Configuring SNMP

You can configure the appliance to receive SNMP queries from specific management systems and send SNMP traps to specific trap receivers. The appliance supports SNMPv1, SNMPv2, and SNMPv3. You can set up either SNMPv1/SNMPv2 or SNMPv3, or all of them for the Master Grid. You can also override the Master Grid settings at a member level.

To configure SNMPv1 and SNMPv2 on the appliance, do the following:

- Enable the appliance to accept queries, as described in **Accepting Queries**.
- Specify the management systems to which the appliance sends traps, as described in **Adding Trap Receivers**.
- Specify system information using managed objects in MIB-II, the standard MIB defined in RFC 1213. For information, see **Setting SNMP System Information**.

To configure SNMPv3 on the appliance, do the following:

- Add an SNMPv3 user and set up authentication and privacy protocols. For information, see **Configuring SNMPv3 Users**. After you set up an SNMPv3 user, you can modify and delete it. For information, see **Modifying SNMPv3 Users** and **Deleting SNMPv3 Users**.
- Enable the appliance to accept queries, as described in **Accepting Queries**.
- Specify the management systems to which the appliance sends traps, as described in **Adding Trap Receivers**.
- Specify system information using managed objects in MIB-II, the standard MIB defined in RFC 1213. For information, see **Setting SNMP System Information**.

Configuring SNMPv3 Users

To enable SNMPv3, you must first configure SNMPv3 users on the appliance. For information about SNMPv3, see **About User-Based Security Model in SNMPv3**. To configure an SNMPv3 user:

1. From the **Administration** tab, select the **Administrators** tab -> **SNMPv3 Users** tab, and then click the Add icon.
2. In the **Add SNMPv3 User** wizard, complete the following:
   - **Name**: Enter a user name for the SNMPv3 management system.
   - **Authentication Protocol**: Select one of the following:
     - **MD5**: Select this to use the HMAC-MD5-96 authentication protocol to authenticate the SNMPv3 user. This protocol uses the MD5 (Message-Digest algorithm 5) hash function in HMAC (Hash-based Message Authentication Code) and truncates the output to 96 bits. The output is included as part of the SNMP message sent to the receiver. For detailed information about the protocol, refer to RFC1321, *The MD5 Message-Digest Algorithm*.
     - **SHA**: Select this to use the HMAC-SHA-96 authentication protocol to authenticate the SNMPv3 user. This protocol uses the SHA (Secure Hash Algorithm) hash function and truncates the output to 96 bits. The output is included as part of the SNMP message sent to the receiver.
     - **None**: Select this to decline using any authentication protocol for this SNMPv3 user. When you select this option, you are not required to enter a password.
   - **Password**: Enter a password for the selected authentication protocol.
   - **Confirm Password**: Enter the same password.
   - **Privacy Protocol**: Select one of the following:
     - **DES**: Select this to use DES for data encryption. DES is a block cipher that employs a 56-bit key size and 64-bit block size in the encryption.
     - **AES**: Select this to use AES for data encryption. AES is a symmetric-key encryption standard that comprises three block ciphers, AES-128, AES-192, and AES-256. Each of these ciphers has a 128-bit block size and a key size of 128, 192, and 256 bits, respectively. **None**: Select this to decline using any privacy protocol for this SNMPv3 user. When you select this option, you are not required to enter a password.
   - **Password**: Enter a password for the privacy protocol.
   - **Confirm Password**: Enter the same password.
   - **Comment**: Enter useful information about the SNMP user, such as location or department.
   - **Disable**: Select this check box to retain an inactive profile for this SNMP user in the configuration. You can clear this check box to activate the profile.

   **Note**: If an SNMPv3 user is configured to send SNMP queries, you cannot delete the user.

3. Click **Next** to define extensible attributes. For information, see **Using Extensible Attributes**.
4. Save the configuration.

Modifying SNMPv3 Users

1. From the **Administration** tab, select the **Administrators** tab -> **SNMPv3 Users** tab -> **snmpv3user**, and then click the Edit icon.
2. The **SNMPv3 User** editor provides the following tabs from which you can edit data:
   - **General**: Modify the data as described in **Configuring SNMPv3 Users**.
   - **Extensible Attributes**: Add and delete extensible attributes that are associated with the SNMPv3 user account. You can also modify the values of extensible attributes. For information, see **Using Extensible Attributes**.
3. Save the configuration.

Deleting SNMPv3 Users

1. From the **Administration** tab, select the **Administrators** tab -> **SNMPv3 Users** tab -> **snmpv3user**, and then click the Delete icon.
When you delete an SNMPv3 user that is configured to send queries or receive traps, a warning message states that the SNMPv3 is associated with the corresponding function. You can then decide whether you want to delete the user or not.

To delete an SNMPv3 user:

1. From the Administration tab, select the Administrators tab -> SNMPv3 Users tab -> snmpv3user, and then click the Delete icon.
2. In the Delete confirmation dialog box, click Yes.

Note: You cannot schedule the deletion of an SNMPv3 user.

Accepting Queries

You can allow specific management systems to send SNMP queries to the appliance. For SNMPv1 and SNMPv2, you must specify a community string. The appliance accepts queries only from management systems that provide the correct community string. You can also specify SNMPv3 users to send queries. For information about configuring SNMPv3 users, see Configuring SNMPv3 Users.

