Framework Management Layer User's Guide

How to Configure Alarm Conditions and Alarm Reactions

4/6/2026

Contents

How to Configure Alarm Conditions and Alarm Reactions

Although you can configure Alarm Condition objects and Alarm Reaction scripts manually, using Genesys Administrator, the Management Layer provides an automated procedure.

You can configure new Alarm Conditions based on either source for their detection:

- Log Events—These Alarm Conditions trigger an alarm when an application or applications generate a specified log event.
- Alarm Detection Scripts—These Alarm Conditions trigger an alarm when a certain system variable changes in a specified manner.

For alarms based on log events, alarm detection takes place in Message Server. Therefore, if you configure log event–based Alarm Conditions, you must configure your applications to connect to Message Server.

Using Log Events for Alarm Detection

To configure alarm conditions or alarm reactions in Genesys Administrator, create the alarm condition or alarm reaction under **Provisioning > Environment > Alarm Conditions**, being sure to specify the appropriate log event on the **Configuration** tab. You can also use pre-configured Alarm Condition objects. Refer to *Genesys Administrator Help* for detailed instructions about creating and using these necessary objects.

You can also use the Alarm Condition Wizard to associate Alarm Reactions with the Alarm Condition you are configuring.

For complete specifications of log events reported at the Alarm, Interaction, Standard, and Trace levels, see *Framework Combined Log Events Help*.

Using Detection Scripts for Alarm Detection

Management Layer provides an additional alarm-detection mechanism, called Advanced Alarm Detection. Through this mechanism, you can configure Alarm Conditions:

- Based on the threshold for a system performance variable (CPU or memory usage).
- Based on the threshold for a local or remote SNMP variable (available only when you have enabled SNMP functionality).

Set alarms based on the Advanced Alarm Detection methods using Alarm Detection scripts, and then

associate them with corresponding Alarm Conditions. When an Alarm Condition object refers to an Alarm Detection script, the alarm detection for this Alarm Condition is performed as specified by the Alarm Detection script, regardless of whether any log event is specified as a Detection Event.

Using Alarm Detection and Reaction Scripts with Alarm Conditions

To configure an Alarm Detection Script, do the following:

[+] Show steps

1. Log in to GAX if required.
2. **Configuration** > **Environment** > **Detection/Reaction Scripts**.
3. Navigate to the folder in which you want to store the new script, and click **New**.
4. Enter the following information for the new script:
   a. Enter the **Name** of the script.
   b. Make sure that **State Enabled** is checked.
   c. From the **Script Type** drop-down list, select **Alarm Detection**.
   d. From the **Detection Types** drop-down list, select one of the following tabs and proceed accordingly. Note that you must have SNMP functionality in your environment to monitor SNMP variables.

Host System Variable Threshold

To monitor a performance variable for a given Host, provide the following information:

i. Enter the DNS or IP address of the **Host** to be monitored.
ii. From the **Select Monitored Resource** drop-down list, select the resource to be monitored, either **Host CPU Usage (%)** or **Host Memory Usage (MB)**.

Application System Variable Threshold

To monitor a performance variable for a given Application, provide the following information:

i. Select the **Application** to be monitored.
ii. From the **Select Monitored Resource** drop-down list, select the resource to be monitored, either **Process CPU Usage (%)** or **Process Memory Usage (MB)**.

Local SNMP Variable Threshold

> **Important**
> You must have SNMP functionality configured in your environment to monitor SNMP variables.

To monitor a local SNMP variable, enter the oid of the variable in **Specify Local SNMP Variable**.

Remote SNMP Variable Threshold

> **Important**
> You must have SNMP functionality configured in your environment to monitor SNMP variables.

To monitor a remote SNMP variable, provide the following information:

i. Select the **SNMP Agent Application** in which the variable is used.

ii. Enter the name of the variable to be monitored in **Specify Local SNMP Variable**.

e. In **Specify Sample Interval**, specify (in seconds) the frequency with which to take a sample of the required information.

f. In **Specify Falling Threshold**, specify the level at which the monitored attribute must fall below to clear the alarm. Your entry must be in the same units of measure as the units of measure specified for the resource or variable that you are monitoring.

g. In **Specify Rising Threshold**, specify the level at which the monitored attribute must rise above to trigger the alarm. Your entry must be in the same units of measure as the units of measure specified for the resource or variable that you are monitoring.

5. Click **Save.**

If there is a specific automated action that you want to happen as a result of the alarm, configure an Alarm Reaction script. For example, to generate an SNMP trap when this alarm is triggered, do the following:

[+] Show steps

1. Log in to GAX if required.
2. **Configuration** > **Environment** > **Detection/Reaction Scripts**.
3. Navigate to the folder in which you want to store the new script, and click **New**.
4. Enter the following information for the new script:
   a. Enter the **Name** of the script.
   b. Make sure that **State Enabled** is checked.
   c. From the **Script Type** drop-down list, select **Alarm Reaction**.
   d. From the **Alarm Reaction Types** drop-down list, select **Send an SNMP trap**. You must have SNMP

functionality in your environment to monitor SNMP variables.

e. Click **Save**.

