Contents

Chapter 1: Valet ......................................................... 1

Chapter 2: Cisco Connect ................................. 4

Chapter 3: Advanced Configuration ...................... 14

Appendix A: Troubleshooting ............................... 36

Appendix B: Specifications ................................. 37
Chapter 1: Valet

Thank you for choosing a Cisco Valet wireless hotspot. This Quick Reference Guide covers both the Valet and Valet Plus models. Valet will be used as a general reference to both models and all details in this Quick Reference Guide apply to both models unless Valet Plus is noted.

Top

LEDs (1-4) light up once the Valet is connected to a device using a network (Ethernet) cable. The LED flashes when there is activity over that port. **Valet Plus** lights up green when connected to a device at gigabit speed or blue when connected to a device at 10/100 speed.

The **Wi-Fi Protected Setup Button** doesn’t need to be used if you use the Easy Setup Key to connect devices to your network.

If you have client devices, such as wireless adapters, that support Wi-Fi Protected Setup™, then you can use the Wi-Fi Protected Setup button to automatically configure wireless security for your wireless network(s).

To use Wi-Fi Protected Setup, refer to “**Wi-Fi Protected Setup**” on page 21.

The **Power LED** lights up when the Valet is powered on. It is normal for this to flash during startup.

The **Internet LED** lights up when connected to the Internet and flashes to indicate activity. **Valet Plus** lights up green when connected to a device at gigabit speed or blue when connected to a device at 10/100 speed.

The **Wireless LED** lights up when wireless is on. It flashes when the Valet sends or receives data over the wireless network.
The **Internet Port** connects to the network (Ethernet) cable from your Internet connection. In most cases you will be connecting one end of the network cable to the Ethernet port on your cable or DSL modem and the other end to the Internet port on your Valet.

The **Power Port** connects the power adapter.

The **Reset Button** resets the Valet to its factory default settings when held for approximately ten seconds.

**Ethernet Ports** connect the Valet to computers or other devices that have Ethernet ports such as gaming consoles, HDTVs, Blu-ray disc players, or printers using network (Ethernet) cables.

Easy Setup Key

The **Easy Setup Key** is used to install the Cisco Connect software on your computer(s). Be sure to store it in a safe place so that you can add additional computers in the future.
Chapter 1: Valet

Horizontal Placement

The Valet has four rubber feet on its bottom panel. Place the Valet on a level surface near an electrical outlet.

Wall-Mounting Placement

The Valet has two wall-mount slots on its bottom panel. The distance between the slots is 152 mm.

Two screws are needed to mount the Valet.

Suggested Mounting Hardware

| 2.5-3.0 mm | 4-5 mm | 1-1.5 mm |

**NOTE:** Cisco is not responsible for damages incurred by unsecured wall-mounting hardware.

Follow these instructions:

1. Determine where you want to mount the Valet. Make sure that the wall you use is smooth, flat, dry, and sturdy. Also make sure the location is within reach of an electrical outlet.
2. Drill two holes into the wall. Make sure the holes are 152 mm apart.
3. Insert a screw into each hole and leave 3 mm of its head exposed.
4. Position the Valet so the wall-mount slots line up with the two screws.
5. Place the wall-mount slots over the screws and slide the Valet down until the screws fit snugly into the wall-mount slots.

Wall-Mounting Template

Print this page at 100% size.

Cut along the dotted line, and place on the wall to drill precise spacing.
Chapter 2: Cisco Connect

During installation, the setup software installs the Cisco Connect software on your computer. Cisco Connect offers options to connect additional computers or devices to your Valet and allows you to modify the Valet’s settings.

Installation

To install the Valet:

1. Insert the Easy Setup Key into a USB port on your computer.

2. Click Connect to your Cisco Valet.

3. Read the Software End User License Agreement. To accept the agreement and continue with the installation, click Next.

4. The connection steps are displayed.

   a. Plug the power cord into the Power port on the back of the Valet.

Windows XP

a. Go to Start > My Computer and select Easy Setup Key.

b. Double-click Connect.exe.

Mac OS X

a. Double-click the USB drive on your desktop.

b. Double-click Connect.

Windows 7

a. Go to Start > Computer.

b. Double-click Easy Setup Key in the list of available drives.

c. Double-click Connect.exe.

Windows Vista

a. Go to Start > Computer.

b. Double-click Easy Setup Key in the list of available drives.

c. Double-click Connect.exe.
b. Plug the power adapter into an electrical outlet.

![Connect to Electrical Outlet](image1)

6. When you see the Congratulations screen, your computer is connected to the Internet. Remove your Easy Setup Key and keep it in a safe place. You can use it to connect additional computers to your Valet’s local network. Click OK.

![Installation is Complete](image2)

**NOTE:** If you have any trouble during the installation process, refer to the FAQs in the setup software or use a computer with an active Internet connection to visit [www.thevalet.com/support](http://www.thevalet.com/support).

5. Please wait while your Valet is being set up.

![Please Wait](image3)

**NOTE:** You can view detailed connection steps by clicking Show me how in the setup software.

**Main Menu**

The main menu offers four options: Computers and Devices, Parental Controls, Guest Access, and Valet Settings. To select an option, click on it.

![Main Menu](image4)

**Local Access versus Guest Access**

You can connect computers or devices to your Valet by giving them local access (Computers and Devices option) or Guest Access (Guest Access option).

Computers and devices with local access will have access to the Internet and to other devices on your local network, including shared computers and printers which are connected to the Valet. Local access can be given to a wired or wireless device. Refer to “Computers and Other Devices” on page 6 for more information.

![Main Menu](image5)
Guest Access allows you to provide guests visiting your home with Internet access. Your guests will not have access to your other computers or personal data. Provide your guest with the Guest Network name and password. Guest computers must connect to your network using a wireless network connection. Refer to “Main Menu – Guest Access” on page 6 and “Guest Access Settings” on page 11 for more information.

The following diagram shows a typical example of how local access and guest access are used in the same home.

![Guest Access versus Local Access Diagram](image)

**Main Menu – Computers and Devices**

Use this option to connect other computers or devices to your Valet’s local network, one at a time.

**There is(are) x device(s) connected to your Valet** The number of devices connected to the Valet is displayed.

**Add device** To connect another computer or device to the Valet, click Add device and go to “Computers and Other Devices” on page 6.

**Main Menu – Parental Controls**

Parental controls restrict Internet access for up to five computers. For the computers you select, you can block or limit Internet access to specific times. You can also block specific websites.

