SIP Server HA Deployment Guide

Using SIP Proxy

12/18/2025

Contents

Using SIP Proxy

Complete these steps to set up SIP Server HA using SIP Proxy. The procedure applies to both Windows and Linux deployments.

1. Configure the sip-outbound-proxy DN
2. Configure SIP Proxy
3. Configure primary and backup SIP Servers
4. Configure multi-site call handling

Configure the sip-outbound-proxy DN

1. In the SIP Server Switch, create a DN of type `Voice over IP Service`. For a multi-site deployment, you must create several DNs of this type, one for each Switch/Site served by a SIP Server HA pair.
2. In the Options > **[TServer]** section, configure the following mandatory options:
   - **contact**—Set this option to the SIP Proxy FQDN resolved into a single or multiple SRV records.
   - **external-contact**—Set this option to the SIP Proxy address using the `host:port` format.
   - **oos-check**—Specify how often, in seconds, SIP Server checks SIP Proxy for out-of-service status.
   - **oos-force**—Specify the time interval, in seconds, that SIP Server waits before placing an unresponsive SIP Proxy in out-of-service state when the **oos-check** option is enabled.
   - **service-type**—Set this option to `sip-outbound-proxy`.

> **Important**
>
> Active Out-of-Service Detection feature (**oos-check** and **oos-force** options) must be enabled for SIP Proxy to work.

Configure SIP Proxy

1. Create a SIP Proxy Application of the *Genesys Generic Server* type by importing the SIP Proxy Application Template `SIPProxy_811.apd` from the product installation package. A SIP Proxy Application must be created for each SIP Proxy instance.
2. On the Server Info tab, set the following parameters:

- Host—Specify the host on which this SIP Proxy is installed.
- Port IDs—Specify the following SIP Proxy ports:
  - `sip-port`, Connection Protocol: `sip`
  - `http-port`, Connection Protocol: `http` (Optional)

3. On the Options tab, create a section named `sipproxy`. In the **[sipproxy]** section, add the following options:
   - **applications**—For a multi-site environment, specify the application names of all primary SIP Servers in the environment, separated by a comma.
   - **oos-check**—Set to 5 by default.
   - **oos-force**—Set to 5 by default.
   - **serving-sipserver**—Specify the primary SIP Server application name to which all requests from endpoints and media gateways will be forwarded.
   - **sipproxy-role**—Set to `10`.
4. (Optional) On the Options tab, in the **[log]** section, you can add log options as necessary. Refer to the Framework 8.1 SIP Server Deployment Guide for detailed information about log options.
5. Install SIP Proxy by completing the following steps:
   1. On the product CD, navigate to the SIP Proxy [/media_layer/SIP_Proxy/windows_x64/] folder, and open the subdirectory windows.
   2. Double-click `Setup.exe` to start the InstallShield installation wizard.
   3. Follow the InstallShield wizard instructions to install SIP Proxy. InstallShield creates a batch file in the folder of the component it installs.
   4. Open the batch file and ensure that it includes the parameter `-app <appname>`, where `appname` is the name of the SIP Proxy application object that you have created in the Configuration Layer.

Configure primary and backup SIP Servers

- In the Options > **[TServer]** section, configure the following options in both primary and backup SIP Server Applications:
  - **sip-address**—Set this option to the IP address of the SIP interface of SIP Server.
  - **sip-outbound-proxy**—Set this option to `true`.
  - **sip-enable-rfc3263**—Set this option to `true`.
  - **sip-enable-gdns**—Ensure this option is set to `true`.

> ### Important
> Both primary and backup SIP Servers must have the same **sip-port** setting.

Configure multi-site call handling

In the SIP Server Switch, create DNs of type Trunk. In the Options > **[TServer]** section, configure the mandatory options depending on whether DNS resolution is used:

- ***If DNS resolution is used***, configure the following mandatory options:
  - **contact**—Set this option to the FQDN resolved into the SRV records of the primary and backup SIP Servers at the destination site.
  - **oos-check**
  - **oos-force**
  - **peer-proxy-contact**—Specify the address of the SIP Proxy pool that serves the remote SIP Server. The value must be the same as the value of the **external-contact** option of the sip-outbound-proxy DN at the remote switch.
  - **resolve-external-contact**—Set this option to `true` on all trunks that have **peer-proxy-contact** configured.
  - **replace-uri-contact**—Set this option to `true`.

> **Important**
>
> For a Business Continuity deployment, DNS resolution must be used.

- ***If DNS resolution is not used***, create one Trunk DN for each SIP Server in an HA pair.
  - In the first Trunk DN, configure the following mandatory options:
    - **contact**—Set this option to the `host:port` of the primary SIP Server at the destination site.
    - **oos-check**
    - **oos-force**
    - **peer-proxy-contact**—Specify the address of the SIP Proxy pool that serves the remote SIP Server. The value must be the same as the value of the **external-contact** option of the sip-outbound-proxy DN at the remote switch.
  - In the second Trunk DN, configure the following mandatory options:
    - **contact**—Set this option to the `host:port` of the backup SIP Server at the destination site.
    - **oos-check**
    - **oos-force**
    - **peer-proxy-contact**—Specify the address of the SIP Proxy pool that serves the remote SIP Server. The value must be the same as the value of the **external-contact** option of the sip-outbound-proxy DN at the remote switch.

Important

For additional configuration options that might be configured for a particular device, see the Framework 8.1 SIP Server Deployment Guide.