Framework Management Layer User's Guide

SNMP Interface

4/14/2025

SNMP Interface

Contents

The Management Layer provides support for SNMP-compliant third-party NMS. Solution Control Server (SCS) processes various NMS commands and generates SNMP traps based on changes in the current status of an individual application. With this support for SNMPv1–v3, you can access Management Layer functions through your existing NMS interface.

> **Important**
>
> The Genesys built-in SNMP implementation, provided by the Genesys SNMP Master Agent component, for SNMPv1 passed all the tests developed and published by CERT/CC for this sort of application. For information about tests with which you can check your system against vulnerability to SNMPv1 malformed SNMP packets, go to http://www.cert.org/advisories/CA-2002-03.html.

Architecture

The Management Layer provides you, as a network administrator, with three ways to monitor and control Genesys products via an NMS user interface:

- You can start, stop, and monitor the status of any Genesys or third-party application that the Management Layer monitors and controls. In addition, you can modify log options for Genesys server applications.
- You can retrieve application-specific SNMP statistics and data as defined in the MIB file for those Genesys server applications that support application-specific SNMP requests.
- You can receive alarms from any Genesys server application in the form of SNMP traps.

With all three options, the communications between SCS and NMS require an SNMP Master Agent application that is compliant with the AgentX protocol. If your NMS does not contain such an application, you can use Net-SNMP (release 8.5.1 and later) and/or Genesys SNMP Master Agent to integrate the Management Layer into your NMS. The Genesys MIB file, which the NMS uses, defines the communication interface between the Management Layer and the NMS.

SNMP Command Processing

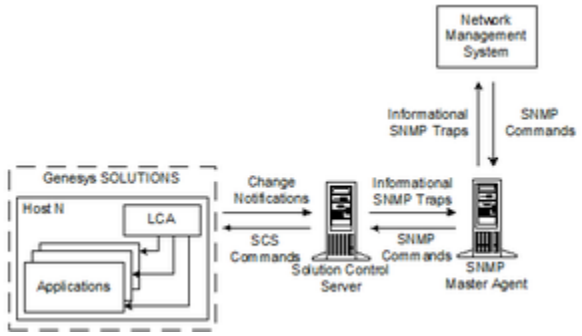
The figure below illustrates how the Management Layer processes the SNMP commands it receives from an NMS. The commands include:

- Start and stop commands for any Genesys or third-party application that the Management Layer monitors and controls.
- Change of log options settings for Genesys server applications.

With this architecture, you can also:

- View the configuration of any Genesys or third-party product that the Management Layer monitors and controls.

- Monitor the current status of an application (see if it is running or not) and, for redundant configurations, view the current redundancy mode (Primary or Backup) of a running application.
- View the configuration and status of any host registered as a Host object in the Configuration Database, including the LCA configuration of that host.
- View configured solutions and their statuses (see if solutions are running).



Management Layer Processing of an SNMP Command from an NMS

Requesting SNMP Data

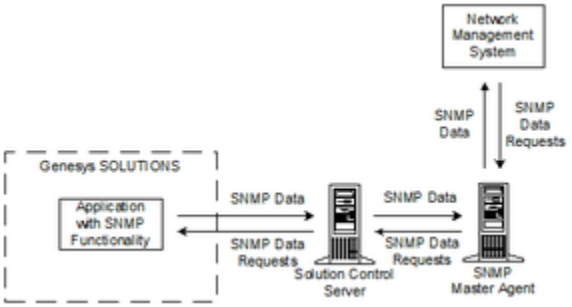
In addition to its application-monitoring functions, you can use the Management Layer to retrieve some SNMP data particular to applications of a given type. For example, you can request from T-Server the number of calls it is currently handling.

You can only retrieve SNMP data and prompt application-specific SNMP traps for applications built with the Genesys management library, such as:

- Call Concentrator
- Configuration Server
- Universal Routing Server
- T-Server

The following diagram illustrates how these applications interact with an NMS. All requests from the NMS and data and traps from the applications come through Solution Control Server.

Consult product-specific documentation to see if your product supports SNMP.



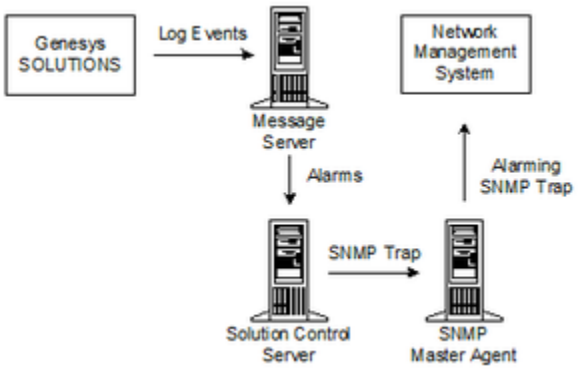
SNMP Information Exchange Between Some Servers

and NMS

Alarms and SNMP Trap Processing

To transmit the content of an alarm message to an SNMP-compliant third-party NMS, the Management Layer converts that information into an SNMP trap. An *alarm* is a message generated by a Genesys application when a certain Alarm Condition is met. For more information about alarm signaling, see Alarm-Signaling Functions and *Genesys Administrator Help*.

The following diagram illustrates how the Management Layer reacts to an alarm of type Send an SNMP trap.



Management Layer Processing of an SNMP Trap Alarm Reaction

How to Activate SNMP Support

You must make some changes in your Genesys installation to enable SNMP communications between the Management Layer and your Network Management System.