**Parental controls restrictions are being applied to x device(s)** The number of devices with parental controls restrictions is displayed.

**Change** To enable parental controls or change settings, click Change and go to “Parental Controls” on page 9.

**Main Menu – Guest Access**

The guest network provides Internet access only. To grant Internet access to friends or family, provide the guest network name and password displayed on this screen.

**NOTE:** Guest Access provides Internet access only; it does not provide access to your local network and its resources or your personal information. For example, the guest computer cannot print to a printer on the local network or access files on a computer on the local network. Guest access helps minimize exposure of your local network and your family’s private information.

**Guests can connect to x-guest using the password xyz** When a guest wants Internet access in your home, have the guest do the following:

1. Connect to the wireless guest network, which is the name of your wireless network followed by -guest.
2. Open a web browser.
3. On the login screen, enter the guest access password and click Login.

**Change** To disable guest access or change settings, click Change and go to “Guest Access Settings” on page 11.

**Main Menu – Valet Settings**

Use this option to personalize the Valet’s settings.

**Valet name is x** The name of the Valet is displayed.

**Safe Web Surfing** Displays the on/off status of the Safe Web Surfing option.

**Change** To change settings, click Change and go to “Valet Settings” on page 12.

**Computers and Other Devices**

The computers or devices you connect will have access to the Internet and your local network, including computers or other devices, such as a printer, connected to the Valet. If you have a guest visiting your home, you can provide Internet access only (no access to your local network) through the guest access feature. Refer to “Guest Access Settings” on page 11 for more information.

**Computers and Other Devices**

**Computer** Click this option to connect another computer in your home. Go to “Computer” on page 7.
Wireless printer  Click this option to connect a wireless printer. Go to “Wireless printer” on page 8.

Other devices  Click this option to connect a device that is not a computer, such as a smartphone or game console. Go to “Device” on page 9.

Computer

Your Cisco Valet came with an Easy Setup Key. The Easy Setup Key holds the settings for the Valet. There are three options available when you choose to add a computer.

• Yes, I have an Easy Setup Key  If you already have an Easy Setup Key, select this option. Click Next and go to “Connect with the Easy Setup Key” on page 7.

• No, I don’t have an Easy Setup Key — create a new one now  If you want to create or update an Easy Setup Key, select this option. Click Next and go to “Update or create an Easy Setup Key” on page 7.

• I want to connect manually using my wireless settings  If you want to connect manually (without an Easy Setup Key), select this option. Click Next and go to “Connect without the Easy Setup Key” on page 8.

3. Follow the on-screen instructions to connect that computer to your Valet.

4. Return to the original computer running the Cisco Connect software and enter a name that will be used to identify the device. Click Finish.

Update or create an Easy Setup Key

1. Insert the Easy Setup Key or your own USB flash drive into an available USB port on your computer.

2. Please wait while the settings are copied to the Easy Setup Key.

Connect with the Easy Setup Key

1. Insert the Easy Setup Key into an available USB port on the computer that you want to connect to the Valet.

2. On that computer, click Connect to your Cisco Valet. If you do not see this, open the Easy Setup Key folder and double-click Connect.
3. Remove the Easy Setup Key and click Close. You can now use it to connect other computers to the Valet. Refer to “Connect with the Easy Setup Key” on page 7 to complete the process of adding another computer.

Wireless printer

1. Refer to your printer’s documentation to learn how to connect it to a wireless network.

2. Enter the Network name (SSID), Security Key, and Security Type settings on your wireless device. To print this information, click Print these settings.

3. Enter a name that will be used to identify this device. Then click Finish.

4. Enter a name that will be used to easily identify your printer.
Device

1. Enter the **Network name (SSID)**, **Security Key**, and **Security Type** settings on your wireless device. To print this information, click **Print these settings**.

2. After connecting your device, click **Next**.

3. Enter a name that will be used to identify the device and click **Finish**.

Parental Controls

For the computers you select, you can block or limit Internet access to specific times. You can also block specific websites.

First-Time Access of Parental Controls

1. The first time you access parental controls, you will be asked to create a parental controls password. Complete the following:
   - **Parental controls password** Create a password that protects access to parental controls.
   - **Verify password** Re-enter the password.
   - **Secret question** Create a secret question and answer pair. If you forget the password, you can reset it by correctly answering the secret question. Enter your question.
   - **Answer** Enter the answer to your secret question.

Click **OK** to save your settings.

2. Select the computer that you want to set up parental controls for. Then click **OK**.
3. The Parental controls main screen appears.

You have the following options:

**Restrict Internet access on** The list of computer(s) you have selected for parental controls is displayed. To add, remove, or rename computers on this list, refer to “Restrict Internet Access List” on page 10. To set up parental controls on a computer, refer to “Set Up Parental Controls” on page 10.

**Change parental controls password** Click this option to change the password that protects access to parental controls. Refer to “Change Parental Controls Password” on page 11.

**Restrict Internet Access List**

**Add** If you want to apply parental controls to additional computers, click Add, and the Set up parental controls for screen appears.

Select the computer whose parental controls you want to set up. Then click OK.

**Remove** If there is a computer that should not have parental controls applied, select the computer and click Remove.

**Rename** To give a computer a new name, select the computer and click Rename, and the Rename the device screen appears.

Enter the new name. Then click Rename.

**Set Up Parental Controls**

To set up parental controls for a computer, follow these instructions:

1. Select the computer from the Restrict Internet access on list. (If the computer is not listed, click Add to select the computer.)

2. The Block Internet access option offers the following:
   - **Always** To always block Internet access, select this option.
   - **Specific times** To block Internet access during specific days and times, select this option and set the schedule:
     - **School nights** Select the appropriate start and end times.
     - **Weekends** Select the appropriate start and end times
   - **Never** To never block (always allow) Internet access, keep the default, Never.
3. The *Block sites inappropriate for* option allows you to block websites based on content. The following options are available:
   - **Don’t Block** Does not block any websites.
   - **Teen** Blocks websites that may be inappropriate for teenagers.
   - **Child** Blocks websites that may be inappropriate for children.
4. For the *Block specific sites* option, click **Edit** to create a list of websites you want to block. The default is **None**. If you clicked **Edit**, the *Block these sites* screen appears.

![Block These Sites](image1)

a. On each line, enter a website address that you want to block.
   
   For example, to block http://www.example.com, you would enter `example.com` on a line.

b. Click **Save** to save your settings.

