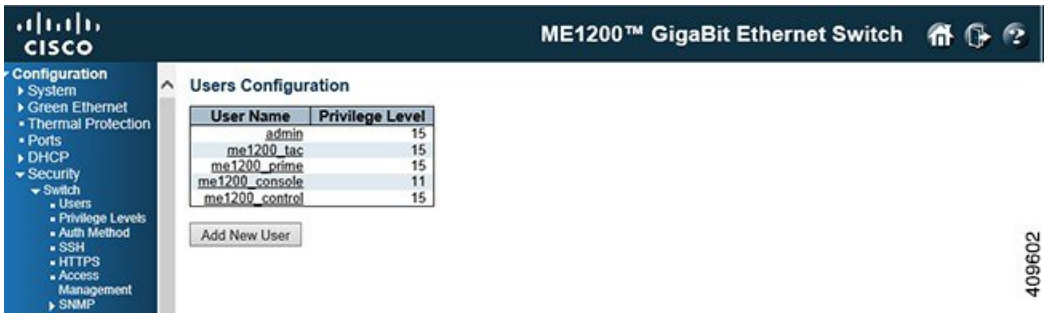
Configuring Security

The Security feature available on the ME 1200 Web GUI allows you to set the security configurations for the ME 1200.

Switch

Users Configuration

This option provides an overview of the current users. Currently, the only way to log in as another user on the web server is to close and reopen the browser.



The displayed values for each user are:

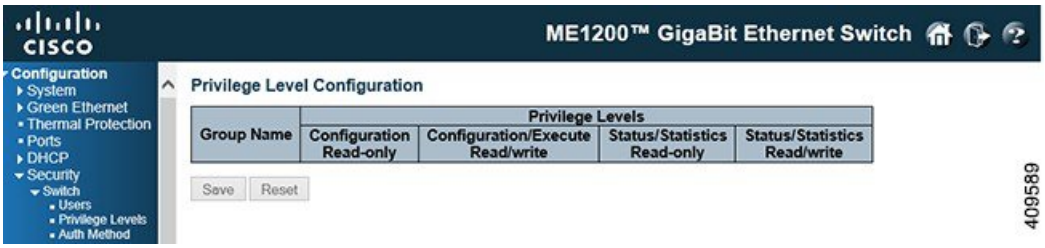
- **User Name**: The name identifying the user. This is also a link to edit a user.
- **Privilege Level**: The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, that is, that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software

upload, factory defaults, and so on) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

- **Add New User**: Click this button to add a new user.

Privilege Levels Configuration

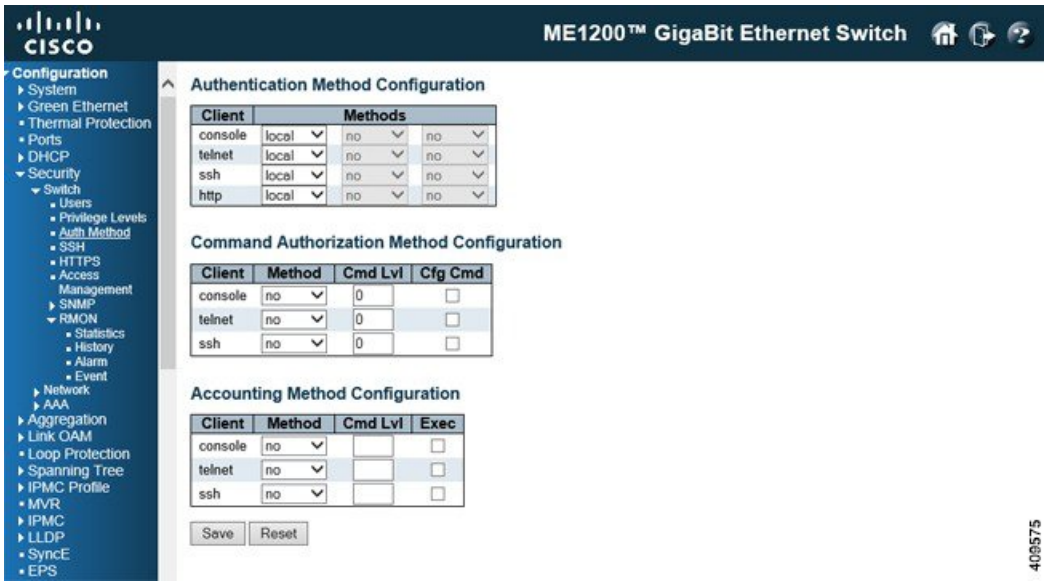
This option provides an overview of the privilege levels configuration.