To create the corresponding Alarm Condition object, follow these steps:

[+] Show steps

1. Log in to GAX if required.
2. **Configuration** > **Environment** > **Alarm Conditions**.
3. Navigate to the folder in which you want to store the new Alarm Condition, and click **New**.
4. On the **General** tab, enter the following information for the new script:
   a. Enter the **Name** of the Alarm Condition.
   b. (Optional) Provide a short **Description** of the Alarm Condition.
   c. From the **Category** drop-down list, select the severity of the Alarm Condition, either **Critical**, **Major**, or **Minor**.
   d. In the **Detect Script** field, specify the name of the Alarm Detection Script that you created above, using the provided browser control if necessary.
   e. In the **Cancel Timeout** field, specify the time interval (in seconds) after which the alarm will be cleared by SCS. If the host CPU is still not normalized, the alarm will be generated again.
   f. In the **Detect Log Event ID** and **Cancel Log Event ID** fields, enter any numeric dummy value. These two fields are not used if you are using an Alarm Detection Script, and while ignored by the Management Layer in this case, are still mandatory.
   g. From the **Detect Selection** drop-down list, select the mode for event selection that the Management Layer uses for Alarm Condition analysis. Refer to Alarm Conditions in GAX Help for a detailed description of this field.
   h. Make sure that **State Enabled** is checked.
5. If you have created an Alarm Reaction Script for this Alarm Condition, link the Reaction Script to this Alarm Condition, as follows:
   a. On the **Reactions Scripts** tab, click **Add**.
   b. Navigate to, and select, the Alarm Reaction Script that you created above.
6. If you have created an Alarm Clearance Script for this Alarm Condition, link the Clearance Script to this Alarm Condition. In this case, an Alarm Reaction of type "Send an SNMP trap" also acts as its own Alarm Clearance Script, since there is no waiting involved; that is, once the Alarm Reaction is complete, the Alarm can be cleared—the trap has been sent. So, you just need to specify the same script as the Clearance Script, as follows:
   a. On the **Clearance Scripts** tab, click **Add**.
   b. Navigate to, and select, the Alarm Reaction Script that you created above.
7. Click Save.

Important

If you select **Select By Any** in the **Detect Selection** field (step 4g) when creating the Alarm Condition object, be aware that SCS creates an alarm if a situation involving *any* application or host produces the Detect Event ID. Likewise, it clears the alarm if *any* application or host produces the Clearance Event ID. As a result, specific Alarm Conditions such as Host Inaccessible, Host Unavailable, and Host Unreachable (see Predefined Alarm Conditions) will trigger an alarm for the first Host that encounters one of the conditions, and stay triggered for all other hosts that encounter one of these conditions. The alarm is cleared only when the first of the affected hosts recovers.
To avoid this problem, and to more accurately monitor these conditions, Genesys suggests that you manually clear each alarm as it occurs on a host, so that next time it occurs, it will be generated by the affected host. Or, you can set **Cancel Timeout** (step 4e) to a minimal value so the alarm is automatically cleared shortly after detection.

Types of Alarm Reactions

You can configure alarm reactions of the following types:

- Start a specified application
- Stop a specified application
- Restart the application that generated the alarm
- Start a specified solution
- Send an email
- Send an SNMP trap
- Switch over to the backup application
- Execute OS command
- Change application option

The configuration procedure for most of the alarm reactions is self-explanatory in the Alarm Reaction Wizard. You must supply information for these configuration parameters:

- A unique name for the Alarm Reaction configuration object (for all types of alarm reactions).
- A name of the application or solution the alarm reaction is configured for (for alarm reactions of such types as Start a specified application, Stop a specified application, Start a specified solution, and Restart the application that generated the alarm).

You must provide additional information for alarm reactions of the following types:

- Switchover
- Send an E-Mail

- Send an SNMP Trap
- Execute OS command
- Change application option

Switchover

> **Warning**
> You must have a high-availability (HA) license to enable Solution Control Server to successfully process an alarm reaction of the Switchover type. The lack of the license prevents the switchover between primary and backup applications of any type.

When configuring an alarm reaction of the Switchover type, you can specify whether Solution Control Server should perform the switchover when an application, which generates an alarm, is running in a particular mode:

- Select `primary` if you want SCS to perform a switchover only if the application that has generated an alarm is currently operating in Primary mode.
- Select `backup` if you want SCS to perform a switchover only if the application that has generated an alarm is currently operating in Backup mode.
- Select `perform switchover always` if you want SCS to perform a switchover regardless of the operating mode of the application that generates the alarm.

You might use these options, for instance, when associating an alarm reaction of the Switchover type for T-Server with the CTI Link Disconnected log event. Selecting `primary` for the alarm reaction configuration may prevent an unwanted switchover if the T-Server that produced this log event currently operates in Backup mode.

Send an E-Mail

To configure an alarm reaction of type Send an E-Mail, specify the recipients of the email in the Alarm Reaction Wizard. Then, compose the subject and text of the email message, using reserved variables. See *Genesys Administrator Help* for detailed instructions on configuring the email script, including an example. See E-Mail Alarm Reactions for more information about the email interface itself.

