Chapter 3: Advanced Configuration

After setting up the Valet with the Setup Wizard (located on the Setup Key), the Valet is ready for use. For more technically knowledgeable users, the Valet does include Advanced Configuration settings. If you'd like to change some of the Valet's advanced settings, you can modify settings using the browser-based utility.

WARNING: Modifying some settings in the browser-based utility may disable settings you've already applied using the Easy Setup Key.

This chapter describes each web page of the utility and the key functions on each page. You can access the utility via a web browser on a computer connected to the Valet.

The browser-based utility has the following main tabs:

- Setup
- Wireless
- Security
- Access Restrictions
- Applications & Gaming
- Administration
- Status

Additional sub tabs become available after you click one of the main tabs.

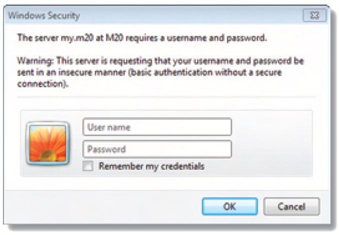
How to Access the Browser-Based Utility

To access the browser-based utility, launch the web browser on your computer, and enter the IP address of the Valet in the *Address* field. The default IP address of the Valet is 192.168.1.1

http://192.168.1.1

Then, press **Enter**.

A login screen will appear. (Non-Windows 7 users will see a similar screen.) In the *User name* field, enter **admin**. Then enter the password created during the setup software. (If you did not run the setup software, then use the default password, **admin**. You can set a new password on the *Administration > Management* screen (refer to , **page 31**.) Click **OK** to continue.



Windows Security

The server my.m20 at M20 requires a username and password.

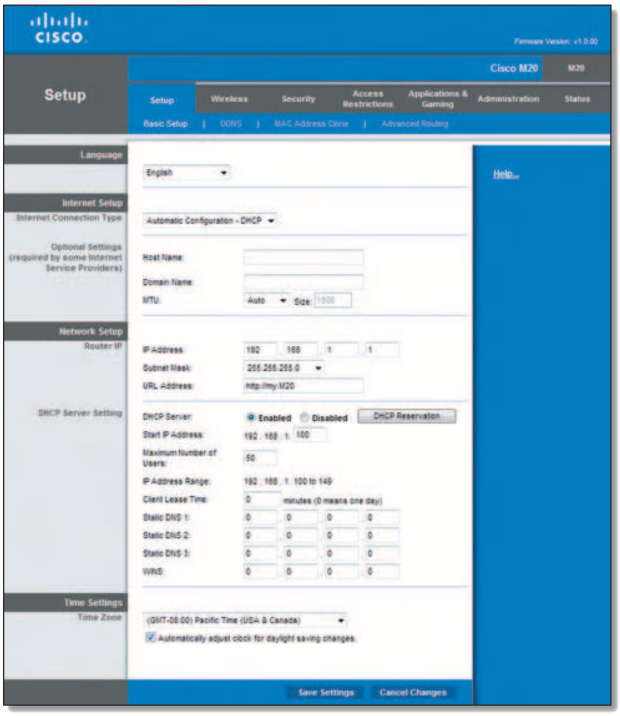
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

Windows 7 Login Screen

NOTE: You can also access the browser-based utility through the Cisco Connect software. For more information, refer to **Valet Settings**, **page 11**.

Setup > Basic Setup

The first screen that appears is the *Basic Setup* screen. This screen allows you to change the language of the text displayed in the browser-based utility, configure the Internet connection settings, configure the network settings, and select time zone settings.



Firmware Version: v1.0.00

Language: English

Internet Setup
Internet Connection Type: Automatic Configuration - DHCP
Optional Settings (required by some Internet Service Providers)
Host Name:
Domain Name:
MTU: Auto Size: 1500

Network Setup
Router IP
IP Address: 192 . 168 . 1 . 1
Subnet Mask: 255.255.255.0
URL Address: http://my.M20

DHCP Server Setting
DHCP Server: ● Enabled ○ Disabled
Start IP Address: 192 . 168 . 1. 100
Maximum Number of Users: 50
IP Address Range: 192 . 168 . 1. 100 to 149
Client Lease Time: 0 minutes (0 means one day)
Static DNS 1: 0 . 0 . 0 . 0
Static DNS 2: 0 . 0 . 0 . 0
Static DNS 3: 0 . 0 . 0 . 0
WINS: 0 . 0 . 0 . 0

Time Settings
Time Zone: (GMT-08:00) Pacific Time (USA & Canada)
☑ Automatically adjust clock for daylight saving changes.

Setup > Basic Setup

Language

The Language section allows you to change the language of the text displayed in the browser-based utility.

Internet Setup

The *Internet Setup* section configures the Valet to your Internet connection. Most of this information can be obtained through your Internet Sevice Provider (ISP).

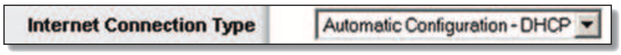
Internet Connection Type

Select the type of Internet connection your ISP provides from the drop-down menu. These are the available types:

- Automatic Configuration - DHCP
- Static IP
- PPPoE
- PPTP
- L2TP
- Telstra Cable

Automatic Configuration - DHCP

The default Internet Connection Type is **Automatic Configuration - DHCP**. Keep the default only if your ISP supports DHCP (Dynamic Host Configuration Protocol) or if you connect using a dynamic IP address.

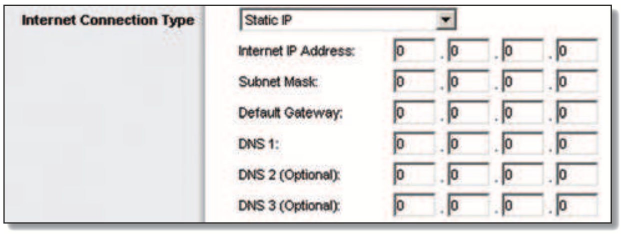


Internet Connection Type | Automatic Configuration - DHCP ▾

Internet Connection Type > Automatic Configuration - DHCP

Static IP

If you are required to use a permanent IP address to connect to the Internet, select **Static IP**.



Internet Connection Type | Static IP ▾

Internet IP Address:	0	0	0	0
Subnet Mask:	0	0	0	0
Default Gateway:	0	0	0	0
DNS 1:	0	0	0	0
DNS 2 (Optional):	0	0	0	0
DNS 3 (Optional):	0	0	0	0

Internet Connection Type > Static IP

Internet IP Address This is the Valet's IP address, when seen from the Internet. Your ISP will provide you with the IP address you need to specify here.

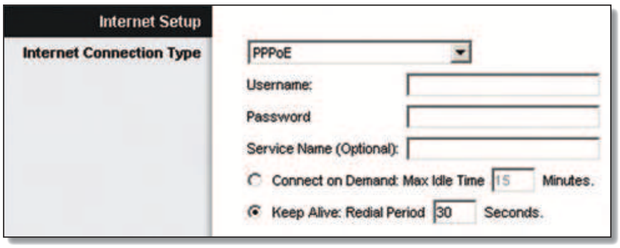
Subnet Mask This is the Valet's Subnet Mask, as seen by users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

Default Gateway Your ISP will provide you with the IP address of the ISP server.

DNS 1-3 Your ISP will provide you with at least one DNS (Domain Name System) server IP address.

PPPoE

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable **PPPoE**.



Internet Setup

Internet Connection Type | PPPoE ▾

Username:
Password
Service Name (Optional):
○ Connect on Demand: Max Idle Time 15 Minutes.
● Keep Alive: Redial Period 30 Seconds.

Internet Connection Type > PPPoE

Username and Password Enter the Username and Password provided by your ISP.

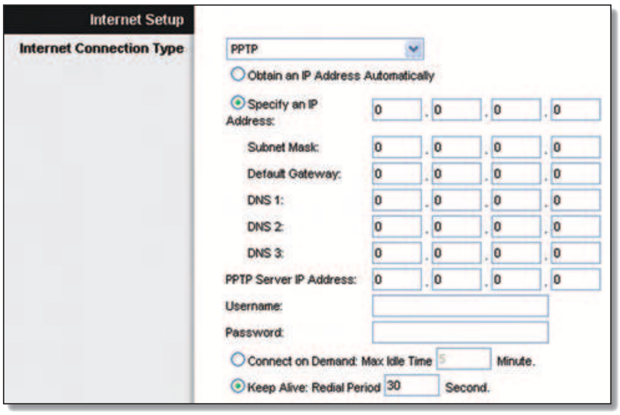
Service Name If provided by your ISP, enter the Service Name.