- **Group Name**: The name identifying the privilege group. In most cases, a privilege level group consists of a single module (for example, LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details:
  - *System*: Contact, Name, Location, Timezone, Daylight Saving Time, Log.
  - *Security*: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.
  - *IP*: Everything except **ping**.
  - *Port*: Everything except **VeriPHY**.
  - *Diagnostics*: 'ping' and **VeriPHY**.
  - *Maintenance*: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.
  - *Debug*: Only present in CLI.
- **Privilege Levels**: Every group has an authorization Privilege level for the following sub groups: *configuration read-only*, *configuration/execute read-write*, *status/statistics read-only*, *status/statistics read-write* (for example, for clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

Authentication Method Configuration

This option allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.



The table has one row for each client type and a number of columns which are as follows:

- **Client**: The management client for which the configuration below applies.
- **Methods**: Method can be set to one of the following values:
  - *no*: Authentication is disabled and login is not possible.
  - *local*: Uses the local user database on the switch for authentication.
  - *radius*: Uses one or more of the remote RADIUS servers for authentication.
  - *tacacs*: Uses one or more of the remote TACACS+ servers for authentication.

  Methods that involves remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as **local**. This will enable the management client to log in via the local user database if none of the configured authentication servers are alive.

Command Authorization Method Configuration

The command authorization section allows you to limit the CLI commands available to a user. The table has one row for each client type and a number of columns which are as follows:

- **Client**: The management client for which the configuration below applies.
- **Method**: This can be set to one of the following values:
  - *no*: Command authorization is disabled. User is granted access to CLI commands according to his privilege level.
  - *tacacs*: Uses one or more of the remote TACACS+ servers for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.

- **Cmd Lvl**: Authorizes all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15.
- **Cfg Cmd**: Also, authorizes configuration commands.

Accounting Method Configuration

The accounting section allows you to configure command and exec (login) accounting. The table has one row for each client type and a number of columns which are as follows:

- **Client**: The management client for which the configuration below applies.
- **Method**: can be set to one of the following values:
  - *no*: Accounting is disabled.
  - *tacacs*: Uses one or more of the remote TACACS+ servers for accounting.
- **Cmd Lvl**: Enables accounting of all commands with a privilege level higher than or equal to this level.Valid values are in the range 0 to 15. Leave the field empty to disable command accounting.
- **Exec**: Enables exec (login) accounting.

SSH Configuration

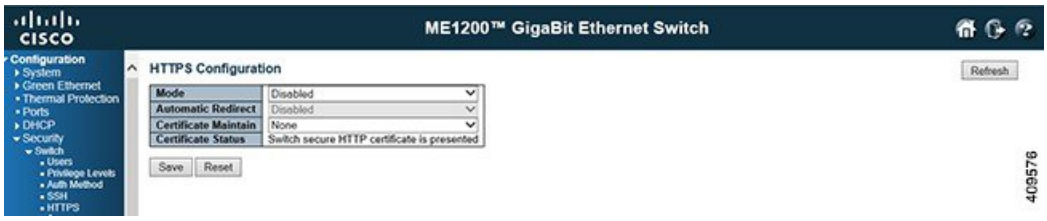
This option allows you to configure SSH.

The **Mode** option indicates the SSH mode operation. Possible modes are:

- *Enabled*: Enables SSH mode operation.
- *Disabled*: Disables SSH mode operation.

HTTPS Configuration

This option allows you to configure HTTPS.



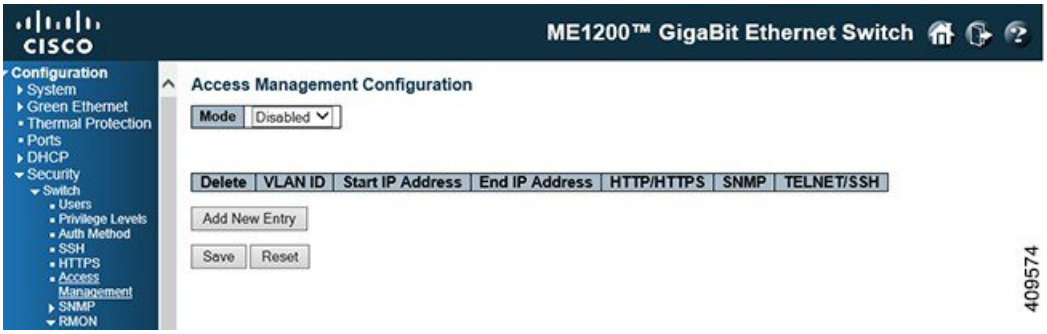
- **Mode**: Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. Possible modes are:
  - *Enabled*: Enables HTTPS mode operation.
  - *Disabled*: Disables HTTPS mode operation.
- **Automatic Redirect**: Indicates the HTTPS redirect mode operation. It is only significant if HTTPS mode *Enabled* is selected. Automatically redirects web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled.

