



Your PDF Guides

You can read the recommendations in the user guide, the technical guide or the installation guide for TRENDNET TV-IP422W. You'll find the answers to all your questions on the TRENDNET TV-IP422W in the user manual (information, specifications, safety advice, size, accessories, etc.). Detailed instructions for use are in the User's Guide.

User manual TRENDNET TV-IP422W
User guide TRENDNET TV-IP422W
Operating instructions TRENDNET TV-IP422W
Instructions for use TRENDNET TV-IP422W
Instruction manual TRENDNET TV-IP422W



[You're reading an excerpt. Click here to read official TRENDNET TV-IP422W user guide](http://yourpdfguides.com/dref/3183865)
<http://yourpdfguides.com/dref/3183865>

Manual abstract:

@@@Advanced intuitive software includes motion detection recording, email alerts and scheduled recordings. This camera's brilliant image quality, pan/tilt functionality, day/night recording capabilities and built-in 2-way audio make it ideal for home, small office and business use. Chapter 1 Introduction to Your Camera describes the features of the camera. You will also know the components and functions of the camera. Hardware Installation helps you install the camera according to your application environment. You can use this camera at home, at work, at any where you want. Accessing the Camera lets you start using your camera without problem. The camera can be set up easily and work within your network environment instantly. Configuring the Camera guides you through the configuration of the camera using the Web browser on your PC. SecurView Software using the convenience software to monitor your camera Chapter 2 Chapter 3 Chapter 4 Chapter 5 Chapter 6 Appendix provides the specification of the camera and some useful information for using your camera. NOTE The illustrations and configuration values in this guide are for reference only. The actual settings depend on your practical application of the camera.

-1- Contents P R E F A C E ...

.....
.....

.....
.....
.....

.....
.....
.....

..... 1 CHAPTER 1 ...

.....
.....

.....
.....
.....

.....
.....

..... 4 INTRODUCTION .

.....
.....
.....

.....
.....
.....

.....
.....

. 4 CHAPTER 2

.....
.....
.....
.....

.....
.....
.....

..... 10 HARDWARE INSTALLATION ...

.....
.....

.....
.....
.....
.....

..... 1 0 1.1 1.2 1.3 1.4 2.
1 2.2 2.3 3.1 3.2 3.
3 PACKAGE CONTENTS

.....
.....
.....
.....

.....
.....
.....

4 GETTING TO KNOW YOUR CAMERA

.....
.....
.....

.....5 FEATURES AND BENEFITS..

.....
.....
.....
.....

.....
.....
.....

.....7 SYSTEM REQUIREMENT..

.....
.....
.....
.....

.....
.....
.....
.....

.8 INSTALLING THE WALL MOUNT KIT

.....
.....
.....

.....
.....
.....

10 CONNECTING THE CAMERA TO LAN/WLAN

.....
.....
.....

.....
.....
.....

.11 APPLICATIONS OF THE CAMERA....

.....
.....
.....
.....

.....12 USING IPSETUP

.....
.....
.....

.....
.....
.....
.....

.....

13 ACCESSING TO THE CAMERA

.....
.....
.....
.....
.....

.....18 CONFIGURING THE IP ADDRESS OF THE PC ..

.....
.....
.....

.23 USING THE WEB CONFIGURATION...

.....
.....

.....
.....
.....

.....24 USING SMART WIZARD ...

.....
.....
.....
.....

.....
.....
.....

.....25 BASIC SETUP ...

.....
.....
.....
.....

.....
.....
.....
.....

.29 NETWORK SETTINGS

.....
.....

.....
.....
.....
.....

.....
.....

34 PANTILT SETTINGS

.....
.....
.....
.....
.....
.....
.....

40 SETTING UP VIDEO & AUDIO

.....
.....
.....
.....

...42 EVENT SERVER CONFIGURATION ..

.....
.....
.....
.....
.....

.47 MOTION DETECT.....

.....
.....
.....
.....
.....
.....

51 EVENT CONFIG

.....
.....
.....
.....
.....
.....
.....
.....

.52 TOOLS

.....
.....
.....
.....
.....
.....
.....

...58 USB.

.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
60 INFORMATION

.....
.....

.....
.....
.....
.....

.....
.....

.....
..61 -2- CHAPTER 3

.....
.....
.....
.....

.....
.....
.....
.....

.....
.. 13 ACCESSING THE CAMERA ..

.....
.....

.....
.....
.....
.....

.....
... 13 CHAPTER 4 ..

.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
... 24 CONFIGURING THE CAMERA

.....
.....

.....
.....

.....
.....
.....

2 4 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 4.9 4.
10 4.11 4.12 CHAPTER 5 ...

.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.. 62 SECURVIEW TMS SOFTWARE

.....
.....
.....

.....
.....
.....
.....

... 62 APPENDIX

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

..... 9 3 5.1 INSTALLATION

.....
.....
.....
.....

.....
.....
.....
.....

....62 5.2 USING INSTALLATION

.....
.....
.....

.....
.....
.....
.....

.67 ITEM FEATURES

.....
.....

.....

.....

.....

.....

.....

.....

.....

.....

.68 TO ADD A CAMERA

.....

.....

.....

.....

.....

.....

.....

.....75 TO REMOVE A CAMERA

.....

.....

.....

.....

.....

.....

.....

.....

.....

.78 TO LINK TO THE WEB PAGE OF THE CAMERA....

.....

.....

.....

.....

.....79 TO RECORD VIDEO ..

.....

.....

.....

.....

.....

.....

.....

.....

....80 TO CONFIGURE THE RECORDING SETTINGS .

.....

.....

.....

.....

.....

.....85 TO PLAYBACK THE RECORDED VIDEO ..

.....

.....

.....

.....

.....
.....
...87 TO SET UP MOTION DETECTION OPTIONS .
.....

.....
.....
.....
.....
....88 ACCOUNT

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

..90 OTHER.....

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

....90 INFORMATION

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

....91 A.1 SPECIFICATION

.....
.....
.....
.....
.....
.....
.....
.....

.....93 A.2 GPIO TERMINAL APPLICATION..

.....

Multiple Platforms Supported The camera supports multiple network protocols, including TCP/IP, SMTP e-mail, HTTP, and other Internet related protocols. Therefore, you can use the camera in a mixed operating system environment, such as Windows 2000 and Windows XP and Windows Vista and Windows 7.

