Genesys 8.1

SIP Proxy Deployment Guide Wiki Redirect

ALERT: This document is available as a PDF only to support searches from the Technical Support Knowledge Base. Click here (SIP Proxy Deployment Guide) to be redirected to the content in its original format.

Table of Contents

SIP Proxy 8.1 Deployment Guide

Welcome to the *SIP Proxy 8.1 Deployment Guide*. This document introduces you to the concepts, terminology, and procedures relevant to SIP Proxy. See the summary of chapters below.

About SIP Proxy

Find out how SIP Proxy works.

- Overview
- Supported features

SIP Proxy Deployment

Find procedures to set up SIP Proxy.

- Configuration
- Installation
- Configuration options
- Starting and stopping SIP Proxy

Overview

The primary purpose of Genesys SIP Proxy is to provide high availability without requiring a virtual IP address.

There are five fundamental concepts to understand:

1) The purpose of SIP Proxy is to provide high availability for a primary/backup SIP Server HA pair without requiring a "virtual" or floating IP address.

2) An N+1 pool of proxy instances is defined for each SIP Server HA pair. The proxy instances monitor the SIP Server pair to determine which is active and which is backup.

3) Incoming SIP messages are proxied to the primary SIP Server instance. It is the responsibility of external SIP user agents to select a proxy instance based either on DNS or static configuration of multiple IP addresses, and to fall back to an alternate instance if the select instance is not responding.

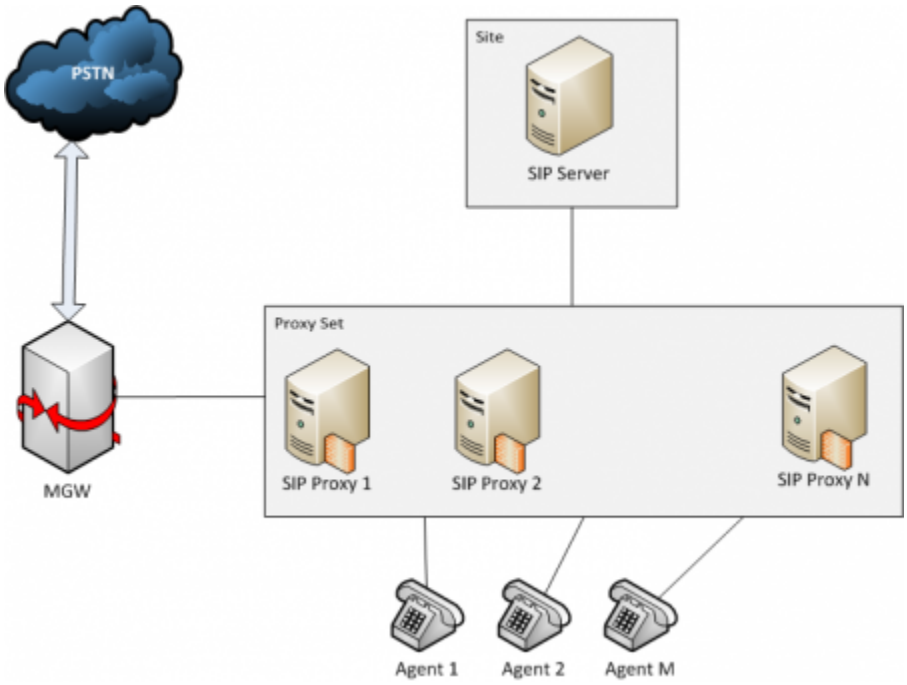
4) The SIP Server HA pair is configured to use this pool of SIP Proxy instances as the "outbound proxy."

5) SIP Proxy functions as a proxy defined in RFC 3261 section 16.

As of March 2013, SIP Proxy has been tested with only two SIP endpoints - the Genesys SIP Endpoint v8.1, and Polycom SoundPoint IP Phones; additional endpoints are scheduled for testing.

Standalone deployment

In a standard deployment, an N+1 pool of SIP Proxy instances handles incoming & outgoing SIP transactions between a SIP Server HA pair and external SIP elements. Each SIP transaction would be handled by a single proxy instance. Subsequent transactions may be handled by the same or different proxy instance(s). Each SIP Server HA pair requires a unique pool of proxy instances.



Supported features

This section describes features that are supported by SIP Proxy.

Contents

Routing

SIP Proxy is responsible for proxying SIP messages from external SIP user agents to the appropriate SIP Server. It is the responsibility of each external user agent to choose a SIP Proxy instance when sending a SIP message. Typically a deployment should have an overall configuration resulting in load balancing across the SIP Proxy instances.

SIP Proxy stores SIP session information in shared call storage. Each SIP session (and subsequent sessions like consultation calls) can contain several SIP dialogs that are established through different SIP Proxies. In SIP Cluster mode, Session storage ensures that each message from the same or related SIP session is routed to the same SIP Server. In standard mode, all messages are directed from SIP Proxy to the same SIP Server HA pair.