Connect on Demand: Max Idle Time You can configure the Valet to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand automatically reestablishes the connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to elapse before your Internet connection terminates. The default Max Idle Time is **5** minutes.

Keep Alive: Redial Period If you select this option, the Valet will periodically check your Internet connection. If you are disconnected, your connection will automatically be reestablished. To use this option, select **Keep Alive**. In the *Redial Period* field, you specify how often you want the Internet connection checked on. The default Redial Period is **30** seconds.

PPTP

Point-to-Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe only.



Internet Setup

Internet Connection Type | PPTP ▾

○ Obtain an IP Address Automatically

● Specify an IP Address:	0	0	0	0
Subnet Mask:	0	0	0	0
Default Gateway:	0	0	0	0
DNS 1:	0	0	0	0
DNS 2:	0	0	0	0
DNS 3:	0	0	0	0
PPTP Server IP Address:	0	0	0	0

Username:
Password:
○ Connect on Demand: Max Idle Time 5 Minute.
● Keep Alive: Redial Period 30 Second.

Internet Connection Type > PPTP

If your ISP supports DHCP or you are connecting through a dynamic IP address, then select **Obtain an IP Address Automatically**. If you are required to use a permanent IP address to connect to the Internet, then select **Specify an IP Address**. Then configure the following:

- **Specify an IP Address** This is the Valet's IP address, as seen from the Internet. Your ISP will provide you with the IP address you need to specify here.
- **Subnet Mask** This is the Valet's Subnet Mask, as seen by users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.
- **Default Gateway** Your ISP will provide you with the IP address of the ISP server.
- **DNS 1-3** Your ISP will provide you with at least one DNS (Domain Name System) server IP address.

PPTP Server IP Address Your ISP will provide you with the IP address of the PPTP server.

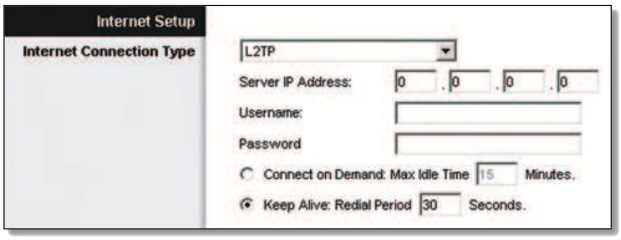
Username and Password Enter the Username and Password provided by your ISP.

Connect on Demand: Max Idle Time You can configure the Valet to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand automatically reestablishes the connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is **5** minutes.

Keep Alive: Redial Period If you select this option, the Valet will periodically check your Internet connection. If you are disconnected, your connection will automatically be reestablished. To use this option, select **Keep Alive**. In the *Redial Period* field, you specify how often you want the Internet connection checked on. The default value is **30** seconds.

L2TP

L2TP is a service that applies to connections in Israel only.



Internet Setup

Internet Connection Type

L2TP

Server IP Address: 0 . 0 . 0 . 0

Username:

Password

○ Connect on Demand: Max Idle Time 15 Minutes.

● Keep Alive: Redial Period 30 Seconds.

Internet Connection Type > L2TP

Server IP Address This is the IP address of the L2TP Server. Your ISP will provide you with the IP address you need to specify here.

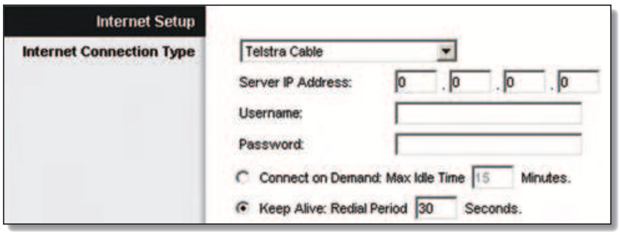
Username and Password Enter the Username and Password provided by your ISP.

Connect on Demand: Max Idle Time You can configure the Valet to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand automatically reestablishes the connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is **5** minutes.

Keep Alive: Redial Period If you select this option, the Valet will periodically check your Internet connection. If you are disconnected, then the Valet will automatically re-establish your connection. To use this option, select **Keep Alive**. In the *Redial Period* field, you specify how often you want the Internet connection checked on. The default Redial Period is **30** seconds.

Telstra Cable

Telstra Cable is a service that applies to connections in Australia only.



Internet Setup

Internet Connection Type

Telstra Cable

Server IP Address: 0 . 0 . 0 . 0

Username:

Password:

○ Connect on Demand: Max Idle Time 15 Minutes.

● Keep Alive: Redial Period 30 Seconds.

Internet Connection Type > Telstra Cable

Server IP Address This is the IP address of the Heartbeat Server. Your ISP will provide you with the IP address you need to specify here.

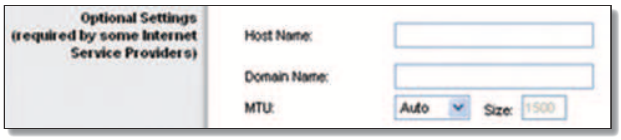
Username and Password Enter the Username and Password provided by your ISP.

Connect on Demand: Max Idle Time You can configure the Valet to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand automatically reestablishes the connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is **5** minutes.

Keep Alive: Redial Period If you select this option, the Valet will periodically check your Internet connection. If you are disconnected, your connection will automatically be reestablished. To use this option, select **Keep Alive**. In the *Redial Period* field, you specify how often you want the Internet connection checked on. The default value is **30** seconds.

Optional Settings

Some of these settings may be required by your ISP. Verify these settings with your ISP before making any changes.



Optional Settings
(required by some Internet Service Providers)

Host Name:

Domain Name:

MTU: Auto Size: 1500

Optional Settings

Host Name and Domain Name These fields allow you to supply a host and domain name. Some ISPs, usually cable ISPs, require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Select Manual if you want to manually enter the largest packet size that is transmitted. To allow the Valet to select the best MTU for your Internet connection, keep the default setting, **Auto**.

Size When Manual is selected in the *MTU* field, this option is enabled. Leave this value in the 1200 to 1500 range. The default size depends on the Internet Connection Type:

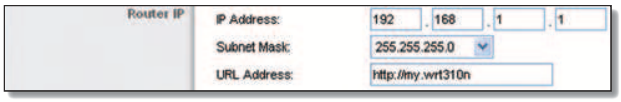
- DHCP, Static IP, or Telstra: **1500**
- PPPoE: **1492**
- PPTP or L2TP: **1460**

Network Setup

The *Network Setup* section configures the IP settings for your local network.

Router IP

This presents the IP Address of the Valet, Subnet Mask, and URL as seen by your network.



Router IP

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255.255.0

URL Address: http://my.wrt310n

Router IP

IP Address This is the IP address of the Valet and is used as the base for all of your local network settings.

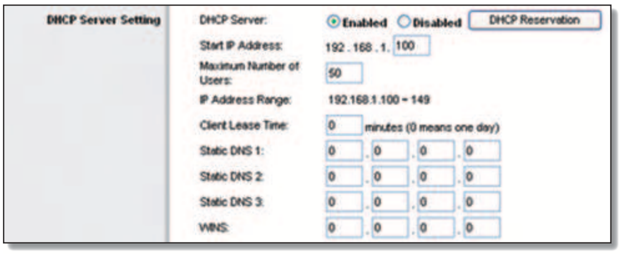
Subnet Mask This is the subnet mask address for your Valet. It offers a selection of addresses from a drop-down menu. Most users will not need to change this setting.

URL Address This value entered here can be typed into a web browser's address field to access the Valet's browser-based utility instead of typing in the IP address of the Valet.

DHCP Server Setting

The Valet includes a DHCP server that automatically assigns IP addresses to computers, cell phones, gaming systems, and other DHCP enabled devices on your home network.

NOTE: If you choose to enable the DHCP server option, make sure there is no other DHCP server on your network.



