IONMM

Application Note M07

Access Control Lists (ACLs)

ACLs can be configured in the IONMM to allow access to authorized users and to deny access to all other users.

The rules of an ACL define the policy to be followed for certain defined conditions.

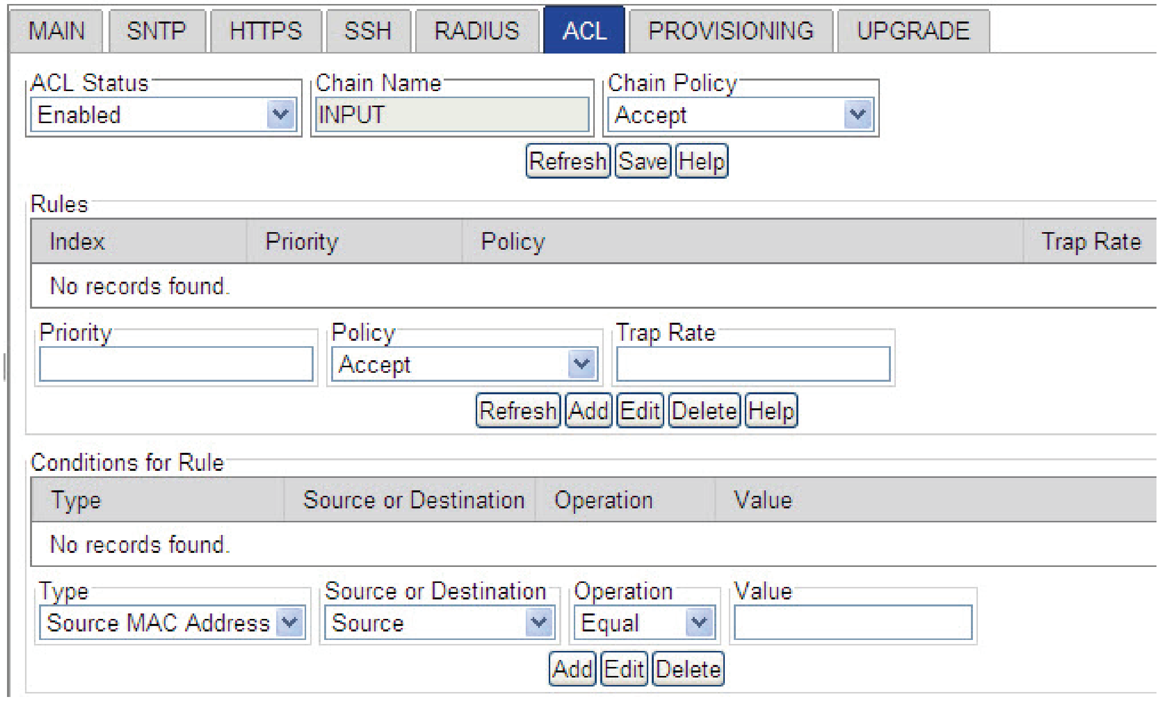
There are three different policies (rules) that can be defined for the IONMM:
- Accept – allow communication from the device
- Drop – disallow communication from the device
- Trap – initiate an SNMP trap message

The conditions of an ACL define the objects the policies apply to (e.g., MAC or IP addresses, ports, etc.).

The IONMM reads ACLs from top to bottom. When a packet comes into the IONMM, it is matched against the first line in the ACL, if it does not meet the criteria, then it drops to the next line and so on until it reaches a permit or deny that fits it. For all ACLs there is an implied deny beneath the last line of the ACL. When applying an ACL to an interface it is required that there be at least one permit statement otherwise nothing will be able to access the management interface via the web.

ACL Config – Web Method

1. Access the IONMM through the Web interface
2. Select the **ACL** tab.



ACL Status: Enabled
Chain Name: INPUT
Chain Policy: Accept

Rules

Index	Priority	Policy	Trap Rate
No records found.			

Priority:
Policy: Accept
Trap Rate:

Conditions for Rule

Type	Source or Destination	Operation	Value
No records found.			

Type: Source MAC Address
Source or Destination: Source
Operation: Equal
Value:

3. In the **ACL Status** field, select **Enabled**.

4. In the **Chain Name** field, INPUT is the default and the only valid entry.

5. In the **Chain Policy** field, select the default policy if a policy is not determined by the end of the table:
   - **Accept** (allows communication; default value)
   - **Drop** (disallows communication)

6. Define a rule.
   a) In the **Priority** field, enter a number indicating the relative position of the rule to other rules in the table.
   b) In the **Policy** field, select the policy to be associated with this rule.
   c) In the **Trap Rate** field, enter a value indicating the number of traps that will be sent in one minute.
   This field is only valid if:
   - The policy selected is **Trap**.
   - A trap server is defined on the **Main** tab.
   - A trap server is in the network and available.

   d) Click Add.

7. Define additional rules as needed.

8. Define a condition:
   a) Select a rule by clicking its index number.
   b) In the **Type** field, select the condition type.
   c) In the **Source or Destination** field, select whether the type is a source or a destination.
   d) In the **Operation** filed, select whether the match for this condition is equal to type or not equal to type.
   e) In the **Value** field, specify the address, port number or type associated with the selection in the **Type** field.
   f) Click **Add**.

9. Define additional conditions as needed.

10. After all rules and conditions have been defined, click **Save**.

IMPORTANT
An ACL does not control access to the IONMM through a serial interface (USB connection).