Multiple Applications Supported Through the remote access technology, you can use the cameras to monitor various objects and places for your own purposes. For example, babies at home, patients in the hospital, offices and banks, and more. The camera can capture both still images and video clips, so that you can keep the archives and restore them at any time. 1.

4 System Requirement Networking LAN: 10Base-T Ethernet or 100Base-TX Fast Ethernet. WLAN: IEEE 802.11b/g. Accessing the Camera using Web Browser Platform: Microsoft® Windows® 2000/XP/Vista/Windows 7 CPU: Intel Pentium III 800MHz or above RAM: 512MB -8- Resolution: User Interface: 800x600 or above Microsoft® Internet Explorer 6.0 or above Accessing the Camera using SecurView® Platform: Microsoft® Windows® 2000/XP/Vista

Hardware Requirement: 1 camera connected: Intel Pentium III 800MHz; 512MB RAM 2 ~ 4 cameras connected: Intel Pentium 4 1.3GHz; 512MB RAM 5 ~ 8 cameras connected: Intel Pentium 4 2.4GHz; 1GB RAM 9 ~ 16 cameras connected: Intel Pentium 4 3.4GHz; 2GB RAM Resolution: 1024x768 or above NOTE: Monitoring multiple cameras may require a high performance CPU. -9- CHAPTER 2 HARDWARE INSTALLATION 2.1 Installing the Wall Mount Kit The camera comes with a Wall Mount Kit, which allows you to place your camera anywhere by mounting the camera through the three screw holes located in the base of the Wall Mount Kit.

Screw Wall Mount Kit Screw Screw - 10 - 2.2 Connecting the Camera to LAN/WLAN Use the provided Ethernet cable to connect the camera to your local area network (LAN). When you connect the AC power adapter, the camera is powered on automatically. You can verify the power status from the Power LED on the front panel of the camera. Once connects the camera's location and the current date & time. The information can be modified in the Web Configuration. Live View Image Displays the real-time image of the connected camera. - 20 - Move your mouse to the Live View area and click on anywhere, the camera lens will then move to the position where you clicked to display it in the central part of Live View area. When you enlarge the Live View by clicking the Zoom In buttons (2x or 3x), you can move the displayed image by right-clicking your mouse on the Live View area. The position where you rightclicked will be displayed in the central part of Live View area.

Zoom In Buttons Click the buttons to zoom in the live view image by 1x, 2x, and 3x. Nightmode Button Click the button to enable the "nightshot mode" to deliver clearer images in the dark environment. However, this will reduce the frame rate of video setting. Live View/Setup Switch Click Setup to configure the camera. For details, see Chapter 4. Compression Buttons Select to transmit and record the video using MPEG4 or MJPEG compression. Pan/Tilt Buttons Provides the buttons to control the camera lens: Left/Right/Up/Down/Home buttons allow you to move the camera lens position. Clicking the Home button will move the camera lens to the assigned home position. Home Up Left Right Down - 21 - Auto Patrol button controls the camera to automatically scan the preset positions once. Click Stop to stop patrolling.

Click the Number button (1~8) to move the camera lens to the preset position immediately. To set up the preset positions, move the camera lens by clicking the Left/Right/Up/Down buttons to the desired position first, then select the number (1~8) from the pull-down list and click the Apply button. You can enter a descriptive name for the assigned position in the text box to identify it easily. Function Buttons Use these buttons to control the audio, video, and trigger functions. Manual Record allows you to record and save a video clip.

Snapshot allows you to capture and save a still image. Browse allows you to assign the destination folder to store the video clips and still images. Talk allows you to speak out through the camera. Please note only one user is allowed to use this function at a time. Listen allows you to receive the on-site sound and voice from the camera.

Trigger Out allows you to trigger on/off the GPIO output manually. - 22 - 3.3 Configuring the IP Address of the PC If you are failed to access to the camera, please check the IP address of your computer. When you connect the camera to your computer directly to proceed with configuration of the camera, you need to set up the IP addresses to be in the same segment for the two devices to communicate. 1. On your computer, click Start > Control Panel to open the Control Panel window. 2. Double-click Network Connection to open the Network Connection window. 3. Right-click Local Area Connection and then click Properties from the shortcut menu.

4. When the Local Area Connection Properties window appears, select the General tab. 5. Select Internet Protocol [TCP/IP] and then click Properties to bring up the Internet Protocol [TCP/IP] Properties window. 6. To configure a fixed IP address that is within the segment of the camera, select the Use the following IP address option. Then, enter an IP address into the empty field. The suggested IP address is 192.168.xxx.xxx (x is 0~254, please avoid same IP address with your network devices), and the suggested Subnet mask is 255.255.255.0. 7.

When you are finished, click OK. - 23 - CHAPTER 4 CONFIGURING THE CAMERA 4.1 Using the Web Configuration You can access and manage the camera through the Web browser and the provided software application SecurView. This chapter describes the Web Configuration, and guides you through the configuration of the camera by using the Web browser. To configure the camera, click Setup on the main page of Web Configuration.

The Web Configuration will start from the Basic page. The Web Configuration contains the settings that are required for the camera in the left menu bar, including Smart Wizard, Basic, Network, Video/Audio, Event Server, Motion detect, Event Config, Tools, USB, and Information. Enter the desired camera name and location, then click Apply. You can also configure the camera by using the Smart Wizard as describe below. - 24 - 4.2 Using Smart Wizard The camera's Smart Wizard lets you configure your camera easily and quickly. The wizard will guide you through the necessary settings with detailed instructions on each step. To start the wizard, click Smart Wizard in the left menu bar. Step 1. Camera Settings Enter desired Camera Name, Location and Admin Password.

By default, the password is admin. You can also leave the password field blank. It is highly recommend that you enter the new password. Once you have - 25 - changed to new password, please keep a record.



[You're reading an excerpt. Click here to read official TRENDNET TV-IP422W user guide](http://yourpdfguides.com/dref/3183865)
<http://yourpdfguides.com/dref/3183865>

You will need the new password to view or configure the camera later on. Step 2. IP Settings Choose DHCP, Static IP or PPPoE - 26 - Step 3. Email Settings Enter mail server information for sending still image to email account. Step 4. Wireless Networking Enter wireless network information - 27 - Step 5. Confirm Settings Review your setting. Click Apply to save the setting and reboot the camera. Click <Prev to go back to previous setting. Click Cancel to existing the setting without any changes. - 28 - 4.