DHCP Server Setting

DHCP Server: ● Enabled ○ Disabled DHCP Reservation

Start IP Address: 192 . 168 . 1. 100

Maximum Number of Users: 50

IP Address Range: 192.168.1.100 ~ 149

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 0 . 0 . 0 . 0

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

DHCP Server Setting

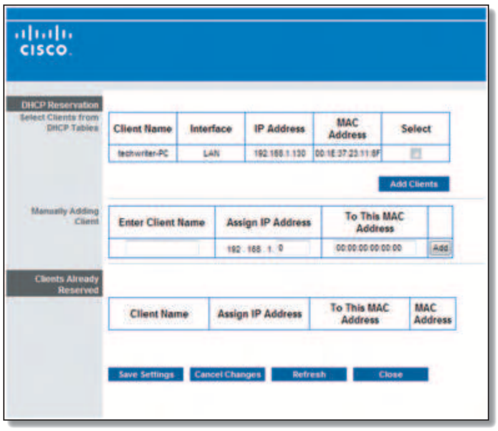
DHCP Server DHCP is enabled by factory default. If you already have a DHCP server on your network, or you do not want a DHCP server, then select **Disabled** (no other DHCP features will be available).

NOTE: If you disconnect a computer or device from your network and reconnect it to the network at a later time, it may be assigned a new IP address. If you want to ensure that the computer or device uses the same IP address all the time, you can use the DHCP Reservation option.

DHCP Reservation Click this button if you want to assign a fixed local IP address to a specific device on your network. This is helpful if you have a device you need to access at the same address all the time such as a media server or print server. You can reserve the IP address for the specific device by selecting it from the list of devices or by manually entering the MAC address of the device.

DHCP Reservation

You will see a list of DHCP clients with the following information: Client Name, Interface, IP Address, and MAC Address.



DHCP Reservation
Select Clients from DHCP Tables

Client Name	Interface	IP Address	MAC Address	Select
techwriter-PC	LAN	192.168.1.130	00:1E:37:23:11:8F	□

Add Clients

Manually Adding Client

Enter Client Name	Assign IP Address	To This MAC Address	
	192 . 168 . 1 . 0	00:00:00:00:00:00	Add

Clients Already Reserved

Client Name	Assign IP Address	To This MAC Address	MAC Address

Save Settings | Cancel Changes | Refresh | Close

DHCP Reservation

- **Select Clients from DHCP Table** Click the **Select** check box to reserve a client's IP address. Then click **Add Clients**.
- **Manually Adding Client** To manually assign an IP address, enter the client's name in the *Enter Client Name* field. Enter the IP address you want it to have in the *Assign IP Address* field. Enter its MAC address in the *To This MAC Address* field. Then click **Add**.

Clients Already Reserved

A list of DHCP clients and their fixed local IP addresses will be displayed at the bottom of the screen. If you want to remove a client from this list, click **Remove**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. To view the most up-to-date information, click **Refresh**. To exit this screen, click **Close**.

Start IP Address Enter a value for the DHCP server to start with when issuing IP addresses. Because the Valet's default IP address is 192.168.1.1, the Start IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.253. The default Starting IP Address is **192.168.1.100**.

Maximum Number of Users Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. The default is **50**.

IP Address Range Displayed here is the range of available IP addresses.

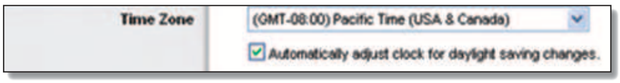
Client Lease Time Client Lease Time is the amount of time that a device will be "leased" a dynamic IP address. After the time is up, the user will be automatically assigned a new dynamic IP address, or the lease will be renewed with the same IP address. The default is **0** minutes, which means one day.

Static DNS 1-3 The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. If you wish to use another, enter that IP Address in one of these fields. You can enter up to three DNS Server IP Addresses here. The Valet will use these for quicker access to functioning DNS servers.

WINS The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter that server's IP Address here. Otherwise, leave this blank.

Time Settings

Time Zone Select the time zone in which your network functions from this drop-down menu. (You can even automatically adjust for daylight saving time.)



Time Zone: (GMT-08:00) Pacific Time (USA & Canada)

☑ Automatically adjust clock for daylight saving changes.

Time Setting

Click **Save Settings** to apply your changes, or click **Cancel Changes** to clear your changes.

Setup > DDNS

The Valet offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Valet.

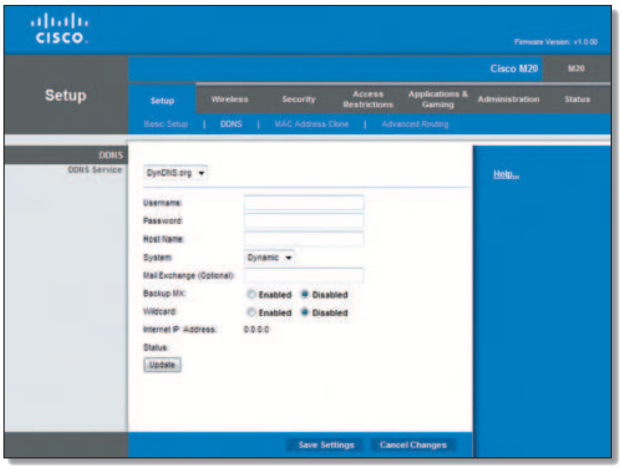
Before you can use this feature, you need to sign up for DDNS service with a DDNS service provider, **www.dyndns.org** or **www.TZO.com**. If you do not want to use this feature, keep the default setting, **Disabled**.

DDNS

DDNS Service

If your DDNS service is provided by DynDNS.org, then select **DynDNS.org** from the drop-down menu. If your DDNS service is provided by TZO, then select **TZO.com**. The features available on the *DDNS* screen will vary, depending on which DDNS service provider you use.

DynDNS.org



DDNS Service: DynDNS.org

Username:

Password:

Host Name:

System: Dynamic

Mail Exchange (Optional):

Backup MX: ○ Enabled ● Disabled

Wildcard: ○ Enabled ● Disabled

Internet IP Address: 0.0.0.0

Status:

Update

Setup > DDNS > DynDNS

Username Enter the Username for your DDNS account.

Password Enter the Password for your DDNS account.

Host Name The is the DDNS URL assigned by the DDNS service.

System Select the DynDNS service you use: **Dynamic**, **Static**, or **Custom**. The default selection is **Dynamic**.

Mail Exchange (Optional) Enter the address of your mail exchange server, so e-mails to your DynDNS address go to your mail server.

Backup MX This feature allows the mail exchange server to be a backup. To disable this feature, keep the default, **Disabled**. To enable the feature, select **Enabled**. If you are not sure which setting to select, keep the default, **Disabled**.

Wildcard This setting enables or disables wildcards for your host. For example, if your DDNS address is *myplace.dyndns.org* and you enable wildcards, then *x.myplace.dyndns.org* will work as well (x is the wildcard). To disable wildcards, keep the default, **Disabled**. To enable wildcards, select **Enabled**. If you are not sure which setting to select, keep the default, **Disabled**.

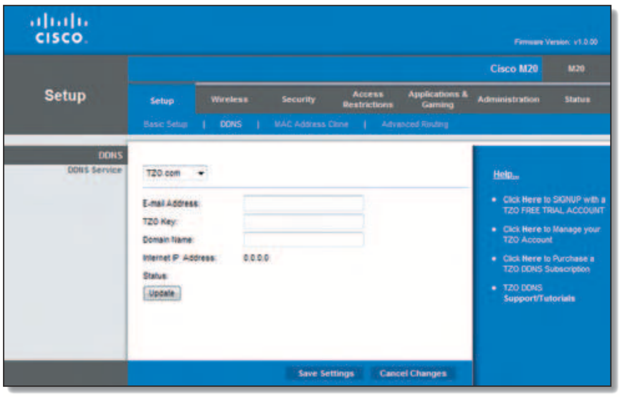
Internet IP Address The Valet's Internet IP address is displayed here. Because it is dynamic, it will change.

Status The status of the DDNS service connection is displayed here.