5. On the *Parental controls* screen, click **Finish** to save your settings.

![Blocked Site](image2)

**NOTE:** Repeat steps 1-4 to set up parental controls for different computers.

### Change Parental Controls Password

If you clicked **Change parental controls password**, the *Change your parental controls password* screen appears.

![Change Your Parental Controls Password](image3)

- **Old password** Enter the old password.

- **New password** Enter a new password of 4-32 characters.

- **Verify password** Re-enter the new password.

  Click **Change** to save your setting.

### Blocked Sites

When you attempt to access a website that has been blocked on your computer, you will see a screen telling you that the site has been blocked and the reason it was blocked. You can override the blocking for one hour by entering the parental controls password in the *Password* field and clicking **Unblock**.

### Guest Access Settings

**Allow guest access** By default, **Guest Access** is enabled. To disable **Guest Access**, select **no**.

**Guest network name** By default, the setup software sets up the name of the guest network.

**Password** By default, the setup software sets up the password for the guest network. To change the password, click **Change**.

If you clicked **Change**, the *Change guest password* screen appears.
Easy Setup Key

Update or create key The Easy Setup Key is a USB flash drive that holds the settings for the Valet. To create or update the Easy Setup Key, click Create or update key. For more information, refer to “Update or create an Easy Setup Key” on page 7.

Safe Web Surfing

On/off Safe web surfing alerts you when you are about to visit a potentially harmful website. You can choose whether to visit the site or not. Safe web surfing is enabled by default.

Other Options

Register now to receive special offers and updates To sign up to receive special offers and updates, click this option.

Valet details To view more information about the Valet, click Valet details and go to “Valet Details” on page 13.

Advanced settings To access settings for advanced users, click Advanced settings and go to “Advanced Settings” on page 13.

Click Finish to save your settings.

Change Valet Name or Password

NOTE: When you change the Valet name or password, the name or password of your wireless network also changes, and the Valet is reset. ALL computers and devices connected to your Valet will momentarily lose their Internet connection. Wired computers and devices will reconnect automatically; however, you will need to reconnect all wireless computers and devices using the wireless network's new name or password (for more information, refer to “Computers and Other Devices” on page 6).

If you clicked Change, the Changing Valet name or password screen appears.

1. To change the Valet name or password, click Yes. Otherwise, click No.

Change Valet Name or Password

· Enter a new guest password Enter a password of 4-32 characters.

· Click Change to save your setting.

Total guests allowed By default, 5 guests are allowed Internet access through your guest network. If you want to allow more or less, select the desired number of guests from the drop-down menu; you can select up to 10 guests.

NOTE: Computers that are connected to the local network do not count towards the number of guests allowed.

Click Finish to save your settings.

Valet Settings

Personalize

Valet name The name of your Valet is displayed (this is also the name of your wireless network). To change the name, click Change and go to “Change Valet Name or Password” on page 12.

Password The password that protects access to the Valet’s settings is displayed (this also protects wireless access to your local network). To change the password, click Change and go to “Change Valet Name or Password” on page 12.
2. Complete the following:
   - **Valet name** Enter a name of 1-32 characters.
   - **Password** Enter a password of 8-63 characters.
   - Click **Change** to save your settings.

*Valet Details*

The **Valet details** screen appears, displaying the Model name, Model number, Serial number, Firmware version, Operating system, Software version, Connection type (WAN), IP address (LAN), IP address (WAN), and Computer IP address. (WAN stands for Wide Area Network, such as the Internet. IP stands for Internet Protocol. LAN stands for Local Area Network.)

**Copy** To copy the details to a text file, click **Copy** and follow these instructions:
1. Open a text editor, such as Microsoft Word or Notepad.
2. Go to **Edit > Paste**.
3. Go to **File > Save**.

Click **Close** to return to the **Valet settings** screen.

*Advanced Settings*

If you are an advanced user, you can access the browser-based utility to access the advanced configuration settings of the Valet.

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

**Username** Enter this username to access the browser-based utility.

**Password** Enter this password to access the browser-based utility.

**Copy password** To copy the password to the Clipboard, click this option.

**How to Access Cisco Connect**

**Windows**

To access Cisco Connect, go to **Start > All Programs > Cisco Connect**.

**Mac**

To access Cisco Connect, go to **Go > Applications > Cisco Connect**.
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.

![Windows 7 Login Screen](image)

**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 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**

Then, press **Enter**.

![Setup > Basic Setup](image)

**NOTE:** You can also access the browser-based utility on Windows computers by entering the device name in the Address field. Refer to Device name under “Router IP” on page 16.

A login screen will appear. (Non-Windows 7 users will see a similar screen.)

1. In the **User name** field, enter **admin**.
2. In the **Password** field, enter the password created by 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 “Administration > Management” on page 31.)
3. Click **OK** to continue.

**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 Service 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. (This option usually applies to cable connections.)

Static IP

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

Internet IP Address This is the Valet’s IP address, when seen from the Internet. Enter the IP address provided by your ISP.

Subnet Mask This is the Valet’s Subnet Mask, as seen by users on the Internet (including your ISP). Enter the subnet mask provided by your ISP.

Default Gateway This is the IP address of your ISP’s gateway server. Enter the gateway IP address provided by your ISP.

DNS 1-3 This is the IP address of your ISP’s Domain Name System (DNS) server. Enter the DNS server IP address(es) provided by your ISP.

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.

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 or Keep Alive

Choose one of these options: Connect on Demand or Keep Alive. The default is Keep Alive.

Connect on Demand: Max Idle Time If your Internet connection has been terminated due to inactivity, the Connect on Demand option enables the Valet to automatically reconnect when you attempt to access the Internet again. To use this option, select Connect on Demand. In the Max Idle Time field, enter the duration of inactivity allowed before your Internet connection terminates. The default is 5 minutes.

Keep Alive: Redial Period The Keep Alive option causes the Valet to periodically check your Internet connection and automatically reconnect if the connection is down. To use this option, keep the default, Keep Alive. In the Redial Period field, specify how often the Router should check the Internet connection. The default is 30 seconds.

PPTP

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

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. Enter the IP address provided by your ISP.

• **Subnet Mask**  This is the Valet’s Subnet Mask, as seen by users on the Internet (including your ISP). Enter the subnet mask provided by your ISP.

• **Default Gateway**  This is the IP address of your ISP’s gateway server. Enter the gateway IP address provided by your ISP.

