

How to Setup the ENVIROMUX Enterprise Environment Monitoring System to Send SNMP Traps

Follow these steps to prepare the ENVIROMUX to send SNMP traps to ENVIROMUX users. This procedure applies to all ENVIROMUX Enterprise Environment Monitoring Systems and Server Environment Monitoring Systems.

Under Network Settings:

1. Enable the proper SNMP Agent type (v1/v2c , v1/v2c/v3, or just v3) depending upon what type of SNMP browser you use.
 - v1/v2c = no security required
 - v1/v2c/v3 = messages with or without security
 - v3= only secure messages will be sent
2. Place a checkmark in “Enable SNMP Traps”.
3. Enter names for the Read-write community and Read-only community (usually just “private” and “public” as shown).

SNMP Settings	
Enable SNMP Agent	SNMPv1v2cV3 <small>Allow access to SNMP agent on this device</small>
Enable SNMP Traps	<input checked="" type="checkbox"/> Enable sending of SNMP traps from this device
Read-write community name	private <small>Read-write community name for SNMP agent</small>
Read-only community name	public <small>Read-only community name for SNMP agent</small>

Under Sensor Configuration:

4. Under the sensor configuration for each sensor, enter a Group number that the sensor should belong to. Users can receive alert messages from some, all, or no sensor groups, as configured under User Settings.

Temperature 1 Configuration (Type: Temperature Combo)

Sensor Settings	
Description	Temperature 1 <small>Descriptive name for the sensor</small>
Group	1 <small>Select which group the sensor belongs to</small>
Units	Deg. F <small>Select the units for the sensor</small>
Min. Level	-4.0 <small>Min. supported value for the sensor</small>
Max. Level	167.0 <small>Max. supported value for the sensor</small>
Min. Non-Critical Threshold	65.0 <small>Min. threshold below which indicates a non-critical alert condition</small>
Max. Non-Critical Threshold	85.0 <small>Max. threshold above which indicates a non-critical alert condition</small>
Min. Critical Threshold	60.0 <small>Min. threshold below which indicates an alert condition</small>
Max. Critical Threshold	90.0 <small>Max. threshold above which indicates an alert condition</small>
Refresh Rate	5 Sec <small>The refresh rate at which the sensor view is updated</small>
Non-Critical Alert Settings	

5. Place a checkmark in “Enable SNMP Traps” checkbox under the sensor configuration for each sensor that should send traps when there is an alert. If you want them sent for Critical Alerts and Non-Critical Alerts, there is a checkbox for each level.

Non-Critical Alert Settings	
Disable Alerts	<input type="checkbox"/> Disable alert notifications for this sensor
Alert Delay	15 Sec Duration the sensor must be out of thresholds before alert is generated
Notify Again Time	6 Hr Time after which alert notifications will be sent again
Notify on return to normal	<input checked="" type="checkbox"/> Send a notification when this sensor returns to normal status
Enable Syslog Alerts	<input checked="" type="checkbox"/> Send alerts for this sensor via syslog
Enable SNMP Traps	<input checked="" type="checkbox"/> Send alerts for this sensor via SNMP traps
Enable E-mail Alerts	<input checked="" type="checkbox"/> Send alerts for this sensor via e-mail
E-mail Subject	Temperature 1 Warning Subject of e-mails sent for alerts
Enable SMS Alerts	<input type="checkbox"/> Send alerts for this sensor via SMS
Enable Siren	<input type="checkbox"/> Turn on the siren when this sensor goes to alert
Enable Beacon	<input type="checkbox"/> Turn on the beacon when this sensor goes to alert
Associated Output Relay	None Name of the output relay that can be controlled by this sensor
Output Relay status on alert	Inactive Status of the output relay when going to alert
Output Relay status on return from alert	Inactive Status of the output relay when returning from alert

Under User Settings:

6. Apply a checkmark to the Group number(s) for the sensor(s) you want to receive SNMP traps about.
7. Be sure to apply a checkmark in the “SNMP Traps” box under Configure User ->Contact Settings for each user that should receive SNMP traps
8. Enter a valid IP address where traps are to be sent for each user.

Group Settings	
Group 1	<input checked="" type="checkbox"/> User receives notifications for Group 1
Group 2	<input type="checkbox"/> User receives notifications for Group 2
Group 3	<input type="checkbox"/> User receives notifications for Group 3
Group 4	<input type="checkbox"/> User receives notifications for Group 4
Group 5	<input type="checkbox"/> User receives notifications for Group 5
Group 6	<input type="checkbox"/> User receives notifications for Group 6
Group 7	<input type="checkbox"/> User receives notifications for Group 7
Group 8	<input type="checkbox"/> User receives notifications for Group 8

Contact Settings	
E-mail Alerts	<input type="checkbox"/> User receives alerts via e-mail
Brief E-mail	<input type="checkbox"/> User receives brief e-mail
E-mail Address	<input type="text"/> E-mail address for the user
Syslog Alerts	<input type="checkbox"/> User receives alerts via syslog
SNMP Traps	<input type="checkbox"/> User receives alerts via SNMP traps
Syslog/SNMP IP Address	<input type="text"/> IP address where syslog messages/SNMP traps are sent for this user
SMS Alerts	<input type="checkbox"/> User receives alerts via SMS
SMS Number	<input type="text"/> Phone number where SMS messages are sent for this user

9. If the “Enable SNMP Agent” setting under “Network Settings” was SNMPv1/v2c/v3, then the Authentication Protocol (MD5 or SHA), Authentication Passphrase, Privacy Protocol (DES or AES), and Privacy Passphrase will only need to be filled in for users that will receive secure messages.

If only v3 was selected, then these settings must be filled in for each user.

The protocol types will be dependent upon the type of SNMP Agent you are using (refer to your SNMP Agent specifications).

- Authentication Protocol = MD5 or SHA
- Privacy Protocol = DES or AES

If only SNMPv1/v2c will be used, the default settings of “None” will apply.

The Passphrases will be those that have been setup in your agent for the user being configured.

Note: The username in the ENVIROMUX user configuration must match the username in the SNMP browser configuration.

Configure User

The screenshot shows the 'Configure User' form with the following fields and values:

- Account Settings** (expanded)
- Username:** root (with a callout box: "Must match user in SNMP browser configuration")
- Admin:** Grant this user administrative privileges
- Enabled:** Users can only access the system if their account is enabled
- Password:** [Redacted]
- Confirm:** [Redacted]
- Title:** [Empty]
- Department:** [Empty]
- Company:** [Empty]

10. Select which Traps type the user should receive. If SNMPv1 or SNMPv2c are selected, the Authentication and Privacy settings above do not need to be configured as they are only required to receive SNMPv3 messages.

The screenshot shows the 'SNMP Settings' form with the following fields and values:

- SNMP Settings** (expanded)
- Authentication Protocol:** None (dropdown)
- Authentication Passphrase:** [Empty]
- Privacy Protocol:** None (dropdown)
- Privacy Passphrase:** [Empty]
- Traps Type:** SNMPv1 (dropdown)

11. Use the MIB file supplied on your manual CD with your SNMP browser to setup and manage SNMP traps.

The MIB file is also available for download from the firmware update website:

<http://www.networktechinc.com/download/d-environment-monitor-16.html> for ENVIROMUX-16D / -5D

<http://www.networktechinc.com/download/d-environment-monitor-2d.html> for ENVIROMUX-2D

<http://www.networktechinc.com/download/d-environment-monitoring.html> for ENVIROMUX-LXO