Update To manually trigger an update, click this button.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

TZO.com



DDNS Service: TZO.com

E-mail Address:

TZO Key:

Domain Name:

Internet IP Address: 0.0.0.0

Status:

Update

- Click Here to SIGNUP with a TZO FREE TRIAL ACCOUNT
- Click Here to Manage your TZO Account
- Click Here to Purchase a TZO DDNS Subscription
- TZO DDNS Support/Tutorials

Setup > DDNS > TZO

E-mail Address, TZO Key, and Domain Name Enter the settings of the account you set up with TZO.

Internet IP Address The Valet's Internet IP address is displayed here. Because it is dynamic, it will change.

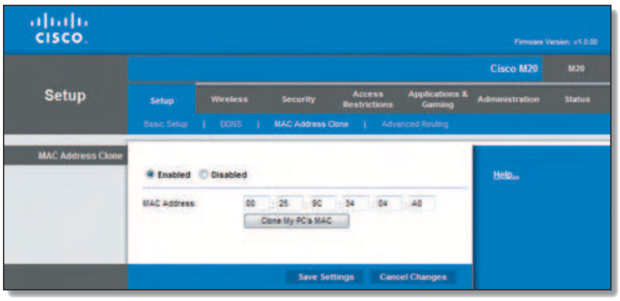
Status The status of the DDNS service connection is displayed here.

Update To manually trigger an update, click this button.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Setup > MAC Address Clone

A MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs will require you to register a MAC address in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you can use the MAC Address Clone feature to assign the currently registered MAC address to the Valet.



MAC Address Clone: ● Enabled ○ Disabled

MAC Address: 00 : 25 : 9C : 34 : 04 : A0

Clone My PC's MAC

Setup > MAC Address Clone

MAC Address Clone

Enabled/Disabled To have the MAC Address cloned, select **Enabled**.

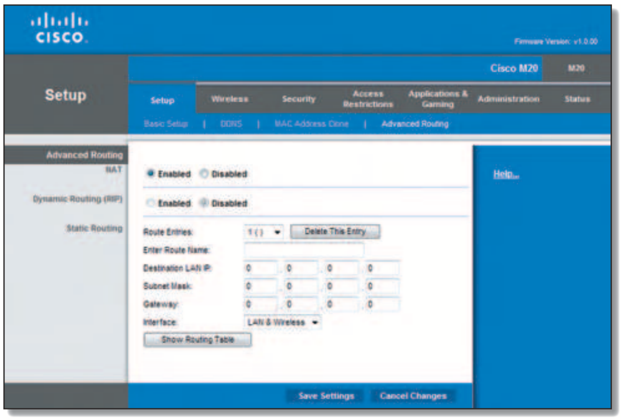
MAC Address Enter the MAC Address registered with your ISP here.

Clone My PC's MAC Click this button to clone the MAC address of the computer you are using.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Setup > Advanced Routing

This screen is used to set up the Valet’s advanced functions. Operating Mode allows you to select the type(s) of advanced functions you use. Dynamic Routing automatically adjusts how packets travel on your network. Static Routing sets up a fixed route to another network destination.



NAT: ● Enabled ○ Disabled

Dynamic Routing (RIP): ○ Enabled ● Disabled

Static Routing

Route Entries: 1 ( )

Enter Route Name:

Destination LAN IP: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Gateway: 0 . 0 . 0 . 0

Interface: LAN & Wireless

Setup > Advanced Routing

Advanced Routing

NAT

Enabled/Disabled If the Valet is hosting your network’s connection to the Internet, keep the default, **Enabled**. If another router exists on your network, select **Disabled**. When the NAT setting is disabled, dynamic routing will be enabled.

Dynamic Routing (RIP)

Enabled/Disabled This feature enables the Valet to automatically adjust to physical changes in the network’s layout and exchange routing tables with the other router(s). The Valet determines the network packets’ route based on the fewest number of hops between the source and the destination. When the NAT setting is enabled, the Dynamic Routing feature is automatically disabled. When the NAT setting is disabled, this feature is available. Select **Enabled** to use the Dynamic Routing feature.

Static Routing

A static route is a pre-determined pathway that network information must travel to reach a specific host or network. Enter the information described below to set up a new static route.

Route Entries To set up a static route between the Valet and another network, select a number from the drop-down list. Click **Delete This Entry** to delete a static route.

Enter Route Name Enter a name for the Route here, using a maximum of 25 alphanumeric characters.

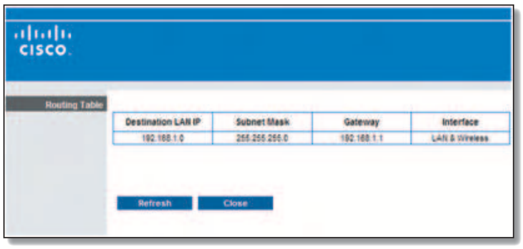
Destination LAN IP The Destination LAN IP is the address of the remote network or host to which you want to assign a static route.

Subnet Mask The Subnet Mask determines which portion of a Destination LAN IP address is the network portion, and which portion is the host portion.

Gateway This is the IP address of the gateway device that allows for contact between the Valet and the remote network or host.

Interface This interface tells you whether the Destination IP Address is on the **LAN & Wireless** (Ethernet and wireless networks) or the **Internet (WAN)**.

Click **Show Routing Table** to view the static routes you have already set up.



Destination LAN IP	Subnet Mask	Gateway	Interface
192.168.1.0	255.255.255.0	192.168.1.1	LAN & Wireless

Advanced Routing > Routing Table

Routing Table

For each route, the Destination LAN IP address, Subnet Mask, Gateway, and Interface are displayed. Click **Refresh** to update the information. Click **Close** to exit this screen.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Wireless > Basic Wireless Settings

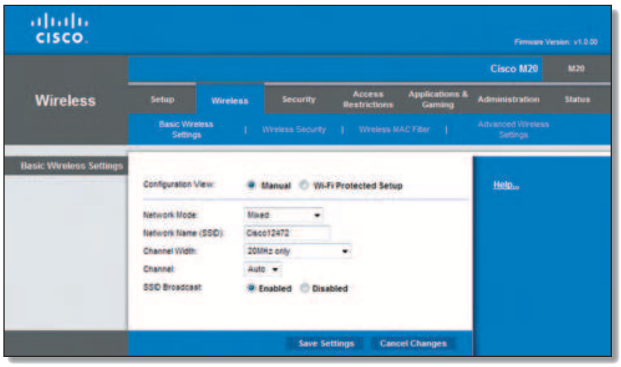
The basic settings for wireless networking are set on this screen.

There are two ways to configure the Valet’s wireless network(s), manual and Wi-Fi Protected Setup.

Wi-Fi Protected Setup is a feature that makes it easy to set up your wireless network. If you have client devices, such as wireless adapters, that support Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup.

Configuration View To manually configure your wireless network, select **Manual**. Proceed to the “Basic Wireless Settings” section. To use Wi-Fi Protected Setup, select **Wi-Fi Protected Setup**. Proceed to the “Wi-Fi Protected Setup” section.

Basic Wireless Settings (Manual)



Configuration View: ● Manual ○ Wi-Fi Protected Setup

Network Mode: Mixed

Network Name (SSID): Cisco12472

Channel Width: 20MHz only

Channel: Auto

SSID Broadcast: ● Enabled ○ Disabled

Wireless > Basic Wireless Settings (Manual Setup)

Network Mode From the drop-down menu, select the wireless standards running on your network:

- **Mixed** Use this option if you have Wireless-N, Wireless-G, and Wireless-B devices on your network.
- **BG-Mixed** Use this option if you have only Wireless-G and Wireless-B devices on your network.
- **Wireless-G Only** Use this option if you have only Wireless-G devices on your network.
- **Wireless-B Only** Use this option if you have only Wireless-B devices on your network.
- **Wireless-N Only** Use this option if you have only Wireless-N devices on your network.
- **Disabled** Use this option if your network has no wireless devices, or if you want to disable wireless networking.

NOTE: If you are unsure of what network mode to use, keep the default **Mixed** setting.

Network Name (SSID) The SSID is the network name shared among all points in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard).

Channel Width Select **Auto** if you want the Valet to automatically determine the proper channel width (20 MHz or 40 MHz) to use. For best performance, select **Auto**, otherwise keep the default **20MHz only**.