  The browser may not allow the redirect operation due to the security consideration unless the switch certificate is trusted to the browser. Initialize the HTTPS connection manually under this case. Possible modes are:
  - *Enabled*: Enables HTTPS redirect mode operation.
  - *Disabled*: Disables HTTPS redirect mode operation.
- **Certificate Maintain**: This field only can be configured when HTTPS is disabled. It is used to maintain the certification. Possible actions are:
  - *None*: No action for certification.
  - *Delete*: To delete certification.
  - *Upload*: To upload certification, there are two types of upload methods that can be selected: Web Browser or URL.
  - *Generate*: To generate certification.
- **Certificate Algorithm**: HTTPS can generate two types of certification. Possible types are:
  - *RSA*: RSA certification.
  - *DSA*: DSA certification.
- **PassPhrase**: The pattern is used for encrypting the certification.
- **Certificate Upload**: Possible modes are:
  - *Web Browser*: To Upload certification via Web browser.
  - *URL*: To Upload certification via URL, the supported protocols are HTTP, TFTP and FTP, the URL format is **<protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]**

- **Certificate Status**: Possible status is:
  - *Switch secure HTTP certificate is presented*: The certification is stored in HTTPS' database.
  - *Switch secure HTTP certificate is not presented*: No certification is stored in HTTPS' database.
  - *Switch secure HTTP certificate is generating*: The certification is generating.

Access Management Configuration

This option allows you to configure access management. The maximum number of entries is 16. If the type of the application matches any one of the access management entries, it allows access to the switch.



- **Mode**: Indicates the access management mode operation. Possible modes are:
  - *Enabled*: Enables access management mode operation.
  - *Disabled*: Disables access management mode operation.

- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **VLAN ID**: Indicates the VLAN ID for the access management entry.
- **Start IP address**: Indicates the start IP address for the access management entry.
- **End IP address**: Indicates the end IP address for the access management entry.
- **HTTP/HTTPS**: Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.
- **SNMP**: Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.
- **TELNET/SSH**: Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.
- **Add New Entry**: Click this button to add a new access management entry.

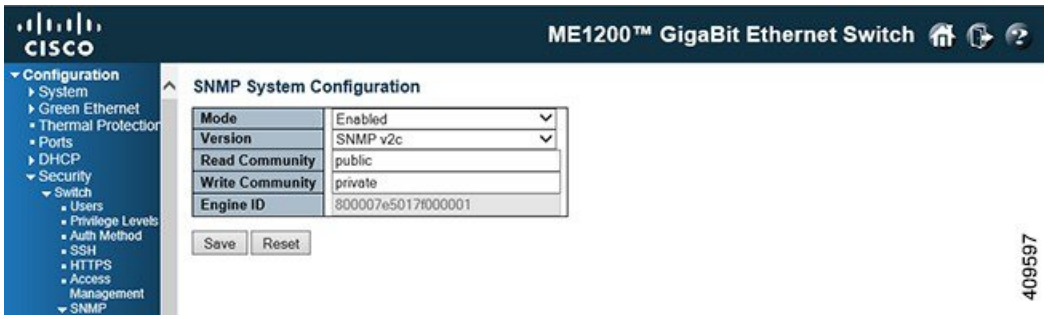
Related Topics

Monitoring Security

SNMP

SNMP System Configuration

This option allows you to system configure the SNMP feature.



- **Mode**: Indicates the SNMP mode operation. Possible modes are:
  - *Enabled*: Enables SNMP mode operation.
  - *Disabled*: Disables SNMP mode operation.
- **Version**: Indicates the SNMP supported version. Possible versions are:
  - *SNMP v1*: Sets SNMP supported version 1.
  - *SNMP v2c*: Sets SNMP supported version 2c.
  - *SNMP v3*: Sets SNMP supported version 3.
- **Read Community**: Indicates the community read access string to permit access to SNMP agent. The allowed string length is 1 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string is associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.
- **Write Community**: Indicates the community write access string to permit access to SNMP agent. The allowed string length is 1 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string is associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.
- **Engine ID**: Indicates the SNMPv3 engine ID. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

SNMP Trap Configuration

This option allows you to configure the SNMP trap feature.

Global Settings

- **Mode**: Indicates the trap mode operation. Possible modes are as follows:
  - *Enabled*: Enables SNMP trap mode operation.
  - *Disabled*: Disables SNMP trap mode operation.