• **DNS 1-3**  This is the IP address of your ISP’s Domain Name System (DNS) server. Enter the DNS server IP address(es) provided by your ISP.

**PPTP Server IP Address**  This is the IP address of the PPTP server. Enter the IP address provided by your ISP.

**Username and Password**  Enter the username and password provided by your ISP.

**Connect on Demand or Keep Alive**  Refer to “Connect on Demand or Keep Alive” on page 15 for details.

**L2TP**

Layer 2 Tunneling Protocol (L2TP) is a service that applies to connections in Israel only.

**Server IP Address**  This is the IP address of the L2TP Server. Enter the IP address provided by your ISP.

**Username and Password**  Enter the username and password provided by your ISP.

**Connect on Demand or Keep Alive**  Refer to “Connect on Demand or Keep Alive” on page 15 for details.

**Telstra Cable**

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

**Server IP Address**  This is the IP address of the Telstra Cable server. Enter the IP address provided by your ISP.

**Username and Password**  Enter the username and password provided by your ISP.

**Connect on Demand or Keep Alive**  Refer to “Connect on Demand or Keep Alive” on page 15 for details.

**Optional Settings**

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

**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.

**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 for your Valet. It offers a selection of subnet masks from a drop-down menu. Most users will not need to change this setting.
Device Name The default is Cisco followed by the last 5 digits of the Router’s serial number, which is found on the bottom of the Valet. If you used the setup software for installation, then the Device Name is the name of your wireless network (up to 15 characters). (The Device name is also the Valet’s NetBIOS name.)

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

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 **DHCP Reservation** 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 whose IP address must always remain the same, such as a media server or print server. To reserve an IP address for a specific device, select it from the list of devices or manually enter the Media Access Control (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.

- **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 is 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 clear your changes. To update the on-screen information, click Refresh. To exit this screen and return to the Basic Setup 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 192.168.1.254. The default Start 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 length of time that a device will be “leased” a dynamic IP address. After the time is up, the device will be automatically assigned a new dynamic IP address, or the lease will be renewed with the same IP address. Enter the length of time, in minutes, that a device will be “leased” a dynamic 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, however, you wish to use a different DNS server, enter its IP address (you can enter up to three DNS server IP addresses). The static DNS server(s) will have higher priority than the ISP’s DNS servers. The Valet will assign the static DNS server(s) to the computers and other devices in your local network.

**WINS** The Windows Internet Naming Service (WINS) manages each computer’s interaction with the Internet. If you use a WINS server, enter its IP Address. Otherwise, leave this field blank.

**Time Settings**

**Time Zone** Select your network’s time zone from this drop-down menu.

**Automatically adjust clock for daylight saving changes** Select this option to have the Router automatically adjust for daylight saving time.

**Reboot**

Click this option to restart your Valet.

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, File Transfer Protocol (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](http://www.dynDNS.org) or [www.TZO.com](http://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**

**Username** Enter the username for your DDNS account.

**Password** Enter the password for your DDNS account.

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

**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 option allows the Mail eXchange (MX) 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. Because it is dynamic, it will change periodically.

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

**Update** To manually trigger an update, click **Update**.

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

E-mail Address, TZO Key, and Domain Name Enter the email address, password, and domain name of the account you set up with TZO.

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

Status The status of the DDNS service connection is displayed.

Update To manually trigger an update, click Update.

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

Setup > MAC Address Clone

A Media Access Control (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 for Internet access. If your computer’s MAC address is registered with your ISP and you do not wish to re-register the MAC address, you may assign the registered MAC address to the Valet with the MAC Address Clone feature.

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 option to clone the MAC address of the computer you are using.

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

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 Network Address Translation (NAT) is disabled, dynamic routing will be available.

Dynamic Routing (RIP)

Dynamic routing uses the Routing Information Protocol (RIP). This option 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.

Enabled/Disabled When NAT is disabled, the Dynamic Routing option is available. To use the Dynamic Routing option, select Enabled.

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 dropdown list. Click Delete This Entry to delete a static route.

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

Destination LAN IP Enter the IP address of the remote network or host to which you want to assign a static route. (LAN stands for Local Area Network.)

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

Gateway Enter the IP address of the gateway server that allows contact between the Valet and the remote network or host.

Interface Select the location of the Destination LAN IP address, the LAN & Wireless (Ethernet and wireless networks) or the Internet (WAN). (WAN stands for Wide Area Network.)

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

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 clear your changes.

Basic Wireless Settings (Manual)

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 clear your changes.
Wi-Fi Protected Setup

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

![Wireless > Basic Wireless Settings (Wi-Fi Protected Setup)](image)

**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.

4. **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.

5. **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.

6. **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: WPA2/WPA Mixed Mode, WPA2 Personal, WPA Personal, WPA2/WPA Enterprise Mixed Mode, WPA2 Enterprise, WPA Enterprise, 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.

### Personal Options

<table>
<thead>
<tr>
<th>Security Option</th>
<th>Strength</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA2 Personal</td>
<td>Strongest</td>
</tr>
<tr>
<td>WPA2/WPA Mixed Mode</td>
<td>WPA2: Strongest WPA: Strong</td>
</tr>
<tr>
<td>WPA Personal</td>
<td>Strong</td>
</tr>
<tr>
<td>WEP</td>
<td>Basic</td>
</tr>
</tbody>
</table>

### Office Options

The office options are available for networks that use a RADIUS server for authentication. The office options are stronger than the personal options because WPA2 or WPA provides encryption while RADIUS provides authentication.

<table>
<thead>
<tr>
<th>Security Option</th>
<th>Strength</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA2 Enterprise</td>
<td>Strongest</td>
</tr>
<tr>
<td>WPA2/WPA Enterprise Mixed Mode</td>
<td>WPA2: Strongest WPA: Strong</td>
</tr>
<tr>
<td>WPA Enterprise</td>
<td>Strong</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Basic</td>
</tr>
</tbody>
</table>
Security Mode
Select the security method for your wireless network: WPA2/WPA Mixed Mode, WPA2 Personal, WPA Personal, WPA2/WPA Enterprise Mixed Mode, WPA2 Enterprise, WPA Enterprise, WEP, RADIUS, or Disabled.

WPA2/WPA Mixed Mode

NOTE: If you select WPA2/WPA Mixed Mode as your Security Mode, each device in your wireless network MUST use WPA2/WPA and the same passphrase.

Passphrase Enter a Passphrase of 8-63 characters. The setup software that you use to install your Valet and set up your wireless network changes the default passphrase. Click Save Settings to apply your changes, or click Cancel Changes to clear your changes.