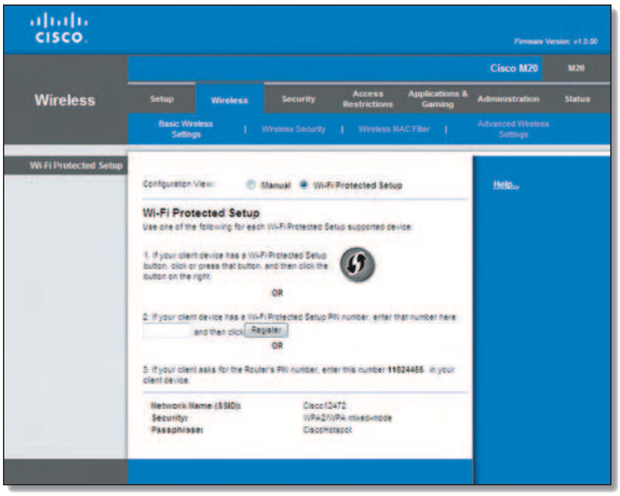
Channel Select a channel from 1 to 11, or **Auto** (default).

SSID Broadcast When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Valet. To broadcast the Valet's SSID, keep the default setting, **Enabled**. If you do not want to broadcast the Valet's SSID, then select **Disabled**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Wi-Fi Protected Setup

There are three methods available. Use the method that applies to the client device you are configuring.



Configuration View: ○ Manual ● Wi-Fi Protected Setup

Wi-Fi Protected Setup

Use one of the following for each Wi-Fi Protected Setup supported device

1. If your client device has a Wi-Fi Protected Setup button, click or press that button, and then click the button on the right.

OR

2. If your client device has a Wi-Fi Protected Setup PIN number, enter that number here and then click Register

OR

3. If your client asks for the Router's PIN number, enter this number 11824486 in your client device.

Network Name (SSID): Cisco12472

Security: WPA2/WPA mixed-mode

Passphrase: CiscoHotspot

Wireless > Basic Wireless Settings (Wi-Fi Protected Setup)

NOTE: Wi-Fi Protected Setup configures one client device at a time. Repeat the instructions for each client device that supports Wi-Fi Protected Setup.

1. **Use the Wi-Fi Protected Setup Button** Use this method if your client device has a Wi-Fi Protected Setup button.

   a. Click or press the **Wi-Fi Protected Setup** button on the client device.

   b. Click the **Wi-Fi Protected Setup** button on this screen.

   The Wi-Fi Protected Setup LED on the Valet flashes blue for two minutes during the setup process and lights up solid blue when the Wi-Fi Protected Setup process is successful.

   The LED lights up amber if there is an error during the Wi-Fi Protected Setup process. Make sure the client device supports Wi-Fi Protected Setup. Wait until the LED is off, and then try again.

   The LED flashes when a Wi-Fi Protected Setup session is active. The Valet supports one session at a time. Wait until the LED is solidly lit, or off before starting the next Wi-Fi Protected Setup session.

   c. After the client device has been configured, click **OK**. Then refer back to your client device or its documentation for further instructions.

2. **Enter the client device's PIN on the Valet** Use this method if your client device has a Wi-Fi Protected Setup PIN number.

   a. Enter the PIN number in the field on this screen.

b. Click **Register**.

c. After the client device has been configured, click **OK**. Then refer back to your client device or its documentation for further instructions.

3. **Enter the Valet's PIN on your client device** Use this method if your client device asks for the Valet's PIN number.

   a. Enter the PIN number listed on this screen. (It is also listed on the label on the bottom of the Valet.)

   b. After the client device has been configured, click **OK**. Then refer back to your client device or its documentation for further instructions.

The Wi-Fi Protected Setup Status, Network Name (SSID), Security, Encryption, and Passphrase are displayed at the bottom of the screen.

NOTE: If you have client devices that do not support Wi-Fi Protected Setup, note the wireless settings, and then manually configure those client devices.

Wireless > Wireless Security

The wireless security settings configure the security of your wireless network(s). The Valet supports the following wireless security options: WPA/WPA2 Mixed Mode (default), WPA2 Personal, WPA Personal, WEP, and RADIUS. (WPA stands for Wi-Fi Protected Access. WEP stands for Wireless Equivalent Privacy. RADIUS stands for Remote Authentication Dial-In User Service.)

The default option is **WPA/WPA2 Mixed Mode**, which allows your devices to connect using the strongest security option they support, WPA2 or WPA.

Personal Options

Security Option	Strength
WPA2 Personal	Strongest
WPA/WPA2 Mixed Mode (default)	WPA2: Strongest WPA: Strong
WPA Personal	Strong
WEP	Basic

Office Option

RADIUS is the security option offered for networks that use a RADIUS server for authentication.

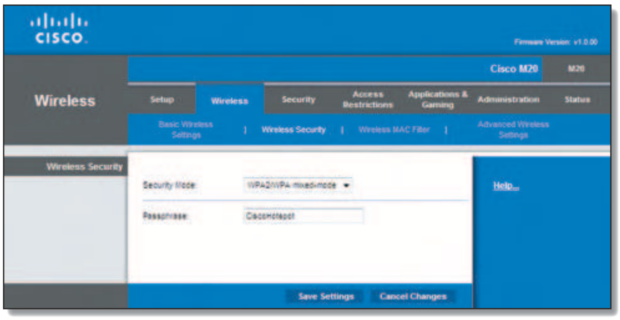
Security Mode

Select the security method for your wireless network. If you do not want to use wireless security, keep the default, **Disabled**.

NOTE: If you are not using WPA2/WPA Mixed-Mode then each device in your wireless network MUST use the same encryption method and shared key, or else the network will not function properly.

WPA/WPA2 Mixed Mode

WPA/WPA2 Mixed Mode allows you to use devices on your network that use either WPA or WPA2 security mode.



Security Mode: WPA2/WPA mixed-mode

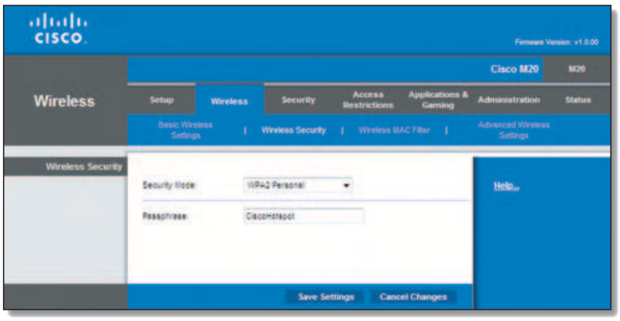
Passphrase: CiscoHotspot

Security Mode > WPA/WPA2 Mixed Mode

Passphrase Enter a Passphrase of 8-63 characters.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

WPA2 Personal



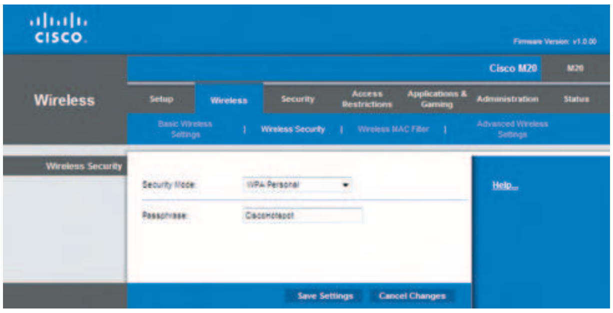
Security Mode: WPA2 Personal

Passphrase: CiscoHotspot

Security Mode > WPA2 Personal

Passphrase Enter a Passphrase of 8-63 characters.

WPA Personal



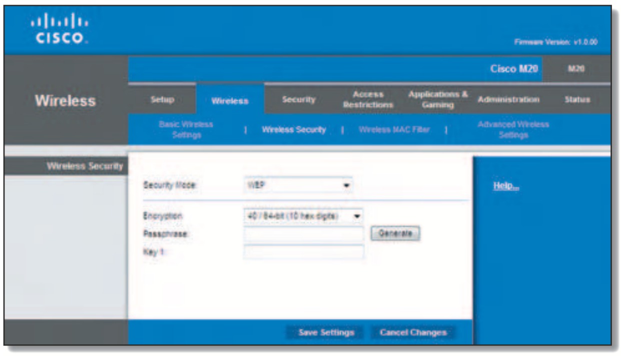
Security Mode: WPA Personal

Passphrase: CiscoHotspot

Security Mode > WPA Personal

Passphrase Enter a Passphrase of 8-63 characters.

