Genesys Administrator Extension Help

Alarm Conditions

12/18/2025

Alarm Conditions

Alarm Conditions specify the events that you might want to know about and manage as soon as they occur, such as if a Host or Solution is unresponsive. Genesys software contains predefined Alarm Conditions, or you can create your own.

Alarm Conditions work with the following Scripts:

- Alarm Detection Scripts, which identify what system variables the Management Layer must monitor to trigger an alarm.
- Alarm Reaction Scripts, which identify what the Management Layer must do when alarms occur in, or are cleared from, the system. Alarm Reaction Scripts that identify what happens when alarms are cleared are referred to as alarm Clearance Scripts.

To associate Alarm Detection and Alarm Reaction Scripts with Alarm Conditions, specify them in the tabs of the Alarm Condition.

Display Options

Display Options

The `Alarm Conditions` list shows the Alarm Conditions that are in your environment. It is sorted in a hierarchy by tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
> Alarm Conditions that are disabled will appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the `Quick Filter` field.
- Click the magnifying glass button to open the `Tenant Directory` filter panel. In this panel, click the Tenant that you want to select. Use the `Quick Filter` field in this panel to filter the Tenant list.

To select or de-select multiple objects at once, click the `Select` button.

Procedures

Possible Procedures from this Panel

To create a new Alarm Condition object, click the New button. To view or edit details of an existing object, click on the name of the object, or click the check box beside an object and click the Edit button.

To delete one or more objects, click the check box beside the object(s) in the list and click the Delete button. You can also delete individual objects by clicking on the object and then clicking the Delete button.

Otherwise, click the More button to perform the following tasks:

- Clone—Copy an Alarm Condition.
- Move To—Move an Alarm Condition to another hierarchical structure.
- Enable or disable Alarm Conditions
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click on the name of an Alarm Condition to view additional information about the object. You can also set options and permissions.

Creating Alarm Condition Objects

To create an Alarm Condition object, perform the following actions:

1. Go to Configuration > System > Configuration Manager.
2. Click Alarm Conditions. The Alarm Conditions list displays.
3. Click the New button.
4. Enter the following information. For some fields, you can either enter the name of a value or click the Browse button to select a value from a list:
   - Name—The name of the Alarm Condition. You must specify a value for this property and that value must be unique within the Configuration Database.
   - Description—A brief description of the Alarm Condition.
   - Category—The category of the Alarm Condition: Critical, Major, or Minor. You must specify a value for this property.
   - Detect Script—The Script that describes the logic applied to detect the alarm.
   - Cancel Timeout—The amount of time, in seconds, that the Alarm Condition is registered in the Log Database, unless another event cancels it or a user clears it. When this timeout expires, the Alarm Condition is unconditionally cleared.
   - Detect Log Event ID—The identifier of the event that triggers the alarm. You must specify a value for this property.

- Detect Selection—The mode for event selection that the Management Layer uses for Alarm Condition analysis. The modes are as follows:
  - Select By Any—The specified event from any application results in an alarm.
  - Select By Application—The specified event from a selected application results in an alarm. Select this option to display the Application field. Click the Browse icon to select an item from a list, or type the name or partial name of the item in the Quick Filter field. The list is populated with Application objects that are stored in Configuration Server.
  - Select By Application Type—The specified event from a selected application type results in an alarm. Select this option to display the Type field. Click the drop-down button to select an item from the list. The list is populated with Application objects that have defined subtypes.
- Cancel Log Event ID—The identifier of the event that triggers clearance of the alarm. For alarm clearance, the Management Layer uses the event from the same application(s) as specified for the detect event for this Alarm Condition.
- Tenant—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the Tenant Directory field in the object list.
- State Enabled—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

5. Click the Save button.

You can also set the Alarm Detection Scripts and Alarm Reaction Scripts.

Predefined Alarm Conditions

Predefined Alarm Conditions

Genesys provides the predefined Alarm Conditions listed in the following table. If required, you can further configure these conditions to meet your requirements.

Alarm Type	Description
Application Failure	Reports that the specified application has either terminated or stopped responding.
Connection Failure	Reports that the specified connection between any two applications has been lost.
CTI Link Failure	Reports that the connection between the specified T-Server and its switch has been lost.
Host Inaccessible	Reports that the Management Layer cannot contact the Local Control Agent (LCA) on the host where Genesys daemon applications are running. LCA is not started, or it is listening on a port other than the one specified in the configuration. A condition of Host Inaccessible is also referred to as being Down.
Licensing Error	Reports that a licensing error has occurred.

