The Start button, or Start from the File menu, starts the SNMP Agent, making it possible for an SNMP network manager to manage your workstation.

The Stop button, or Stop from the File menu, stops the SNMP Agent, making your workstation unavailable to the SNMP network manager.

The Save Settings button, or Save Settings from the File menu, saves the SNMP settings. You must save the settings for them to be available to the SNMP network manager.

The Exit button, or Exit from the File menu, exits the SNMP Agent application. If you exit the application, your workstation cannot be managed by the SNMP network manager.

Check Minimize on Startup to have the SNMP Agent initially start minimized on the desktop. If you automatically start the SNMP Agent during system boot, minimizing the SNMP Agent helps keep your desktop clear.

Check Prompt on Exit if you want to be prompted when you try to exit the SNMP Agent application.

Check Toolbar Help if you want bubble help when passing your cursor over the buttons on the toolbar.

Check Status Bar to show the status bar at the bottom of the SNMP Agent window. The status bar shows help for menu items.

Check Toolbar to display the quick-access buttons for some of the options on the menus.

Enter a description of your workstation in the sysDescr field. The description can contain up to 255 characters. Your network administrator might have specific rules for the information to be included in this description (for example, the make and model of the machine, and so forth). Contact your network administrator for help.

Enter the contact information for you or the person responsible for your machine in the sysContact field. The contact information can contain up to 255 characters. Your network administrator might have specific rules for the information to be included in this field (for example, name, telephone number, email address, and so forth). Contact your network administrator for help.

Enter a description of the location of your workstation in the sysLocation field. The description can contain up to 255 characters. Your network administrator might have specific rules for the information to be included in this description (for example, the building and number of your office, and so forth). Contact your network administrator for help.

Enter the read community, which is a character string that the SNMP Agent uses to authenticate read requests from SNMP servers. This case-sensitive string can contain up to 255 characters, and defaults to **public**. When an SNMP server asks your SNMP Agent to send information to it, the server must include this string or your agent rejects any request the SNMP server makes. Contact your network administrator for help in setting your read community.

Enter the write community, which is a character string that the SNMP Agent uses to authenticate write requests from SNMP servers. This case-sensitive string can contain up to 255 characters, and there is no default (all write requests are rejected unless a write community is defined). When an SNMP server tries to make changes to your machine's setup (IP routing, ARP, and interface information), the server must include this string or your agent rejects any request the SNMP server makes. Contact your network administrator for help in setting your write community.

Click the Defaults button to prime the sysDescr, sysContact, and sysLocation fields with information that can be discovered from your workstation's setup. You can then change the text to contain the information required by your network administrator.

Check Enable Authentication Failure Traps if you want the SNMP Agent to send SNMP traps to an SNMP trap destination machine. If an SNMP server contacts your machine with an invalid read or write community string, your SNMP agent sends an authentication failure trap to the SNMP trap destination machine. The network administrator uses these traps to help maintain the security of your network. The trap destination only accepts your trap message if your trap community string matches that of the destination's trap community.

Enter the trap community, which is a character string that the SNMP Agent sends with traps to SNMP trap destination machines. The trap destination machines use the trap community string to authenticate your machine's message. This case-sensitive string can contain up to 255 characters. Contact your network administrator for help in setting your trap community.

Trap Destinations lists the machines that have been designated to receive SNMP traps. Contact your network administrator for the list of trap destinations and their trap communities. The name of a trap destination can be a host name or IP address.

Click the Add button to add trap destinations to the trap destination list.

Click the Delete button to delete the selected trap destination from the trap destination list.

Add Trap Destination Dialog Box

The Add Trap Destination dialog box lets you add an SNMP trap destination to the list of trap destinations.

{button ,KL(`Add Trap Destination dialog box')} Things you can do with the Add dialog box

Enter the host name or IP address of a machine that has been designated to receive SNMP traps. Contact your network administrator for the list of trap destinations.

Click the OK button to close the dialog box and save your changes.

Click the Cancel button to close the dialog box without saving any changes.

Click the Help button to display online help.

Enter the port used for sending and receiving SNMP messages. The default port is 161.

Enter the maximum size of SNMP messages, in bytes, that the agent can send or receive. The size can range from 2048 to 32767. The default size is 2048.

To identify your workstation to an SNMP network manager:

1 Choose the System tab.
2 Edit the sysDescr, sysContact, and sysLocation fields if they do not contain the desired information.
3 Click the Save Settings button to save your changes.

Tips:

- If the Agent is running when you change settings, you must restart the Agent so that the new settings are available to the SNMP network manager. Restart the SNMP Agent by clicking the Stop button, and then clicking the Start button.
- You must leave the SNMP Agent application active for it to accept or reject requests from an SNMP server.
- You can click the Defaults button to reset these fields to their default values.
- Your network administrator might have specific guidelines for the information you should provide in the sysDescr, sysContact, and sysLocation fields. Contact your network administrator for help.

{button ,AL(`System tab')} Related Topics

To set the read and write communities for the workstation:

1 Choose the System tab.
2 Enter the read community string in the Read Community field.
3 Enter the write community string in the Write Community field.
4 Click the Save Settings button to save your changes.