WPA2 Personal

NOTE: If you select WPA2 Personal as your Security Mode, each device in your wireless network MUST use WPA2 Personal and the same passphrase.

Passphrase Enter a Passphrase of 8-63 characters. The setup software that you use to install your Valet and set up your wireless network changes the default passphrase. Click Save Settings to apply your changes, or click Cancel Changes to clear your changes.

WPA2/WPA Enterprise Mixed Mode

This option features WPA2/WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Valet.)

NOTE: If you select WPA2/WPA Enterprise Mixed Mode as your Security Mode, each device in your wireless network MUST use WPA2/WPA Enterprise and the same shared key.

RADIUS Server Enter the IP address of the RADIUS server.
RADIUS Port Enter the port number of the RADIUS server. The default is 1812.
Shared Key Enter the key shared between the Valet and the server.
Click Save Settings to apply your changes, or click Cancel Changes to clear your changes.
WPA2 Enterprise
This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Valet.)

NOTE: If you select WPA2 Enterprise as your Security Mode, each device in your wireless network MUST use WPA2 Enterprise and the same shared key.

RADIUS Server Enter the IP address of the RADIUS server.
RADIUS Port Enter the port number of the RADIUS server. The default is 1812.
Shared Key Enter the key shared between the Valet and the server.
Click Save Settings to apply your changes, or click Cancel Changes to clear your changes.

WPA Enterprise
This option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Valet.)

NOTE: If you select WPA Enterprise as your Security Mode, each device in your wireless network MUST use WPA Enterprise and the same shared key.

RADIUS Server Enter the IP address of the RADIUS server.
RADIUS Port Enter the port number of the RADIUS server. The default is 1812.
Shared Key Enter the key shared between the Valet and the server.
Click Save Settings to apply your changes, or click Cancel Changes to clear your changes.

Security Mode > WEP

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 clear your changes.
If you choose to disable wireless security, you will be informed that wireless security is disabled when you first attempt to access the Internet. You will be given the option to enable wireless security, or confirm that you understand the risks but still wish to proceed without wireless security.

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.

**NOTE:** When wireless security is disabled, anyone can access your wireless network at any time.
Wireless Client List  Click this to open the Wireless Client List screen.

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 clear 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.

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 clear 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** 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 a 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 clear 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.

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 clear your changes.

Applications and Gaming > Single Port Forwarding

The **Single Port Forwarding** screen allows you to customize port services for common applications on this screen.

When users send these types of requests to your network via the Internet, the Valet will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation feature on the Basic Setup screen, refer to “**DHCP Reservation**” on page 17 for more details).

Single Port Forwarding

Common applications are available for the first five entries. Select the appropriate application. Then enter the IP address of the server that should receive these requests. Select **Enabled** to activate this entry.

For additional applications, complete the following fields:

**Application Name** Enter the name you wish to give the application. Each name can be up to 12 characters.

**External Port** Enter the external port number used by the server or Internet application. Check with the Internet application documentation for more information.

**Internal Port** Enter the internal port number used by the server or Internet application. Check with the Internet application documentation for more information.

**Protocol** Select the protocol used for this application, either **TCP** or **UDP**, or **Both**.

**To IP Address** For each application, enter the IP address of the PC that should receive the requests. If you assigned a static IP address to the PC, then you can click **DHCP Reservation** on the Basic Setup screen to look up its static IP address (refer to “**DHCP Reservation**” on page 17 for more details).

**Enabled** For each application, select **Enabled** to enable port forwarding.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to clear your changes.
Applications and Gaming > Port Range Forwarding

The Port Range Forwarding screen allows you to set up public services on your network, such as web servers, FTP servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.)

When users send these types of requests to your network via the Internet, the Valet will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation feature on the Basic Setup screen, refer to “DHCP Reservation” on page 17 for more details).

If you need to forward all ports to one computer, click the DMZ tab.

Port Range Forwarding

To forward a port, enter the information on each line for the criteria required.

**Application Name** In this field, enter the name you wish to give the application. Each name can be up to 12 characters.

**Start–End Port** Enter the number or range of port(s) used by the server or Internet applications. Check with the Internet application documentation for more information.

**Protocol** Select the protocol used for this application, either TCP or UDP, or Both.

**To IP Address** For each application, enter the IP address of the PC running the specific application. If you assigned a static IP address to the PC, then you can click DHCP Reservation on the Basic Setup screen to look up its static IP address (refer to “DHCP Reservation” on page 17 for more details).

Enabled Select Enabled to enable port forwarding for the applications you have defined.

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

Applications & Gaming > Port Range Triggering

The Port Range Triggering screen allows the Valet to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the Valet, so that when the requested data returns through the Valet, the data is pulled back to the proper computer by way of IP address and port mapping rules.

**Port Range Triggering**

**Application Name** Enter the application name of the trigger.

**Triggered Range** For each application, enter the starting and ending port numbers of the triggered port number range. Check with the Internet application documentation for the port number(s) needed.

**Forwarded Range** For each application, enter the starting and ending port numbers of the forwarded port number range. Check with the Internet application documentation for the port number(s) needed.

Enabled Select Enabled to enable port triggering for the applications you have defined.

Click Save Settings to apply your changes, or click Cancel Changes to clear your changes.
Applications and Gaming > DMZ

The DMZ feature allows one network computer to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Range Forwarding feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet.

DMZ

Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

Enabled/Disabled To disable DMZ hosting, select Disabled. To expose one PC, select Enabled. Then configure the following settings:

Source IP Address If you want any IP address to be the source, select Any IP Address. If you want to specify an IP address or range of IP addresses as the designated source, select and complete the IP address range fields.

Destination If you want to specify the DMZ host by IP address, select IP Address and enter the IP address in the field provided. If you want to specify the DMZ host by MAC address, select MAC Address and enter the MAC address in the field provided. To retrieve this information, click DHCP Client Table.

DHCP Client Table

The DHCP Client Table lists computers and other devices that have been assigned IP addresses by the Valet. The list can be sorted by Client Name, Interface, IP Address, MAC Address, and Expired Time (how much time is left for the current IP address). To select a DHCP client, click Select. To retrieve the most up-to-date information, click Refresh. To exit this screen and return to the DMZ screen, click Close.

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

Applications and Gaming > QoS

Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as videoconferencing.

