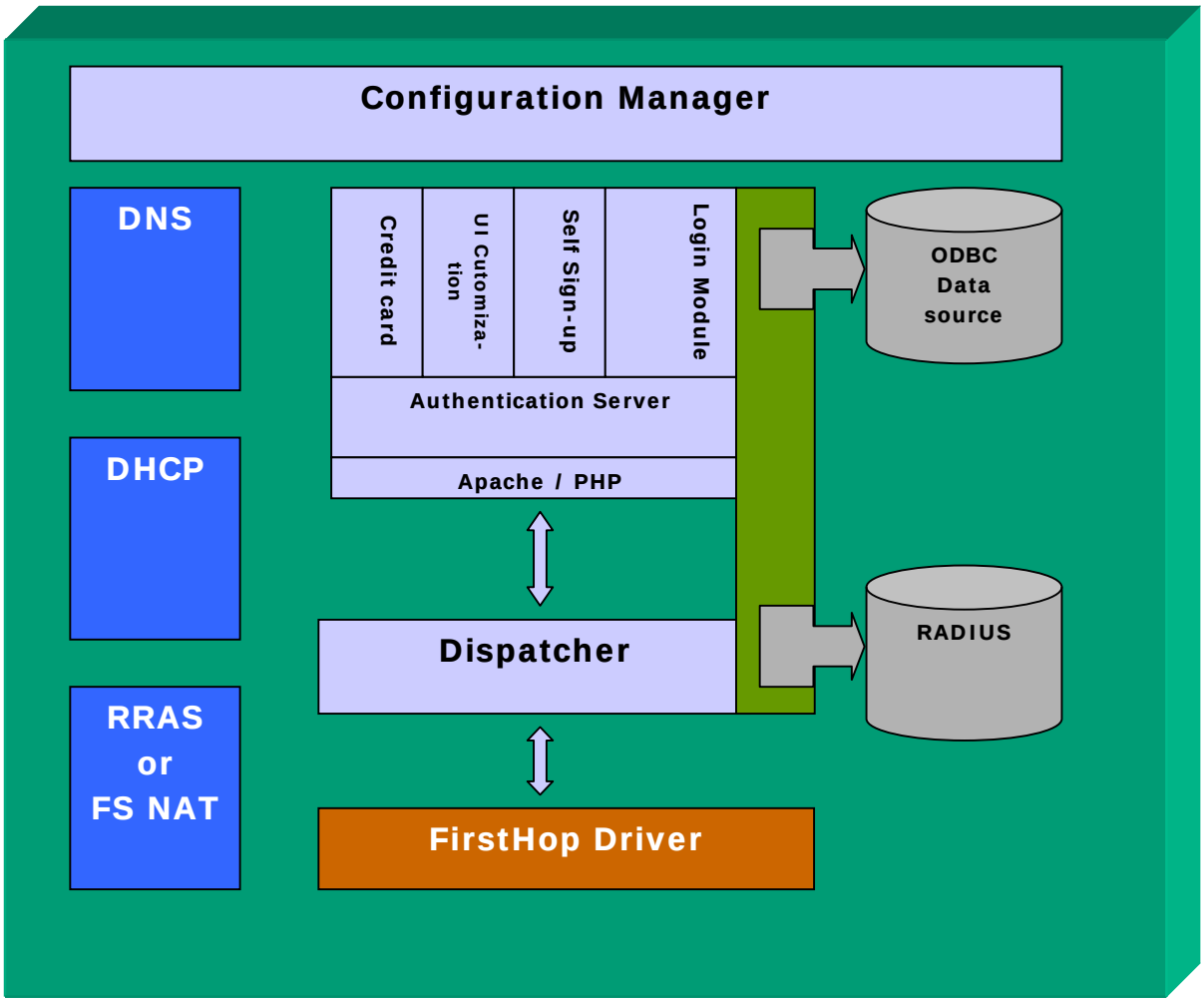
Please remember to back up these 3 files for future recovery purposes

8. After you have all the cert and key files in place, you can then go to Configuration Manager. Under the “Authentication Server” tab, enable both the "SSL-enable authentication pages" and "Use 3rd party SSL Certificate" and click Save. Please also make sure the domain name for your **FirstSpot login page URL (under Configuration Manger -> Authentication Server -> Show IP or domain name in login page URL)** matches the one issued to the SSL cert you obtained. With the "Use 3rd party SSL Certificate" option enabled, FirstSpot will not generate or use its self-signed SSL certificates.

9. Restart FirstSpot and try to login from a client machine, your browser should show the authentication pages encrypted with a trusted SSL cert.

10. If you have encounter problem in the Apache server, you might want to switch your cert to SHA-1 hash function and try again.

6. FirstSpot® Architecture



7. Credit Card Support

WHAT ARE CREDIT CARD MODULES IN FirstSpot?

Credit card modules in FirstSpot provide the bridge between an online credit card payment gateway and the corresponding update of FirstSpot user database to reflect the correct account status for users purchasing hotspot services online.

Currently FirstSpot supports the following credit card modules – PayPal Website Payments Standard, PayPal Website Payments Pro Direct Payment, Authorize.Net and Interswitch WebPAY.

Please note that, FirstSpot does not support “recurring payment” for PayPal Website Payments Pro Direct Payment, Interswitch WebPAY and Authorize.Net currently.

NETWORK PREPARATION TO RECEIVE TRANSACTION DETAILS FROM A PAYMENT GATEWAY

In order for a payment gateway to post back transaction details to your FirstSpot server, your Internet Network Interface (or if you have a router between FirstSpot and the Internet, the WAN port of your router connecting to the Internet) must have a fixed “public-accessible” IP address or a Internet-resolvable hostname (e.g. subdomain.yourmain.com). If your ISP distributes dynamic IP address every time your FirstSpot connects to the Internet, you may consider using those dynamic DNS services available in the market (e.g. zoneedit.com, dyndns.com)

For PayPal Website Payment Standard and PayPal Website Payment Pro Direct Payment, FirstSpot listens at port 5789 (by default) for a payment gateway notification on credit card transaction status.

Authorize.Net mandates the use of port 80 for such credit card transaction status.

If you are using a broadband router or firewall to connect to the Internet, please remember to configure them to allow traffic coming through the corresponding port. In some devices, such setting is done through the so-called port forwarding feature.

CONFIGURING THE SHOPPING CART

Inside InfoBox, users can click on the “Buy more credit” button to access the shopping cart

page. Administrators can define shopping cart items under the Shopping Cart category inside Configuration Manager. A shopping item is essentially a pre-defined plan (under the category, Plans) with a description and price tag.

CONFIGURING THE PAYPAL WEBSITE PAYMENTS STANDARD MODULE

From the PayPal web site

Please make sure your PayPal account is capable of receiving credit card payment. Usually, this requires your account as a "verified" one. Please refer to PayPal for detailed instruction and requirements.