Alarm Type	Description
`Service Unavailable`	Reports that a Genesys component cannot provide service for some internal reasons.
`Host Unavailable`	Reports that a host where Genesys daemon applications are running is unavailable (turned off).
`Host Unreachable`	Reports that the Management Layer cannot reach the host where Genesys daemon applications are running (no route to the host).
`Unplanned Solution Status Change`	Reports that the status of a Solution has changed from Started to Pending, but without any requests to stop the Solution. This may indicate a failure of one of the Solution components.
`Message Server Loss of Database Connection`	Reports that Message Server has lost connection to the Centralized Log Database.

For more information about predefined Alarm Conditions, see the Framework 8.1 Management Layer User's Guide.

Scripts

Scripts

Choose one of the following script types to learn more:

- Alarm Detection Scripts
- Alarm Reaction Scripts

Alarm Detection Scripts

Alarm Detection Scripts identify what system variables the Management Layer must monitor to trigger an alarm.

Alarm Detection Scripts are Script objects of type Alarm Detection, and are created in the same way as other Scripts.

The system variables that the Management Layer can monitor (also called advanced alarm detection parameters) include:

- `Host System Variable Threshold`—Enables you to specify the value for an irregular change that might occur over a certain interval, in either CPU or memory use, on a given host.
- `Application System Variable Threshold`—Enables you to specify the value for an irregular change that might occur over a certain interval in either an application's CPU or memory use.
- `Local SNMP Variable Threshold`—Enables you to specify the value for an irregular change that might occur over a certain interval in any SNMP variable retrieved from the Genesys MIB file.

- `Remote SNMP Variable Threshold`—Enables you to specify the value for an irregular change that might occur over a certain interval in any SNMP variable retrieved from a non-Genesys MIB file.

> **Warning**
>
> The SNMP-related alarm detection capabilities require that you have a Genesys SNMP license for Solution Control Server.

> **Important**
>
> The Rising Threshold, which triggers an alarm when crossed only if the value is rising, must be a higher number than the Falling Threshold, which clears the alarm when crossed only if the value is falling. For example, if the Rising Threshold is `300`, the Falling Threshold must be less than `300`.

Alarm Reaction Scripts

Alarm Reaction Scripts identify what the Management Layer must do when alarms occur in, or are cleared from, the system. They are Script objects of type Alarm Reaction, and are created in the same way as other Scripts.

The Management Layer supports the following types of Alarm Reaction Scripts:

- Shutdown of a specified application.
- Startup of a specified application.
- Restart of the application that reported the alarm.
- Startup of a specified solution.
- Sending an e-mail message with information about the alarm to specified Internet addresses. You can customize the e-mail with specific details about the alarm. See the Alarm E-mails tab, above, for more information.
- Switchover of operations from the application that reported the alarm to its backup application, for applications running in primary mode, backup mode, or regardless of the mode.
- Sending an SNMP trap with detailed information about the alarm to a general-purpose network management system.
- Execution of an operating system command.

> **Important**
>
> For a description of the OS commands you can specify in an Alarm Reaction Script, refer to the Framework 8.1 Management Layer User's Guide.

- Changing a configuration option value for the specified application or for the application that reported the alarm.

Alarm E-mails

Customizing Alarm Reaction E-mails

You can customize the Subject line and body of an Alarm Reaction e-mail by creating a template, using plain text, and any of the following reserved variables that represent the specific information about the alarm:

Variable	Description
$REACT_NAME	The name of the Alarm Reaction.
$COND_ID	The Alarm Condition ID.
$COND_NAME	The name of the Alarm Condition.
$COND_CTGR	The category of the Alarm Condition.
$APP_ID	The Application ID.
$APP_NAME	The name of the Application.
$APP_TYPE	The Application type.
$MSG_ID	The Message ID.
$MSG_DESCR	The text of the Message.
$$	The dollar sign character ($).

You can then use this Alarm Reaction script as often as appropriate. For each use, the e-mail text is automatically customized for the specific situation.

Example

An example Alarm Reaction e-mail uses the following template:

```
Subject:

$COND_ID detected in $APP_NAME

Message:

CPU Overload has been detected by Genesys Solution Management Layer for Host1.

Alarm Reaction: $REACT_NAME

Alarm Condition:

ID: $COND_ID

NAME: $COND_NAME
```

```
Category: $COND_CTGR

Application:

ID: $APP_ID

Name: $APP_NAME

Type: $APP_TYPE
```

In the following scenario, the system detects that a CPU overload has occurred in the Solution Control Server, an alarm is triggered, and the following e-mail is sent in response. Note how the variable names have been replaced with actual values that are appropriate to the alarm scenario.:

```
Subject:

CPU_overload detected in Solution_Control_Server_760

Message:

CPU Overload has been detected by Genesys Solution Management Layer for Host1.

Alarm Reaction: cpu_overload_mail

Alarm Condition:

ID: 118

NAME: CPU_overload

Category: Major

Application:

ID: 105

Name: Solution_Control_Server_760

Type: SCS
```