WEP



Security Mode: WEP

Encryption: 40 / 64-bit (10 hex digits)

Passphrase:

Key 1:

Security Mode > WEP

IMPORTANT: If you are using WEP encryption, always remember that each device in your wireless network MUST use the same WEP encryption method and encryption key, or else your wireless network will not function properly.

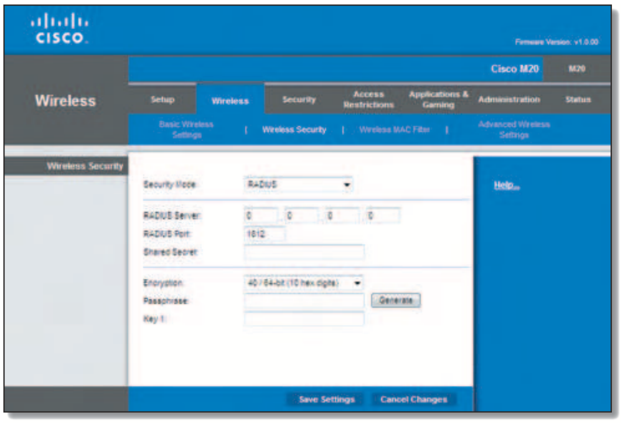
Encryption Select a level of WEP encryption, **40/64 bits (10 hex digits)** or **104/128 bits (26 hex digits)**. The default is **40/64 bits (10 hex digits)**.

Passphrase Enter a Passphrase to automatically generate WEP keys. Then click **Generate**.

Key 1 If you did not enter a Passphrase, enter the WEP key manually.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

RADIUS



Security Mode: RADIUS

RADIUS Server: 0 . 0 . 0 . 0

RADIUS Port: 1812

Shared Secret:

Encryption: 40 / 64-bit (10 hex digits)

Passphrase:

Key 1:

Security Mode > RADIUS

IMPORTANT: If you are using WEP encryption, always remember that each device in your wireless network MUST use the same WEP encryption method and encryption key, or else your wireless network will not function properly.

RADIUS Server Enter the IP Address of the RADIUS server.

RADIUS Port Enter the port number of the RADIUS server. The default value is **1812**.

Shared Secret Enter the key shared between the Valet and the server.

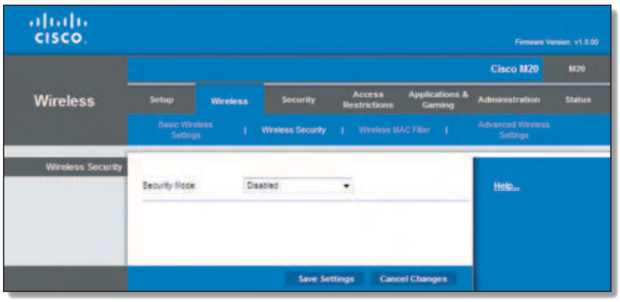
Encryption Select a level of WEP encryption, **40/64 bits (10 hex digits)** or **104/128 bits (26 hex digits)**. The default is **40/64 bits (10 hex digits)**.

Passphrase Enter a Passphrase to automatically generate WEP keys. Then click **Generate**.

Key 1 If you did not enter a Passphrase, enter the WEP key manually.

Disabled

When wireless security is disabled on your network, anyone can access your network at any time.

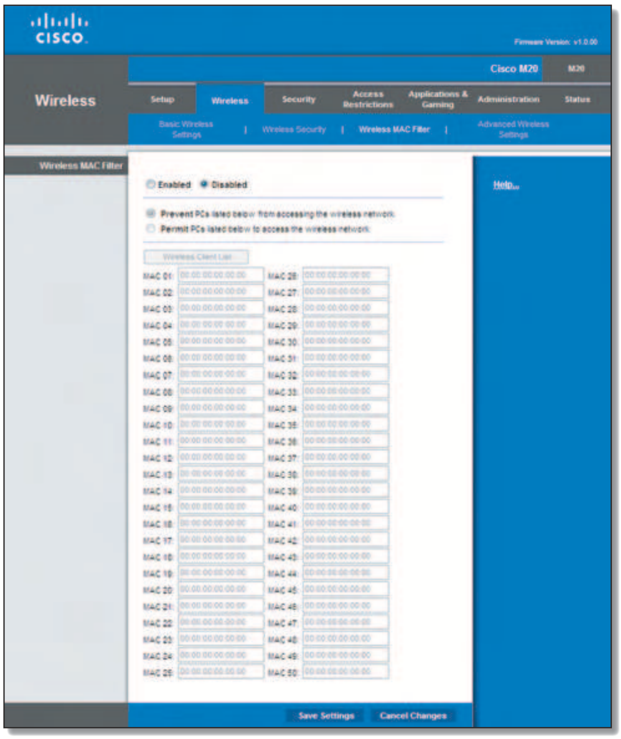


Security Mode: Disabled

Security Mode > Disabled

Wireless > Wireless MAC Filter

The *Wireless MAC Filter* option allows you to block or grant access to your network based on the device's MAC address. Each device on your network has a unique MAC address that was assigned to it by the manufacturer.



○ Enabled ● Disabled

● Prevent PCs listed below from accessing the wireless network
○ Permit PCs listed below to access the wireless network

MAC 01:	00:00:00:00:00:00	MAC 26:	00:00:00:00:00:00
MAC 02:	00:00:00:00:00:00	MAC 27:	00:00:00:00:00:00
MAC 03:	00:00:00:00:00:00	MAC 28:	00:00:00:00:00:00
MAC 04:	00:00:00:00:00:00	MAC 29:	00:00:00:00:00:00
MAC 05:	00:00:00:00:00:00	MAC 30:	00:00:00:00:00:00
MAC 06:	00:00:00:00:00:00	MAC 31:	00:00:00:00:00:00
MAC 07:	00:00:00:00:00:00	MAC 32:	00:00:00:00:00:00
MAC 08:	00:00:00:00:00:00	MAC 33:	00:00:00:00:00:00
MAC 09:	00:00:00:00:00:00	MAC 34:	00:00:00:00:00:00
MAC 10:	00:00:00:00:00:00	MAC 35:	00:00:00:00:00:00
MAC 11:	00:00:00:00:00:00	MAC 36:	00:00:00:00:00:00
MAC 12:	00:00:00:00:00:00	MAC 37:	00:00:00:00:00:00
MAC 13:	00:00:00:00:00:00	MAC 38:	00:00:00:00:00:00
MAC 14:	00:00:00:00:00:00	MAC 39:	00:00:00:00:00:00
MAC 15:	00:00:00:00:00:00	MAC 40:	00:00:00:00:00:00
MAC 16:	00:00:00:00:00:00	MAC 41:	00:00:00:00:00:00
MAC 17:	00:00:00:00:00:00	MAC 42:	00:00:00:00:00:00
MAC 18:	00:00:00:00:00:00	MAC 43:	00:00:00:00:00:00
MAC 19:	00:00:00:00:00:00	MAC 44:	00:00:00:00:00:00
MAC 20:	00:00:00:00:00:00	MAC 45:	00:00:00:00:00:00
MAC 21:	00:00:00:00:00:00	MAC 46:	00:00:00:00:00:00
MAC 22:	00:00:00:00:00:00	MAC 47:	00:00:00:00:00:00
MAC 23:	00:00:00:00:00:00	MAC 48:	00:00:00:00:00:00
MAC 24:	00:00:00:00:00:00	MAC 49:	00:00:00:00:00:00
MAC 25:	00:00:00:00:00:00	MAC 50:	00:00:00:00:00:00

Wireless > Wireless MAC Filter

Wireless MAC Filter

Enabled/Disabled To filter wireless users by MAC Address, either permitting or blocking access, select **Enabled**. If you do not wish to filter users by MAC Address, keep the default setting, **Disabled**.

