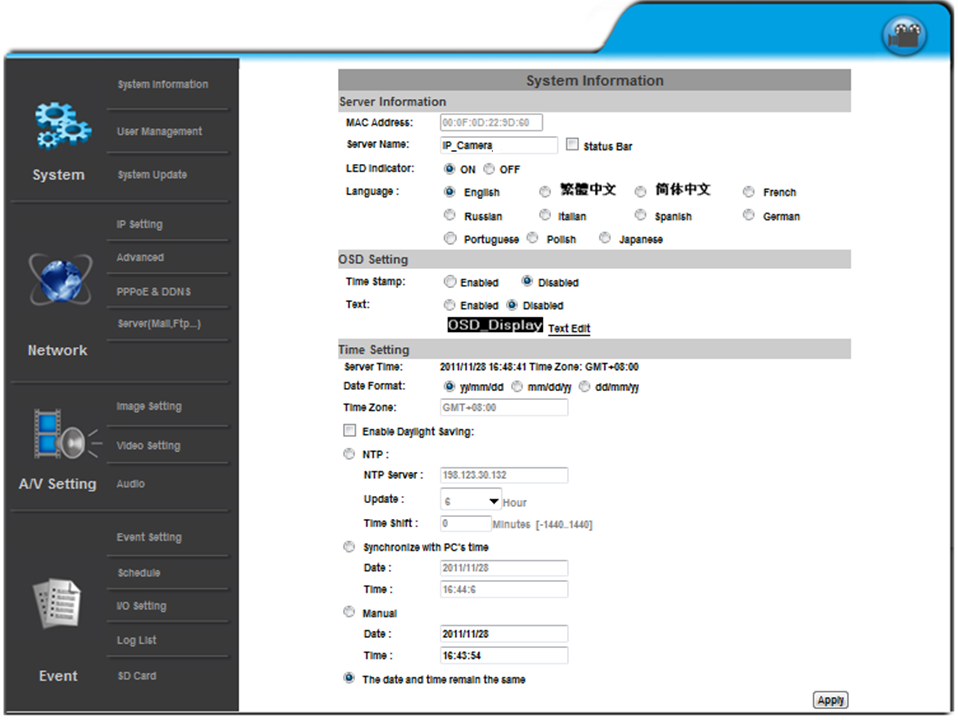


Network

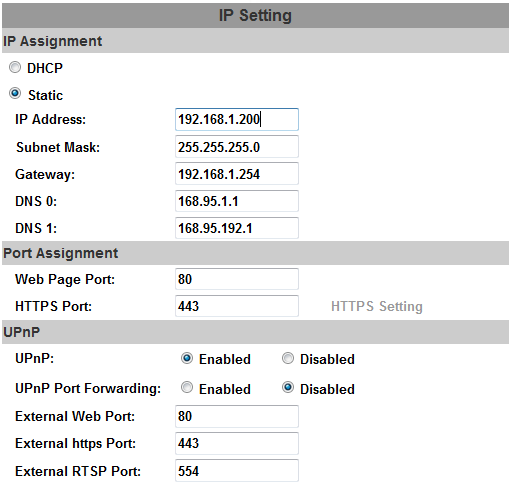
Click 83-003 to get into the administration page. Click 83-007 to go back to the live video page.



1. **IP Settings**

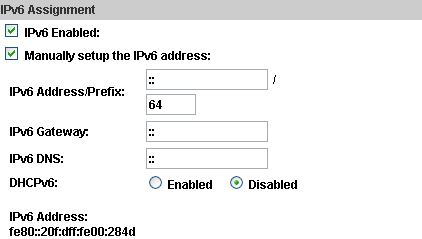
IP Assignment

The IP Camera supports DHCP and static IP.



1. DHCP: The IP Camera will get all the network parameters automatically.
2. Static IP: Type-in the IP address subnet mask, gateway, and DNS.