QoS (Quality of Service)

Wireless

You can configure the WMM Support and No Acknowledgement settings in this section.

WMM Support If you have other devices that support Wi-Fi Multimedia (WMM) on your network, keep the default, Enabled. Otherwise, select Disabled.

No Acknowledgement If you want to disable the Valet’s Acknowledgement feature, so the Valet will not re-send data if an error occurs, then select Enabled. Otherwise, keep the default, Disabled.

Internet Access Priority

In this section, you can set the bandwidth priority for a variety of applications and devices. There are four levels priority: High, Medium, Normal, or Low. When you set priority, do not set all applications to High, because this will defeat the purpose of allocating the available bandwidth. If you want to select below normal bandwidth, select Low.
Depending on the application, a few attempts may be needed to set the appropriate bandwidth priority.

**Enabled/Disabled** To use the QoS policies you have set, select **Enabled**. Otherwise, keep the default **Disabled**.

**Upstream Bandwidth**

**Upstream Bandwidth** This option sets the maximum outgoing bandwidth that applications can use. To allow the Valet to set the maximum, keep the default, **Auto**. To specify the maximum, select **Manual**. Then enter the appropriate value and select **Kbps** or **Mbps**.

**Category**

You can define the Internet access priority level for as many categories as you want. The **Summary** section will display all of the priority selections that you enter. Select from the following categories:

- **Applications** Allows you to assign the bandwidth priority level for a pre-defined application (selected from the list) or add a new application and port settings and then prioritize it.

- **Online Games** Allows you to assign a priority level for a pre-defined game selection that you can select from the list or add the settings for a game that isn’t listed and select the priority level.

- **MAC Address** This option lets you prioritize network traffic based on the device that is accessing the network. For example, if you want your gaming console to have higher priority accessing the Internet than your computer, you can define that here based on their MAC addresses.

- **Voice Device** Voice devices demand a higher level of Internet prioritization. If you have a voice device or devices on your network that you want to prioritize, you can enter their MAC address using this option.

Proceed to the instructions for your selection.

**Applications**

Select the appropriate application. If you select **Add a New Application**, follow the **Add a New Application** instructions.

**Priority** Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

**Add a New Application**

![Add a New Application](image)

**Enter a Name** Enter any name to indicate the name of the entry.

**Port Range** Enter the port range that the application will be using. For example, if you want to allocate bandwidth for FTP, you can enter 21-21. If you need services for an application that uses from 1000 to 1250, you enter 1000-1250 as your settings. You can have up to three ranges to define for this bandwidth allocation. Port numbers can range from 1 to 65535. Check your application’s documentation for details on the service ports used.

Select the protocol **TCP** or **UDP**, or select **Both**.

**Priority** Select the appropriate priority: **High**, **Medium (Recommend)**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

**Online Games**

![Online Games](image)

**Game** Select a game from the drop-down list of pre-defined game settings. If the game that you are playing is not listed, select **Add a New Game**. When you select **Add a New Game**, you will need to enter the name of the game, the port range, and the priority level for the game. Refer to the documentation for the game or the game manufacturer’s website to find the necessary port information.

**Priority** Select the appropriate priority: **High**, **Medium (Recommend)**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.
Chapter 3: Advanced Configuration

MAC Address

![QoS > MAC Address](image)

**Enter a Name**  Enter a name for your device.

**MAC Address**  Enter the MAC address of your device.

**Priority**  Select the appropriate priority: High, Medium (Recommend), Normal, or Low.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

Voice Device

![QoS > Voice Device](image)

**Enter a Name**  Enter a name for your voice device.

**MAC Address**  Enter the MAC address of your voice device.

**Priority**  Select the appropriate priority: High (Recommend), Medium, Normal, or Low.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

Summary

This lists the QoS entries you have created for your applications and devices.

**Priority**  This column displays the bandwidth priority of High, Medium, Normal, or Low.

**Name**  This column displays the application, device, or port name.

**Information**  This column displays the port range or MAC address entered for your entry. If a pre-configured application or game was selected, there will be no valid entry shown in this section.

**Remove**  Click this button to remove an entry.

**Edit**  Click this button to make changes.

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

Administration > Management

The Administration > Management screen allows the network’s administrator to manage specific Valet functions for access and security.

![Administration > Management](image)

Management

**Router Access**

To ensure the Valet’s security, you will be asked for your password when you access the Valet’s browser-based utility. The default is admin.

**Router Password**  Enter a new password for the Valet.

**Re-enter to confirm**  Enter the password again to confirm.

**Web Access**

**Web Utility Access**  HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTPS uses SSL (Secure Socket Layer) to encrypt data transmitted for higher security. Select HTTP or HTTPS. HTTP is the default.

**Web Utility Access via Wireless**  If you are using the Valet in a public domain where you are giving wireless access to your guests, you can disable wireless access to the Valet’s browser-based utility. You will only be able to access the utility via a wired connection if you disable the setting. Keep the default, Enabled, to allow wireless access to the utility, or select Disabled to block wireless access to the utility.

**Remote Access**

**Remote Management**  To permit remote access of the Valet, from outside the local network, select Enabled. Otherwise, keep the default, Disabled.
**Web Utility Access** HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTPS uses SSL (Secure Socket Layer) to encrypt data transmitted for higher security. Select HTTP or HTTPS. HTTP is the default.

**Remote Upgrade** If you want to be able to upgrade the Valet firmware remotely, from outside the local network, select Enabled. (You must have the Remote Management feature enabled as well.) Otherwise, keep the default, Disabled.

**Allowed Remote IP Address** If you want to be able to access the Valet from any external IP address, select Any IP Address. If you want to specify an external IP address or range of IP addresses, then select the second option and complete the fields provided.

**Remote Management Port** Enter the port number that will be open to outside access.

---

### NOTE:
When you are in a remote location and wish to manage the Valet, enter http://<Internet_IP_address>:<port> or https://<Internet_IP_address>:<port>, depending on whether you use HTTP or HTTPS. Enter the Valet’s specific Internet IP address in place of <Internet_IP_address>, and enter the Remote Management Port number in place of the word port.

---

**UPnP**

Universal Plug and Play (UPnP) allows computers to automatically configure the Valet for various Internet applications, such as gaming and videoconferencing.

**UPnP** If you want to use UPnP, keep the default setting, Enabled. Otherwise, select Disabled.

**Allow Users to Configure** Keep the default, Enabled, if you want to be able to make manual changes to the Valet while using the UPnP feature. Otherwise, select Disabled.

