Genesys Administrator Extension Help

Hosts

4/16/2025

Hosts

Hosts are the computers that run the various server applications in the environment.

Register only those hosts on which you will install and run Genesys servers or third-party servers that you configure in the Configuration Database.

Viewing Hosts

The **Hosts** list shows the hosts 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**
>
> Hosts that are disabled 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 cube icon 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.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with Hosts

To create a new Host object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check box beside an object and click **Edit**. To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**.

> **Important**
> You can delete a Host only if there are no server applications currently assigned to it.

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

- **Clone**—Copy a Host.
- **Move To**—Move a Host to another hierarchical structure.
- Enable or disable Hosts.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.
- Configure Logging

Click the name of a Host to view additional information about the object. You can also set options and permissions, and view dependencies.

Creating Host Objects

[+] Click to show procedure

Procedure: Creating Host Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the host. You must specify a value for this property, and that value must be unique within the Configuration Database. Because applications use this host name to establish connections with the servers running on this host, make sure that the name exactly matches the name of this host in the data network configuration.

     > **Important**
     > You cannot change this host name if any server applications are assigned to this host.

- **IP Address**—The IP address of the host. This value must be unique within the Configuration Database. Because applications may be using the specified IP address to establish connections with the servers running on this host, make sure that the value that you enter exactly matches the IP address of this host in the data network configuration.

  > **Tip**
  >
  > Click the magnifying glass in the **Name** field to have GAX automatically enter the IP address for the host.

- **OS Type**—The type of the operating system of this host. You must specify a value for this property.
- **Version**—The version of the operating system.
- **LCA Port**—The port number on which Local Control Agent (LCA) for this host is running. The LCA port must be set to a value between 2000 and 9999, inclusive. When the LCA port is specified as less than 2000, LCA starts on port number 4999 (the default value).

  > **Important**
  >
  > Do not change the value of the LCA port if any application has already connected to LCA or if Solution Control Server (SCS) has already started to control LCA.

- **Solution Control Server**—The SCS that monitors and controls this host. This property is valid only if you enable distributed SCS functionality. See the *Management Layer User's Guide* for details.
- Certificate—The security certificate value. In Windows, select the certificate value from the list of installed certificates. In UNIX, enter the full path to the **<serial_#>_<host_name>_cert.pem** file.
- **Certificate Description**—An optional description of the Certificate.
- **Certificate Key**—The full path to the **<serial_#>_<host_name>_priv_key.pem** file of the security certificate key. This field is used only if Genesys Security is deployed on UNIX; otherwise this field is empty.
- **Trusted CA**—The full path to the **ca_cert.pem** file of the CA that issued the default security certificate. This field is used only if Genesys Security is deployed on UNIX; otherwise this field is empty.

  > **Important**
  >
  > Refer to the *Genesys Security Deployment Guide* for more information about deploying Genesys

> TLS Security.

- **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.

3. Click **Save**.

Configuring Logging

[+] Click to show procedure

Procedure: Configuring Logging

Steps

1. In the **Hosts** list, select one or more Hosts.
2. Click **More** and select **Configure Logging**.
3. In the **Configuration of Logging** window, set the following options:
   - The Hosts that you selected from the **Hosts** list appears in the **Hosts** section. You can select or de-select Hosts to include in this procedure.
   - In the **Log Level** section, select one of the following options:
     - **All**—Generates all log events from the **Trace**, **Interaction**, and **Standard** levels.
     - **Trace**—Generates all log events from the **Trace**, **Interaction**, and **Standard** levels. This setting might adversely affect application performance. Set this level only when you are testing new interaction-processing functions or scenarios.
     - **Interaction**—Generates all log events of **Interaction** and **Standard** levels. Set this level only when you are testing events on a particular interaction.

> **Important**
>
> Interaction-level records contain the Interaction ID attribute that helps to search for log events that are generated by various applications but related to the same interaction.

> **Warning**
>
> Using the Interaction level generates a higher number of logging events on the network, which might adversely affect the performance of the DBMS, Message Servers, and interaction-processing components.

- **Standard**—Genesys recommends you permanently enable only a Standard level of logging during the operation of Solutions in regular production mode. This level reports events for significant problems and normal operations of in-service Solutions. An event is reported at the Standard level if it satisfies one of these criteria:
  - Indicates that an attempt to perform any external operation has failed
  - Indicates that the latest attempt to perform an external operation that previously failed has succeeded
  - Indicates detection of a condition that has a negative impact on operations, actual or projected
  - Indicates that a previously detected condition, which had a negative impact on operations, no longer exists
  - Indicates a security violation of any kind
  - Indicates a high-level data exchange that cannot be recognized or does not follow the expected logical sequence
  - Indicates inability to process an external request
  - Indicates successful completion of a logical step in an initialization process
  - Indicates a transition of an Application from one operational mode to another
  - Indicates that the value of a parameter associated with a configurable threshold has exceeded that threshold
  - Indicates that the value of a parameter associated with a configurable threshold that earlier exceeded the threshold has returned to its normal range.
- **None**—No logging is performed.

4. In the **Log Outputs Adjustment** section, you can fine-tune the logging level for the following output types: **Network Log Server**, **Plain Text File**, and **Console**.
5. Perform one of the the following:
   - If you selected **Network Log Server** in the previous step, go to the **Message Server**

section and select the Message Server to receive logs.

- If you selected **Plain Text File** in the previous step, go to the **Log File Name** section and specify the log file name to receive logs. You can also specify the following:
  - **Create Segment**—If checked, segment the log file into chunks specified by the **Segment Size (MB)** field.
  - **Segment Size (MB)**—If **Create Segment** is checked, specify a segment size for the log file, in megabytes.
  - **Segment Expiration**—If checked, segments are deleted after a maximum number of segments is reached, as defined by **Maximum Segments**.
  - **Maximum Segments**—If **Segment Expiration** is checked, specify how many segments to retain before segments beyond this limit are removed.

6. Click **OK**.

ADDP

To configure the Advanced Disconnect Detection Protocol (ADDP) protocol between the LCA of a given host and SCS, use the **Options** tab of the Host object. If you are using the Management Layer for application failure management, set up ADDP parameters for the host as described.

Procedure: Setting up ADDP Connections

Steps

1. Open the **Options** tab of the Host.
2. Create a section called addp.
3. In the addp section, specify the following configuration options:

Option Name	Option Value	Option Description
`addp-timeout`	Any integer	Sets the ADDP timeout in seconds. If one application in the connection does not receive messages from the other application

Option Name	Option Value	Option Description
		in the connection within this interval, the first application sends a polling message. If the first application does not receive a response to the polling message within this time interval, it interprets the lack of response as a loss of connection. The recommended setting for this option is 3 seconds for a LAN connection or 10 seconds for a WAN connection.
addp-trace	local	LCA prints ADDP-related messages into its log.

> **Important**
>
> You configure ADDP between servers by using the Application's **Connections** tab.

Check Ports

You can click the name of a Host to view more information about the host's configuration, as well as check port information and identify port conflicts. Click **Check Ports** to display all applications and configured ports for the Host object, as well any port conflicts. Ports that are duplicated in multiple applications are highlighted in the list, as these ports might be in conflict. You can click an Application in the **Check Ports** list to view details about the Application object. Click **Export** to export the items in the list to a Microsoft Excel-compatible file.