3 Basic Setup The Basic menu contains three sub-menus that provide the system settings for the camera, such as the Camera Name, Location, Date & Time, and User management. Basic >> System Basic - Camera Name: Enter a descriptive name for the camera. - Location: Enter a descriptive name for the location used by the camera. Indication LED - 29 - This item allows you to set the LED illumination as desired. There are two options: Normal and OFF. Basic >> Date & Time - TimeZone: Select the proper time zone for the region from the pull-down menu. - Synchronize with PC: Select this option and the date & time settings of the camera will be synchronized with the connected computer. - Synchronize with NTP Server: Select this option and the time will be synchronized with the NTP Server. You need to enter the IP address of the server and select the update interval in the following two boxes. - 30 - - Manual: Select this option to set the date and time manually. Basic >> User Administrator To prevent unauthorized access to the camera's Web Configuration, you are strongly recommend to change the default administrator password. Type the administrator password twice to set and confirm the password. General User - 31 - - User Name: Enter the user's name you want to add to use the camera. - Password: Enter the password for the new user. When you are finished, click Add/Modify to add the new user to the camera.

To modify the user's information, select the one you want to modify from UserList and click Add/Modify. - UserList: Display the existing users of the camera.

To delete a user, select the one you want to delete and click Delete. Guest - User Name: Enter the guest's name you want to add to use the camera. - Password: Enter the password for the new guest. - UserList: Display the existing guests of the camera. To delete a user, select the one you want to delete and click Delete. Direct Video Stream Authentication: - Enabled = Direct link to the video stream prompts for authentication. - Disable = Direct link to video does not prompt for authentication for ease of use when implementing or embedding the video stream into a custom application or webpage. Examples of the

Direct Link to video: MPEG4 Mode http://camera_ip_address:port number/mpgview.

htm MJPEG Mode http://camera_ip_address:port number/jpgview.htm - 32 - NOTE The "General User" can access the camera and control the Function buttons of the camera's Web Configuration; the "Guest" can only view the live view image from the main page of the Web Configuration while accessing the camera. Only the "Administrator" is allowed to configure the camera through the Web Configuration. - 33 - 4.4 Network Settings The Network menu contains three sub-menus that provide the network settings for the camera, such as the IP Setting, DDNS Setting, IP Filter, and Wireless network.

Network >> Network IP Setting This item allows you to select the IP address mode and set up the related configuration. The default setting is DHCP mode enabled. - 34 - - DHCP: Select this option when your network uses the DHCP server. When the camera starts up, it will be assigned an IP address from the DHCP server automatically. - Static IP: Select this option to assign the IP address for the camera directly.

You can use IPSetup to obtain the related setting values. IP Subnet Mask Default Gateway Primary/ Secondary DNS Enter the IP address of the camera. The default setting is DHCP. Enter the Subnet Mask of the camera. The default setting is 255.255.255.0. Enter the Default Gateway of the camera. The default setting is your router's LAN IP address.

DNS (Domain Name System) translates domain names into IP addresses. Enter the Primary DNS and Secondary DNS that are provided by ISP. - PPPoE: Select this option when you use a direct connection via the ADSL modem. You should have a PPPoE account from your Internet service provider. Enter the User Name and Password. The camera will get an IP address from the ISP as starting up. NOTE Once the camera get an IP address from the ISP as starting up, it automatically sends a notification email to you. Therefore, when you select PPPoE as your connecting type, you have to set up the email or DDNS configuration in advance. DDNS Setting With the Dynamic DNS feature, you can assign a fixed host and domain name to a dynamic Internet IP address.

Select the Enable option to enable this feature.

Then, select the Provider from the pulldown list and enter the required information in the Host Name, User Name, and Password boxes. Please note that you have to sign up for DDNS service with the service provider first. - 35 - UPnP The camera supports UPnP (Universal Plug and Play), which is a set of computer network protocols that enable the device-to-device interoperability. In addition, it supports port auto mapping function so that you can access the camera if it is behind an NAT router or firewall. Select the Enable option to enable this feature.

Ports Number - HTTP Port: The default HTTP port is 80. - RTSP Port: Configure the transmission of streaming data within the network. The default RTSP (Real Time Streaming Protocol) port is 554. NOTE If the camera is behind an NAT router or firewall, the suggested to be used is from 1024 to 65535. - 36 - Network >> IP Filter The IP Filter setting allows the administrator of the camera to limit the users within a certain range of IP addresses to access the camera.

Start/End IP Address Assign a range of IP addresses that are not allowed to access the camera by entering the Start IP address and End IP address. When you are finished, click Add to save the range setting. You can repeat the action to assign multiple ranges for the camera. For example, when you enter 192.168.10.50 in Start IP Address and 192.168.10.80 in End IP Address, the user whose IP address located within 192.

168.10.50 ~ 192.168.10.80 will not be allowed to access the camera. - 37 - Deny IP List The list displays the range setting(s) of IP addresses that are not allowed to access the camera. To clear the setting, select a range of IP addresses from the list and click Delete. Network >> Wireless Setting The camera supports WLAN while you use the wireless network. Select the Enable option to enable this feature.

- Network ID (SSID): Keep the default setting of this option to connect the camera to any access point under the infrastructure network mode.



[You're reading an excerpt. Click here to read official TRENDNET TV-IP422W user guide](http://yourpdfguides.com/dref/3183865)

<http://yourpdfguides.com/dref/3183865>

To connect the camera to a specified access point, set a SSID for the camera to correspond with the access point's ESS-ID. To connect the camera to an Ad-Hoc wireless workgroup, set the same wireless channel and SSID to match with the computer's configuration. - 38 - Click Site Survey to display the available wireless networks, so that you can easily connect to one of the listed wireless networks. - Wireless Mode: Select the type of wireless communication for the camera: Infrastructure or Ad-Hoc.

- Channel: Select the appropriate channel from the list. - Authentication: Select the authentication method to secure the camera from being used by unauthorized user: Open, Shared-key, WPA-PSK, and WPA2-PSK. The following table explains the four options: Open Shared-key WPA-PSK/ WPA2-PSK The default setting of Authentication mode, which communicates the key across the network. Allow communication only with other devices with identical WEP settings. WPA-PSK/WPA2-PSK is specially designed for the users who do not have access to network authentication servers.