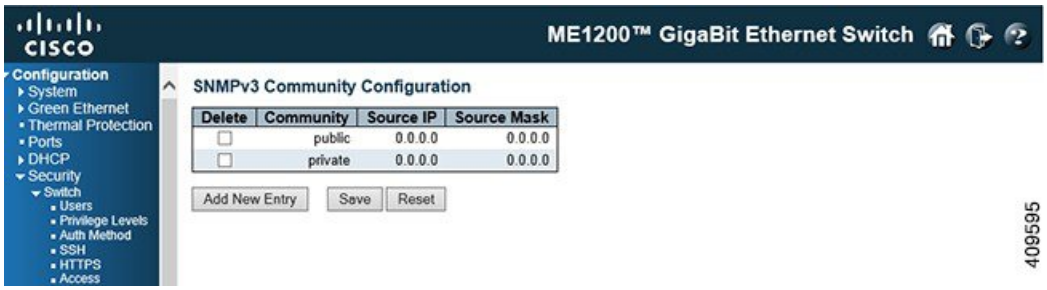
Trap Destination Configurations

Configure trap destinations on this page.

- **Name**: Indicates the name of the trap configuration.
- **Enable**: Indicates the trap destination mode operation. Possible modes are as follows:
  - *Enabled*: Enables SNMP trap mode operation.
  - *Disabled*: Disables SNMP trap mode operation.
- **Version**: Indicates the SNMP trap supported version. Possible versions are as follows:
  - *SNMPv1*: Sets SNMP trap supported version 1.
  - *SNMPv2c*: Sets SNMP trap supported version 2c. SNMPv3: Set SNMP trap supported version 3.
- **Destination Address**: Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w') as well as a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash. Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
- **Destination port**: Indicates the SNMP trap destination port. SNMP Agent sends an SNMP message via this port. The port range is 1~65535.

SNMPv3 Community Configuration

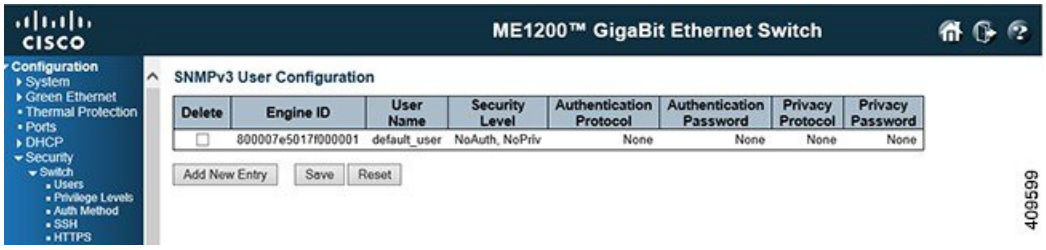
This option allows you to configure SNMPv3 community table. The entry index key is Community.



- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **Community**: Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.
- **Source IP**: Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.
- **Source Mask**: Indicates the SNMP access source address mask.
- **Add New Entry**: Click this button to add a new community entry.

SNMPv3 User Configuration

This option allows you to configure SNMPv3 user table. The entry index keys are Engine ID and User Name.



- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **Engine ID**: An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID

of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is a local user; otherwise it is a remote user.

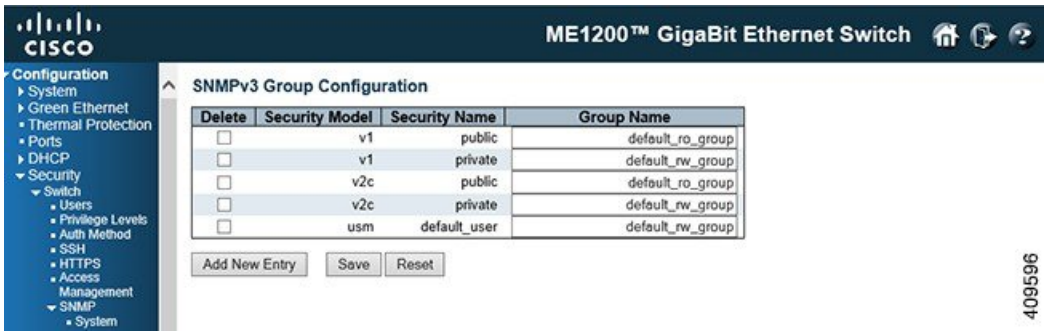
- **User Name**: A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
- **Security Level**: Indicates the security model that this entry should belong to. Possible security models are:
  - *NoAuth, NoPriv*: No authentication and no privacy.
  - *Auth, NoPriv*: Authentication and no privacy.
  - *Auth, Priv*: Authentication and privacy.

    The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.
- **Authentication Protocol**: Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:
  - *None*: No authentication protocol.
  - *MD5*: An optional flag to indicate that this user uses MD5 authentication protocol.
  - *SHA*: An optional flag to indicate that this user uses SHA authentication protocol.