Route and Record-Route headers

SIP Proxy adds a Record-Route header into the initial INVITE message with the internal representation of the target and the source of the request. The value of this header consists of the FQDN of SIP Proxy, the SIP port of SIP Proxy , SIP Server index, and DN. Subsequent requests within the same dialog are routed to the specified SIP Proxy and SIP Server index, or SIP Proxy uses the DN name to determine the correct destination.

Registrar

SIP Proxy acts as a SIP registrar. SIP Proxy has shared registration-info storage. Any endpoint can be reached by any SIP Proxy.

SIP Proxy uses SIP Server as an authentication server. It passes REGISTER requests to SIP Server and waits for a response. If the response is the 200 OK message, registration is stored. All responses are always forwarded to the initiator.

Related configuration option:

- registrar-default-timeout

Active out-of-service detection

Each SIP Proxy instance pings each primary SIP Server using an OPTIONS message. If the primary SIP Server does not respond during a configured timeout, SIP Proxy starts to ping the backup SIP Server. If the backup SIP

Server responds, the backup SIP Server address will be used as a destination for calls. If both the primary and backup SIP Server instances do not respond, SIP Proxy will mark this SIP Server HA pair as out-of-service and will not use it for calls; however, SIP Proxy will continue pinging them.

Related configuration options:

- oos-check
- oos-force

MWI subscription

SIP Proxy forwards SUBSCRIBE messages from registered endpoints to Feature Server/SIP Voicemail server. SIP Proxy identifies a message as an MWI subcription message if the Event header contains message-summary. SIP Proxy processes MWI subscription messages according to RFC3842.

SIP Proxy does not support the retransmission of SUBSCRIBE messages to another destination in case of destination failure.

Related configuration option:

- feature-server-address

Load balancing

SIP Proxy provides load balancing of incoming traffic across SIP Servers and Feature Servers. This is achieved by using the random or round-robin SIP Server selection routine within the data center to which SIP Proxy belongs.

Related configuration option:

- geo-location

Overload detection

SIP Proxy has the ability to control and restrict a dialog (incoming INVITE messages) rate. This feature is enabled by the overload-ctrl-dialog-rate configuration option. When the overload is detected, SIP Proxy rejects new INVITE requests by generating a 503 Service Unavailable error message.

SIP Server inactive state support

SIP Proxy supports the inactive state of SIP Server. In this state, SIP Server maintains existing calls but rejects new calls. When SIP Proxy receives a 503

message in response to an OPTIONS message from a SIP Server, SIP Proxy interprets this to mean that SIP Server is in an inactive state. From this point, SIP Proxy will no longer send new dialogs to this SIP Server, but keeps sending requests within existing dialogs.

SIP address binding

SIP Proxy uses the sip-address configuration option to identify on which network interface it should bind the SIP port. If this option is not set, SIP Proxy binds the SIP port on all network interfaces.

Client-side port definition

The client-side port definition feature enables the definition of a port for sending outgoing messages. This feature is enabled by the client-side-port configuration option. This option defines the first port in the range for management connections with other SIP Proxy instances. The range size is not limited by the upper value.

Error handling

SIP Proxy can inform SIP Cluster components about errors and problems through:

- logs
- SCI Alarms
- HTTP Server interface

The following is the list of SIP Proxy log messages of level Standard:

Log Event ID	Text	Description
40000	SPR_OWN_PROXY_ADDR_NOT_FOUND	Initialization failed, proxy address (host:port) is not found in the list
40001	SPR_SIPS_HA_PAIR_UNAVAILABLE	SIP Server HA pair (primary host:port) is unavailable

40002	SPR_OTHER_PROXY_INSTANCE_DISCONNECTED	SIP Proxy instance is disconnected
40003	SPR_ERROR_READING_CONFIG_DATA	Error while reading configuration data
40004	SPR_PROXY_INITIALIZED	SIP Proxy has initialized successfully
40005	SPR_HOST_NOT_RESOLVED	Cannot resolve SIP Proxy host
40006	SPR_SIP_LISTENER_CANNOT_START	Cannot start SIP listener
40007	PR_MGMT_LISTENER_CANNOT_START	Cannot start Mgmt listener

Limitations

- Loop-detection check mechanism is not supported in this release of SIP Proxy.

Prerequisites

Before configuring SIP Proxy, you must:

- Configure the Domain Name System (DNS) Server to resolve the SIP Proxy FQDN by A and SRV records.

See DNS server configuration for details.

Deploying SIP Proxy

This is the recommended sequence to follow when deploying SIP Proxy.