**IPv6 Assignment**



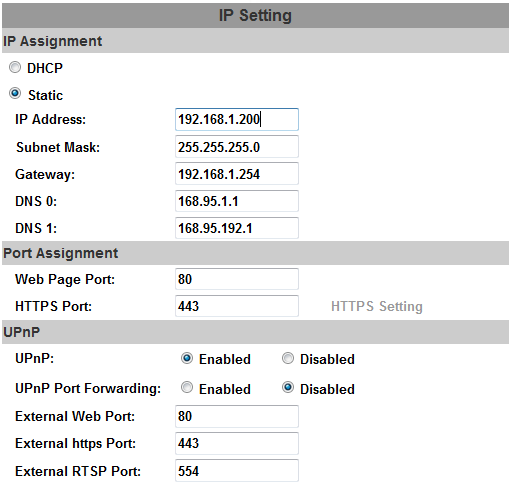
By enabling DHCPv6 you can configure the following IPv6 address settings:

* + - Manually setup the IPv6 address: Key-in the Address, Gateway, and DNS.
    - DHCPv6: If you have a DHCPv6 server, enable it to assign the IPv6 automatically. The assigned IP address will be displayed beside the column.
    - Automatically generated IPv6 Address: Indicates a virtual IPv6 address generated automatically by the IP camera. This virtual IPv6 address cannot be used on WAN.

To use IPv6 address to access the IP camera, open the web browser, and key-in the **[IPv6 address]** in the address bar. The [ ] parentheses mark is necessary.

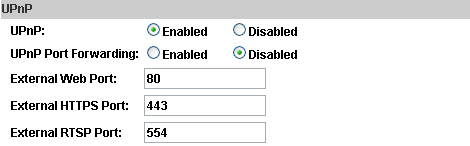


1. Port Assignment: The user might need to assign a different port to avoid conflicts when setting up the IP.



1. Web Page Port: setup the web page connecting port and video transmitting port (Default: 80)
2. HTTPs Port: setup the https port(Default: 443)

**UPnP**



This IP camera supports UPnP, if this service is enabled on your computer, the camera will automatically be detected and a new icon will be added to **My Network Places**.

UPnP Port Forwarding：Enable UPnP Port Forwarding for accessing the IP Camera from the Internet; this option allows the IP Camera to open ports on the router automatically so that video streams can be sent out from a LAN. There are three external ports for being set: **Web Port**, **Http Port** and **RTSP** port. To utilize of this feature, make sure that your router supports **UPnP** and is activated.

***Note:*** *UPnP must be enabled on your computer.*

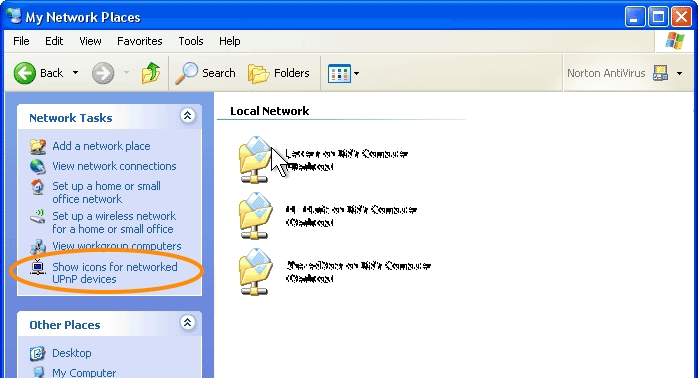
Please follow the procedure to activate UPnP:

<Approach 1>

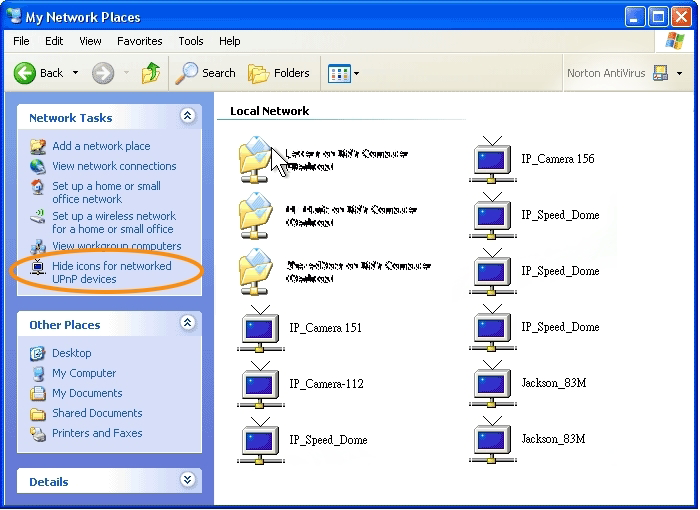
* + - * 1. open the **Control Panel** from the **Start Menu**
        2. Select **Add/Remove Programs**
        3. Select **Add/Remove Windows Components** and open **Networking Services** section
        4. Click **Details** and select **UPnP** to setup the service.
        5. The IP device icon will be added to **My Network Places.**
        6. The user may double click the IP device icon to access IE browser