    The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
- **Authentication Password**: A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.
- **Privacy Protocol**: Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:
  - *None*: No privacy protocol.
  - *DES*: An optional flag to indicate that this user uses DES authentication protocol.
  - *AES*: An optional flag to indicate that this user uses AES authentication protocol.
- **Privacy Password**: A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.
- **Add New Entry**: Click this button to add a new user entry.

SNMPv3 Group Configuration

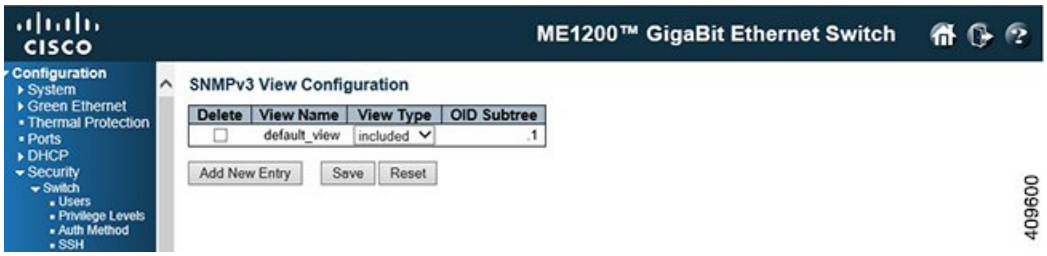
This option allows you to configure the SNMPv3 group table. The entry index keys are Security Model and Security Name.



- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **Security Model**: Indicates the security model that this entry should belong to. Possible security models are as follows:
  - *v1*: Reserved for SNMPv1.
  - *v2c*: Reserved for SNMPv2c.
  - *usm*: User-based Security Model (USM).
- **Security Name**: A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
- **Group Name**: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
- **Add New Entry**: Click this button to add a new group entry.

SNMPv3 View Configuration

This option allows you to configure the SNMPv3 view table. The entry index keys are View Name and OID Subtree.



- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **View Name**: A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
- **View Type**: Indicates the view type that this entry should belong to. Possible view types are:

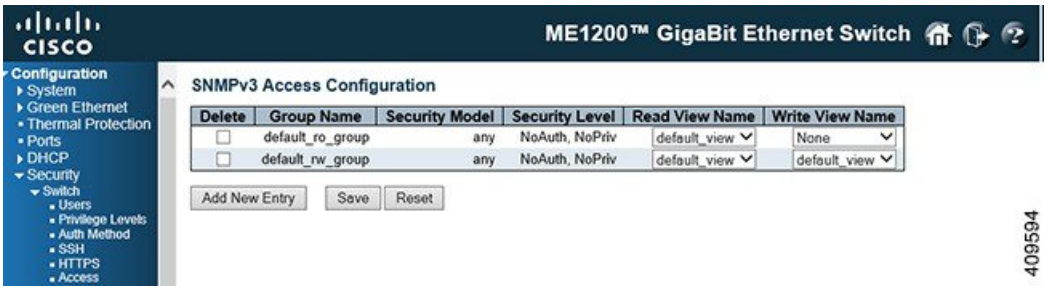
- *included*: An optional flag to indicate that this view subtree should be included.
- *excluded*: An optional flag to indicate that this view subtree should be excluded.

  In general, if the view type of a view entry is *excluded*, there should be another view entry existing with view type as *included* and its OID subtree should overstep the *excluded* view entry.

- **OID Subtree**: The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).
- **Add New Entry**: Click this button to add a new view entry.

SNMPv3 Access Configuration

This option allows you to configure the SNMPv3 access table. The entry index keys are Group Name, Security Model and Security Level.



- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **Group Name**: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
- **Security Model**: Indicates the security model that this entry should belong to. Possible security models are as follows:
  - *any*: Any security model accepted(v1|v2c|usm).
  - *v1*: Reserved for SNMPv1.
  - *v2c*: Reserved for SNMPv2c.
  - *usm*: User-based Security Model (USM).
- **Security Level**: Indicates the security model that this entry should belong to. Possible security models are as follows:
  - *NoAuth, NoPriv*: No authentication and no privacy.
  - *Auth, NoPriv*: Authentication and no privacy.
  - *Auth, Priv*: Authentication and privacy.

- **Read View Name**: The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
- **Write View Name**: The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
- **Add New Entry**: Click this button to add a new access entry.

RMON

RMON Statistics Configuration

This option allows you to configure the RMON Statistics table. The entry index key is ID.