The user has to manually enter the starting password in their access point or gateway, as well as in each PC on the wireless network. If you select Open or Shared-key as the Authentication mode, you need to complete the following settings: Encryption: Select the WEP option to enable the data encryption feature to secure the camera within the wireless network. Format: Once you enable the Encryption feature, you need to determine the encryption format by selecting ASCII or HEX. ASCII format causes each character you type to be interpreted as an eight-bit value. Hex format causes each pair of characters you type to be interpreted as an eight-bit value in hexadecimal (base 16) notation. - 39 - Key Length: Select the WEP key length you use: 64 bits or 128 bits. WEP Key 1/2/3/4: Enter the WEP key(s) in the following boxes. If you select WPA-PSK or WPA2-PSK as the Authentication mode, you need to complete the following settings: Encryption: Select TKIP or AES. TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10,000 packets to insure much greater security than the standard WEP security. AES (Advanced Encryption Standard) is used to ensure the highest degree of security and authenticity for digital information.

Pre-Shared Key: This is used to identify each other in the network. Enter the name in the box, and this name must match the Pre-shared key value in the remote device. 4.5 Pan/Tilt Settings The Pan/Tilt menu allows you to configure the pan/tilt functions of the camera. Pan & Tilt >> Pan & Tilt Settings - 40 - - Pan/Tilt Calibration: Click Calibration to calibrate the position of the camera lens. - Pan Steps: Set the changing range (1~20 degrees) when you click the Left/Right button. - Tilt Steps: Set the changing range (1~20 degrees) when you click the Up/Down button. - Auto Patrol Stay Time: Set the stay time (1~999 seconds) of each preset positions when the camera is patrolling. - 41 - 4.6 Setting up Video & Audio The Video & Audio menu contains three sub-menus that provide the video and audio settings for the camera.

Video & Audio >> Camera Image Setting - Brightness: Adjust the brightness level from 0 ~ 100. - Contrast: Adjust the contrast level from 0 ~ 100. - Saturation: Adjust the colors level from 0 ~ 100. Click Default to restore the default settings of the three options above. - 42 - - Mirror: Select the Horizontal option to mirror the image horizontally.

Select the Vertical option to mirror the image vertically. - Light Frequency: Select the proper frequency according to the camera's location: 50Hz, 60Hz, or Outdoor. Overlay Setting - Includes Date & Time: Select this option to display the date & time stamp on the live view image. - Enable Opaque: Select this option to set a black background to the displayed date & time stamp. - 43 - Video & Audio >> Video MPEG4 - Video Resolution: Select the desired video resolution from the three formats: VGA, QVGA and QQVGA.

The higher setting (VGA) obtains better video quality while it uses more resource within your network. - Video Quality: Select the desired image quality from five levels: Lowest, Low, Medium, High, and Highest. - Frame Rate: Select Auto or a proper setting depending on your network status. - 44 - MJPEG - Video Resolution: Select the desired video resolution from the three formats: VGA, QVGA and QQVGA. The higher setting (VGA) obtains better video quality while it uses more resource within your network. - Video Quality: Select the desired image quality from five levels: Lowest, Low, Medium, High, and Highest. - Frame Rate: Select Auto or a proper setting depending on your network status. NOTE The camera supports both MPEG4 and MJPEG compression. MJPEG capture the images in JPEG format, which require higher bandwidth to view smooth video. The administrator can control the bandwidth of each connection well through the setting options above.

3GPP The camera supports 3GPP specification. Select the Disable option to disable this feature. Otherwise, select 3GPP Without Audio or 3GPP With Audio to transfer the video clips without or with audio. If you use a mobile phone that supports 3GPP, you can also view the real-time streaming image captured by the camera on your phone (with the default player on the phone) by entering the RTSP link: rtsp://(IP address of the camera)/3gp. NOTE Your mobile phone and the service provider must support 3GPP function. Please contact your service provider when you are failed to use this service. - 45 - Video & Audio >>

Audio Camera Microphone In Select the Enable option to enable the camera's audio function, so that you can receive the on-site sound and voice from the camera. Camera Speaker Out Select the Enable option to enable the camera's external speaker function, so that the connected speaker can play the sound and voice through the camera. - Volume: Set the speaker's volume. - 46 - 4.

7 Event Server Configuration The Event Server menu contains three sub-menus that allow you to upload images to FTP, send emails that include still images, and store the images to a NAS system. When you complete the required settings for FTP, Email, or Network Storage, click Test to test the related configuration is correct or not. Once the camera connects to the server successfully, click Apply. Event Server Setting>> FTP - Host Address: Enter the FTP server IP address. - Port Number: Enter the FTP port number.

- User Name: Enter the user name to login into the FTP server. - 47 - - Password: Enter the password to login into the FTP server. - Directory Path: Enter the destination folder for uploading the images. For example, /Test. - Passive Mode: Select the Enable option to enable passive mode.

- 48 - Event Server Setting >> Email - SMTP Server Address: Enter the mail server address.



[You're reading an excerpt. Click here to read official TRENDNET TV-IP422W user guide](http://yourpdfguides.com/dref/3183865)

<http://yourpdfguides.com/dref/3183865>

- Sender Email Address: Enter the email address of the user who will send the email. - Sender User Name: Enter the user name to login the mail server. - Sender Password: Enter the password to login the mail server. - Receiver #1 Email Address: Enter the first email address of the user who will receive the email. - Receiver #2 Email Address: Enter the second email address of the user who will receive the email. - 49 - Event Server Setting >> Network Storage - Samba Server Address: Enter the IP address of the Network Storage server. - Share: Assign the folder on the Network Storage server to share the files to users. - Path: Assign the path for uploading the files on the Network Storage server. For example, /Test/.

- User Name: Enter the user name to login into the Network Storage server. - Password: Enter the password to login into the Network Storage server. @@The camera provides two detecting areas. @@@@Otherwise, leave this option blank to use the default setting.

@@@@@@@@@@@@@@@@@@@@Click Delete to remove the selected time period. @@@@@@@@@@@@@@@@@@NOTE Setting the Prevent/Post-event time for sending email or uploading to FTP may cause the system overloads. - 57 - 4.10 Tools The Tools menu provides the commands that allow you to restart or reset the camera. You can also backup and restore your configuration, and upgrade the firmware for the camera. Factory Reset Click Reset to restore all factory default settings for the camera.

System Reboot Click Reboot to restart the camera just like turning the device off and on. The camera configuration will be retained after rebooting. Configuration - 58 - You can save your camera configuration as a backup file on your computer. Whenever you want to resume the original settings, you can restore them by retrieving the backup file. - Backup: Click Get the backup file to save the current configuration of the camera.