Please notice that the "Instant Payment Notification Preferences" on your PayPal account setting will be overridden by the "Publicly accessible URL to receive transaction update from PayPal" parameter (under "Credit Cards" -> "PayPal Payments Standard"). This URL will be sent to PayPal server during the process of credit card transaction for receiving notifications.

From the Configuration Manager (under the Credit Cards category)

PayPal ID – your account id (email address) registered in PayPal to receive credit card payments.

Success Return Path – the URL users can click on to proceed after a successful credit card entry.

Failure Return Path – the URL user can click on to proceed after a cancelled or failed credit card entry.

Treat Pending Transaction as Completed – apart from the "completed" payment status, one can be "pending". FirstSpot PayPal Plug-in, by default, will only credit the timeleft field for the "completed" status. Optionally, you can ask the Plug-in to credit a user when the reported status is "pending".

Base Currency – the base currency for credit card payments.

Publicly accessible URL to receive transaction update from PayPal – the URL location of FirstSpot server that PayPal is instructed to post back transaction details. The URL address must be an Internet-resolvable address (do not put any 192.168.x.y or 10.a.b.c address). An example of a valid entry is http://202.94.237.227:5789.

Transaction update module listening port - the port number that FirstSpot will listen for transaction update posted from PayPal.

Transaction history table name - the name of database table storing transaction history (change this only if you use an external database with a different table name from default).

CONFIGURING THE PAYPAL WEBSITE PAYMENTS PRO DIRECT PAYMENT MODULE

The Direct Payment module accepts credit cards directly on your site for paying access plans. The payment requests are sent to PayPal for verification. If the transaction is successful, a receipt with a message of success payment, the paid item and the transaction id will be shown to the user for reference.

Please make sure your PayPal account supports Website Payment Pro and "verified". An "API Credential" provided by PayPal is required for the Direct Payment Module to work. "API Credential" consists of a username and password with an "API signature" for identifying yourself to PayPal. Please refer to PayPal for instructions to get your own "API Credential".

For security concerns, the Direct Payment web pages are compulsively SSL-enabled. Please refer to "SSL-enabled login pages" under Chapter 5 ("Other Deployment Issues") for more information about SSL-enabled pages and SSL certificates. Please notice that the SSL certificate for direct payment module will share the setting with the "Use 3rd-party SSL certificates" parameter (Under "Authentication server").

From the Configuration Manager (under the Credit Cards category)

PayPal API username - the username of your own PayPal API credential.

PayPal API password - the password of your own PayPal API credential.

PayPal API signature - the signature of your own PayPal API credential.

For other parameters, please refer to the previous section "CONFIGURING THE PAYPAL WEBSITE PAYMENTS STANDARD MODULE".

CONFIGURING THE AUTHORIZE.NET MODULE

From the Configuration Manager (under the Credit Cards category)

Login ID - the merchant ID in Authorize.Net

Success return path - the URL users can click on to proceed after a successful credit card entry.

Failure return path - the URL users can click on to proceed after a cancelled or failed credit card entry.

Transaction Key - given by Authorize.Net. Please obtain it from Authorize.Net's Merchant Interface (under *Settings and Profile* >> *Security* >> *Obtain Transaction Key).*

MD5 Hash - this is an added security provided by Authorize.Net to minimize the chance of spoofed incoming credit card transaction update. Different from Transaction Key, you will have to generate this value in Authorize.Net's Merchant Interface yourself (under *Settings and Profile* >> *Security* >> *MD5 Hash) and then tell* FirstSpot the same value in this field.

Base Currency - the base currency for credit card payments

Publicly accessible URL to receive transaction update from Authorize.Net - the URL location of FirstSpot server that Authorize.Net is instructed to post back transaction details. The URL address must be an Internet-resolvable address (do not put any 102.168.x.y or 10.a.b.c address). A sample valid entry is http://202.94.237.227.

Authorize.Net requires the URL to be entered into their Merchant Interface as well (under *Settings and Profile* >> *Transaction Response* >> *Response/Receipt URLs). A sample valid entry is* http://202.94.237.227/authorizeNet_callback.php. Please note the suffix "authorizeNet_callback.php" is required as well.

Test mode - If you want to put your Authorize.Net account in Test Mode (i.e. without actual card processing), please enter **1** (one) in this field **AND** configure at Authorize.Net's Merchant Interface (under *Settings and Profile* >> *General* >> *Test Mode).*

Likewise, to turn off Test Mode, put **0** (zero) in this field **AND** go back to Authorizet.Net's Merchant Interface to revert the setting.

Transaction history table name – the name of the database table storing transaction history (change this only if you use an external database with a different table name from default)

REPORTING

From the Configuration Manager

Under the *Credit Cards* tab, clicking on the *Show Log* button will display information stored

in the transaction history.

Under the *Status* column, the possible values are:

Completed: a completed and successful payment status received from the payment gateway and FirstSpot has updated the corresponding user account accordingly

Pending: (for PayPal only) a pending payment status has been received from the payment gateway. Whether FirstSpot will update the user database depends on the setting “Treat Pending Transaction as Completed”.

Refunded: a refunded payment status has been received from payment gateway. Most often, this will only happen if you manually refund the transaction to the payer. Please note that FirstSpot *will not* deduct the minute from the user database in the case.

<empty>: no update from payment gateway about a particular transaction. Possible reasons: (i) Users didn’t completed the transaction; (ii) The payment gateway hasn’t posted back anything yet.

User-Level Log

In the shopping cart page, users can check their recent payment history.

Transaction History Log

Apart from the Configuration Manager, a log is also provided under the FirstSpot\log directory, called *txn.log*. It will be created the first time FirstSpot receives a posting from a particular payment gateway. Note that if this file is not created, this means the payment gateway traffic doesn’t go through at all. You should check your firewall (e.g. port forwarding) or payment gateway setup.

From the Web Site of the Payment Gateway

For accounting purpose, the most accurate transaction history and log is available at the corresponding payment gateway’s web site.