1. Configure SIP Proxy.
2. Install SIP Proxy.

Configuring SIP Proxy

Standalone deployment

Switch configuration

1. Create a Voice over IP Service type DN for every switch involved in the standalone environment.
2. In the Annex tab, TServer section, configure the following mandatory options:
    - contact—Set to the SIP Proxy DNS-SRV name.
    - external-contact—Set to the SIP Proxy DNS-A name 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 SIP Proxy that does not respond in out-of-service state when the oos-check option is enabled.
    - service-type—Set to the value of sip-outbound-proxy.

SIP Proxy configuration

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:
    - Host—Specify the host on which this SIP Proxy is installed.
    - Port IDs—Specify the following SIP Proxy ports:

        - sip-port, Connection Protocol: sip
        - mgmt-port, Connection Protocol: mgmt
3. On the Options tab, create a section named sipproxy. In the sipproxy section, add the following options:
    - applications—Specify a comma-separated list of all SIP Server applications names in the environment. (Only primary servers must be specified.)
    - contact-address—Set to the SIP Proxy DNS-A name using the host:port format.
    - internal-domain—Set to the SIP Proxy DNS-SRV name.
    - 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-applications—Specify a comma-separated list of all SIP Proxy applications names in the environment.
    - 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.

Installing SIP Proxy

Prerequisites

- A SIP Proxy Application object exists.

To install SIP Proxy, complete 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.

SIP Proxy configuration options

applications

Default Value: NULL
Valid Values: String value
Change Take Effect: After restart

(Standalone only) Specifies a comma-separated list of all SIP Server applications names in the environment. Only primary servers need to be specified.

client-side-port

Default Value: 0
Valid Values: 0–65535
Changes Take Effect: After SIP Proxy restart

Specifies the first port in the range of ports that will be used for client management connections to other SIP Proxy instances. If this option is not configured, random ports are used for client management connections.

contact-address

Default Value: NULL
Valid Values: String value
Change Take Effect: After restart

(Standalone only) Specifies the SIP Proxy DNS-A name using the host:port format.

feature-server-address

Default Value: NULL
Valid Values: String value
Changes Take Effect: Immediately

(Cluster only) Specifies the FQDN:port of the SIP Feature Server.

geo-location

Default Value: NULL
Valid Value: Any alphanumeric string
Changes Take Effect: After SIP Proxy restart

Specifies the data center to which SIP Proxy belongs.

internal-domain

Default Value: NULL
Valid Values: String value
Change Take Effect: After restart

(Standalone only) Specifies the SIP Proxy DNS-SRV name.

oos-check

Default Value: 5
Valid Values: 0–300
Changes Take Effect: Immediately

Specifies how often, in seconds, SIP Proxy checks SIP Servers for out-of-service status.

oos-force

Default Value: 5
Valid Values: 1–32
Changes Take Effect: Immediately

Specifies how often, in seconds, SIP Proxy checks whether the out-of-service SIP Server starts to respond.

overload-ctrl-dialog-rate

Default Value: 0
Valid Values: Any positive integer
Changes Take Effect: Immediately

Specifies a dialog rate (incoming INVITE requests per second) threshold. All over-threshold INVITE requests will be rejected. When set to a value of 0 (the default), this functionality is disabled.

registrar-default-timeout

Default Value: 0
Valid Values: Positive integer value
Changes Take Effect: On the next SIP REGISTER request

(Cluster only) Specifies the expiration timeout, in seconds, for a SIP REGISTER request as a value in the 200 OK response that SIP Proxy sends to the SIP endpoint and as a value in the REGISTER request that is forwarded to SIP Server. If the option is set to 0, or is not defined, the expires value from the Contact or Expires header of the REGISTER request is used as the expiration timeout. If this option is set to any value other than 0, the timeout is set to the lesser of the option value and the value specified by the client.

resolve-host

Default Value: false
Valid Values: true, false
Changes Take Effect: After SIP Proxy restart

If this option is set to false, the name of the host where SIP Proxy runs is specified in the Via header. If this option is set to true, the resolved IP address is specified in the Via header.

send-data-timeout

Default Value: 100
Valid Values: 1–30000
Changes Take Effect: Immediately

(Cluster only) Specifies the timeout, in milliseconds, between data transmissions in the replication procedure.

serving-sipserver

Default Value: NULL
Valid Values: Any string
Change Take Effect: After restart

(Standalone only) Specifies the SIP Server application name to which all requests from endpoints and media gateways will be forwarded.

sip-address

Default Value: NULL
Valid Values: String value
Changes Take Effect: After SIP Proxy restart

Specifies the IP address of the SIP Proxy interface. This option must be set when deploying SIP Proxy on a host with multiple network interfaces. If this option is specified, SIP Proxy inserts the option value into the Via header of outgoing SIP messages.

sip-ip-tos

Default Value: 256
Valid Values: 0–255
Changes Take Effect: After SIP Proxy restart