- Restore: Click Browse to locate the backup file and then click Restore. Update Firmware This item displays the current firmware version. You can upgrade the firmware for your camera once you obtained a latest version of firmware. - Select the firmware: Click Browse to locate the backup file (.pck) and then click Update.

NOTE Make sure to keep the camera connected to the power source during the process of upgrading firmware. Otherwise, the camera might be damaged because of failure of upgrading firmware. - 59 - 4.11 USB The USB menu provides the information and controls of the connected USB device. USB Dismount To safely remove the connected USB device, you can press the Unmount button for four seconds on the camera or click Dismount from this item. USB Information Display the Total space and Free space of the USB device. USB Setting - When Disk Full: Select Stop Recording or Recycle Delete Oldest Folder of File when the storage space on the USB device is full. - 60 - NOTE The connected USB storage device can be used to store still images only and as your host system backup. It is not recommended to use the USB device as your major storage device. 4.

12 Information The Information menu displays the current configuration and events log of the camera. Device Info Display the Basic, Video & Audio, Network, and Wireless settings of the camera. System Log The Logs table displays the events log recorded by the system. - 61 - CHAPTER 5 SECURVIEW™ SOFTWARE This Chapter describes detail instructions on operating SecurView™ software, a useful friendly application for ease of control and navigation requirement. 5.1 INSTALLATION 1. Insert the Installation CD-ROM into your computer's CD-ROM drive to initiate the Auto-Run program. 2. Click the SecurView from the Auto-Run menu screen. - 62 - NOTE To use SecurView™, you must have Microsoft .NET Framework 2.0 installed in the computer. The setup wizard will detect it and, if the program is not installed yet, ask you to install it during the process of installing SecurView™. 3. Then SecurView Setup Wizard will appear.

Click "Next" when the Welcome to the SecurView Setup Wizard appears - 63 - 4. Click "Browse" to choose the desired destination location. By default, the destination location is C:\Program Files\TRENDnet\SecurView. Then Click "Next". - 64 - 5.

Click "Next" to confirm the SecurView software to be installed to the computer. - 65 - 6. Click t When the Installation Complete window appears, click "Close". - 66 - 7. After installing the IPSetup utility, the application is automatically installed to your computer, and creates a folder in "Start \Program\TRENDnet\SecurView". 5.2 1. USING INSTALLATION To launch the program, click Start > Program > TRENDnet > SecurView, and then click SecurView™. The main screen will appear as below. - 67 - NOTE Please set the resolution to 1024x768 or above on your computer while using SecurView™; otherwise, the displayed main screen may be distorted.

Item features The following describes the function of each item on the main screen: CONTROLS Panel - 68 - - SETTING: Click to enter the Setting screen of SecurView™. Click again to return to the main screen of SecurView™. - PLAY: Click to play the recorded video file using the media player on the computer (for example, Windows Media Player by default). - LOCK: Click to lock the camera controls. Click again to resume controls for the camera. If you have set ID and Password in SETTING > Account, you will be asked to enter the required information to unlock. - 69 - - ALL RECORD: Click to start recording video clips using ALL connected cameras. To stop recording, please click Record button to stop the individual camera. Please note: stop recording only stop the manual recording camera. For schedule recording, please change the setting on configuration.

TIP By default, the ID and Password boxes are "blank." Click SETTING > Account to change the ID and password of lock/unlock function. - 70 - VIEW SELECTION Panel - View mode buttons: SecurView™ provides multiple view modes, including 1/4/9/16 windows and Full screen mode. - SCAN: When multiple cameras connected, click this button to display the video views between cameras. Click the Scan button again to stop scanning.

- PREV: When multiple cameras connected, click this button to switch the video view to the previous camera. - NEXT: When multiple cameras connected, click this button to switch the video view to the next camera. TIP To set the time interval of scanning, click SETTING > Other and then adjust the time from 1 to 10 seconds in the Time interval of scan option. - 71 - CAMERA Panel - TRIGGER OUT: Click to turn on the trigger out connector of the camera. This button is available only when the connected camera supports the trigger out connector, which is used to control the external device connected to the camera, such as a light.

- SNAPSHOT: Click to capture a still image using the selected camera and save the file in the computer.



[You're reading an excerpt. Click here to read official TRENDNET TV-IP422W user guide](http://yourpdfguides.com/dref/3183865)
<http://yourpdfguides.com/dref/3183865>

- **RECORD**: Click to start recording a video clip using the selected camera. Click again to stop recording and save the file in the computer. - **TALK**: Click to speak out through the camera. Please note only one user is allowed to use this function at the same time. - **LISTEN**: Click to receive the on-site sound and voice from the camera. - **72 - SYSTEM Panel** This panel displays the current date and time. **PAN-TILT CONTROL Panel** When you connect a pan/tilt camera, the system will detect the camera's function automatically and the **PAN-TILT CONTROL** buttons will become functional. Otherwise, these buttons are displayed as gray out buttons. - **Direction/Home buttons**: Click these buttons to adjust the camera's viewing angle to Up () / Down () / Left (Right () / Left-Up () / Left-Down () / Right-Up (Right-Down ().

Click the Home button (position.)/) to return the camera to the default - **SWING**: If you have saved two or more positions for the selected camera, click this button to control the camera swinging from one position to another position. **Video View Window and Camera List - 73 - Video Viewing Window Camera List - Video Viewing Window**: This window displays the video view of the selected camera, which can be divided into 4/9/16 windows according to your selection in **VIEW SELECTION** panel. - **Camera List**: This list displays the information of the connected camera(s). - **74 - To add a camera 1**. Click **SETTING** in the **CONTROLS** panel to display the Setting screen. 2. Click **Add New Camera**. - **75 - 3**. In the pop-up **Add New Camera** dialog window, you can: Select the **Search** tab if you are not sure of the camera's IP address.

Click **Search camera** to search the available camera within the network. Once the camera is found and is shown in the list, select it and click **Add Camera**. Select the **Input** tab to add a camera by entering its IP address directly. Enter the camera's IP address and Port (default: 80), and then click **Add Camera**. - **76 - 4**.

Enter the User name and Password for the camera, and then click **OK**. The connected camera will be displayed in the **Camera List**. 5. Click **SETTING** to return to the **Video View Window**. The video view of the selected camera will be displayed now.