TESTING AND TROUBLESHOOTING

Testing PayPal Website Payments Standard

1. There is a testing and development platform called "Sandbox" at https://developer.paypal.com/
2. You need to need to create test accounts before testing. To use the PayPal sandbox account for testing , select “Use PayPal sandbox for testing” under Configuration Manager -> Credit Cards

Testing PayPal Website Payments Pro Direct Payment

1. There is a testing and development platform called "Sandbox" at https://developer.paypal.com/
2. You need to create test accounts before testing and changing the PayPal URL in the PHP files.

    i. Open "ppal_ipn.php" which is located in FirstSpot\local directory
    ii. Search for “$url="www.paypal.com";”
    iii. You should see code as shown below:

    ```
    include_once '..\\authserv\\common_functions.php';
    include_once "transaction.php";
    $url="www.paypal.com";
    ```

    iv. Change the value of $url, replace

    ```
    $url="www.paypal.com";
    ```

    with

    ```
    $url="www.sandbox.paypal.com";
    ```

    v. Open “caller_service.php” which is located in FirstSpot\ppal_pro directory
    vi. Search for “$API_Endpoint ="https://api-3t.paypal.com/nvp";”
    vii. You should see code as shown below:

    ```
    $API_Endpoint ="https://api-3t.paypal.com/nvp";
    ```

    viii. Change the value of $API_Endpoint, replace

    ```
    $API_Endpoint ="https://api-3t.paypal.com/nvp";
    ```

    with

    ```
    $API_Endpoint ='https://api-3t.sandbox.paypal.com/nvp';
    ```

3. Choose PayPal “Website Payments Pro Direct Payment” as your payment gateway.
4. Obtain your API credential from the PayPal Sandbox and change the API username, API

password and API signature in the configuration manager.
5. Save the settings and restart FirstSpot.
6. Use the test credit card information obtained from PayPal sandbox for testing.

Testing Authorize.Net

Authorize.Net provides a test mode for merchants to verify integration with their gateway. To turn on or off test mode, please remember to configure in BOTH FirstSpot's Configuration Manager AND Authorize.Net's Merchant Interface.

Troubleshooting

If a distorted status change happens to the transaction history, please check the following:

The corresponding credit card transaction log file txn.log under the *FirstSpot\log* directory. FirstSpot will write all incoming notifications into the file.

If no entry is found, please open the *FirstSpot\www\Apache\logs\access.log* file and check if any entry of the payment gateway's IP address with the latest time stamp exists. If a relevant entry is found while nothing is written to the credit card transaction log file, please report this to our support team.

If there is no relevant entry found in the access.log, the most probable reason would be a wrong publicly accessible URL has been defined in Configuration Manager, which causes the payment gateway not being able to post to the right host or port. Please contact your ISP or configure your broadband router appropriately if needed.

It may also be possible the payment gateway has delay in notifications. Notifications should normally come in within a few minutes.

8. Using External Datasource as User Database

Creating Tables

First, create all necessary tables under your MySQL or Microsoft SQL Server database using the below SQL statements:

```
create table fsusr
(
name varchar(80),
pwd varchar(40),
timeleft integer,
btul integer,
btdl integer,
reserved1 varchar(40),
reserved2 integer,
reserved3 integer,
reserved4 integer,
reserved5 numeric(10),
reserved12 integer,
reserved13 integer,
reserved14 integer,
reserved17 integer,
accumbw numeric,
bwquota numeric,
bwcount integer,
accumbwUL numeric,
bwquotaUL numeric,
bwcountUL integer,
accumbwSha numeric,
bwquotaSha numeric,
bwcountSha integer,
status integer,
attempt integer,
startmod integer,
edate varchar(40),
sdate varchar(40),
logins integer,
eminutes integer,
auto_del integer,
bwrmethod varchar(10),
bwrperiod integer,
lastrbw integer,
bwrdate integer,
anonymous varchar(1),
```

```
MACasUsr varchar(1),
groupname varchar(40),
pagenum integer,
ReqSignUp varchar(1),
acl varchar(1),
signuptime integer,
signupmac varchar(40),
signup01 varchar(40),
signup02 varchar(40),
signup03 varchar(40),
signup04 varchar(40),
signup05 varchar(40),
signup06 varchar(40),
signup07 varchar(40),
signup08 varchar(40),
signup09 varchar(40),
signup10 varchar(40),
roption integer,
rsdate varchar(40),
redate varchar(40),
weeksch integer,
resetopt integer,
macmap integer,
loginmac varchar(40),
ipmap integer,
siteID varchar(40),
iBMsg_glo varchar(40),
iBMsg_per varchar(40),
loginseg integer,
emonth integer,
eyear integer,
portflt varchar(40),
faflag integer,
faregtime varchar(40),
acctype integer,
used varchar(1),
max_logins integer,
signupseg integer,
spare01 integer,
login_cpw varchar(4),
emailVer varchar(40),
socialnet integer,
socialname varchar(40),
socialdesc varchar(40),
primary key (name)
);

create table fsusrlog
```

```
(
name varchar(80),
logintime varchar(40),
logouttime varchar(40),
duration integer,
ipormac varchar(40),
reserved10 integer,
reserved11 integer,
bwusage numeric,
bwusageUL numeric,
bwusageSha numeric,
siteID varchar(40)
);

create table fsplans
(
pname varchar(40),
timeleft integer,
btul integer,
btdl integer,
bwquota numeric,
bwcount integer,
bwquotaUL numeric,
bwcountUL integer,
bwquotaSha numeric,
bwcountSha integer,
status integer,
startmod integer,
edate varchar(40),
sdate varchar(40),
logins integer,
eminutes integer,
auto_del integer,
bwrmethod varchar(10),
bwrperiod integer,
bwrdate integer,
ReqSignUp varchar(1),
pagenum integer,
acl varchar(1),
roption integer,
rsdate varchar(40),
redate varchar(40),
weeksch integer,
resetopt integer,
macmap integer,
ipmap integer,
loginseg integer,
emonth integer,
```

```
eyear integer,
portflt varchar(40),
faflag integer,
faregtime varchar(40),
acctype integer,
max_logins integer,
login_cpw varchar(4),
primary key (pname)
);

create table ppal
(
invoice numeric,
username varchar(127),
item_name varchar(127),
amount varchar(127),
planname varchar(254),
quantity varchar(127),
order_date numeric,
curr varchar(127),
pay_status varchar(127),
pendreason varchar(127),
pay_date varchar(127),
txn_id varchar(17),
pay_type varchar(127),
first_name varchar(127),
last_name varchar(127),
payeremail varchar(127),
payer_id varchar(127),
txn_type varchar(127),
subscrdate varchar(127),
subscr_id varchar(127),
method varchar(50),
timeleft integer,
btul integer,
btdl integer,
bwquota numeric,
bwcount integer,
bwquotaUL numeric,
bwcountUL integer,
bwquotaSha numeric,
bwcountSha integer,
sdate varchar(40),
edate varchar(40),
logins integer,
eminutes integer,
status integer,
startmod integer,
```

```
auto_del integer,
bwrmethod varchar(10),
bwrperiod integer,
lastrbw integer,
bwrdate integer,
pagenum integer,
useMethod integer,
emonth integer,
eyear integer,
topup integer,
primary key (invoice)
);

create table aExLog
(
aExMAC varchar(40),
SignUpTime varchar(40),
aEx01 varchar(40),
aEx02 varchar(40),
aEx03 varchar(40),
aEx04 varchar(40),
aEx05 varchar(40),
aEx06 varchar(40),
aEx07 varchar(40),
aEx08 varchar(40),
aEx09 varchar(40),
aEx10 varchar(40)
);

create table fssecret
(
groupname varchar(40),
secret varchar(40),
btul integer,
btdl integer,
bwcount integer,
accumbw numeric(20),
bwquota numeric(20),
reserved15 numeric(20),
bwcountUL integer,
accumbwUL numeric(20),
bwquotaUL numeric(20),
reserved16 numeric(20),
bwcountSha integer,
accumbwSha numeric(20),
bwquotaSha numeric(20),
reserved18 numeric(20),
bwrmethod varchar(10),
```

```
bwrperiod integer,
lastrbw integer,
bwrdate integer,
sdate varchar(40),
primary key (groupname),
CONSTRAINT SecretUniqueKey UNIQUE (secret)
);

create table ibmsg
(
ibmsgID integer,
ibmsgType integer,
ibmsgTime integer,
conRefID integer,
name varchar(80),
reserved1 varchar(40),
siteID varchar(40),
CONSTRAINT IBMsgKey UNIQUE (ibmsgID, ibmsgType, ibmsgTime)
);

create table fssninfo
(
name varchar(80),
type integer,
data varchar(254),
lastupd varchar(40),
primary key(name, type)
);

create table fssnityp
(
type integer,
typename varchar(254),
sntype integer,
primary key(type, sntype)
);

insert into fsusr (name, pwd, timeleft) values ('alice', 'a03af780c0f2959f26512a2cc8c2efb6',
100);
insert into fsusr (name, pwd, btul, btdl, bwquota, bwcount, bwquotaul, bwcountul,
bwrmethod, bwrperiod, bwrdate) values ('bruce', 'a03af780c0f2959f26512a2cc8c2efb6', 50,
100, 51200, 2, 51200, 2, 'month', 1, 1);
insert into fsusr (name, pwd, btul, btdl, bwcount, bwcountul, bwquotasha, bwcountsha,
eminutes, bwrmethod, bwrperiod, bwrdate) values ('cat',
'a03af780c0f2959f26512a2cc8c2efb6', 0, 0, 0, 0, 102400, 2, 1440, 'month', 1, 1);
insert into fsusr (name, pwd, bwcount, bwcountul, bwrmethod, bwrperiod, bwrdate) values
('sample', 'a03af780c0f2959f26512a2cc8c2efb6', 1, 1, 'month', 1, 1);
```