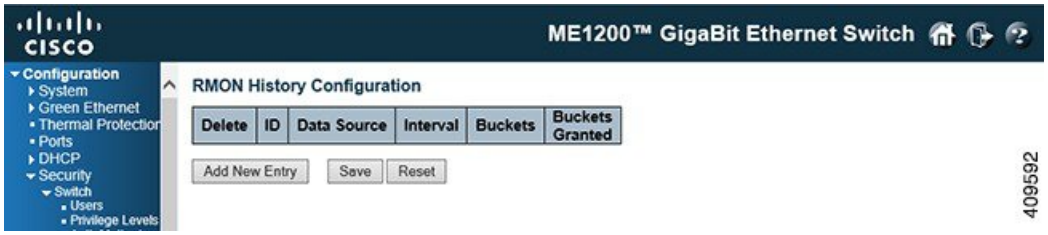
- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **ID**: Indicates the index of the entry. The range is from 1 to 65535.
- **Data Source**: Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.
- **Add New Entry**: Click this button to add a new community entry.

Related Topics

Monitoring Security

RMON History Configuration

This option allows you to configure the RMON History table. The entry index key is ID.



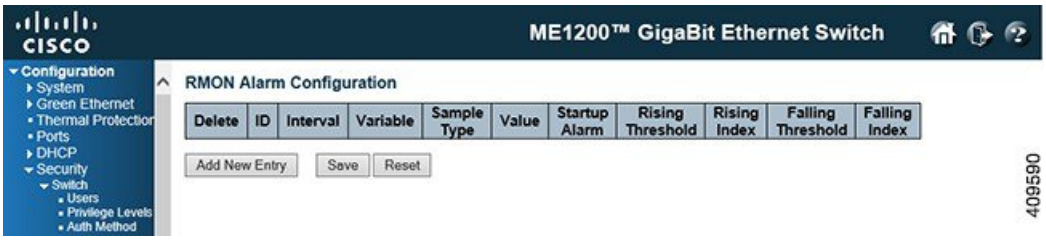
- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **ID**: Indicates the index of the entry. The range is from 1 to 65535.
- **Data Source**: Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.
- **Interval**: Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
- **Buckets**: Indicates the maximum data entries associated with this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.
- **Buckets Granted**: The number of data entries saved in the RMON.
- **Add New Entry**: Click this button to add a new community entry.

Related Topics

Monitoring Security

RMON Alarm Configuration

This option allows you to configure the RMON Alarm table. The entry index key is ID.



- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **ID**: Indicates the index of the entry. The range is from 1 to 65535.
- **Interval**: Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.
- **Variable**: Indicates the particular variable to be sampled, the possible variables are as follows:
  - *InOctets*: The total number of octets received on the interface, including framing characters.
  - *InUcastPkts*: The number of uni-cast packets delivered to a higher-layer protocol.
  - *InNUcastPkts*: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.
  - *InDiscards*: The number of inbound packets that are discarded even the packets are normal.
  - *InErrors*: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

- *InUnknownProtos*: The number of the inbound packets that were discarded because of the unknown or un-support protocol.
- *OutOctets*: The number of octets transmitted out of the interface , including framing characters.
- *OutUcastPkts*: The number of uni-cast packets that request to transmit.
- *OutNUcastPkts*: The number of broad-cast and multi-cast packets that request to transmit.
- *OutDiscards*: The number of outbound packets that are discarded event the packets is normal.
- *OutErrors*: The number of outbound packets that could not be transmitted because of errors.
- *OutQLen*: The length of the output packet queue (in packets).

- **Sample Type**: The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are as follows:
  - *Absolute*: Get the sample directly.
  - *Delta*: Calculate the difference between samples (default).
- **Value**: The value of the statistic during the last sampling period.
- **Startup Alarm**: The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are as follows:
  - *Rising* Trigger alarm when the first value is larger than the rising threshold.
  - *Falling* Trigger alarm when the first value is less than the falling threshold.
  - *RisingOrFalling* Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).
- **Rising Threshold**: Rising threshold value (-2147483648-2147483647).
- **Rising Index**: Rising event index (1-65535).
- **Falling Threshold**: Falling threshold value (-2147483648-2147483647).
- **Falling Index**: Falling event index (1-65535).
- **Add New Entry**: Click this button to add a new community entry.

Related Topics

Monitoring Security

RMON Event Configuration

This option allows you to configure the RMON Event table. The entry index key is ID.

- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **ID**: Indicates the index of the entry. The range is from 1 to 65535.
- **Desc**: Indicates this event, the string length is from 0 to 127, default is a null string.
- **Type**: Indicates the notification of the event, the possible types are as follows:
  - *none*: No SNMP log is created, no SNMP trap is sent
  - *log*: Create SNMP log entry when the event is triggered.
  - *snmptrap*: Send SNMP trap when the event is triggered.
  - *logandtrap*: Create SNMP log entry and sent SNMP trap when the event is triggered.
- **Community**: Specify the community when trap is sent, the string length is from 0 to 127, default is *public*.
- **Event Last Time**: Indicates the value of sysUpTime at the time this event entry last generated an event.
- **Add New Entry**: Click this button to add a new community entry.

