# Framework Management Layer User's Guide

Troubleshooting

12/20/2025

# Troubleshooting

## Contents

This section contains suggestions on how to identify and handle the most common mistakes made when you are enabling the Management Layer functionality.

## Major Checkpoints

The Management Layer must be configured correctly to function properly. When you are configuring the Management Layer, ensure that it operates properly by using the following checklist:

- SQL server is running and configured properly.
- Configuration Server is running.
- Solution Control Server (SCS) is running.
- Local Control Agent (LCA) is running with sufficient permissions on each monitored host.
- At least one instance of Message Server is running.
- Message Server, used for centralized logging, has the **db_storage** configuration option set to `true`. (Check the `messages` section on the **Options** tab of the Message Server Application object.)
- The Log Database scripts have been executed successfully.
- The user account that is specified in the **DB Info** section of the Database Access Point Application object, and is used for accessing the Log Database, has Write permissions configured in the Database Management System (DBMS).
- All monitored applications have the verbose configuration option set to a value other than none. (Check the `log` section in the **Options** tab of the Application object.)
- All monitored applications have the network output type specified. (Check the `log` section in the **Options** tab of the Application object.)
- A connection to Message Server is configured in the Application object's **Connections**.
- A connection to Message Server is configured in the SCS Application object's **Connections**.
- In Genesys Administrator:
    - A connection to the correct SCS is configured in the Configuration Manager Application object's **Connections**.
    - The same Database Access Point Application object is specified in the **Connections** of both Configuration Manager and Message Server Application objects.

### Important

Refer to the *Framework Configuration Options Reference Manual* for configuration option descriptions and information about their valid values.

## Application Start/Stop

This section suggests actions to take if you have difficulty enabling Management Layer's control functionality.

### Applications Cannot Be Started

- Make sure that LCA is running on the host on which the application is installed.
- Check the SCS log to make sure that connection to the LCA running on the application's host is established.
- Make sure that the command-line parameters are specified in the Application object's properties.
- Make sure LCA has sufficient permissions to start an application.
- Make sure that the application is installed on the host specified in the Application object's **Start Info** section in Genesys Administrator.

### Applications Cannot Be Stopped

- Make sure LCA has sufficient permissions to stop an application.

### Connectivity Failure and Microsoft's Media-Sense Feature

In the Microsoft Windows XP operating system, when a host is disconnected from the network, LCA may start second instances of Solution Control Server and Configuration Server even though these components are already running. That in itself is harmless because Framework detects and terminates the additional CS instance and the additional SCS instance never connects to Framework.

The probable cause of this effect is Microsoft's media-sense feature, included with Windows XP system, which enables a NIC (Network Interface Card) to detect if a network cable is connected to it. The default setting of this feature (on) has these effects:

- If any cable is disconnected, Windows disables the protocols on the adapter, which affects TCP/IP (although loopback of 127.0.0.1 in your HOSTS file still works). This affects applications that require IP connectivity to remain constant; for example, laptops.
- If a network cable is disconnected, Windows also disables the entire network protocol stack, which means that you cannot reach network addresses on your own system.

If you find these effects undesirable, you should disable media-sense. Use the following steps to do this for systems that use TCP/IP.

1. Start the registry editor (`regedit`).
2. Move to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`
3. From the **Edit** menu select `New - DWORD value`.
4. Name the new item `DisableDHCPMediaSense` and press **Enter**.
5. Double click the new value and set it to 1.

6.  Click **OK**.

7.  Reboot the computer.

Point your browser to www.microsoft.com, and search for *media-sense* to read more information about disabling this feature.

# Alarming

This section suggests actions to take if you have difficulty enabling Management Layer's alarm-signaling functionality.

## No Active Alarms in Genesys Administrator

*   Check the configuration of the Alarm Condition Application object and make sure that the correct Detect Log Event ID is specified.

*   Make sure that the log message appears in a local log file.

*   Make sure that all monitored applications have the network output type. (Check the `log` section in the Application object's **Options** tab.)

*   Make sure that the **verbose** configuration option is set to send log messages of the needed level.

*   Check the Message Server log to make sure that Message Server receives log messages.

*   Make sure that the correct Message Server is configured in the SCS Application object's **Connections**.

*   Check the Message Server log to make sure that Message Server sends messages to SCS.

*   In Genesys Administrator, make sure that the correct SCS is configured in the Configuration Manager Application object's **Connections**.