insert into fsusr (name, pwd, acctype, used, timeleft) values ('1924888929', '7a848454627ccf6a677633725586fd16', 1, 0, 100);
insert into fsusr (name, pwd, acctype, used, timeleft) values ('2665981624', '5f6cd28ccdefd76c04d3e4c974464704', 1, 0, 100);
insert into fsusr (name, pwd, acctype, used, timeleft) values ('3498111328', 'b3ac256d77909bce52e7e3b05a36ace9', 1, 0, 100);
insert into fsusr (name, pwd, acctype, used, timeleft) values ('4284561667', '306d5c51858db84ae152668b84b6c623', 1, 0, 100);
insert into fsusr (name, pwd, acctype, used, timeleft) values ('5956998923', 'f56396b08a5e0f50c6f483d99a7ac900', 1, 0, 100);

insert into fsplans (pname, bwcount, bwcountul, status, startmod) values ('Social Network Plan', 1, 1, 0, 1);
insert into fsplans (pname, timeleft, bwquota, bwcount, bwquotaul, bwcountul, status, startmod) values ('Plan A', 1440, 51200, 2, 51200, 2, 0, 1);
insert into fsplans (pname, bwquotasha, bwcountsha, status, startmod, eminutes) values ('Plan B', 102400, 2, 0, 1, 1440);
insert into fsplans (pname, bwcount, bwcountul, bwcountsha, status, startmod, eminutes, auto_del, roption, weeksch, resetopt, macmap, ipmap, faflag) values ('Free Access Plan', 0, 0, 1, 0, 1, 30, 0, 0, 0, 0, 0, 0, 1);
insert into fsplans (pname, bwcount, bwcountul, bwcountsha, status, startmod, edate, auto_del, roption, weeksch, resetopt, macmap, ipmap) values ('Self Sign-up for After X Minutes', 1, 1, 0, 0, 1, 'Sat Jan 01 00:00:00 2000', 0, 0, 0, 0, 0, 0);
insert into fsplans (pname, timeleft, bwcount, bwcountul, bwcountsha, status, startmod, auto_del, roption, weeksch, resetopt, macmap, ipmap) values ('Self Sign-up for Access Minutes', 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0);
insert into fsplans (pname, bwquotasha, bwcount, bwcountul, bwcountsha, status, startmod, auto_del, roption, weeksch, resetopt, macmap, ipmap) values ('Self Sign-up for Total Quota', 0, 0, 0, 2, 0, 1, 0, 0, 0, 0, 0, 0);

insert into fssnityp (type, typename, sntype) values (0, 'email', 1);
insert into fssnityp (type, typename, sntype) values (1, 'first_name', 1);
insert into fssnityp (type, typename, sntype) values (2, 'last_name', 1);
insert into fssnityp (type, typename, sntype) values (3, 'gender', 1);
insert into fssnityp (type, typename, sntype) values (4, 'link', 1);
insert into fssnityp (type, typename, sntype) values (5, 'locale', 1);
insert into fssnityp (type, typename, sntype) values (6, 'timezone', 1);
insert into fssnityp (type, typename, sntype) values (7, 'updated_time', 1);
insert into fssnityp (type, typename, sntype) values (8, 'verified', 1);

insert into fssnityp (type, typename, sntype) values (0, 'id', 2);
insert into fssnityp (type, typename, sntype) values (1, 'username', 2);
insert into fssnityp (type, typename, sntype) values (2, 'full_name', 2);
insert into fssnityp (type, typename, sntype) values (3, 'profile_picture', 2);
insert into fssnityp (type, typename, sntype) values (4, 'bio', 2);
insert into fssnityp (type, typename, sntype) values (5, 'website', 2);