<Approach 2>

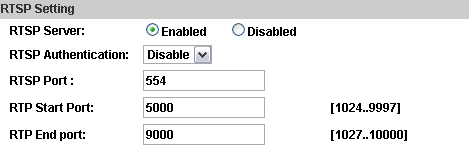
1. Open My **Network Space**
2. Click **Show icons for networked UPnP devices** in the tasks column on the left of the page.
3. Windows might ask your confirmation for enabling the components. Click **Yes**.



1. Now the IP device is displayed under the LAN. Double-click the icon to access the camera via web browser. To disable the UPnP, click **Hide icons for networked UPnP devices** in the tasks column.



**RTSP setting**



If you have a media player that supports RTSP protocol, you can use it to receive video streaming from the IP camera. The RTSP address can be set for two streamings respectively.

1. RTSP Server: enable or disable

**Disable** means everyone who knows your camera IP Address can link to your camera via RTSP. No username and password are required.

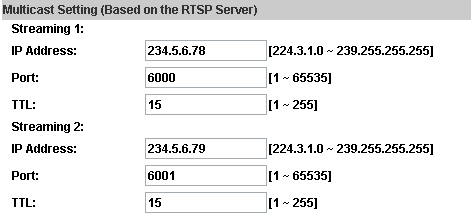
Under **Basic** and **Digest** authentication mode, the camera asks for a username and password before allows access.

The password is transmitted as a clear text under basic mode, which provides a lower level of security than under **digest** mode.

Make sure your media player supports the authentication schemes.

1. RTSP Port: setup port for RTSP transmitting (Default: 554)
2. RTP Start and End Port: in RTSP mode, you can use TCP and UDP for connecting. TCP connection uses RTSP Port (554). UDP connection uses RTP Start and End Port.

Multicast Setting (Based on the RTSP Server)

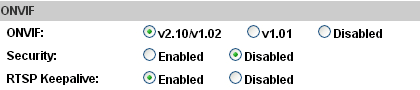


Multicast is a bandwidth conservation technology. This function allows several users to share the same packet sent from the IP camera.

For using Multicast, appoint here an IP Address and port. TTL means the life time of packet, the larger the value is, the more users can receive the packet.

For using Multicast, be sure to enable the function **Force Multicast RTP via RTSP** in your media player. Then key in the RTSP path of your camera: **rtsp ://( IP address)/** to receive the multicast.

**ONVIF**



1. Choose your ONVIF version and settings.

Under ONVIF connection, the video will be transmitted by RTSP. Be sure to enable the RTSP server in IP setting, otherwise the IP Camera will not be able to receive the video via ONVIF.

1. Security

By selecting **Disable**, the username and password are not required for accessing the camera via ONVIF. By selecting **Enable** the username and password are necessary.

1. RTSP Keepalive:

When the function is enabled, the camera checks once in a while if the user who is connected to the camera via ONVIF is still connected. If the connection has been broken the camera will stop transmitting video to the user.