## No Alarm Reactions Executed

*   Make sure that the alarm is triggered (see No Active Alarms in Genesys Administrator).

*   Make sure that a Script object of the Alarm Reaction type is specified on the **Reaction Scripts** tab of the Alarm Condition's properties.

## No Alarm Reactions "Send SNMP Trap" Executed

*   Make sure that the alarm is triggered (see No Active Alarms in Genesys Administrator).

*   Make sure that a Script object of the Alarm Reaction type is specified on the **Reaction Scripts** tab of the Alarm Condition's properties.

*   Make sure that the Genesys or a third-party SNMP Master Agent is installed and configured as required. See SNMP Support.

## No Alarm Reactions "Send E-Mail" Executed

- Make sure that the alarm is triggered (see No Active Alarms in Genesys Administrator).

- Make sure that a Script object of the Alarm Reaction type is specified on the **Reaction Scripts** tab of the Alarm Condition's properties.

- Make sure that the email system is installed and configured as required. (See Configuring E-mail Systems.)

- Make sure that the correct email address is specified for the Alarm Reaction Script object.

# Alarm Reaction

This section suggests actions to take if you have difficulty enabling alarm reactions of the Send an email and Send an SNMP Trap types.

## E-Mail

- Make sure the host on which SCS is running has an email system, which is installed, configured, and running correctly.

See also E-Mail Alarm Reactions.

## SNMP Traps

- Make sure that the SNMP Master Agent Application object is configured in the SCS Application object's **Connections**.

- Make sure that the host and port parameters are specified correctly on the SNMP Master Agent Application object's **Server Info** section in Genesys Administrator).

- Make sure that the configuration options are set correctly in the SNMP Master Agent Application object's **Options** tab.

See also SNMP Traps.

# Logging

This section suggests actions to take if you have difficulty enabling Management Layer's logging functionality.

## No Application Logs

- Check the log section in the Application object's **Options** tab and make sure that the **verbose** configuration option is set to a value other than none.

- Check the `log` section in the Application object's **Options** tab and make sure that at least one output type is specified.

## No Log Messages in Genesys Administrator

- Check the `log` section in the Application object's **Options** tab and make sure that the **verbose** configuration option is set to a value other than none. Then check the value of the configuration option that corresponds to the value of **verbose** and make sure that it is set to **network**.

- Make sure that Message Server is configured in the Application object's **Connections**.

- Check the `messages` section in the Message Server Application object's **Options** tab and make sure that the **db_storage** configuration option is set to `true`.

- Make sure that a user with Write permission is configured in the DBMS and that the same user account is specified in the **DB Info** section of the Database Access Point.

- In Genesys Administrator, make sure that the same Database Access Point Application object is specified in the **Connections** of both Configuration Manager and Message Server.


# Distributed SCS Functionality

This section suggests actions to take if you have difficulty enabling Distributed mode for Solution Control Servers that control your environment. Refer to the *Framework Deployment Guide* for detailed instructions and information about configuring distributed Solution Control Servers.

## Incorrect Message Server Configuration

- Make sure you have a Message Server dedicated to support communications among Distributed Solution Control Servers. Verify that the **signature** configuration option is set to the **scs_distributed** value in the `MessageServer` section in that Message Server Application object's Options tab.

## Incorrect SCS Configuration

- Make sure that the **distributed_mode** configuration option is set to the `ON` value in the `general` section in each configured SCS Application object's Options.

- Make sure that the Message Server Application object that you dedicated to support Distributed SCS communications is specified on each configured SCS Application object's **Connections**.

## Incorrect SCS Role Configuration

- If you decide not to have a main Distributed SCS control all unassigned configuration objects, make sure that the **distributed_rights** configuration option is either not configured or not set to the `MAIN` value in the `general` section in each configured SCS Application object's Options.

- If you decide to have a main Distributed SCS control all unassigned configuration objects, make sure that the **distributed_rights** configuration option in the general section is set to:

    - The `MAIN` value in the Options of the SCS Application object you designate as the main Distributed

SCS.

- The DEFAULT value in the Options for the rest of the SCS Application objects.

## Incorrect Configuration of Controlled Objects

- If you decide not to have a main Distributed SCS control all unassigned configuration objects, make sure that you assign a particular SCS to each Host, Application, and Solution object:
  - For Host objects, specify a Distributed SCS for the Host object.
  - For Application objects, specify a Distributed SCS for the Host object with which the Application is associated.
  - For Solution objects, specify a Distributed SCS for the Solution object.