insert into fssnityp (type, typename, sntype) values (0, 'id', 4);

```
insert into fssnityp (type, typename, sntype) values (1, 'class', 4);
insert into fssnityp (type, typename, sntype) values (2, 'screen_name', 4);
insert into fssnityp (type, typename, sntype) values (3, 'name', 4);
insert into fssnityp (type, typename, sntype) values (4, 'province', 4);
insert into fssnityp (type, typename, sntype) values (5, 'city', 4);
insert into fssnityp (type, typename, sntype) values (6, 'location', 4);
insert into fssnityp (type, typename, sntype) values (7, 'description', 4);
insert into fssnityp (type, typename, sntype) values (8, 'url', 4);
insert into fssnityp (type, typename, sntype) values (9, 'profile_image_url', 4);
insert into fssnityp (type, typename, sntype) values (10, 'profile_url', 4);
insert into fssnityp (type, typename, sntype) values (11, 'domain', 4);
insert into fssnityp (type, typename, sntype) values (12, 'weihao', 4);
insert into fssnityp (type, typename, sntype) values (13, 'gender', 4);
insert into fssnityp (type, typename, sntype) values (14, 'followers_count', 4);
insert into fssnityp (type, typename, sntype) values (15, 'friends_count', 4);
insert into fssnityp (type, typename, sntype) values (16, 'pagefriends_count', 4);
insert into fssnityp (type, typename, sntype) values (17, 'statuses_count', 4);
insert into fssnityp (type, typename, sntype) values (18, 'favourites_count', 4);
insert into fssnityp (type, typename, sntype) values (19, 'created_at', 4);
insert into fssnityp (type, typename, sntype) values (20, 'following', 4);
insert into fssnityp (type, typename, sntype) values (21, 'allow_all_act_msg', 4);
insert into fssnityp (type, typename, sntype) values (22, 'geo_enabled', 4);
insert into fssnityp (type, typename, sntype) values (23, 'verified', 4);
insert into fssnityp (type, typename, sntype) values (24, 'remark', 4);
insert into fssnityp (type, typename, sntype) values (25, 'ptype', 4);
insert into fssnityp (type, typename, sntype) values (26, 'allow_all_comment', 4);
insert into fssnityp (type, typename, sntype) values (27, 'avatar_large', 4);
insert into fssnityp (type, typename, sntype) values (28, 'avatar_hd', 4);
insert into fssnityp (type, typename, sntype) values (29, 'follow_me', 4);
insert into fssnityp (type, typename, sntype) values (30, 'online_status', 4);
insert into fssnityp (type, typename, sntype) values (31, 'bi_followers_count', 4);
insert into fssnityp (type, typename, sntype) values (32, 'lang', 4);
insert into fssnityp (type, typename, sntype) values (33, 'star', 4);
insert into fssnityp (type, typename, sntype) values (34, 'mbtype', 4);
insert into fssnityp (type, typename, sntype) values (35, 'mbrank', 4);
insert into fssnityp (type, typename, sntype) values (36, 'block_word', 4);
insert into fssnityp (type, typename, sntype) values (37, 'block_app', 4);
insert into fssnityp (type, typename, sntype) values (38, 'credit_score', 4);

insert into fssnityp (type, typename, sntype) values(0,'id',8);
insert into fssnityp (type, typename, sntype) values(1,'name',8);
insert into fssnityp (type, typename, sntype) values(2,'email',8);
```

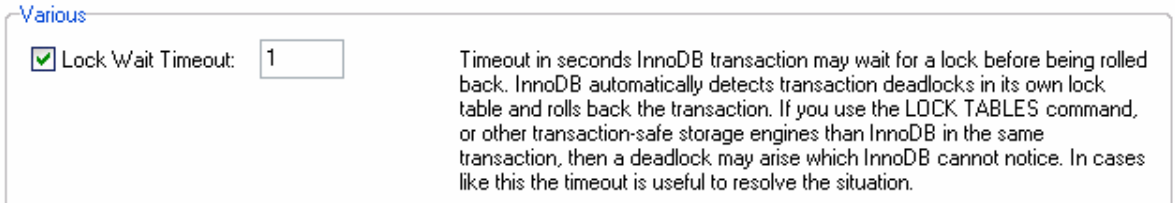
Using Scenario 2 or Load Balancing

You need to setup the database so that it will return immediately if the row is locked. Also, you need to create a table fsmsg (the create table statement is different between MySQL and MS SQL).

For MySQL

Method 1:

1. Use MySQL Administrator Tools (which can download form MySQL website)
2. Connet to your MySQL Server (please make sure it connects to localhost, otherwise it can't modify startup variables)
3. Click [View] -> [Startup Variables]
4. Click [InnoDB Paramters] Tab
5. In [Various], click check box of [Lock Wait Timeout] and modify textbox value to 1.



6. Click [Apply changes]
7. Restart your MySQL Server

Method2:

1) Find the MySQL Server's configuration file (my.ini)
2) Use Notepad to open configuration file
3) Below [mysqld], insert below

innodb_lock_wait_timeout=1

4) Save it
5) Restart your MySQL Server

* Checking innodb_lock_wait_timeout value MySQL Statement:

```
SHOW VARIABLES  LIKE "innodb_lock_wait_timeout";
```

Also, execute the below create table statement to create table fsmsg:

```
create table fsmsg
(
msgID integer NOT NULL AUTO_INCREMENT,
toSiteID varchar(40),
msgState varchar(40),
name varchar(80),
reserved1 varchar(40),
msgTime integer,
fromSiteID varchar(40),
primary key (msgID)
) ENGINE=InnoDB;
```

For MS SQL
1) run the below SQL:

ALTER DATABASE [enter_your_firstspot_database_name] SET READ_COMMITTED_SNAPSHOT ON;

* you can use the below SQL to check:

select is_read_committed_snapshot_on from sys.databases where name = '[enter_your_firstspot_database_name]';

(you should get the value 1 if the above alter database statement is successful)

* When the database is enabled for READ_COMMITTED_SNAPSHOT, all queries running under the read committed isolation level use row versioning, which means that read operations do not block update operations.

Also, execute the below create table statement to create table fsmsg:

```
create table fsmsg
(
msgID integer NOT NULL IDENTITY(1,1),
toSiteID varchar(40),
msgState varchar(40),
name varchar(80),
reserved1 varchar(40),
msgTime integer,
fromSiteID varchar(40),
primary key (msgID)
);
```

Install MySQL ODBC driver at FirstSpot server

You can have your user database installed on the same machine as FirstSpot or you can have it sits remotely. You have to make sure FirstSpot can communicate properly with your MySQL database. You need to install MySQL ODBC driver on the FirstSpot server. You can download the driver, which is released under GPL licence, from MySQL AB.