To configure an appliance to accept SNMP queries:

1. From the Master Grid tab, click Master Grid Properties -> Edit from the Toolbar.
   or From the Master Grid tab, select the Members tab -> master_grid_member, and then click the Edit icon.
2. In the Master Grid Properties or Master Grid Member Properties editor, select the SNMP tab. To override Master Grid settings, click Override in the Master Grid Member Properties editor.
3. Complete the following in the SNMP section:
   - Enable SNMPv1/SNMPv2 Queries: Select this to accept SNMPv1 and SNMPv2 queries from management systems.
     + Community String: Enter a text string that the management system must send with its queries to the appliance. A community string is similar to a password in that the appliance accepts queries only from management systems that send the correct community string. Note that this community string must match exactly what you enter in the management system.
   - Engine ID: Displays the engine ID of the appliance that manages the SNMP agent. The management system needs this ID to send traps to the appliance. If the appliance is an HA pair, this field displays the engine IDs for both the active and passive nodes.
   - Enable SNMPv3 Queries: Select this to enable queries from SNMPv3 management systems. Click the Add icon to add SNMPv3 users that you have configured on the appliance. In the SNMPv3 User Selector dialog box, click the SNMPv3 user you want to add. The appliance displays the selected SNMPv3 users in the table. You can add comments in the table. You can also select an SNMPv3 user and click the Delete icon to remove it from the table. Note that a disabled SNMPv3 user cannot send queries to the appliance.
4. Save the configuration.

Adding Trap Receivers

You can enable the appliance to send traps to specific management systems using either SNMPv1/SNMPv2 or SNMPv3, or all versions of SNMP. You can then add management systems that are allowed to receive traps from the appliance. Note that you cannot enable both SNMPv1/SNMPv2 and SNMPv3 on the same trap receiver. The appliance sends traps when certain events occur. You can enable SNMP traps and add trap receivers to the Master Grid. You can also override the Master Grid settings at the member level.

To enable the appliance to send traps and to add trap receivers, do the following:

1. From the Master Grid tab, click Master Grid Properties -> Edit from the Toolbar.
   or From the Master Grid tab, select the Members tab -> master_grid_member, and then click the Edit icon.
2. In the Master Grid Properties or Master Grid Member Properties editor, select the SNMP tab. To override Master Grid settings, click Override in the Master Grid Member Properties editor.
3. Complete the following in the SNMP tab:
   - Enable SNMPv1/SNMPv2 Traps: Select this to enable the appliance to send traps to specified management systems.
     + Community String: Enter a text string that the appliance sends to the management system together with its traps. Note that this community string must match exactly what you enter in the management system.
   - Enable SNMPv3 Traps: Select this to enable the appliance to send traps to specified SNMPv3 users.
4. Click the Add icon and select one of the following from the drop-down menu to add an SNMP trap receiver:
   - SNMPv1/SNMPv2: Select this to add an SNMPv1 or SNMPv2 management system as a trap receiver. Multi-Grid Manager adds a row to the table. In the Address field, enter the IP address of the SNMP management system to which you want the SNMP agent on the appliance to send traps. You can enter more than one trap receiver. To remove a trap receiver from the list, select the address, and then click the Delete icon.
   - SNMPv3: Select this to add an SNMPv3 management system as a trap receiver. Multi-Grid Manager displays the SNMPv3 User Selector dialog box. Click the name of the SNMPv3 user in the dialog box. Multi-Grid Manager adds the user to the table. In the Address field, enter the IP address of the SNMP management system to which you want the SNMP agent on the appliance to send traps. You can add more than one trap receiver. To remove a trap receiver from the list, select the address, and then click the Delete icon.
5. Save the configuration.

Setting SNMP System Information
You can enter values for certain managed objects in MIB-II, the standard MIB defined in RFC 1213. Management systems that are allowed to send queries to the appliance can query these values. You can enter these values for the Master Grid and specific members. You can also override the Master Grid values at a member level.

To enter system information:

1. From the Master Grid tab, click Master Grid Properties -> Edit from the Toolbar.
   or
2. From the Master Grid tab, select the Members tab -> master_grid_member, and then click the Edit icon.
3. In the Master Grid Properties or Master Grid Member Properties editor, select the SNMP tab. To override Master Grid settings, click Override in the Master Grid Member Properties editor.
4. Complete the following in the SNMP tab. For an HA member, click Override Node 2 settings to enter information for node 2 of the HA pair.
   - sysContact: Enter the name of the contact person for the appliance.
   - sysLocation: Enter the physical location of the appliance.
   - sysName: Enter the fully qualified domain name of the appliance.
   - sysDescr: Enter useful information about the appliance, such as the software version it is running.
5. Save the configuration.

Testing the SNMP Configuration

After you configure SNMP on the appliance, you can do the following to test your SNMP configuration:

- From the Master Grid tab, select the Members tab -> master_grid_member, and then select Test SNMP from the Toolbar.

The appliance sends a "test trap" string to the trap receiver and displays a confirmation message at the top of the screen if your SNMP configuration is properly set up. If your SNMP configuration is not complete or if it is invalid, the appliance displays an error message. You can check your configuration and try again.

The following is a sample test trap that the trap receiver can get:

```
2011-04-04 17:37:14 10.32.2.80 [UDP: [10.32.2.80]:49244->[10.32.2.80]]:

SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-MIB::snmpTrapOID SNMPv2-MIB::sysName.0 = STRING: 'Test trap'
```