Framework Management Layer User's Guide

Predefined Alarm Conditions

5/5/2025

Predefined Alarm Conditions

Genesys software includes several predefined alarm conditions that are available immediately after you set up Framework. The conditions under which alarms are generated, the actions automatically taken by the system to cope with or recover from the failure, and the maintenance actions appropriate in each situation are discussed for each alarm condition.

The following alarm conditions are predefined:

- Connection Failure
- Application Failure
- Licensing Error
- CTI Link Failure
- Host Inaccessible
- Service Unavailable
- Host Unavailable
- Host Unreachable
- Unplanned Solution Status Change
- Message Server Loss of Database Connection

Connection Failure

The Connection Failure Alarm Condition reports that the specified connection between any two applications has been lost. It is always reported by the client application and might indicate one of the following:

- The connection was intentionally closed by the server (for example, in response to an overload situation).
- The connection was closed by a networking software (for example, in response to a long interval without any data exchange through the given connection).
- The server terminated.
- The server stopped responding.
- The server host failed.
- A network connectivity problem occurred between the computers that run the given client application and the server.

The following table describes the fields of this Alarm Condition. **[+] Show fields**

Connection Failure Predefined Alarm Condition

Field Name	Value and Description
Name	Connection Failure
Description	The connection between any two Genesys components has been lost.
Category	Major
Detect Event	**00-04504**: `Connection to [server type] [server name] at host [host name] port [port number] lost`
Selection Mode	Select By Any
Cancel Event	**00-04503**: `Connected to [server type] [server name] at host [host name] port [port number]`
Cancel Timeout	48 hours
Reaction Scripts	None
Clearance Scripts	None
State Enabled	True

Refer to *Framework Combined Log Events Help* for full descriptions of the Detect and Cancel Events.

Automatic Recovery Actions

- If a backup server for the specified server is not configured, the client application that reported the connection failure periodically attempts to reconnect to the specified server.
- If a backup server for the specified server is configured, the client application that reported the connection failure attempts to connect interchangeably to the specified server and the backup server.

> **Important**
>
> The number of reconnect attempts is unlimited.

- After a successful reconnect attempt, the alarm condition is automatically cleared.

Suggested Maintenance Actions

1. Check the condition of the server host computer.
2. Check the condition of the server.
3. Check the server log to see if the given application has disconnected intentionally. Look for log events with ID **04523**.
4. Check the network connectivity between the computers that run the given application and the server.

Application Failure

The Application Failure Alarm Condition Reports that the specified application has either terminated or stopped responding. It might indicate one of the following:

- The application terminated because of an internal condition.
- The application was closed by means other than the Management Layer (for example, with an operating system command).
- The application entered a no-response condition.

The following table describes the fields of this Alarm Condition. **[+] Show fields**

Application Failure Predefined Alarm Condition

Field Name	Value and Description
Name	Application Failure
Description	Failure of any daemon Genesys component monitored by the Management Layer
Category	Major
Detect Event	**00-05064**: `Application terminated due to internal condition`
Selection Mode	Select by any
Cancel Event	**00-05090**: `Application start detected by Management Layer`
Cancel Timeout	48 hours
Reaction Scripts	None
Clearance Scripts	None
State Enabled	True

Refer to *Framework Combined Log Events Help* for full descriptions of the Detect and Cancel Events.

Automatic Recovery Actions

- If a backup application for the specified application is not configured and **Auto-Restart** is selected in the application's properties, the Management Layer attempts to restart the specified application.
- If a backup application for the specified application is not configured and **Auto-Restart** is not selected in the application's properties, no automatic recovery action takes place.
- If a backup application for the specified application is configured and **Auto-Restart** is selected in the application's properties, the Management Layer switches operations over to the backup application and attempts to restart the specified application in Standby mode.
- Upon a successful attempt to restart the specified application, the alarm is automatically cleared.

Suggested Maintenance Actions

1. Using Genesys Administrator, locate the exact source of the alarm and check the current status of the

application. It is likely that the fault has been eliminated through an automatic recovery action.

2. If the alarm is still active, check the status of the application through the operating system tools.
3. If the application is running but not responding, restart the application with an operating system command.
4. If the application is not running, start the application with an operating system command.
5. Ensure that SCI shows the status of the application correctly.
6. Verify that the Auto-Restart check box for this application is selected.

Licensing Error

The Licensing Error Alarm Condition reports that a licensing error has occurred. Possible violation types are as follows:

- License information is invalid.
- Licensable feature has expired.
- Feature usage level has been exceeded.
- Licensing system has experienced a general failure.

The following table describes the fields of this Alarm Condition. **[+] Show fields**

Licensing Failure Predefined Alarm Condition

Field Name	Value and Description
Name	Licensing Failure
Description	Any licensing error identified by any Genesys component
Category	Critical
Detect Event	**00-07100**: `Licensing violation is identified, the violation type [type]`
Selection Mode	Select by any
Cancel Event	None
Cancel Timeout	48 hours
Reaction Scripts	None
Clearance Scripts	None
State Enabled	True

Refer to *Framework Combined Log Events Help* for a full description of the Detect Event.