Tips:

- If the Agent is running when you change settings, you must restart the Agent so that the new settings are available to the SNMP network manager. Restart the SNMP Agent by clicking the Stop button, and then clicking the Start button.
- You must leave the SNMP Agent application active for it to accept or reject requests from an SNMP server.
- Contact your network administrator for help in identifying your read and write communities. These character strings must be known to the SNMP server if the workstation is to be remotely managed.

{button ,AL(`System tab')} Related Topics

To enable SNMP authentication failure traps:

1 Choose the Trap tab.
2 Check Enable Authentication Failure Traps.
3 Click the Save Settings button to save your changes.

Tips:

- If the Agent is running when you change settings, you must restart the Agent so that the new settings are available to the SNMP network manager. Restart the SNMP Agent by clicking the Stop button, and then clicking the Start button.
- You must leave the SNMP Agent application active for it to accept or reject requests from an SNMP server.

{button ,AL(`Trap tab')} Related Topics

To identify the trap community for the trap destination:

1 Choose the Trap tab.
2 Enter the trap community string in the trap community field.
3 Click the Save Settings button to save your changes.

Tips:

- If the Agent is running when you change settings, you must restart the Agent so that the new settings are available to the SNMP network manager. Restart the SNMP Agent by clicking the Stop button, and then clicking the Start button.
- You must leave the SNMP Agent application active for it to accept or reject requests from an SNMP server.
- Contact your network administrator for the trap community string you should use.

{button ,AL(`Trap tab')} Related Topics

To add a trap destination:

1 Choose the Trap tab.
2 Click the Add button.
3 Enter the host name or IP address of the trap destination and click OK.
4 Click the Save Settings button to save your changes.

Tips:

- If the Agent is running when you change settings, you must restart the Agent so that the new settings are available to the SNMP network manager. Restart the SNMP Agent by clicking the Stop button, and then clicking the Start button.
- You must leave the SNMP Agent application active for it to accept or reject requests from an SNMP server.
- Contact your network administrator for the trap destinations you can use.

{button ,AL(`Trap tab')} Related Topics

To delete a trap destination:

1 Choose the Trap tab.
2 Click the trap destination you want to delete.
3 Click the Delete button.
4 Click the Save Settings button to save your changes.

Tips:

- If the Agent is running when you change settings, you must restart the Agent so that the new settings are available to the SNMP network manager. Restart the SNMP Agent by clicking the Stop button, and then clicking the Start button.
- You must leave the SNMP Agent application active for it to accept or reject requests from an SNMP server.

{button ,AL(`Trap tab')} Related Topics

To disable SNMP authentication failure traps:

1 Choose the Trap tab.
2 Uncheck Enable Authentication Failure Traps.
3 Click the Save Settings button to save your changes.

Tips:

- If the Agent is running when you change settings, you must restart the Agent so that the new settings are available to the SNMP network manager. Restart the SNMP Agent by clicking the Stop button, and then clicking the Start button.
- You must leave the SNMP Agent application active for it to accept or reject requests from an SNMP server.
- The SNMP Agent can send the other types of SNMP traps even if you disable authentication failure traps.

{button ,AL(`Trap tab')} Related Topics

To set advanced settings:

1 Choose the Advanced tab.
2 Enter the port number that should handle SNMP messages if the default port 161 is not correct.
3 Set the maximum message size for the SNMP messages if the default 2048 bytes is not adequate.
4 Click the Save Settings button to save your changes.

Tips:

- If the Agent is running when you change settings, you must restart the Agent so that the new settings are available to the SNMP network manager. Restart the SNMP Agent by clicking the Stop button, and then clicking the Start button.
- You must leave the SNMP Agent application active for it to accept or reject requests from an SNMP server.
- Contact your network administrator for the appropriate port and maximum message size values. Usually the default values are adequate.

To set the execution options for the SNMP agent:

1 Choose the Options menu.
2 Check Minimize on Startup if you want the SNMP Agent minimized on the desktop when started.
3 Check Prompt on Exit if you want to be prompted before exiting the SNMP Agent application.
4 Check Toolbar Help, Status Bar, and Toolbar if you want these features displayed.

To start the SNMP Agent:

- Click the Start button, or check Start on the File menu.

Tips:

- To have your workstation effectively managed by the SNMP network manager, you must start the SNMP Agent every day, preferably during system startup.
- Whenever you make a change to SNMP Agent settings, click the Stop button and then click the Start button. This reloads the SNMP information so that the SNMP network manager can see the updated settings.

{button ,AL(`start and stop')} Related Topics

To start the SNMP Agent automatically:

1 Select Settings, Taskbar from the Windows Start menu.
2 Choose the Start Menu Programs tab.
3 Click Add.
4 Click Browse and select the Mnsnmp32 program in the Cisco TCP/IP Suite installation directory (usually MULTINET).
5 Click Next to proceed to the Select Program Folder window.
6 Select the Startup folder.
7 Click Next and enter SNMP Agent or a name of your choosing in the Select a name for shortcut box.
8 Click Finish.