As already mentioned, the communications between SCS and NMS require an AgentX-compliant SNMP Master Agent application:

- If your NMS already contains such an application, configure an Application object for it in the Configuration Database. See the *Genesys Administrator Help* for instructions.
- If you want to use Genesys SNMP Master Agent or Net-SNMP, deploy it as described in the *Framework Deployment Guide*.

For either configuration, order licenses that enable the SNMP functionality of the Management Layer and modify the licensing system as needed. Refer to the *Genesys Licensing Guide* for more information.

Stand-alone or Redundant SNMP Master Agents

The Management Layer supports two types of configuration—stand-alone and redundant. Stand-alone configuration consists of a single SNMP Master Agent. Redundant configuration consists of two

SNMP Master Agent applications, one primary and one backup. When Solution Control Server loses a connection with the primary SNMP Master Agent, SCS switches all NMS communications to the backup SNMP Master Agent.

> **Important**
>
> You must use 8.5.1 or later versions of SCS and LCA to be able to configure multiple SNMP Master Agent applications as HA pairs that SCS will recognize and connect. With earlier versions of Management Layer components, you must configure each SNMP Master Agent as standalone and make sure autorestart is enabled to allow the automated restart of SNMP in case of failure. In this situation, SCS will always use a single configured SNMP MA to report its status over AgentX protocol.

Both Net-SNMP and Genesys SNMP Master Agent implementations of SNMP support redundant configuration when used with SCS and LCA 8.5.1 or newer. A redundant configuration consists of two SNMP Master Agent Application objects, one primary and one backup. When SCS loses a connection with the primary SNMP Master Agent, SCS switches all NMS communications to the backup. The only difference is in the redundancy type set in the primary Genesys SNMP Master Agent Application object—`Hot Standby` for the Genesys SNMP Master Agent implementation, and `Not Specified` for Net-SNMP.

> **Important**
>
> The mode for both the primary and backup SNMP Master Agents in the HA pair is displayed as Primary.

Refer to the *Framework Deployment Guide* for detailed instructions about deploying both stand-alone and redundant SNMP Master Agents.

Setting Configuration Options

The *Framework Configuration Options Reference Manual* describes configuration options and their values for SNMP Master Agents. You can alter trap configuration (target host, port, community, and multiple trap destinations) by modifying `SNMP_TARGET_MIB`, which you maintain externally with SNMP commands through SNMP Master Agent. Refer to RFC 2273 (SNMPv3 Applications) for further information about how to configure traps via standard management MIBs.

Solution Control Server reads the configuration settings of the SNMP Master Agent Application object and uses option values from the **[agentx]** configuration section to connect to SNMP Master Agent. This is true for both Genesys SNMP Master Agent and a third-party SNMP Master Agent. Therefore, if you are using a third-party SNMP Master Agent, make sure that the option values configured for the SNMP Master Agent Application object in the Configuration Database match the actual configuration settings in your third-party SNMP Master Agent.

How to Use Contact-Center Graceful Shutdown Script

Management Layer provides authorized users with capability to gracefully shut down contact-center software. This functionality, implemented in the form of a PERL script, operates through the Management Layer SNMP Interface.

The Contact-Center Graceful Shutdown script (called `ccgs.pl`) does the following:

1. Enumerates all currently running T-Servers.
2. Determines if there are ongoing interactions in the contact center by querying the number of active calls from each T-Server.
3. If there are active calls, waits one minute and then checks again.
4. When there are no more active calls, shuts down T-Servers.

Installing the Script

If you installed Solution Control Server, `ccgs.pl` is already installed, and is located in the same folder in which Solution Control Server was installed.

Starting in 8.1.2, you can install the Solution Control Server utilities without installing Solution Control Server itself. If you have not installed the utilities, use the procedure “Installing Solution Control Server Utilities” in the *Framework Deployment Guide*. After the utilities are installed, `ccgs.pl` is stored in the location you specified during the installation.

The SCS installation package also includes all additional PERL modules necessary to utilize the Management Layer SNMP Interface with PERL scripts.

Using the Script

Start the script file with the command line in this format:

```
ccgs.pl [<parameter> <value>] [<parameter> <value>] ...
```

Separate parameters from their values with a space.

The script accepts the following command-line parameters:

Contact-Center Graceful Shutdown Script Parameters

Parameter	Description	Default Value
-h	SNMP Master Agent host name or IP address	localhost
-p	SNMP Master Agent SNMP port	161
-c	Community string	public
-v	SNMP version (v1 or v2c)	v2c
-pt	Polling timeout—Time, in seconds, the script waits for the end of data tables refresh; should be equal to or greater than 5.	60

-mic	Maximum number of idle polling cycles the script waits before exit. An idle polling cycle is one when no shutdown requests are sent. Should be equal to or greater than 1.	100
-st	SNMP timeout—Timeout, in seconds, during which the script waits for a response after a request is sent. Note that when a request is retried, the timeout is increased by the SNMP backoff factor (`-sb`). Should be equal to or greater than 1.	2
-sr	SNMP retries—Number of attempts that the script prompts for a reply to the SNMP request. If no response is received within the timeout specified in value -st, the request is resent and a new response awaited with a longer timeout. Should be equal to or greater than 1.	5
-sb	SNMP backoff factor—Used to increase the timeout every time an SNMP request is retried. Should be equal to or greater than 1.	1