- **77 - To remove a camera 1**. Click **SETTING** in the **CONTROLS** panel to display the Setting screen. 2. Select a camera from the list and click **Delete Camera**. - **78 - Select a camera Delete the camera To link to the Web page of the camera** Click **SETTING > Camera List > Camera Configuration** and then **Link web page** to launch the Web browser that displays live view image and Web Configuration of the selected camera. - **79 - To record video SecurView™ provides three methods to record video clips**: one is to click the **RECORD/All Record** button to record manually; the second is to record by motion detection; the third is to set the recording schedule in **Setting > Recording Configuration > Schedule Recording Configuration**. Manually recording Click **RECORD/All Record** and it starts recording. Click the button again to stop. - **80 - Trigger recording by motion detection** When the motion detection function of the selected camera is enabled, you can configure the camera to start recording triggered by the motion detected. Click **SETTING > Motion Configuration**, and then select the **Recording** option to enable the selected camera to record by motion detection.

- **81 - Schedule recording Configuration** This recording method will work after you have completed the required settings in **Schedule Recording Configuration**. The recording schedule can be defined by **Dates** or **Days**. - **Dates**: Select the camera from the pull-down list.. - **82 - Select a camera Add Schedule - Then, click Add** to set the Start/Stop date and time and then click **OK** to add the recording schedule to the list. - Click **Apply** to save the settings - **83 - 84 - Days**: First, select the camera from the pull-down list and select **Days** tab. Then, select the weekday from the day buttons and then set the time period. Click **Apply** to save the settings. To configure the recording settings To configure the recording settings, including the storage folder and storage options, click **SETTING > Recording Configuration**. - **85 - Recording File Path**: To change the destination folder to save the recorded video file, click **Browse** under the **Recording File Path** box to assign a new folder.

Each Recording File Size: This option allows you to select from 20 to 100 MB so that the video will be recorded as another file automatically when the recording file reaches the specified size limit. **Reserved HDD space for each camera**: This option allows you to set to reserve the storage space on the hard disk drive for the recording of each camera. Before setting the reserve space on the - **86 - hard disk drive**, you can check the available storage space that is displayed in the **HDD Free space** field. **Enable Recycle Recording**: Click on the camera number to clear the files when the unreserved space of the hard disk drive is full. To playback the recorded video The recorded video clips are saved in your computer, and can be played using the media player on the computer, such as **Windows Media Player**.

To start playback, simply click the **PLAY** button on the **CONTROLS** panel, and the following dialog screen will appear, allowing you to select the file to playback. Select the recorded video file under the [camera] path and then click **Open** to launch the media player to playback. - **87 - NOTE** If your player on the computer don't have video codec to playback the recorded video. You can download video codec from <http://www.xvid.org/downloads.15.0.html> to support. To set up motion detection options When the motion detection function of the selected camera is enabled, you can set the **Motion Options** by selecting **Alarm, Recording, Send eMail, and Trigger Out** under **SETTING > Motion Configuration**. **Alarm**: Select **Beep** or **Music** to alert you for the motion detected. When you select **Music**, you can customize the sound by clicking - **88 - Browse** and then selecting your favorite music (*.wav or *.mp3 file) in the computer. **Recording**: Select this option to enable the camera to record by motion detected.

Send Email: Select this option so that the system will be able to send an email to the specified receiver. Once the option is selected, you have to complete the required information in **SETTING > Motion Configuration > Email Configuration**. - **Mail Server**: Enter the mail server address. For example, **mymail.com**. - **89 - Mail From**: Enter the email address of the user who will send the email. For example, **John@mymail.com**. - **Mail To**: Enter the email address of the user who will receive the email. - **User Name**: Enter the user name to login the mail server. - **Password**: Enter the password to login the mail server. - **Subject**: Enter a subject for the notification email. **Trigger Out**: If the selected camera supports **Trigger Out** connector, select this option to enable the **Trigger Out** function.



[You're reading an excerpt. Click here to read official TRENDNET TV-IP422W user guide](http://yourpdfguides.com/dref/3183865)
<http://yourpdfguides.com/dref/3183865>

Account Click **SETTING** > Account to setup the username & password to lock & unlock the main screen of the SecurView. Other Click **SETTING** > Other to setup the scanning time between cameras.

The default setting is 2 seconds. You can set the interval time between 2 ~ 20 seconds. - 90 - Information Click **SETTING** > About to display the information of the software application. - 91 - - 92 - APPENDIX A.1 Specification Image Sensor Sensor Resolution Video Compression Video resolution Audio Input Output Codec User Interface LAN Antenna Reset USB 1/4" color CMOS 640x480 MPEG4/MJPEG VGA/QVGA/QQVGA; 30fps max.

Built-in MIC Headphone output jack (Mono) PCM/AMR (AMR is for 3GPP only) One RJ-45 port One external antenna One Reset button USB 1.1 port, with one unmount button; Power distribution: 500mA Max. Support FAT, FAT32 file system 1 in/1 out connectors Input: active high: 9~40V DC; dropout: 0V DC GPIO - 93 - LEDs Output: close circuit current 70mA AC or 100mA DC maximum, 30 Ohm; open circuit voltage 240V AC or 350V DC maximum Power LED (amber); Link LED (green) System Hardware Processor RAM ROM Power Communication LAN WLAN Protocol support ARM9 base 32MB SDRAM 8MB NOR Flash DC 12V 10/100Mbps Fast Ethernet, auto-sensed, Auto-MDIX IEEE 802.11b/g TCP/IP, UDP, ICMP, DHCP, NTP, DNS, DDNS, SMTP, FTP, Samba, PPPoE, UPnP, Bonjour, RTP, RTSP, RTCP Pan/Tilt Pan Tilt 165 degree (left) to 165 degree (right) 90 degree (up) to 15 degree (down) Software OS Support Windows 2000/XP/Vista Browser Internet Explorer 6.0 or above Apple Safari 2 or above Mozilla Firefox 2.00 or above Software SecurView for playback/recording/ configuration features - 94 - Operating Environment Temperature - Operation: 0°C ~ 45°C - Storage: -15°C ~ 60°C Humidity - Operation: 20% ~ 85% non-condensing - Storage: 0% ~ 90% non-condensing EMI FCC Class B, CE Class B A.2 GPIO Terminal Application Typically used in association with programming scripts for developing applications for motion detection, event triggering, alarm notification via e-mail, and a variety of external control functions. The GPIO connectors are located on the rear panel of the camera, which provide the interface of connecting the sensor device (IN) and controlled device (OUT). Connector Pin Assignment PIN IN OUT SPECIFICATION Active High voltage 9~40V DC; Dropout-out voltage 0V DC Close circuit current 70mA AC or 100mA DC maximum, Output resistance 30 Ohm; Open circuit voltage 240V AC or 350V DC maximum - 95 - Interface Schematic A.3 Glossary of Terms NUMBERS 10BASE-T 100BASE-TX 10BASE-T is Ethernet over UTP Category III, IV, or V unshielded twisted-pair media.