Then, create a file DSN using the MySQL ODBC driver. Here are the steps:

Step 1

After the installation, go to the **Administrative Tools** found under Control Panel of your Windows. Click on the **Data Sources (ODBC)** icon

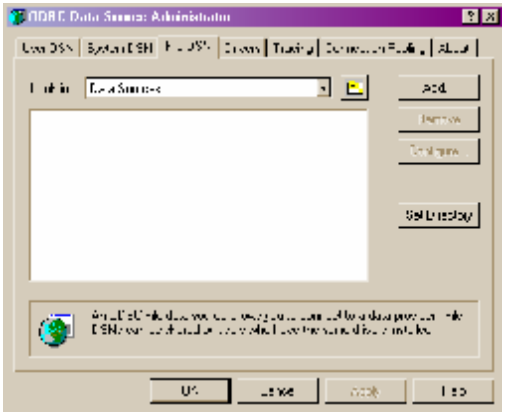
Step 1

Step 2

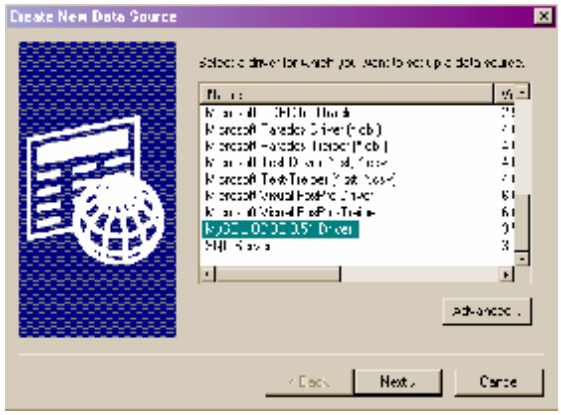
Choose the **File DSN** tab, and the click on the Add button.

Step 3

Select **MySQL ODBC Driver** and the click on Next



Step 2



Step 3

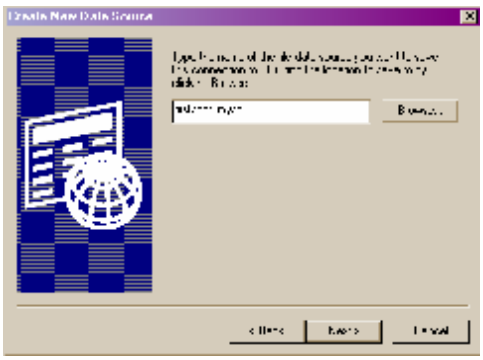
Step 4

Enter a descriptive name for the datasource, a file with this name will be created with extension dsn.

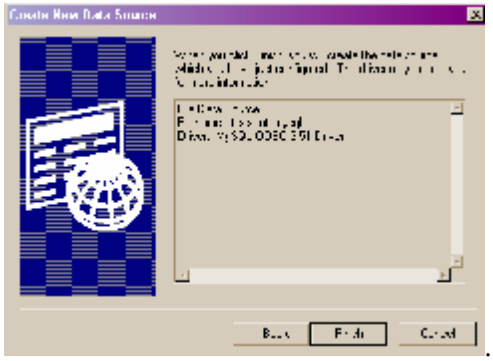
Click on **Next** to continue.

Step 5

Click on **Finish** to confirm the creation of the dsn file specified



Step 4



Step 5

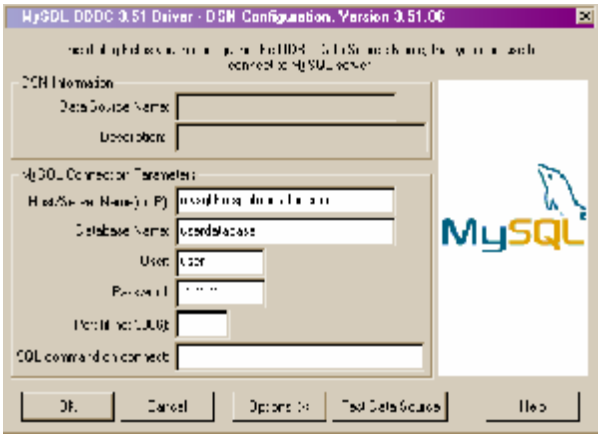
Step 6

Enter the address where your user database is situated. Also, enter the database name, user and password to connect to MySQL server.

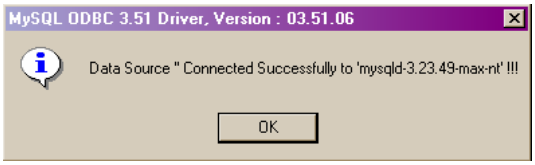
Click on **Test Data Source** button to test the connection.

Step 7

If everything's ok, you should see a dialog box saying "Connected Successfully". Click on **OK** twice to finish.



Step 6

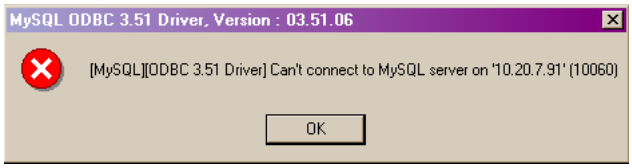


Step 7

Troubleshooting

If you see the following dialog box, you probably have entered something wrong in the database name, user or password fields.

If you see the dialog box below, you probably have entered the wrong address of your MySQL server.



** if you have difficulties using the File DSN generated by ODBC Data Source Administrator, we provide a sample MySQL dsn file named mysql.dsn which you can edit using Notepad.*

Configuration at FirstSpot

After a successful testing on MySQL connection from the FirstSpot server, please make sure you configure FirstSpot to use the dsn file you just created as the information required to talk to the user database (by pointing

to the right location in the *File DSN Location* field under the *Authentication Server* tab in Configuration Manager).

Supported MySQL/ODBC and MS SQL server version

For the latest information on the FirstSpot supported MySQL/ODBC and MS SQL server version, please check out the README file (readme.rtf) that comes with your installation package.

9. Setting up RADIUS server

RADIUS is commonly known as the protocol to solve the AAA issue (i.e. Authentication, Authorization, and Accounting). In practice, while the Authentication and Accounting part are fairly standardized, the Authorization part requires RADIUS server-specific configuration.

Below are the steps to setup Microsoft IAS in Windows 2003 (i.e. RADIUS server) to work with FirstSpot:

Active Directory:

1. Open Manage Your Server Dialog.
2. Add and follow the instruction to setup Domain Controller (Active Directory) if you have not yet setup Active Directory.
3. Open Active Directory Users and Computers Dialog.
4. Right click Active Directory Users and Computers and choose Connect To Domain.
5. Right click your Domain and Raise Domain function level to 2003.

Internet Authentication Service:

1. Open Internet Authentication Service.
2. Register Server in Active Directory.

Routing and Remote Access

1. Open Manage Your Server Dialog.
2. Click Manage This Remote Access/VPN Server.
3. Right click your RRAS Server under Server Status (right click on Server Status to Add Server and follow the instruction to setup)
4. Choose Property.
5. check the Router box.
6. choose LAN and demand-dial Routing
7. check the Remote Access box.
8. Choose Security.
9. Change Authentication Provider to RADIUS Authentication.