**Allow Users to Disable Internet Access** Select Enabled, if you want to be able to prohibit any and all Internet connections. Otherwise, keep the default setting, Disabled.

**Backup and Restore**

**Backup Configurations** To back up the Valet’s configuration settings, click this button and follow the on-screen instructions.

**Restore Configurations** To restore the Valet’s configuration settings, click this button and follow the on-screen instructions. (You must have previously backed up the Valet’s configuration settings.)

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

---

**Administration > Log**

The Valet can keep logs of all traffic for your Internet connection.

---

**Log**

**Log** By default the logging option is Disabled. To monitor traffic between the network and the Internet, select Enabled. With logging enabled, you can choose to view temporary logs.

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

**View Log** To view the logs, click View Log.

---

**Log**

- **Type** Select Incoming Log, Outgoing Log, Security Log, or DHCP Client Log.
- **<Type> Log** The Incoming Log will display a temporary log of the source IP addresses and destination port numbers for the incoming Internet traffic. The Outgoing Log will display a temporary log of the local IP addresses, destination URLs/IP addresses, and service/port numbers for the outgoing Internet traffic. The Security log will display the login information for the browser-based utility. The DHCP Client Log will display the LAN DHCP server status information.

Click Save the Log to save this information to a file on your PC’s hard drive. Click Refresh to update the log. Click Clear to clear all the information that is displayed.
Administration > Diagnostics

The diagnostic tests (Ping and Traceroute) allow you to check the connections of your network devices, including connection to the Internet.

Diagonstics

Ping Test

The Ping test checks the status of a connection.

IP or URL Address  Enter the address of the computer, device, or website whose connection you wish to test.

Packet Size  Enter the packet size you want to use. The default is 32 bytes.

Times to Ping  Enter many times you wish to test it.

Start to Ping  To run the test, click this button. The Ping Test screen will show if the test was successful. Click Close to return to the Diagnostics screen.

Traceroute Test

The Traceroute test tests the performance of a connection.

IP or URL Address  Enter the address of the computer, device, or website whose connection you wish to test.

Start to Traceroute  To run the test, click this button. The Traceroute Test screen will show if the test was successful. Click Close to return to the Diagnostics screen.

Administration > Factory Defaults

The Administration > Factory Defaults screen allows you to restore the Valet’s configuration to its factory default settings.

Factory Defaults

Restore All Settings  To reset the Valet’s settings to the default values, click this button and then follow the on-screen instructions. Any settings you have saved will be lost when the default settings are restored.
Administration > Firmware Upgrade

The **Firmware Upgrade** screen allows you to upgrade the Valet’s firmware. Do not upgrade the firmware unless you are experiencing problems with the Valet or the new firmware has a feature you want to use.

![Administration > Firmware Upgrade](image)

**NOTE:** The Valet may lose the settings you have customized. Before you upgrade its firmware, write down all of your custom settings. After you upgrade its firmware, you may have to re-enter all of your configuration settings.

Firmware Upgrade

Before upgrading the firmware, download the firmware upgrade file specifically for your model from the website, [www.thevalet.com](http://www.thevalet.com).

**Please select a file to upgrade the firmware** Click **Browse** and select the firmware upgrade file.

**Start to Upgrade** After you have selected the appropriate file, click this button, and follow the on-screen instructions.

**WARNING:** Do not interrupt the upgrade process. You should not turn off the power or press the reset button during the upgrade process. Doing so may render the Valet unusable.

---

Status > Router

The **Router** screen displays information about the Valet and its current settings.

![Status > Router](image)

**Router Information**

**Firmware Version** This is the version number of the Valet’s current firmware.

**Firmware Verification** This shows the unique identifier of the firmware.

**Current Time** This shows the time set on the Valet.

**Internet MAC Address** This is the Valet’s MAC Address, as seen by your ISP.

**Host Name** If required by your ISP, this was entered on the **Basic Setup** screen.

**Domain Name** If required by your ISP, this was entered on the **Basic Setup** screen.

**Internet Connection**

This section shows the current network information stored in the Valet. The information varies depending on the Internet connection type selected on the **Basic Setup** screen.

Click **Refresh** to update the on-screen information.
Status > Local Network

The Local Network screen displays information about the local, wired network.

![Status > Local Network](image)

Local Network

**Local MAC Address**  The MAC address of the Valet’s local, wired interface is displayed here.

**Router IP Address**  This shows the Valet’s IP address, as it appears on your local network.

**Subnet Mask**  This shows the Subnet Mask of the Valet.

DHCP Server

**DHCP Server**  The status of the Valet’s DHCP server function is displayed here.

**Start IP Address**  This displays the first available IP address that can be used by devices on your local network.

**End IP Address**  This displays the last available IP address that can be used by devices on your local network.

**DHCP Clients Table**  Click this button to view a list of computers and devices that are using the Valet as a DHCP server.

![DHCP Clients Table](image)

DHCP Client Table

The DHCP Client Table lists computers and other devices that have been assigned IP addresses by the Valet. The list can be sorted by Client Name, Interface, IP Address, MAC Address, and Expired Time (how much time is left for the current IP address). To remove a DHCP client, click **Delete**. To retrieve the most up-to-date information, click **Refresh**. To exit this screen and return to the Local Network screen, click **Close**.

Status > Wireless Network

The Wireless Network screen displays information about your wireless network.

![Status > Wireless](image)

Wireless Network

**MAC Address**  The MAC address of the Valet’s local, wireless interface is displayed here.

**Mode**  Displayed here is the wireless mode used by the network.

**Network Name (SSID)**  Displayed here is the name of the wireless network, which is also called the SSID.

**Channel Width**  Shown here is the Channel Width setting selected on the Basic Wireless Settings screen.

**Channel**  Shown here is the Channel setting selected on the Basic Wireless Settings screen.

**Security**  Displayed here is the wireless security method used by the Valet.

**SSID Broadcast**  Displayed here is the status of the SSID Broadcast feature.
Appendix A: Troubleshooting

Your computer cannot connect to the Internet.

Follow these instructions until your computer can connect to the Internet:

- Verify that the power adapter is connected to the Valet and to a power outlet. If connected to a power strip, make sure the power strip is turned on.
- Make sure that the Power light, Internet light, and Wireless light are on. If you have any wired computers connected to the Valet, make sure the appropriate port light is lit.

**NOTE:** The Power light flashes after the power adapter is plugged in to the Valet. If the light remains flashing for more than 30 seconds, it may indicate the Valet is not working properly. Contact support if you have this problem. The number is listed at the bottom of this page.