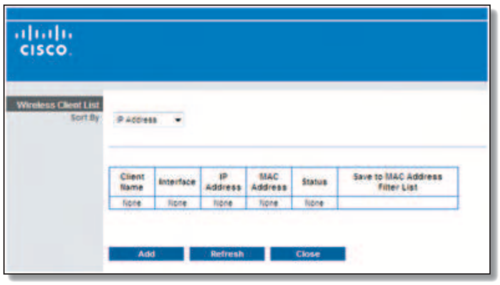
Access Restriction

Prevent Select this option to block a specific device or multiple devices from accessing your wireless network. You can manually enter the unwanted MAC address(es) or select the device(s) from the *Wireless Client List*. When wireless mac filtering is enabled, this option is selected by default.

Permit Select this option to specify which devices can access your wireless network. When this option is enabled, only devices that have their MAC address listed in the *Wireless MAC Filter* list will be able to access your wireless network. You can enter MAC addresses manually or select them from the *Wireless Client List*.

MAC Address Filter List

Wireless Client List Click this to open the *Wireless Client List* screen.



Sort By: IP Address

Client Name	Interface	IP Address	MAC Address	Status	Save to MAC Address Filter List
None	None	None	None	None	

Wireless Client List

Wireless Client List

This screen shows computers and other devices on the wireless network. The list can be sorted by IP Address, MAC Address, Status, Interface, and Client Name.

Select **Save to MAC Address Filter List** for any device you want to add to the MAC Address Filter List. Then click **Add**.

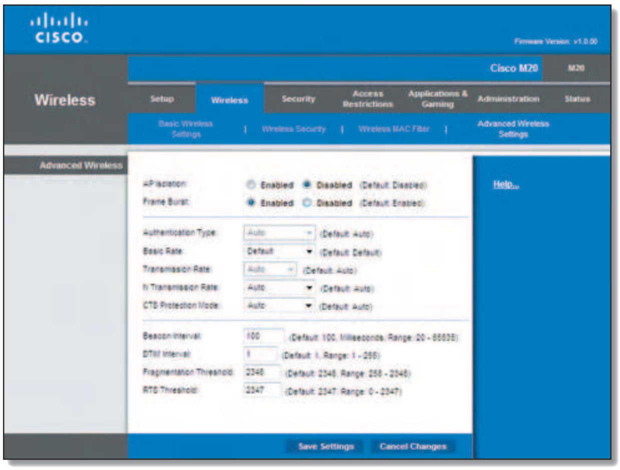
To retrieve the most up-to-date information, click **Refresh**. To exit this screen and return to the *Wireless MAC Filter* screen, click **Close**.

MAC 01-50 Enter the MAC addresses of the devices whose wireless access you want to block or allow.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Wireless > Advanced Wireless Settings

This *Advanced Wireless Settings* screen is used to set up the Valet's advanced wireless functions. These settings should only be adjusted by an advanced user because incorrect settings can reduce wireless performance. In most cases, keep the default settings.



AP Isolation: ○ Enabled ● Disabled (Default: Disabled)
Frame Burst: ● Enabled ○ Disabled (Default: Enabled)

Authentication Type: Auto (Default: Auto)
Basic Rate: Default (Default: Default)
Transmission Rate: Auto (Default: Auto)
N Transmission Rate: Auto (Default: Auto)
CTS Protection Mode: Auto (Default: Auto)

Beacon Interval: 100 (Default: 100, Milliseconds, Range: 20 - 65535)
DTIM Interval: 1 (Default: 1, Range: 1 - 255)
Fragmentation Threshold: 2346 (Default: 2346, Range: 256 - 2346)
RTS Threshold: 2347 (Default: 2347, Range: 0 - 2347)

Wireless > Advanced Wireless Settings

Advanced Wireless

AP Isolation This isolates all wireless clients and wireless devices on your network from each other. Wireless devices will be able to communicate with the Valet but not with each other. To use this function, select **Enabled**. AP Isolation is disabled by default.

Frame Burst Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. To use this option, keep the default, **Enabled**. Otherwise, select **Disabled**.

Authentication Type The default is set to **Auto**, which allows either Open System or Shared Key authentication to be used. With Open System authentication, the sender and the recipient do NOT use a WEP key for authentication. With Shared Key authentication, the sender and recipient use a WEP key for authentication. Select **Shared Key** to only use Shared Key authentication.

Basic Rate The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Valet can transmit. The Valet will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The Valet will also advertise that it will automatically select the best rate for transmission. The default setting is **Default**, for transmission at all standard wireless rates (1-2 Mbps, 5.5 Mbps, 11 Mbps, 18 Mbps, and 24 Mbps). Other options are **1-2Mbps**, for use with older wireless technology, and **All**, when the Valet can transmit at all wireless rates. The Basic Rate is not the actual rate of data transmission. If you want to specify the Valet's rate of data transmission, configure the Transmission Rate setting.

Transmission Rate The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Valet automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Valet and a wireless client. The default is **Auto**.

N Transmission Rate The rate of data transmission should be set depending on the speed of your Wireless-N networking. You can select from a range of transmission speeds, or you can select **Auto** to have the Valet automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Valet and a wireless client. The default is **Auto**.

CTS Protection Mode The Valet will automatically use CTS (Clear-To-Send) Protection Mode when your Wireless-N and Wireless-G products are experiencing severe problems and are not able to transmit to the Valet in an environment with heavy 802.11b traffic. This function boosts the Valet's ability to catch all Wireless-N and Wireless-G transmissions but will severely decrease performance. The default is **Auto**.

Beacon Interval Enter a value between 1 and 65,535 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Valet to synchronize the wireless network. The default value is **100**.

DTIM Interval This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Valet has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is **1**.

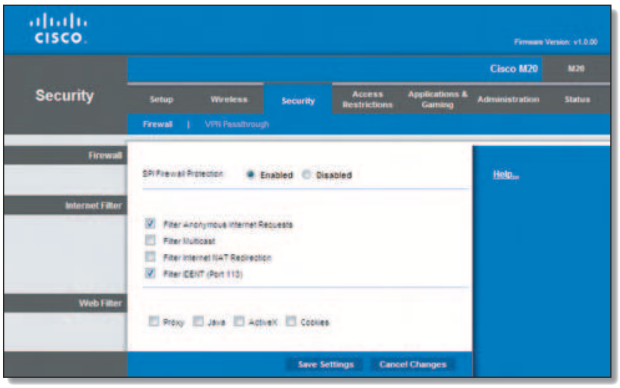
Fragmentation Threshold This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of **2346**.

RTS Threshold Should you encounter inconsistent data flow, only minor reduction of the default value, **2347**, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Valet sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of **2347**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Security > Firewall

The *Firewall* screen is used to configure a firewall that can filter out various types of unwanted traffic on the Valet's local network.



Firewall

SPI Firewall Protection ● Enabled ○ Disabled

Internet Filter

☑ Filter Anonymous Internet Requests
☐ Filter Multicast
☐ Filter Internet NAT Redirection
☑ Filter IDENT (Port 113)

Web Filter

☐ Proxy ☐ Java ☐ ActiveX ☐ Cookies

Security > Firewall

Firewall

SPI Firewall Protection To use firewall protection, keep the default selection, **Enabled**. To turn off firewall protection, select **Disabled**.

Internet Filter

Filter Anonymous Internet Requests This feature makes it more difficult for outside users to work their way into your network. This feature is selected by default. Deselect the feature to allow anonymous Internet requests.

Filter Multicast Multicasting allows for multiple transmissions to specific recipients at the same time. If multicasting is permitted, then the Valet will allow IP multicast packets to be forwarded to the appropriate computers. Select this feature to filter multicasting. This feature is not selected by default.

Filter Internet NAT Redirection This feature uses port forwarding to block access to local servers from local networked computers. Select this feature to filter Internet NAT redirection. It is not selected by default.

Filter IDENT (Port 113) This feature keeps port 113 from being scanned by devices outside of your local network. This feature is selected by default. Deselect this feature to disable it.

Web Filter

Proxy Use of WAN proxy servers may compromise the Gateway's security. Denying Proxy will disable access to any WAN proxy servers. Select this feature to enable proxy filtering. Deselect the feature to allow proxy access.