10. Click Configure button.
11. Click Add Button.
12. Enter Server name.
13. Click Change Button of Secret.
14. Enter the Shared Secret (must be same as FirstSpot RADIUS Shared Secret).
15. Enter Port value (must be same as FirstSpot RADIUS Authentication Port value).
16. Change Accounting Provider to RADIUS Accounting.
17. Click Configure button.
18. Click Add Button.
19. Enter Server name.
20. Click Change Button of Secret.
21. Enter the Shared Secret (Must be same as FirstSpot RADIUS Shared Secret).
22. Enter Port value (Must be same as FirstSpot RADIUS Accounting Port value).

Add User:

1. Add User Under your Domain Users Folder in Active Directory Users and Computers.
2. Right click the user.
3. choose Dial-In tag.
4. Under Remote Access Permission (Dial-in or VPN), choose Control Access Through Remote Access Policy.

Add IAS Policy:

1. Add New RADIUS Client under RADIUS Client folder of IAS.
2. Enter friendly name (e.g. FirstSpot).
3. Enter Client Address, this is the IP of the NIC on the FirstSpot Computer which connect to the RADIUS server.
4. select RADIUS STANDARD under Client-Vendor.
5. Enter Shared Secret and click Finish.
6. Right click Remote Access Policies ,click New Remote Access Policy and click Next.
7. Choose Set up a custom policy ,Enter Policy Name and click Next.
8. Click Add, Choose Client-Friendly-Name, Click Add, Enter the Friendly Name as same as the name which you add under RADIUS Client ,click OK and Click Next.

9. Choose Grant remote access permission and click Next.
10. Click Edit Profile, choose Authentication ,check Unencrypted Authentication (PAP,SPAP), click OK and click Next.
11. Click Finish.
12. Right click Connection Request Policies, Click New Connection Request Policy and Click Next.
13. Choose Set up a custom policy, Enter Policy Name and click Next.
14. Click Add, Choose Client-Friendly-Name, Click Add, Enter the Friendly Name as same as the name which you add under RADIUS Client, click OK and Click Next.
15. Click Next and Click Finish.

Below are the steps to setup Network Policy Server (NPS) in Windows Server 2008 (i.e. RADIUS server) to work with FirstSpot:

Active Directory

1. Open Server Manager.
2. Go to “Roles Summary”, click “Add Roles”.
3. Follow the Wizard to add Active Directory Domain Services if it is not being installed.
4. Choose “Roles” → “Active Directory Domain Services” and click “Run the Active Directory Domain Services Installation Wizard (dcpromo.exe)”.
5. Check “Use advanced mode installation” and click “Next”.
6. Click “Next”.
7. Choose “Create a new domain in a new forest” and click “Next”.
8. Enter fully qualified domain name (e.g. firstspot.org) and click “Next”.
9. Enter NetBIOS name and click “Next”.
10. Select “Windows Server 2008” for the forest functional level and click “Next”.
11. Uncheck “DNS server”, click “Next” and “Yes”.
12. Click “Next” if there is no need to change the service file locations.
13. Enter Directory Services Restore Mode password and click “Next”.
14. Click “Next” to start the installation and click “Finish” to exit.
15. Add domain users by choosing “Users” under the new domain, right click and choose “New” → “User”.
16. Right click the user and choose “Properties”.

17. Go to “Dial-in” tag, choose “Control access through NPS Network Policy” under “Network Access Permission” and click “OK”.

Network Policy Server

1. Open Server Manager.
2. Choose “Roles” → “Network Policy and Access Services”, right click and choose “Add Role Services”.
3. Follow the Wizard to add Network Policy Server if it is not being installed.
4. Right click “NPS (Local)” under “Network Policy and Access Services”, choose “Register server in Active Directory” and click “OK”.
5. Choose “NPS (Local)” → “RADIUS Clients and Servers” → “RADIUS Clients”, right click and choose “New RADIUS Client”.
6. Enter friendly name (e.g. FirstSpot) and address (the IP of the NIC on the FirstSpot Computer which connects to the RADIUS server).
7. Select “RADIUS Standard” for vendor name.
8. Enter shared secret (must be the same as FirstSpot RADIUS shared secret) and click “OK”.
9. Choose “NPS (Local)” → “Policies” → “Network Policies”, right click and choose “New”.
10. Enter a policy name, select “Unspecified” in “Type of network access server” and click “Next”.
11. Click “Add”, choose “Client Friendly Name” and click “Add”.
12. Enter the same friendly name, click “OK” and “Next”.
13. Choose “Access granted” and click “Next”.
14. Check “Unencrypted authentication (PAP, SPAP)” and click “Next”.
15. Click “Next”, “Next” and “Finish”.
16. Back to “Network Policies”, set processing order to 1 for the new policy.

Routing and Remote Access

1. Open Server Manager.
2. Choose “Roles” → “Network Policy and Access Services” → “Routing and Remote Access”, right click and choose “Properties”.
3. Check “IPv4 Router” and choose “LAN and demand-dial routing”.
4. Check “IPv4 Remote access server”.

Note:

- → you need DLL plug-in for IAS/NPS to handle FirstSpot user attributes (e.g. calculate timeleft/data transfer), otherwise you can only do basic authentication and accounting (e.g. login/logout only).
- → About the DLL plug-in please refer to Internet Authentication Service of Microsoft Platform SDK 2003 which is under Networking and Directory Service->Network Security. There is also sample code available in our forum at http://www.patronsoft.com/forum/viewforum.php?f=2 .
- → you need to add the DLL plug-in path in Registry at HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Services\AuthSrv\Parameters\AuthorizationDLLs . E.g. E:\IAS\IASdll.dll with REG_MULTI_SZ type
- → you need to add the ConfigFolder path (which is the location of IASConfig.ini file) in Registry at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AuthSrv\Parameters\ConfigFolder . E.g. E:\\IAS with REG_SZ type
- → update the IASConfig.ini file
- → Below are the FirstSpot Vendor attributes:

	Attributes number	**Definition**
FS_AUTH_TIMELEFT	1	timeleft
FS_AUTH_ACCUMBW	2	accumulative bandwidth (download)
FS_AUTH_BWQUOTA	3	bandwidth quota (download)
FS_AUTH_BWCOUNT	4	bandwidth counting mode (download)
FS_AUTH_ULLIMIT	5	upload bandwidth throttling
FS_AUTH_DLLIMIT	6	download bandwidth throttling
FS_AUTH_LOGINTIME	7	Login time
FS_AUTH_LOGOUTTIME	8	Logout time
FS_AUTH_TIMEDIFF	9	Duration
FS_AUTH_BWUSAGE	10	bandwidth usage (download)
FS_AUTH_ACCUMBWUL	11	accumulative bandwidth (upload)
FS_AUTH_BWQUOTAUL	12	bandwidth quota (upload)
FS_AUTH_BWCOUNTUL	13	bandwidth counting mode (upload)
FS_AUTH_BWUSAGEUL	14	bandwidth usage (upload)
FS_AUTH_ACL	16	IP Block List
FS_AUTH_MACMAP	17	Use Bind MAC address Mapping mode
FS_AUTH_LOGINMAC	18	Binded MAC Address
FS_AUTH_IPMAP	19	Real IP Address Mapping
FS_AUTH_ACCUMBWSHARE	20	accumulative bandwidth (total)
FS_AUTH_BWQUOTASHARE	21	bandwidth quota (total)
FS_AUTH_BWCOUNTSHARE	22	bandwidth counting mode (total)
FS_AUTH_BWUSAGESHARE	23	bandwidth usage (total)