**Bonjour**

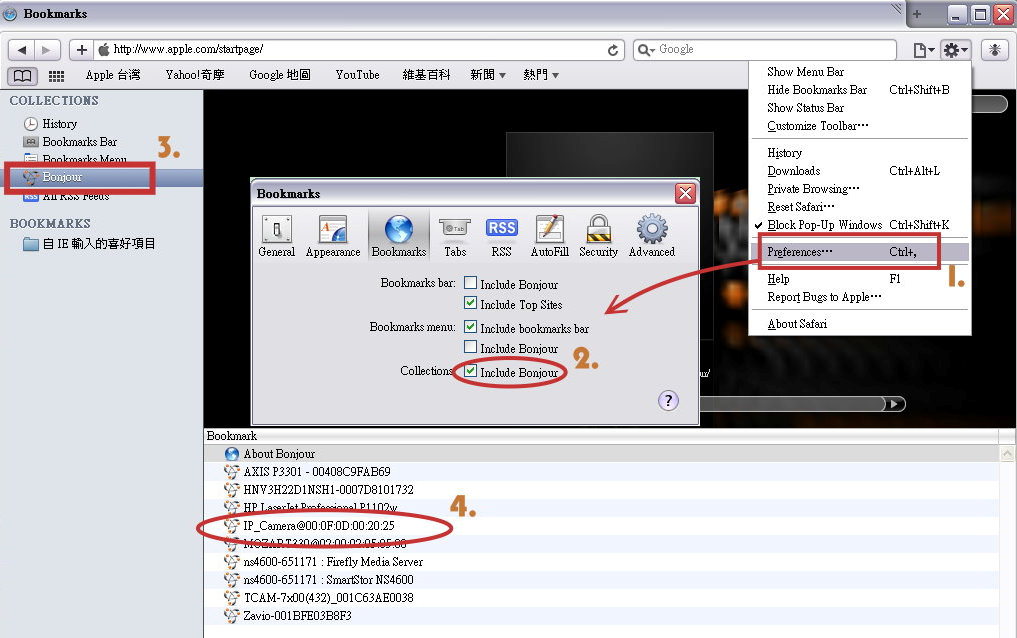


This function allows Apple systems to connect to this IP camera. On **Bonjour Name** key-in the name here.

The web browser **Safari** also has a Bonjour function. Tick **Include Bonjour** in the bookmark setting, for the IP camera to appear under the bonjour category. Click the icon to connect to the IP camera.

The Bonjour function on Safari browser doesn't support HTTPS protocol. If on the camera you select **https**, the camera will appear on Safari's bookmarks but it cannot be accessed.

Take as a reference the following image:



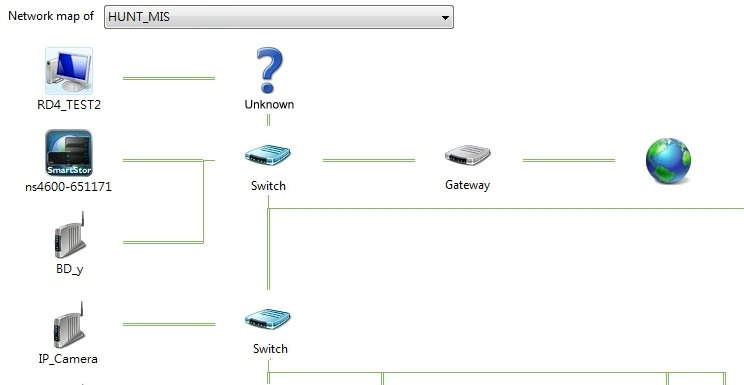
**LLTD**



If your PC supports LLTD, enable this function for allowing checking the connection status, properties, and device location (IP address) in the network map.

If the computer is running Windows Vista or Windows 7, you can find LLTD through the path:

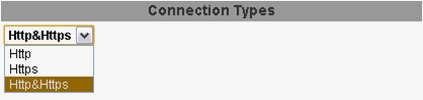
Control Panel → Network and Internet → Network and Sharing Center → Click **See full map**.



1. **Advanced**

**a. Https (Hypertext Transfer Protocol Secure)**

When the users access cameras via Https protocol, the transmitted information will be encrypted, increasing the security level.



Select the connection type:

• Http: the user can access the camera via the Http path but cannot access it via the Https path.

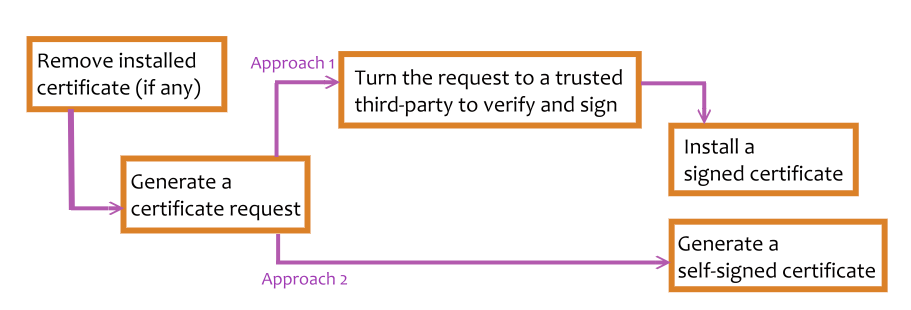
• Https: the user can access the camera via the Https path but cannot access it via the Http path.