Specifies the value of the Type of Service (TOS) byte in the IP header of SIP messages that are sent by SIP Proxy. If this option is not specified, the operating system TOS byte is used. Depending on the network configuration, the TOS byte is treated as one of the following:

- 3-bit IP precedence field, followed by a 4-bit type-of-service. The least significant bit (LSB) is unused and set to 0. (RFC 1349)
- 6-bit DiffServ, with the two least significant bits unused. (RFC 2474)

For example, the following values may be used to assign a higher priority to SIP packets:

- 0x10—IPTOS_LOWDELAY, low-delay type of service
- 0x20—IPTOS_PREC_PRIORITY, priority precedence
- 0x40—IPTOS_PREC_CRITICAL, critical precedence
- 0xB8—DiffServ EF (Expedited Forward)

Note: On most operating systems, applications that are running on behalf of non-privileged user accounts are not permitted to set a non-zero TOS value, so you might have to perform additional actions to enable this functionality. In particular:

- On Linux, the application must have CAP_NET_ADMIN capability (that is, be capable of running from the root account).
- On Windows, the following registry setting must be set (see also http://support.microsoft.com\kb/248611): HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableUserTOSSetting = (DWORD) 0

Refer to operating system documentation for additional information.

sipproxy-applications

Default Value: NULL
Valid Values: String value
Change Take Effect: After restart

(Standalone only) Specifies a comma-separated list of all SIP Proxy applications names in the environment.

sipproxy-role

Default Value: 0
Valid Values: 0,10
Changes Take Effect: After restart

Specifies the mode of the SIP Proxy:

- 0—cluster mode
- 10—standalone mode

wait-response-timeout

Default Value: 5
Valid Values: 1–300
Changes Take Effect: Immediately

(Cluster only) Specifies the timeout, in seconds, during which SIP Proxy waits for a response to a replication request.

DN-Level configuration options

The following configuration options must be set for a Voice over IP Service DN for every switch involved in the standalone environment:

contact

Default Value: NULL
Valid Values: String value
Change Take Effect: After restart

(Standalone only) Specifies the SIP Proxy DNS-SRV name.

external-contact

Default Value: NULL
Valid Values: FQDN of SIP Proxy resolved to A-record (host:port)
Change Take Effect: After restart

Specifies the FQDN used by the SIP phones to access the SIP Proxy instance(s) in the environment. Use the following format: host:port, where

- host is an FQDN that can be resolved using DNS to a list of SIP Proxy IP Addresses (DNS A records)
- port is the TCP/IP port that SIP Proxy uses to listen for SIP messages from SIP phones (all SIP Proxy instances listen on the same port).

For example:
anyproxy.DnsServer.com:7018

oos-check

Default Value: 0
Valid Values: 0–300
Changes Take Effect: Immediately

Specifies how often, in seconds, SIP Server checks SIP Proxy for out-of-service status.

oos-force

Default Value: 0
Valid Values: 0–30
Changes Take Effect: Immediately

Specifies the time interval (in seconds) that SIP Server waits before placing a device that does not respond in out-of-service state when the oos-check option is enabled.

service-type

Default Value: NULL
Valid Values: Any string
Change Take Effect: After restart

Specifies the configured SIP device type or service. For stand-alone configuration, this option must be set to sip-outbound-proxy.

Starting and stopping SIP Proxy

Contents

You can start and stop SIP Proxy manually or by using Genesys Administrator or Solution Control Interface (SCI).

Starting SIP Proxy

1. In Genesys Administrator, go to Provisioning > Environment > Applications.
2. If necessary, navigate to the folder containing the SIP Proxy applications that you want to start.
3. Do one of the following:
   - Open the properties of the application that you want to start, and click Start.
   - Right-click on the application that you want to start, and from the context menu, select Start.

   The application's status changes from Stopped to Started.

Starting SIP Proxy manually

To start SIP Proxy on Windows, do one of the following:

- Start the Genesys SIP Proxy service from the Services menu.
- Select the shortcut Start SIP Proxy from the Start menu.
- Go to the directory where SIP Proxy is installed and click the startServer.bat batch file.

To start SIP Proxy on UNIX:

1. Go to the directory in which SIP Proxy is installed.
2. Type the following command line:
   sh run.sh

Stopping SIP Proxy

1. In Genesys Administrator, go to Provisioning > Environment > Applications.
2. If necessary, navigate to the folder containing the SIP Proxy applications that you want to stop.
3. Do one of the following:
   - Open the properties of the application that you want to stop, and click Stop.
   - Right-click the Application that you want to stop, and from the context menu, select Stop.

   The application's status changes from Started to Stopped.

Stopping SIP Proxy manually

SIP Proxy can be stopped by any means that your operating system supports.