- Make sure your DSL or cable modem is connected to the Internet port on the Valet using a network cable.
- Reset all of the devices on your network:
  1. Turn off all of your network computers and devices, and then unplug the power adapter from your Valet.
  2. Unplug your modem’s power cord (and coaxial cable if you have a cable modem), and wait two minutes.
  3. Reconnect your modem’s power cord (and coaxial cable) and wait two more minutes.
  4. Reconnect the power adapter to the Valet, and then power on all of your network computers and devices.

The modem does not have an Ethernet port.

The modem is a dial-up modem for traditional dial-up service. To use the Valet, you need a cable/DSL modem and high-speed Internet connection.

You cannot use the DSL service to connect manually to the Internet.

After you have installed the Valet, it will automatically connect to your Internet Service Provider (ISP), so you no longer need to connect manually.

The DSL telephone line does not fit into the Valet’s Internet port.

The Valet does not replace your modem. You still need your DSL modem in order to use the Valet. Connect the telephone line to the DSL modem, and then insert the Easy Setup Key into your computer. Click Connect and follow the on-screen instructions.

When you double-click the web browser, you are prompted for a username and password. If you want to get rid of the prompt, follow these instructions.

Launch the web browser and perform the following steps (these steps are specific to Internet Explorer but are similar for other browsers):

1. Select Tools > Internet Options.
2. Click the Connections tab.
3. Select Never dial a connection.
4. Click OK.

The Valet does not have a coaxial port for the cable connection.

The Valet does not replace your modem. You still need your cable modem in order to use the Valet. Connect your cable connection to the cable modem, and then insert the Easy Setup Key into your computer. Click Connect and follow the on-screen instructions.

The computer cannot connect wirelessly to the network.

Make sure the wireless network name or SSID is the same on both the computer and the Valet. If you have enabled wireless security, then make sure the same security method and key are used by both the computer and the Valet.

You need to modify the settings on the Valet.

Valet settings can be modified using the Cisco Connect software, refer to “How to Access Cisco Connect” on page 13. To modify the advanced settings, go to Advanced Settings. Refer to “Advanced Settings” on page 13.

In Windows XP, you do not see the Valet in the My Network Places screen.

In the Network Tasks section, click Show icons for networked UPnP devices. If the Valet does not appear, follow these instructions:

1. Go to Start > Control Panel > Firewall.
2. Click the Exceptions tab.
4. Click OK.

Contacting Support

Our award-winning support resources are available 24/7/365. As a Valet owner you can rest easy, knowing that qualified technical support specialists are just a phone call away. **877-500-8070** (US and Canada)
Appendix B: Specifications

Model Name: Valet
Model Description: Wireless-N Hotspot
Model Number: M10
Standards: IEEE 802.11n, 802.11g, 802.11b, 802.3u
Ports: Internet, Fast Ethernet (1-4), Power
Buttons: Reset, Wi-Fi Protected Setup™
LEDs: Power, Internet, Wireless, Wi-Fi Protected Setup™, Ethernet (1-4)
Cabling Type: CAT 5
Antennas: 2 (internal)
Detachable (y/n): No

Transmitted Power
802.11n (40MHz): 13.5 ± 1.5 dBm @ CH6, mcs15
802.11n (20MHz): 15.0 ± 1.5 dBm @ CH6, mcs0-4, mcs8-12
802.11g: 14.5 ± 1.5 dBm
802.11b: 16.5 ± 1.5 dBm

Receive Sensitivity
-91 dBm @ 1 Mbps
-87 dBm @ 11 Mbps
-71 dBm @ 54 Mbps
-66 dBm @ 270 Mbps

Antenna Gain: 1.5 dBi
UPnP able/cert: Able
Wireless Security: Wi-Fi Protected Access™ 2 (WPA2), WEP, Wireless MAC Filtering
Security Key Bits: Up to 128-Bit Encryption

Environmental

Dimensions: 7.95" x 6.3" x 1.34"
(202 x 160 x 34 mm)
Weight: 9.9 oz (0.2806 kg)
Power: 12V, 0.5A
Certification: FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802.11b/g/n), WPA2™, WMM®, Wi-Fi Protected Setup™

Operating Temp.: 32 to 104°F (0 to 40°C)
Storage Temp.: -4 to 140°F (-20 to 60°C)
Operating Humidity: 10 to 80% Noncondensing
Storage Humidity: 5 to 90% Noncondensing

Specifications are subject to change without notice.

Model Name: Valet Plus
Model Description: Wireless-N Hotspot
Model Number: M20
Standards: IEEE 802.11n, 802.11g, 802.11b, 802.3u, 802.3ab
Ports: Internet, Gigabit Ethernet (1-4), Power
Buttons: Reset, Wi-Fi Protected Setup™
LEDs: Power, Internet, Wireless, Wi-Fi Protected Setup™, Ethernet (1-4)
Cabling Type: CAT 5
Antennas: 3 (internal)
Detachable (y/n): No

Transmitted Power
802.11n (40 MHz): 13.0 ± 1.5 dBm @ CH6, 25°C
802.11n (20 MHz): 15.5 ± 1.5 dBm @ CH6, 25°C
802.11g: 16.5 ± 1.5 dBm @ CH6, 25°C
802.11b: 17.5 ± 1.5 dBm @ CH6, 25°C

Receive Sensitivity
-92 dBm @ 1 Mbps
-87 dBm @ 11 Mbps
-71 dBm @ 54 Mbps
-66 dBm @ 270 Mbps

Antenna Gain: 1.5 dBi (antennas one and two)
2.2 dBi (antenna three)
UPnP able/cert: Able
Wireless Security: Wi-Fi Protected Access™ 2 (WPA2), WEP, Wireless MAC Filtering
Security Key Bits: Up to 128-Bit Encryption

Environmental

Dimensions: 7.95" x 6.3" x 1.34"
(202 x 160 x 34 mm)
Weight: 10.9 oz (0.309 kg)
Power: 12V, 1.0A
Certification: FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802.11b/g/n), WPA2™, WMM®, Wi-Fi Protected Setup™

Operating Temp.: 32 to 104°F (0 to 40°C)
Storage Temp.: -4 to 140°F (-20 to 60°C)
Operating Humidity: 10 to 80% Noncondensing
Storage Humidity: 5 to 90% Noncondensing

Specifications are subject to change without notice.