Automatic Recovery Actions

None

Suggested Maintenance Actions

Depending on the value of the error code:

- Check the condition of License Manager. If the type of license you have requires License Manager, it should be running and accessible by the Genesys applications. Check that the host and port of License Manager are specified correctly.
- Make sure that the actual location of the license file or license server corresponds to the location specified in the command-line parameter used for application startup.
- Make sure that the specified license file is the exact copy of the license file received from Genesys.
- Locate the exact source of the alarm and apply to Genesys for an extension of the license.
- Locate the exact source of the alarm and check the current usage level against the usage level stipulated in the license. Either decrease the usage level or apply to Genesys for a new license that covers the increased usage needs.

CTI Link Failure

The CTI Link Failure Alarm Condition reports that the connection between the specified T-Server and its switch has been lost. It is always reported by T-Server and might indicate one of the following:

- The connection was intentionally closed on the switch side (for example, as an automatic defense action).
- The control system of the switch failed.
- A network connectivity problem occurred between the T-Server host and the switch.

The following table describes the fields of this Alarm Condition. **[+] Show fields**

CTI Link Failure Predefined Alarm Condition

Field Name	Value and Description
Name	CTI Link Failure
Description	Failure of connection between any T-Server and its switch
Category	Major
Detect Event	**01-20002**: `CTI Link disconnected`
Selection Mode	Select by application type T-Server
Cancel Event	**01-20001**: `CTI Link connected`
Cancel Timeout	48 hours
Reaction Scripts	None
Clearance Scripts	None
State Enabled	True

Refer to *Framework Combined Log Events Help* for full descriptions of the Detect and Cancel Events.

Automatic Recovery Actions

T-Server attempts to reconnect to the CTI link.

Suggested Maintenance Actions

- Check the condition of the control system of the switch and of its CTI link.
- Check the network connectivity between the control system of the switch and the computer running T-Server.

Host Inaccessible

The Host Inaccessible Alarm Reaction reports that the Management Layer cannot contact the Local Control Agent on the host on which Genesys daemon applications are running. It might indicate one of the following (in the order of probability of occurrence in a typical production environment):

- The connection between SCS and the LCA of the specified host failed.
- LCA is not started on the specified host.
- LCA is listening on a port that is different from the one specified in the configuration.
- The LCA of the specified host has terminated or stopped responding.

The following table describes the fields of this Alarm Condition. **[+] Show fields**

Host Inaccessible Predefined Alarm Condition

Field Name	Value and Description
Name	Host Inaccessible
Description	The Management Layer cannot access a host computer on which Genesys daemon applications run.
Category	Major
Detect Event	**00-08000**: `Host [host name] inaccessible. LCA is not listening on port [port number].`
Selection Mode	Select by any
Cancel Event	**00-08001**: `Host [host name] operates in normal condition.`
Cancel Timeout	48 hours
Reaction Scripts	None
Clearance Scripts	None
State Enabled	True

Refer to *Framework Combined Log Events Help* for full descriptions of the Detect and Cancel Events.

Automatic Recovery Actions

By default, this failure is treated by the Management Layer as a failure of every Genesys application running on the given host. For the applications located on the given host that have redundancy, the Management Layer makes their backup applications primary. After that, Solution Control Server makes repeated attempts to restore connection with the LCA of the specified host. Once the connection is restored, the Management Layer attempts to start all applications that were running before the alarm occurred.

Suggested Maintenance Actions

1. Check the condition of LCA. If LCA terminated or stopped responding, restart LCA. Notify Genesys Customer Care about the LCA failure.
2. Verify the LCA command line parameters and make sure that LCA listens on the same port as the one specified in the Configuration Database.

Service Unavailable

The Service Unavailable Alarm Condition reports that a Genesys component cannot provide service for some internal reasons.

The following table describes the fields of this Alarm Condition. **[+] Show fields**

Service Unavailable Predefined Alarm Condition

Field Name	Value and Description
Name	Service Unavailable
Description	A Genesys component is unable to provide service for some internal reasons.
Category	Major
Detect Event	**00-05094**: `Application is not able to provide service.`
Selection Mode	Select by any
Cancel Event	**00-05093**: `Application is ready to provide service.`
Cancel Timeout	48 hours
Reaction Scripts	None
Clearance Scripts	None
State Enabled	True

Refer to *Framework Combined Log Events Help* for full descriptions of the Detect and Cancel Events.

Automatic Recovery Actions

If a backup application for the specified application is configured, the Management Layer switches

operations over to the backup application.

Suggested Maintenance Actions

This alarm occurs because of internal application reasons. Examine the log of the application that signaled the alarm to determine and eliminate the source of the problem.

Host Unavailable

The Host Unavailable Alarm Condition reports that a host on which Genesys daemon applications are running is unavailable (turned off). It might indicate one of the following (in the order of probability of occurrence in a typical production environment):

- Specified host has failed or has been turned off.
- Network problems prevents SCS from connecting to LCA at the specified host.

