Navigation

- System
- Status
- Set-up
- Tools
- Security
- Advanced
  - Disable Advanced Alert
  - Port Mirroring
  - Port Trunking
  - Virtual Cable Tester
  - Advanced Security
    - System Authentica
    - Port-Based Auther
    - Trusted MAC Addre
    - MAC Address Lock
  - Advanced Tools
  - Traffic Management
  - VLANS
  - Spanning Tree
  - MAC

Advanced > Advanced Security > Port-Based Authentication

RADIUS Server IP Address: 192.168.0.1

RADIUS Shared Secret:

802.1x Port-Based Authentication Setting:
The Port-Based Authentication setting enables you to authenticate each port before making available any services offered by the switch. After authentication is successful, normal traffic can pass through the port. The default setting is Force **Authorized** (disabled 802.1x function). The user can also choose Force **Unauthorized** (deny client to access network) or **Auto** Detected. The **Reauthentication Timer** allows the user to specify the time interval between the authentication server's checks of users connected to the network. The default time interval is 3600 seconds. This field will take effect when the Authentication mode is Auto.
Note: The RADIUS server IP address and Shared Secret must be configured first before enabling 802.1x. The 802.1x RADIUS server's connected port must be configured as **"Authorized"** only. Otherwise 802.1x won't take effect.

Re-authentication Timer: 3600 (1 - 65535 seconds)

Port	Authentication	Port	Authentication	Port	Authentication	Port	Authentication
1	Authorized	2	Authorized	3	Authorized	4	Authorized
5	Authorized	6	Authorized	7	Authorized	8	Authorized
9	Authorized	10	Authorized	11	Authorized	12	Authorized
13	Authorized	14	Authorized	15	Authorized	16	Authorized
17	Authorized	18	Authorized	19	Authorized	20	Authorized
21	Authorized	22	Authorized	23	Authorized	24	Authorized