Related Topics

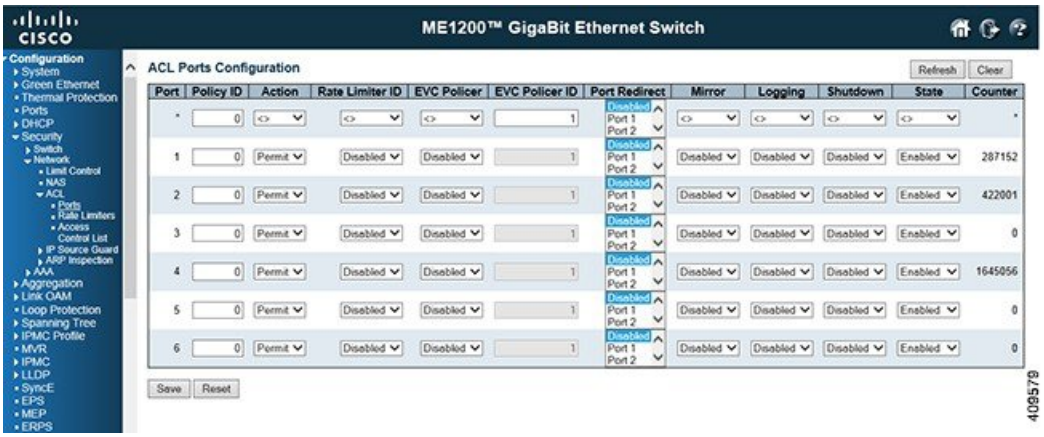
Monitoring Security

Network

ACL

ACL Ports Configuration

This option allows you to configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.



- **Port**: The logical port for the settings contained in the same row.
- **Policy ID**: Select the policy to apply to this port. The allowed values are 0 through 63. The default value is 0.
- **Action**: Select whether forwarding is permitted *Permit* or denied *Deny*. The default value is *Permit*.
- **Rate Limiter ID**: Select which rate limiter to apply on this port. The allowed values are *Disabled* or the values 1 through 16. The default value is *Disabled*.
- **EVC Policer**: Select whether EVC policer is enabled or disabled. The default value is *Disabled*. Note that ACL rate limiter and EVC policer can not both be enabled.
- **EVC Policer ID**: Select which EVC policer ID to apply on this port. The allowed values are Disabled or the values 1 through 1022.
- **Port Redirect**: Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it cannot be set when action is permitted. The default value is *Disabled*.
- **Mirror**: Specifies the mirror operation of this port. The allowed values are:
  - *Enabled*: Frames received on the port are mirrored.
  - *Disabled*: Frames received on the port are not mirrored. The default value is *Disabled*.
- **Logging**: Specifies the logging operation of this port. Notice that the logging message does not include the 4 bytes CRC. The allowed values are:
  - *Enabled*: Frames received on the port are stored in the System Log.
  - *Disabled*: Frames received on the port are not logged. The default value is *Disabled*.

Note The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.

- **Shutdown**: Specifies the port shut down operation of this port. The allowed values are:
  - *Enabled*: If a frame is received on the port, the port will be disabled.
  - *Disabled*: Port shut down is disabled. The default value is *Disabled*.

Note The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).

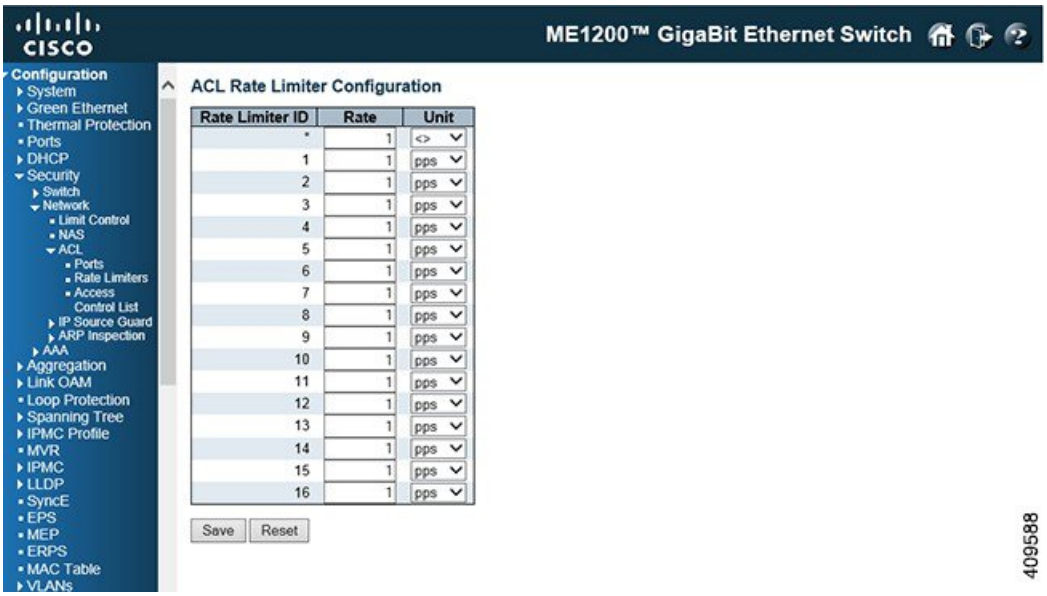
- **State**: Specifies the port state of this port. The allowed values are:
  - *Enabled*: To reopen ports by changing the volatile port configuration of the ACL user module.
  - *Disabled*: To close ports by changing the volatile port configuration of the ACL user module. The default value is *Enabled*.
- **Counter**: Counts the number of frames that match this ACE.