• Http & Https: Both the Http and Https path can be used to access the camera. When you change the connection type settings, it may cause connection error or disconnection error if you switch the protocol directly. Therefore, **Http & Https** mode is necessary.

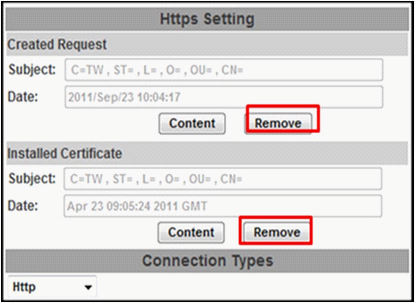
If you want to change from Http to Https, please switch to **Http & Https** mode first, and then switch to **Https** mode and vice versa.

The Https protocol has a verifying mechanism. When the user access a website via Https, the browser will check the certificate of that domain and verify its trustiness and security.

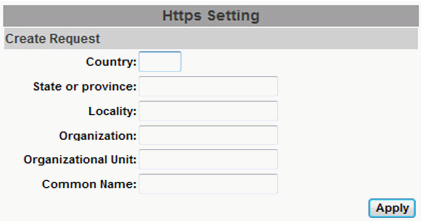
Certificate generation process:



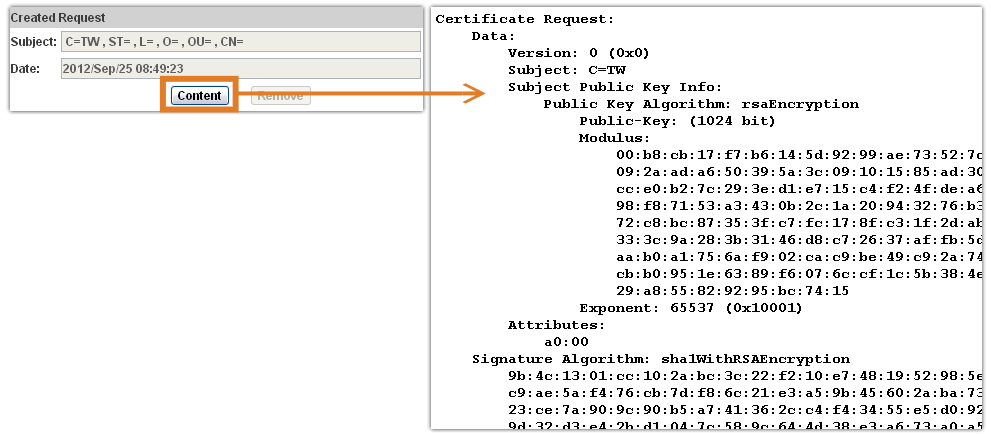
• Remove the existing certificate: Before you generate a new certificate, please remove the installed one. Select the **Http** connection type and click **Remove**. If a dialog box pops up to ask you to confirm, click **Yes**.



• Created Request: Fill-in the following form and click **apply**.



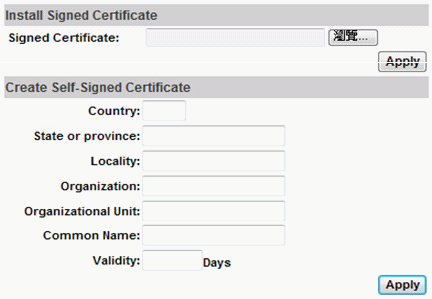
• After generating a certificate request, if you choose to turn it and verified by a trusted third-party, click **Content** and copy all the request content.



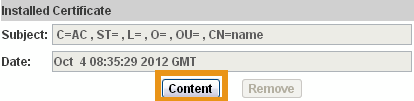
• According to the certificate source, there are two ways to install the certificate:

If you had sent the certificate request for signing and receiving a signed certificate, click **browse** and find the certificate file in your computer. Click **Apply** to install it.

If you choose to generate a self-signed certificate, fill-in the following forms and set the validity day, click **Apply** to finish installed it.



After finishing the installation, click on **Content** to call out and check the certificate content.