Java Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language. Select this feature to enable Java filtering. Deselect the feature to allow Java usage.

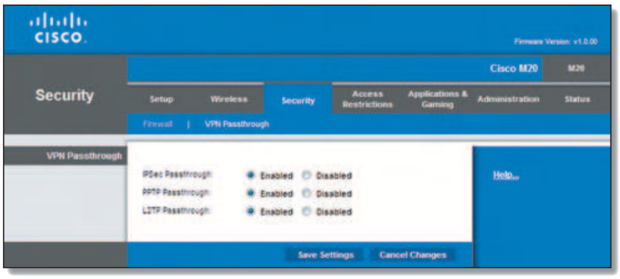
ActiveX ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. Select this feature to enable ActiveX filtering. Deselect the feature to allow ActiveX usage.

Cookies A cookie is data stored on your computer and used by Internet sites when you interact with them. Select this feature to filter cookies. Deselect the feature to allow cookie usage.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Security > VPN Passthrough

The *VPN Passthrough* screen allows you to enable VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Valet's firewall.



IPSec Passthrough: ● Enabled ○ Disabled
PPTP Passthrough: ● Enabled ○ Disabled
L2TP Passthrough: ● Enabled ○ Disabled

Security > VPN Passthrough

VPN Passthrough

IPSec Passthrough Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the Valet, keep the default, **Enabled**.

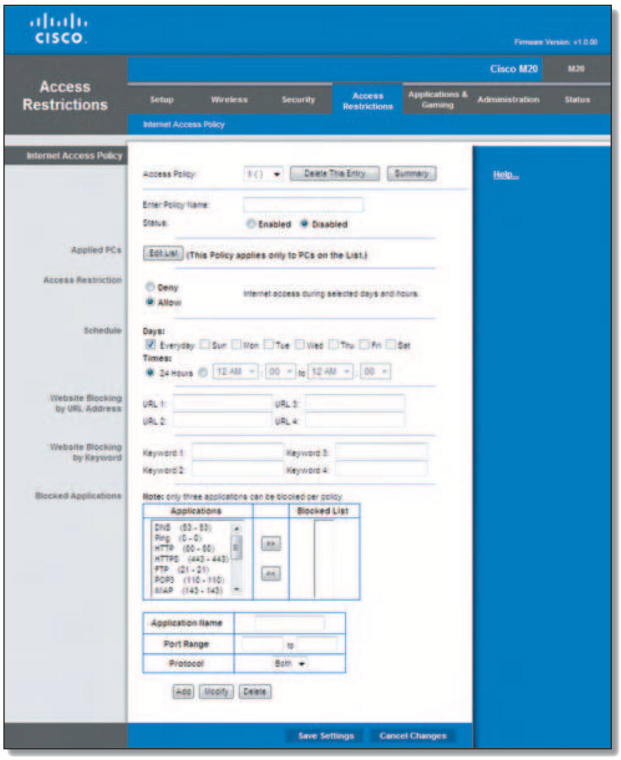
PPTP Passthrough Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Valet, keep the default, **Enabled**.

L2TP Passthrough Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Valet, keep the default, **Enabled**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Access Restrictions > Internet Access Policy

The *Internet Access Policy* screen allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, and websites during specific days and times.



Access Policy: 1 ( ) ▾ [Delete This Entry] [Summary]

Enter Policy Name:

Status: ○ Enabled ● Disabled

Applied PCs: [Edit List] (This Policy applies only to PCs on the List.)

Access Restriction: ○ Deny ● Allow Internet access during selected days and hours.

Schedule: Days: ☑ Everyday ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Times: ● 24 Hours ○ 12 AM ▾ : 00 ▾ to 12 AM ▾ : 00 ▾

Website Blocking by URL Address: URL 1: URL 2: URL 3: URL 4:

Website Blocking by Keyword: Keyword 1: Keyword 2: Keyword 3: Keyword 4:

Blocked Applications: Note: only three applications can be blocked per policy

Applications		Blocked List
DNS (53 - 53) Ping (0 - 0) HTTP (80 - 80) HTTPS (443 - 443) FTP (21 - 21) POP3 (110 - 110) IMAP (143 - 143)	>> <<	

Application Name	
Port Range	to
Protocol	Both ▾

[Add] [Modify] [Delete]

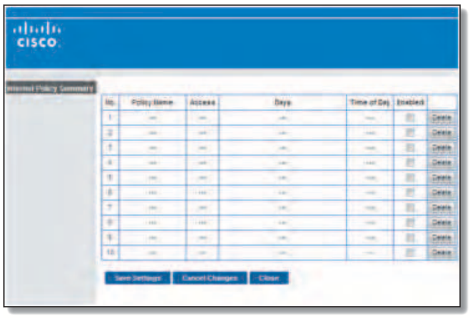
Access Restrictions > Internet Access

Internet Access Policy

Access Policy Access can be managed by a policy. Use the settings on this screen to establish an access policy (after **Save Settings** is clicked). Selecting a policy from the drop-down menu will display that policy's settings. To delete a policy, select that policy's number and click **Delete This Policy**. To view all the policies, click **Summary**.

Summary

The policies are listed with the following information: No., Policy Name, Access, Days, Time, and status (Enabled). To enable a policy, select **Enabled**. To delete a policy, click **Delete**. Click **Save Settings** to save your changes, or click **Cancel Changes** to cancel your changes. To return to the *Internet Access Policy* screen, click **Close**.



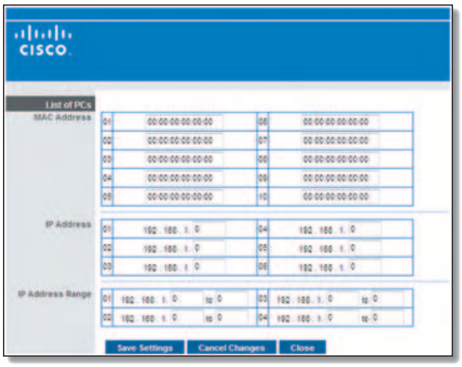
No.	Policy Name	Access	Days	Time of Day	Enabled	
1	--	--	--	--	☐	Delete
2	--	--	--	--	☐	Delete
3	--	--	--	--	☐	Delete
4	--	--	--	--	☐	Delete
5	--	--	--	--	☐	Delete
6	--	--	--	--	☐	Delete
7	--	--	--	--	☐	Delete
8	--	--	--	--	☐	Delete
9	--	--	--	--	☐	Delete
10	--	--	--	--	☐	Delete

Summary

Status Policies are disabled by default. To enable a policy, select the policy number from the drop-down menu, and select **Enabled**.

To create a policy, follow steps 1-11. Repeat these steps to create additional policies, one at a time.

1. Select a number from the *Access Policy* drop-down menu.
2. Enter a Policy Name in the field provided.
3. To enable this policy, select **Enabled**.
4. Click **Edit List** to select which PCs will be affected by the policy. The *List of PCs* screen appears. You can select a PC by MAC address or IP address. You can also enter a range of IP addresses if you want this policy to affect a group of PCs. After making your changes, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Then click **Close**.



MAC Address

01	00:00:00:00:00:00	06	00:00:00:00:00:00
02	00:00:00:00:00:00	07	00:00:00:00:00:00
03	00:00:00:00:00:00	08	00:00:00:00:00:00
04	00:00:00:00:00:00	09	00:00:00:00:00:00
05	00:00:00:00:00:00	10	00:00:00:00:00:00

IP Address

01	192 . 168 . 1 . 0	04	192 . 168 . 1 . 0
02	192 . 168 . 1 . 0	05	192 . 168 . 1 . 0
03	192 . 168 . 1 . 0	06	192 . 168 . 1 . 0

IP Address Range

01	192 . 168 . 1 . 0 to 0	03	192 . 168 . 1 . 0 to 0
02	192 . 168 . 1 . 0 to 0	04	192 . 168 . 1 . 0 to 0

List of PCs

5. Select the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the *List of PCs* screen.
6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.
7. You can block websites with specific URL addresses. Enter each URL in a separate *URL* field.
8. You can also block websites using specific keywords. Enter each keyword in a separate *Keyword* field.