Related Topics

Monitoring Security

ACL Rate Limiter Configuration

This option allows you to configure the rate limiter for the ACL of the switch.



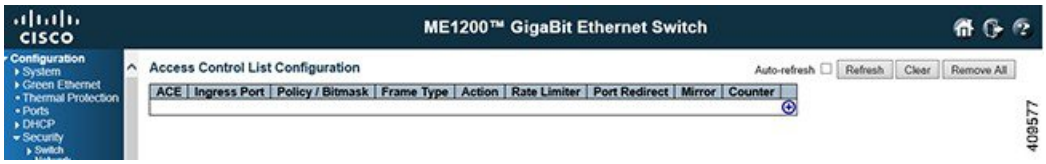
- **Rate Limiter ID**: The rate limiter ID for the settings contained in the same row and its range is 1 to 16.
- **Rate**: The rate range is located 0-128k in pps. The valid rate is 0 - 99, 100, 100, 100, ..., 3276700 in pps or 0, 100, 100, 100, ..., 1000000 in kbps.
- **Unit**: Specify the rate unit. The allowed values are as follows:
  - *pps*: packets per second.
  - *kbps*: Kbit per second.

Related Topics

Monitoring Security

Access Control List Configuration

This option shows the Access Control List (ACL) that is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 512 on each switch.



Click**Add ACE to end of list** icon to add a new ACE to the list. The reserved ACEs used for internal protocol cannot be edited or deleted, the order sequence cannot be changed, and the priority is highest.

- **ACE**: Indicates the ACE ID.
- **Ingress Port**: Indicates the ingress port of the ACE. Possible values are:
  - *All*: The ACE will match all ingress port.
  - *Port*: The ACE will match a specific ingress port.
- **Policy / Bitmask**: Indicates the policy number and bitmask of the ACE.
- *Frame Type*: Indicates the frame type of the ACE. Possible values are:
  - *Any*: The ACE will match any frame type.
  - *EType*: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.
  - *ARP*: The ACE will match ARP/RARP frames.
  - *IPv4*: The ACE will match all IPv4 frames.
  - *IPv4/ICMP*: The ACE will match IPv4 frames with ICMP protocol.
  - *IPv4/UDP*: The ACE will match IPv4 frames with UDP protocol.
  - *IPv4/TCP*: The ACE will match IPv4 frames with TCP protocol.
  - *IPv4/Other*: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
  - *IPv6*: The ACE will match all IPv6 standard frames.
- **Action**: Indicates the forwarding action of the ACE.
  - **Permit**: Frames matching the ACE may be forwarded and learned.
  - **Deny**: Frames matching the ACE are dropped.
  - **Filter**: Frames matching the ACE are filtered.

- **Rate Limiter**: Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When *Disabled* is displayed, the rate limiter operation is disabled.
- **Port Redirect**: Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are *Disabled* or a specific port number. When Disabled is displayed, the port redirect operation is disabled.
- **Mirror**: Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:
  - *Enabled*: Frames received on the port are mirrored.
  - *Disabled*: Frames received on the port are not mirrored. The default value is *Disabled*.
- **Counter**: The counter indicates the number of times the ACE was hit by a frame.
- Modification icons: You can modify each Access Control Entry (ACE) in the table by using the following icons:
  - **Insert new ACE before this ACE** icon: Inserts a new ACE before the current row.
  - **Edit ACE** icon: Edits the ACE row.
  - **Move ACE up** icon: Moves the ACE up the list.
  - **Move ACE down** icon: Moves the ACE down the list.
  - **Delete ACE** icon: Deletes the ACE.
  - **Add ACE to end of list** icon: The lowest plus sign adds a new entry at the bottom of the ACE listings.

Related Topics

Monitoring Security