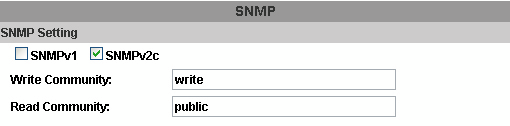
To use Https to access the camera, open your browser, and key-in **https:// (IP address)/** in the address bar. Now your data will be transmitted via encrypted communications. The browser will check your certificate status. It might show the following warning message:



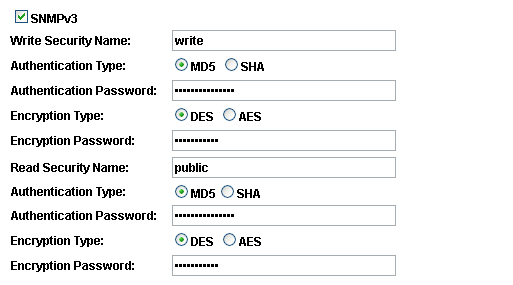
Meaning that certificate is self-signed or signed by a distrusted institution. Click **Proceed anyway** for continuing to the camera page.

**b. SNMP (Simple Network Management Protocol)**

1. **SNMPv1** or **SNMPv2**: write the name of both **Write Community** and **Read Community**.

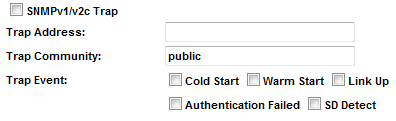


1. **SNMPv3**: Set the Security Name, Authentication Type, Authentication Password, Encryption Type, Encryption Password of Write mode and Read mode.



1. Enable SNMPv1/SNMPv2 Trap for detecting the Trap server.

Please set what event needs to be detected.



• Cold Start: The camera starts up or reboots.

•Setting changed: The SNMP settings have been changed.

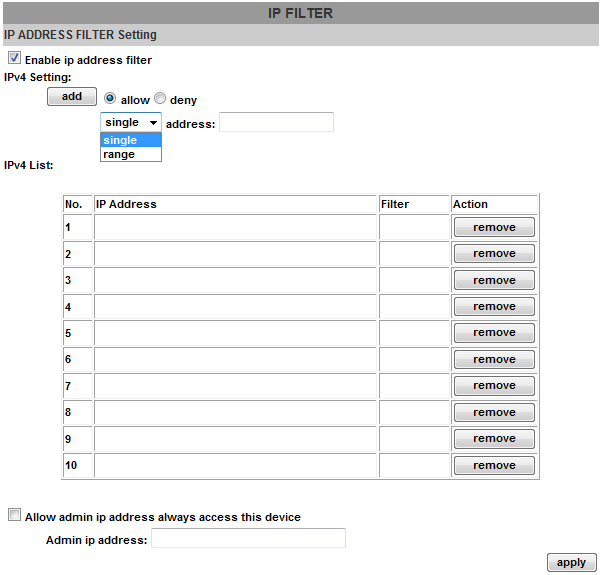
• Network Disconnected: The network connection was broken down (The camera will send trap messages after the network is connected again).

• V3 Authentication Failed: A SNMPv3 user account tries to get authentication but failed. (Due to incorrect password or community)

• SD Insert / Remove: A Micro SD card is inserted or removed.

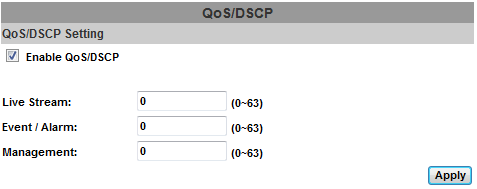
**c. Access list:**

**Enable IP address filter** for setting the IP addresses which allows or denies this camera. There are two options: **single** and **range**.



**d. QoS/DSCP(Quality of Server/Differentiated Services Code-point):**

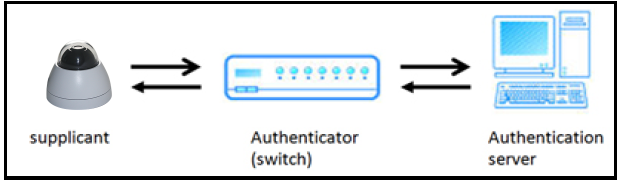
DSCP specifies a simple mechanism for classifying and managing network traffic; and provide QoS on IP networks. DSCP is a 6-bit in the IP header for packet classification purpose. Please define it for **Live Stream**, **Event / Alarm and Management**.