The following features won't work when using RADIUS Authentication Mode:

- → *Use MAC/IP as username*
- → *Anonymous option*
- → *Self sign-up*
- → *Shopping Cart*
- → *FirstSpot administrator cannot add/edit/delete user from Configuration Manager. He has to change in the RADIUS server directly instead. This is due to the fact that RADIUS is an authentication protocol and it does not define way to change the user directory it-self.*
- → *User account attribute "recurring"*

10. FirstSpot® API

Starting from FirstSpot v6, a simple API interface is included to enable administrator perform some FirstSpot operation programmatically. FirstSpot administrator can run our API through the command line utility fsapi.exe. Below are the API calls specification:

1) update_usr_attributes
To update FirstSpot user attributes. This call will ensure data integrity within FirstSpot while performing the update (e.g. when the user is online). This API call will support what we call "live update" (i.e. currently logged in user will get reflected immediately without re-login). Also, it will aware of your current datasource setting if you change the default datasource (by changing the DSN).

Note that you can enter either username or scratch code in the below “username” parameter (except for “adduser” call which has its own “scratchcode” parameter) . Also, RADIUS Authentication is not supported and you need to update RADIUS directory directly.

Usage:
update_usr_attributes username=(value) [attribute=value] [attribute=value] [option=value]

If username is *, it will update all accounts.

It supports five user attributes :
1. timeleft (access minutes) - value must be > 0 or "" (empty sting = unlimited)
2. edate (expiry time) - attributes format: mm-dd-yyyy hh:mm
3. bwquotaUL (Upload Data Transfer Quota) - value must be > 0
4. bwquota (Download Data Transfer Quota) - value must be > 0
5. bwquotaSha (Total Data Transfer Quota) - value must be > 0
6. password

For option:
1. forceddisconnect (forced disconnect before update) - Y or N <default is N>
2. resetquota (reset Data Transfer Counter when the update is successful) - Y or N <default is N>

e.g. fsapi.exe update_usr_attributes username=a timeleft=100 bwquota=2000
fsapi.exe update_usr_attributes username=* timeleft=100 bwquotaul=2000
forceddisconnect=Y resetquota=Y
fsapi.exe update_usr_attributes username=a password=apwd

2) querylogindurationn
To query the login duration of current logged in FirstSpot user. One can use this call to query the login duration for one user or all users.

Usage:
querylogindurationn username=(value) <optional. If not supply, it will show all online users>

e.g. fsapi.exe querylogindurationn usename=abc

output:
abc,0d 0h 1m 16s

3) resetquota
To reset user current data transfer counter to zero. Once the current data transfer counter reaches the quota value, the user will be disconnected. This reset will enable client to be able to use the account again. For example, you can reset the user account daily in order to limit the amount of bandwidth (i.e. data transfer) a user can use in a day.

Note that if you are using Data Transfer (Global Setting) instead of setting individual user quota, this call is not supported.

Note that RADIUS Authentication is not supported and you need to update RADIUS directory directly.

Usage:
resetquota username=(value)

e,g. fsapi.exe resetquota username=abc

4) disconnectuser
To disconnect one or more FirstSpot users

Usage:
disconnectuser username=(value1[, value2, …])

e.g. fsapi.exe disconnectuser username=abc
fsapi.exe disconnectuser username=abc,xyz

5) deleteuser
To delete FirstSpot user account from the user database. This call will ensure data integrity within FirstSpot while performing the update (by disconnecting user first). Also, it will aware of your current datasource setting if you change the default datasource (by changing the DSN).

Note that RADIUS Authentication is not supported and you need to update RADIUS directory directly.

Usage:
deleteuser username=(value1[, value2, …])

e.g. fsapi.exe deleteuser username=abc
fsapi.exe deleteuser username=abc,xyz

6) adduser
To add FirstSpot username or scratch code to the user database. This call will aware of your current datasource setting if you change the default datasource (by changing the DSN)

Note that RADIUS Authentication is not supported and you need to update RADIUS directory directly.

Usage:
adduser [username=(value) password=(value) | scratchcode=(value)] [attribute=value] [attribute=value]

The below attributes are supported (the below attributes are of the same name as the column in table fsusr. Please refer to chapter 5 for the table definition):

- [edate, sdate] attributes format: mm-dd-yyyy hh:mm
- [eminutes] value: >0
- [bwquotaUL, bwquota, bwquotaSha, btul, btdl, attempt, bwcount, startmod, bwrmethod, bwrperiod, lastrbw, bwrdate, bwcountul, pagenum, weeksch, bwcountsha] value: >0
- [rsdate, redate] format: hh:mm
- [macasusr, acl, reqsignup] value "Y", "N"
- [auto_del, resetopt, roption, ipmap, status] value 0 or 1
- [macmap] value 0, 1, or 2
- [timeleft] value: >0 or "" (empty sting = unlimited)
- [max_logins] = max login limit for Multiple Logins (0 means no limit), not specified this

attribute means single login

e.g. fsapi.exe adduser username=a password=pwd timeleft=100
fsapi.exe adduser username=aa password=pwd bwcount=2 bwquota=1000
fsapi.exe adduser username="00-24-5F-03-45-09" password="" macasusr=Y
bwcountul=1 (blank password here means “Passive Login” user)
fsapi.exe adduser scratchcode=12345 eminutes=30 max_logins=3

7) queryCurrentDataTransfer
To query user current data transfer value.

This call will work in both ODBC and RADIUS Authentication Mode.

Usage:
fsapi.exe queryCurrentDataTransfer username=(value)

Output format:
username,download,upload,total

e.g.
sample,NA,NA,NA
sample,123KB,NA,NA
sample,NA,123KB,NA
sample,111KB,111KB,NA
sample,111KB,111KB,222KB

(whether this shows download, upload or total depends on the user’s data transfer setting)

8) addLoginOnceMac
To add Login Once MAC address to existing username. Note that the username must already exist with Multiple Login and Login Once attributes set. Also, the number of MAC must not exceed the max logins limit. Normally, the client MAC will be added automatically when user login the first time. This API call is used for case that the administrator wants to add the client MAC manually (e.g. device without browser)

Usage:
fsapi.exe addLoginOnceMac username=existingUsername mac=AA-BB-CC-DD-EE-FF