The two-pair twisted-media implementation of 100BASE-T is called 100BASE-TX. A ADPCM Adaptive Differential Pulse Code Modulation, a new technology improved from PCM, which encodes analog sounds to digital form. AMR (Adaptive Multi-Rate) is an audio data compression scheme optimized for speech coding, which is adopted as the standard speech codec by 3GPP. Applets are small Java programs that can be embedded in an HTML page. The rule at the moment is that an applet can only make an Internet connection to the computer form that AMR Applet - 96 - the applet was sent. ASCII American Standard Code For Information Interchange, it is the standard method for encoding characters as 8-bit sequences of binary numbers, allowing a maximum of 256 characters. Address Resolution Protocol. ARP is a protocol that resides at the TCP/IP Internet layer that delivers data on the same network by translating an IP address to a physical address. Audio Video Interleave, it is a Windows platform audio and video file type, a common format for small movies and videos. ARP AVI B BOOTP Bootstrap Protocol is an Internet protocol that can automatically configure a network device in a diskless workstation to give its own IP address.

C Communication Communication has four components: sender, receiver, message, and medium. In networks, devices and application tasks and processes communicate messages to each other over media. They represent the sender and receivers. The data they send is the message. The cabling or transmission method they use is the medium.

In networking, two devices establish a connection to communicate with each other. Connection D DHCP Developed by Microsoft, DHCP (Dynamic Host Configuration Protocol) is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. It also supports a mix of - 97 - static and dynamic IP addresses.

This simplifies the task for network administrators because the software keeps track of IP addresses rather than requiring an administrator to manage the task. A new computer can be added to a network without the hassle of manually assigning it a unique IP address. DHCP allows the specification for the service provided by a router, gateway, or other network device that automatically assigns an IP address to any device that requests one. DNS Domain Name System is an Internet service that translates domain names into IP addresses. Since domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses every time you use a domain name the DNS will translate the name into the corresponding IP address. For example, the domain name www.network_camera.com might translate to 192.167.

222.8. E Enterprise network An enterprise network consists of collections of networks connected to each other over a geographically dispersed area. The enterprise network serves the needs of a widely distributed company and operates the company's missioncritical applications. The most popular LAN communication technology. There are a variety of types of Ethernet, including 10Mbps (traditional Ethernet), 100Mbps (Fast Ethernet), and 1,000Mbps (Gigabit Ethernet). Most Ethernet networks use Category 5 cabling to carry information, in the form of electrical signals, between devices. Ethernet is an implementation of CSMA/CD that operates in a bus or star topology. Ethernet F Fast Ethernet Fast Ethernet, also called 100BASE-T, operates at 10 or 100Mbps per second over UTP, STP, or fiber-optic media. - 98 - Firewall Firewall is considered the first line of defense in protecting private information. For better security, data can be encrypted. A system designed to prevent unauthorized access to or from a private network. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially Intranets all messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.



[You're reading an excerpt. Click here to read official TRENDNET TV-IP422W user guide](http://yourpdfguides.com/dref/3183865)
<http://yourpdfguides.com/dref/3183865>

G Gateway Group A gateway links computers that use different data formats together. Groups consist of several user machines that have similar characteristics such as being in the same department.

H HEX Short for hexadecimal refers to the base-16 number system, which consists of 16 unique symbols: the numbers 0 to 9 and the letters A to F. For example, the decimal number 15 is represented as F in the hexadecimal numbering system. The hexadecimal system is useful because it can represent every byte (8 bits) as two consecutive hexadecimal digits. It is easier for humans to read hexadecimal numbers than binary numbers. I Intranet This is a private network, inside an organization or company that uses the same software you will find on the public Internet.

The only difference is that an Intranet is used for internal usage only. The Internet is a globally linked system of computers that are logically connected based on the Internet Protocol (IP). The Internet provides different ways to access private and public information worldwide. Internet - 99 - Internet address To participate in Internet communications and on Internet Protocol-based networks, a node must have an Internet address that identifies it to the other nodes. All Internet addresses are IP addresses Internet Protocol is the standard that describes the layout of the basic unit of information on the Internet (the packet) and also details the numerical addressing format used to route the information. Your Internet service provider controls the IP address of any device it connects to the Internet. The IP addresses in your network must conform to IP addressing rules. In smaller LANs, most people will allow the DHCP function of a router or gateway to assign the IP addresses on internal networks. IP address is a 32-binary digit number that identifies each sender or receiver of information that is sent in packets across the Internet. For example 80.

80.80.69 is an IP address. When you "call" that number, using any connection methods, you get connected to the computer that "owns" that IP address. ISP (Internet Service Provider) is a company that maintains a network that is linked to the Internet by way of a dedicated communication line. An ISP offers the use of its dedicated communication lines to companies or individuals who can't afford the high monthly cost for a direct connection. Java is a programming language that is specially designed for writing programs that can be safely downloaded to your computer through the Internet without the fear of viruses. It is an object-oriented multi-thread programming best for creating applets and applications for the Internet, Intranet and other complex, distributed network. IP IP address ISP J JAVA L LAN Local Area Network a computer network that spans a relatively small area sharing common resources. Most LANs are confined to a single building or group of buildings.

- 100 - M MJPEG MJPEG (Motion JPEG) composes a moving image by storing each frame of a moving picture sequence in JPEG compression, and then decompressing and displaying each frame at rapid speed to show the moving picture. MPEG4 is designed to enable transmission and reception of high-quality audio and video over the Internet and nextgeneration mobile telephones. MPEG4 N NAT Network Address Translator generally applied by a router that makes many different IP addresses on an internal network appear to the Internet as a single address. For routing messages properly within your network, each device requires a unique IP address. But the addresses may not be valid outside your network.

NAT solves the problem. When devices within your network request information from the Internet, the requests are forwarded to the Internet under the router's IP address. NAT distributes the responses to the proper IP addresses within your network. A network consists of a collection of two or more devices, people, or components that communicate with each other over physical or virtual media. The most common types of network are: LAN (local area network): Computers are in close distance to one another.