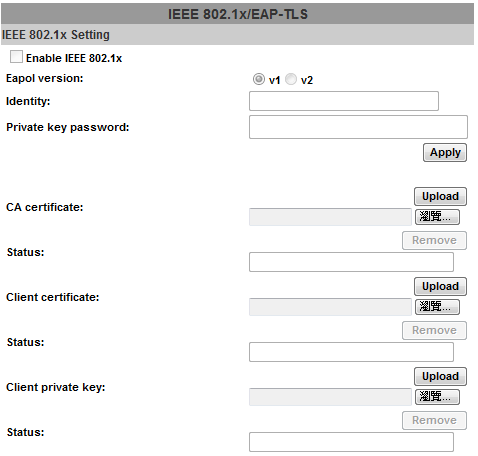
**e. IEEE 802.1x:**

IEEE 802.1x is an IEEE standard for port-based Network Access Control. It provides an authentication mechanism to a device on a LAN or WLAN.

The EAPOL protocol support service identification and optional point to point encryption over the local LAN segment.



Please check what version of the authenticator and authentication server is supported. This camera supports EAP-TLS method. Please enter the ID, password issued by the CA, then upload related certificates.



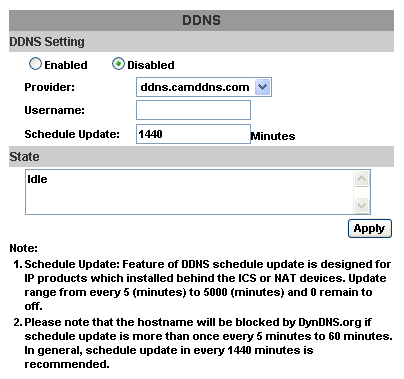
1. **PPPoE & DDNS**



**a. PPPoE:** Select **Enabled** to use PPPoE. Key-in the the Username and password for ADSL connection.

Send mail after dialed: When connected to the internet, the camera will send a mail to a specific mail account.

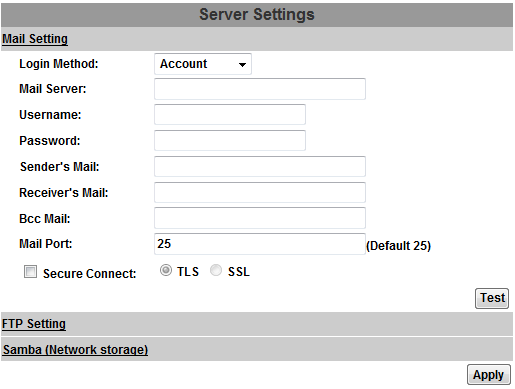
**b. DDNS (camddns example):**



1. Enable this service
2. Key-in the username.
3. IP schedule update. Default: 5 minutes
4. Click **Apply**.
   * + 1. DDNS Status
5. **Updating:** Information update
6. **Idle:** Stop service
7. **DDNS registration successful, can now log by http://<username>.ddns.camddns.com:** Register successfully.
8. **Update Failed, the name is already registered:** The user name has already been used. Please change it.
9. **Update Failed; please check your internet connection:** Network connection failed.
10. **Update Failed, please check the account information you provided:** The server, user name, and password may be wrong.
11. Server settings

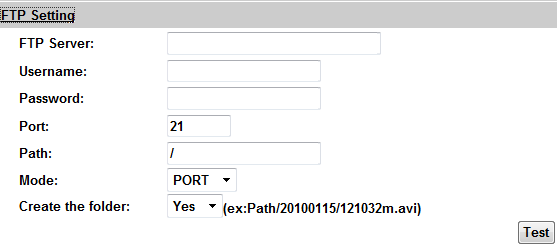
There are three server types available: **Email**, **FTP** and **SAMBA**. Select the item for display detailed configuration options. You can configure either one or all of them.

To send out the video via mail of FTP, please set up the configuration first.



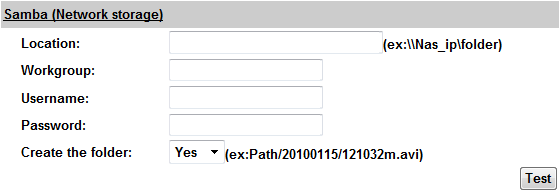
**FTP**

To send out the video via mail of FTP, please set up the configuration.



**Samba**

Select this option to send the media files via a neighbor network when an event is triggered.



Click **Apply** to save the setting, then use **Test** button to test the server connection. A message box will tell you **OK!** if it works, and a test document will be created in the location.

If the test failed, check the sharing setting of your location folder. The folder properties must be **shared** and the permissions must be **Full Control** as the picture.