Send an SNMP Trap

To configure an alarm reaction of the Send an SNMP Trap type, specify a Name for the Alarm Reaction configuration object. All necessary information is automatically provided by SCS, given that the SNMP Master Agent application is configured correctly.

See SNMP Interface for more information about enabling the SNMP alarm signaling.

Execute OS command

To configure an Alarm Reaction of the Execute OS Command type, specify the name of the operating

system command that is to be executed when an alarm is detected. If necessary, include the full path to the executed command.

> **Important**
>
> Although you can specify any valid command name, use alarm reactions of this type with caution. To avoid unauthorized actions, limit access to Solution Control Server and Genesys Administrator to the Administrators group.

SCS executes all alarm reactions. In the case of an alarm reaction of the Execute OS Command type, SCS executes the specified command on its own host computer. Therefore, a currently logged in user must have sufficient permissions to execute the specified operating system command.

SCS passes information about a detected alarm to the operating system command to be executed. For this purpose, SCS adds command-line arguments (listed in the table below) to the command line you specify in the **Command** property when you configure the alarm reaction.

> **Important**
>
> Some applications started as a result of the Execute OS Command alarm reaction may not recognize the command-line arguments added by SCS. This means that these applications might not work properly in this circumstance; for example, they might exit. To make them work, you can call such applications indirectly; for instance, from within a script that passes correct command-line parameters to these applications. You then specify name of this script in the **Command** property of the alarm reaction.

Additional Command-Line Parameters

The following table describes the additional command-line parameters that are added to the **Command** property when you configure an Execute OS Command Alarm Reaction.

[+] Show table

Additional Command-Line Parameters for Execute OS Command Alarm Reactions

Parameter	Description
-msgid	ID of the log event that resulted in the alarm
-msgtext	Text of the log event that resulted in the alarm
-condid	Alarm Condition ID
-condname	Alarm Condition Name
-conddesc	Alarm Condition Description
-appid	ID of the application that generated the log event that resulted in the alarm
-appname	Name of the application that generated the log event that resulted in the alarm

-hostname	Name of the application host that generated the log event that resulted in the alarm

Examples

The following are examples of how to use and configure Execute OS Command Alarm Reactions. **[+] Show examples**

Example 1 - Filtering by type of log event

To log occurrences of certain log events to a database other than the Genesys Log Database, create a ***.bat** file that provides logging in to your independent database. Name this file **process_alarm.bat**. Then using the Alarm Reaction Wizard, configure an Alarm Reaction of the Execute OS Command type and set the **Command** property to:

```
/home/Genesys/SCServer/scripts/process_alarm.bat
```

When a corresponding alarm is detected, SCS executes the following operating system command:

```
/home/Genesys/SCServer/scripts/process_alarm.bat -msgid 20002 -msgtext "CTI Link
disconnected" -condid 103 -condname "CTI Link Failure" -conddesc "Failure of
connection between any T-Server and a switch." -appid 120 -appname "T-
Server_Application" -hostname “NameOfHost”
```

> ### Important
> If a specified operating system command normally would result in a screen display, the alarm reaction is performed, but the screen output cannot be enabled and, therefore, cannot be seen.

Example 2 - Collecting information about alarms

A script called **react_script.sh**, for the bash UNIX shell, saves information about each alarm in the **reaction.log** text file located in the **/home/genesys/logs/** directory:

```
echo `date|cut -c4-16` : msgid=$2 : msgtext=$4 : condid=$6 : condname=$8 :
conddesc=${10} : appid=${12} : appname=${14} >> /home/genesys/logs/reactions.log
```

Example 3 - Filtering by the host that generated the alarm

To save information about alarms generated by a specific host, you must create a script that writes only those logs generated by a specific host. The following sample script, **HostA_alarms.sh** for the

bash UNIX shell, writes only those alarms generated by HostA to the **HostA_reactions.log** text file located in the **/home/genesys/logs/** directory.

```
while [ 0 -lt "$#" ]; do
case "$1" in
"-msgid") shift; MSGID="$1" ;;
"-msgtext") shift; MSGTEXT="$1" ;;
"-condid") shift; CONDID="$1" ;;
"-condname") shift; CONDNAME="$1" ;;
"-conddesc") shift; CONDDESC="$1" ;;
"-appid") shift; APPID="$1" ;;
"-appname")shift; APPNAME="$1" ;;
"-hostname")shift; HOSTNAME="$1" ;;
esac
shift
done
if [ $HOSTNAME = "HostA" ]; then
echo `date|cut -c4-16` : msgid=$MSGID : msgtext=$MSGTEXT : condid=$CONDID :
condname=$CONDNAME : conddesc=$CONDDESC : appid=$APPID : appname=$APPNAME >>
HostA_reactions.log
fi
```

Change application option

Select an application and specify its configuration options to be automatically set upon occurrence of an alarm event. With this type of alarm reaction, you can automatically change a specified configuration option of any given Daemon application on occurrence of same alarm event. Select an application whose configuration option is to be changed. If no application selected, the operation automatically applies to the application that triggered the alarm.