The following table describes the fields of this Alarm Condition. **[+] Show fields**

Host Unavailable Predefined Alarm Condition

Field Name	Value and Description
Name	Host Unavailable
Description	A host on which Genesys daemon applications are running is unavailable (turned off).
Category	Major
Detect Event	**00-08002**: `Host [host name] unavailable.`
Selection Mode	Select by any
Cancel Event	**00-08001**: `Host [host name] operates in normal condition.`
Cancel Timeout	48 hours
Reaction Scripts	None
Clearance Scripts	None
State Enabled	True

Refer to *Framework Combined Log Events Help* for full descriptions of the Detect and Cancel Events.

Automatic Recovery Actions

This failure may occur when an SCS attempt to connect to the LCA at the specified host fails. This failure is determined based on the error code returned by the networking subsystem. No automatic recovery actions are performed when this failure occurs.

Suggested Maintenance Actions

1. Check the condition of the host. If the host failed, take measures to restore its normal operating

condition. Once the normal condition is restored, the Management Layer automatically brings up all Genesys applications that are supposed to be running.

2. Check the condition of the network. Make sure that it is possible to reach the host of interest from the host on which SCS is running.

Host Unreachable

The Host Unreachable Alarm Condition reports that the Management Layer cannot reach the host on which Genesys daemon applications are running (no route to the host). It might indicate the following:

- Network configuration is incorrect: there is no route to the host of interest from the host on which SCS is running.

The following table describes the fields of this Alarm Condition. **[+] Show fields**

Host Unreachable Predefined Alarm Condition

Field Name	Value and Description
Name	Host Unreachable
Description	The Management Layer cannot reach the host on which Genesys daemon applications are running (no route to the host).
Category	Major
Detect Event	**00-08003**: `Host [host name] unreachable.`
Selection Mode	Select by any
Cancel Event	**00-08001**: `Host [host name] operates in normal condition.`
Cancel Timeout	48 hours
Reaction Scripts	None
Clearance Scripts	None
State Enabled	True

Refer to *Framework Combined Log Events Help* for full descriptions of the Detect and Cancel Events.

Automatic Recovery Actions

This failure may occur when an SCS attempt to connect to the LCA at the specified host fails. This failure is determined based on the error code returned by the networking subsystem. No automatic recovery actions are performed when this failure occurs.

Suggested Maintenance Actions

Check the condition of the network. Make sure that routing is configured correctly in the network and that it is possible to reach the host of interest from the host on which SCS is running.

Unplanned Solution Status Change

The Uplanned Solution Status Change alarm Condition reports that a solution status has changed from Started to Pending without any requests to stop the solution. It might indicate the following:

- Failure of one or more of the solution components.

The following table describes the fields of this Alarm Condition. **[+] Show fields**

Unplanned Solution Status Change Predefined Alarm Condition

Field Name	Value and Description
Name	Unplanned Solution Status Change
Description	Solution status has changed from Started to Pending without any requests to stop the solution. This may indicate a failure of one of the solution components.
Category	Major
Detect Event	**43-10385**: `Solution [solution name] nonplanned change of state from Started to Pending.`
Selection Mode	Select by any
Cancel Event	**43-10370**: `Solution [solution name] is started.`
Cancel Timeout	48 hours
Reaction Scripts	None
Clearance Scripts	None
State Enabled	True

Refer to *Framework Combined Log Events Help* for full descriptions of the Detect and Cancel Events.

Automatic Recovery Actions

If this alarm occurred because of the failure of one or more of the solution components, the Management Layer performs the same automatic recovery actions for each failed application as described for the Application Failure alarm condition.

Suggested Maintenance Actions

For each failed solution component, perform the same Maintenance Actions as suggested for the Application Failure alarm condition.

Message Server Loss of Database Connection

The Message Server Loss of Database Connection reports that Message Server has lost connection to

the Centralized Log Database. It might indicate one of the following (in the order of probability of occurrence in a typical production environment):

- Failure of the DB Server used by Message Server to access the Centralized Log Database.
- Failure of the DBMS that stores the Centralized Log Database.

The following table describes the fields of this Alarm Condition. **[+] Show fields**

Message Server Loss of Database Connection Predefined Alarm Condition

Field Name	Value and Description
Name	Message Server Loss of Database Connection
Description	Message Server has lost connection to the Centralized Log Database.
Category	Major
Detect Event	**42-11051**: `Connection with DB Cluster lost.`
Selection Mode	Select by application type Message Server
Cancel Event	**42-11050**: `Connection with DB Cluster established ([host name]:[port number]).`
Cancel Timeout	48 hours
Reaction Scripts	None
Clearance Scripts	None
State Enabled	True

Refer to *Framework Combined Log Events Help* for full descriptions of the Detect and Cancel Events.

Automatic Recovery Actions

If this alarm occurred because of the failure of DB Server used by Message Server to access the Centralized Log Database, the Management Layer performs the same automatic recovery actions for DB Server as described for the Application Failure alarm condition.

Suggested Maintenance Actions

1. In the case of Log DB Server failure, perform the same Maintenance Actions as suggested for the Application Failure alarm condition.
2. Otherwise, make sure that the DBMS that stores the Centralized Log Database is operating in normal condition.