Tips:

- To have your workstation effectively managed by the SNMP network manager, you must start the SNMP Agent every day, preferably during system startup.
- To start the SNMP Agent minimized on your desktop, check Minimize on Startup on the Options menu.
- Ensure that the Start button is selected (or Start on the File menu is checked). Otherwise, the SNMP Agent is not available to the SNMP network manager.
- Whenever you make a change to SNMP Agent settings, click the Stop button and then click the Start button. This reloads the SNMP information so that the SNMP network manager can see the updated settings.

{button ,AL(`start and stop')} Related Topics

To stop the SNMP Agent (without exiting the program):

Click the Stop button, or check Stop on the File menu.

Tips:

- If you stop the SNMP Agent, the SNMP network manager cannot access and manage your workstation.

{button ,AL(`start and stop')} Related Topics

To exit the SNMP Agent application:

- Click the Exit button, or choose Exit from the File menu.

Tips:

- If you exit the SNMP Agent, the SNMP network manager cannot access and manage your workstation.

{button ,AL(`start and stop')} Related Topics

Understanding the Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) allows remote SNMP network managers to manage other machines on a network (for example, routers, hubs, and workstations), if both the SNMP network manager and managed machines abide by the SNMP rules. SNMP is an open standard, so you can mix and match SNMP network managers and SNMP agents (managed machines) from different vendors.

Because SNMP network managers are capable of changing the configuration of managed machines, SNMP uses passwords called communities to ensure that only SNMP network managers known to the agent machines (for example, your workstation) are allowed to view or change information on the agent machine. Every SNMP message sent to an SNMP agent must include a valid community name. Otherwise, the SNMP agent sends notification of the authentication error to an SNMP network manager that is handling these errors (called traps).

SNMP Agents can also send traps for other kinds of events. The SNMP Agent sends all standard SNMP traps.

SNMP maintains information about your workstation in a management information base (MIB). The SNMP Agent complies with the MIB-II definition, which is the Internet standard. If you change the information about your workstation (for example, the description or trap destinations), you must restart the SNMP Agent so that the new information is available to the SNMP network manager. Restart the SNMP Agent by clicking the Stop button, and then clicking the Start button.

The SNMP Agent is based on the SNMPv1 definition.

{button ,AL(`start and stop;System tab;Trap tab')} Related Topics

{button ,KL(`for more information about SNMP')} For more information

Understanding SNMP Communities

An SNMP community is a type of password used by the SNMP network manager and SNMP agents to ensure that only known and trusted machines can send and receive SNMP messages to each other. Every SNMP message includes a community name, so that every message can be validated.

These are the types of community names:

Read	The SNMP network manager must use the correct read community name when asking your SNMP agent to send it information about your machine. The default read community name is **public**.
Write	The SNMP network manager must use the correct write community name when asking your SNMP agent to change some characteristic about your configuration. There is no default write community name.
Trap	If certain events happen in your workstation (for example, you reboot your machine, or an SNMP network manager sends an SNMP message that contains the wrong read or write community password), your SNMP Agent sends a trap message to an SNMP network manager. For your trap message to be handled, the trap community name you send must match the name known to the target SNMP network manager. There is no default trap community name.

{button ,AL(`System tab;Trap tab')} Related Topics

Understanding SNMP Traps

One of the main uses of SNMP is to make it easy to track important events that occur on the managed network. To help automate network management, SNMP agents send **trap messages** to the SNMP network manager when certain events occur. For example, your workstation sends traps when you reboot it. The SNMP Agent sends all standard SNMP traps.

One important type of SNMP trap is the **authentication failure trap**. Because SNMP network managers have access to sensitive configuration settings for the machines on a managed network, it is important that the network administrators guard against breaches in network security that involve illegitimate use of SNMP messages.

For this reason, every SNMP message must be authenticated by SNMP network managers and SNMP agents using passwords called communities. If your agent gets an SNMP message that contains an incorrect community name for the type of operation requested, your agent sends a message to another SNMP network manager. This message contains information about the request your agent received: what the message requested, and why your agent would not fulfill the request.

Ask your network administrator for the address of the machines that handle traps before setting up the SNMP Agent to handle traps.

{button ,AL(`Trap tab')} Related Topics

For More Information About SNMP

Recommended Reading

For an excellent conceptual overview of TCP/IP networking concepts, we recommend the following books:

Comer, Douglas E., **Internetworking with TCP/IP**, Volume I and II, Prentice Hall

Black, Uyless D., **TCP/IP and Related Protocols**, McGraw-Hill

{button ,JI(`glossary.hlp',`Recommended_Books_on_TCP_IP_Connectivity')} List of recommended books

Relevant RFCs

For more information on the SNMP specifications, consult the following RFCs:

Structure of Management Information	RFCs 1155, 1212, 1215
Management Information Bases	RFC 1213
SNMP	RFC 1157
SNMP Administrative Model	RFC 1351

{button ,JI(`glossary.hlp',`How_to_Get_Internet_RFCs')} How to get RFCs