They are usually in the same office space, room, or building. WAN (wide area network): The computers are in different geographic locations and are connected by telephone lines or radio waves. NWay Protocol A network protocol that can automatically negotiate the highest possible transmission speed between two devices. Network - 101 - P PCM PING PCM (Pulse Code Modulation) is a technique for converting analog audio signals into digital form for transmission. Packet Internet Groper, a utility used to determine whether a specific IP address is accessible. It functions by sending a packet to the specified address and waits for a reply. It is primarily used to troubleshoot Internet connections. Point-to-Point Protocol over Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as DSL or cable modem. All the users over the Ethernet share a common connection.

Communication on the network is governed by sets of rules called protocols. Protocols provide the guidelines devices use to communicate with each other, and thus they have different functions. Some protocols are responsible for formatting and presenting and presenting data that will be transferred from file server memory to the file server's network adapter Others are responsible for filtering information between networks and forwarding data to its destination. Still other protocols dictate how data is transferred across the medium, and how servers respond to workstation requests and vice versa. Common network protocols responsible for the presentation and formatting of data for a network operating system are the Internetwork Packet Exchange (IPX) protocol or the Internet Protocol (IP). Protocols that dictate the format of data for transfers the medium include token-passing and Carrier Sense Multiple Access with Collision Detection (CSMA/CD), implemented as token-ring, ARCNET, FDDI, or Ethernet. The Router Information Protocol (RIP), a part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, forwards packets from one network to another using the same network protocol. PPPoE Protocol R - 102 - RJ-45 Router RTP RJ-45 connector is used for Ethernet cable connections. A router is the network software or hardware entity charged with routing packets between networks. RTP (Real-time Transport Protocol) is a data transfer protocol defined to deliver live media to the clients at the same time, which defines the transmission of video and audio files in real time for Internet applications.

RTSP (Real-time Streaming Protocol) is the standard used to transmit stored media to the client(s) at the same time, which provides client controls for random access to the content stream. RTSP S Server SIP It is a simple computer that provides resources, such as files or other information.



[You're reading an excerpt. Click here to read official TRENDNET TV-IP422W user guide](http://yourpdfguides.com/dref/3183865)
<http://yourpdfguides.com/dref/3183865>

SIP (Session Initiated Protocol) is a standard protocol that delivers the real-time communication for Voice over IP (VoIP), which establishes sessions for features such as audio and video conferencing. The Simple Mail Transfer Protocol is used for Internet mail. Simple Network Management Protocol. SNMP was designed to provide a common foundation for managing network devices. In LANs, a station consists of a device that can communicate data on the network. In FDDI, a station includes both physical nodes and addressable logical devices. Workstations, single-attach stations, dual-attach stations, and concentrators are FDDI stations. In TCP/IP, the bits used to create the subnet are called the subnet mask.

SMTP SNMP Station Subnet mask T (TCP/IP) Transmission Control Protocol/Internet Protocol is a widely used transport protocol that connects diverse computers of - 103 - various transmission methods. It was developed y the Department of Defense to connect different computer types and led to the development of the Internet. Transceiver A transceiver joins two network segments together. Transceivers can also be used to join a segment that uses one medium to a segment that uses a different medium. On a 10BASE-5 network, the transceiver connects the network adapter or other network device to the medium. Transceivers also can be used on 10BASE-2 or 10BASE-T networks to attach devices with AUI ports. U UDP User Name Utility UTP The User Datagram Protocol is a connectionless protocol that resides above IP in the TCP/IP suite The USERNAME is the unique name assigned to each person who has access to the LAN. It is a program that performs a specific task. Unshielded twisted-pair. UTP is a form of cable used by all access methods.

It consists of several pairs of wires enclosed in an unshielded sheath. W WAN Wide-Area Network. A wide-area network consists of groups of interconnected computers that are separated by a wide distance and communicate with each other via common carrier telecommunication techniques. WEP is widely used as the basic security protocol in Wi-Fi networks, which secures data transmissions using 64-bit or 128-bit encryption. Windows is a graphical user interface for workstations that use DOS. WPA (Wi-Fi Protected Access) is used to improve the security of Wi-Fi networks, replacing the current WEP standard. It uses its own encryption, Temporal Key Integrity Protocol WEP Windows WPA - 104 - (TKIP), to secure data during transmission. WPA2 Wi-Fi Protected Access 2, the latest security specification that provides greater data protection and network access control for Wi-Fi networks. WPA2 uses the government-grade AES encryption algorithm and IEEE 802.1X-based authentication, which are required to secure large corporate networks.

- 105 - Limited Warranty TRENDnet warrants its products against defects in material and workmanship, under normal use and service, for the following lengths of time from the date of purchase. @@@@All products that are replaced become the property of TRENDnet. Replacement products may be new or reconditioned. TRENDnet does not issue refunds or credit. Please contact the point-of-purchase for their return policies.

@@There are no user serviceable parts inside the product. Do not remove or attempt to service the product by any unauthorized - 106 - service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use (iii) the product was subject to conditions more severe than those specified in the manual. Warranty service may be obtained by contacting TRENDnet within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation a Return Material Authorization (RMA) number will be issued.

An RMA number is required in order to initiate warranty service support for all TRENDnet products. Products that are sent to TRENDnet for RMA service must have the RMA number marked on the outside of return packages and sent to TRENDnet prepaid, insured and packaged appropriately for safe shipment.

Customers shipping from outside of the USA and Canada are responsible for return shipping fees. Customers shipping from outside of the USA are responsible for custom charges, including but not limited to, duty, tax, and other fees. WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES - 107 - OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF TRENDNET'S PRODUCTS. TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD. LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY - 108 - FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California. Some TRENDnet products include software code written by third party developers. These codes are subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL"). Go to <http://www.trendnet.com/gpl> or <http://www.trendnet.com> Download section and look for the desired TRENDnet product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. TRENDnet does not provide technical support for these codes.

Please go to <http://www.gnu.org/licenses/gpl.txt> or <http://www.gnu.org/licenses/lgpl.txt> for specific terms of each license. - 109 - - 110 - .



[You're reading an excerpt. Click here to read official TRENDNET TV-IP422W user guide](http://yourpdfguides.com/dref/3183865)
<http://yourpdfguides.com/dref/3183865>