



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

# High Availability and Disaster Recovery for the Genesys SMS Aggregation Service

Disaster Recovery

---

## Contents

- 1 Disaster Recovery
  - 1.1 HTTP API
  - 1.2 SMSC API

# Disaster Recovery

This section discusses the Disaster Recovery (DR) plan for the SMS Aggregation service. This service follows the *natively multi-homed design*. With this design, all datacenters are set up as hot sites.

To ensure there is no service impact during any major outage (or maintenance), customers are advised to use all the available sites. However, note the following:

- Clients should support receiving MOs from any site.
- DR for MTs sent to one site may be received at another.

Genesys ensures that no duplicate messages are delivered. The rest of this section discusses the requirements for each component.

## HTTP API

There are two strategies you can use for HTTP API DR:

- Single Genesys-provided URL—Genesys maintains short TTLs for external DNS records and, in the event of a failure, updates the DNS information to redirect them to the failover site.
- Client-side failover—customers can configure all site URLs to use as failover sites.

The following section discusses these two approaches.

## Genesys-Provided Failover

The URL to use for this strategy is:

- <https://smc-api.genesyscloud.com/httpapi/receiver>

In the event of a failure, the DNS resolution of this site is updated to the correct location. Therefore, in order to take full advantage of this feature, ensure that the DNS TTL of the authoritative server is obeyed. However, if this cannot be guaranteed (for example, an application layer continues caching forever), then you should use the alternative customer-side approach described below.

## Customer Failover Configuration

As an alternative strategy, you can configure both site URLs to use as potential failover sites in your applications. In this configuration, Genesys recommends that you select one of the sites to be primary and the other site used in the case of failure.

The available URLs are:

- <https://smc-api.dc3.genesyscloud.com/httpapi/receiver>
- <https://smc-api.bos.genesyscloud.com/httpapi/receiver>

In the event of a outage or failure at one site, you may experience connection timeouts and/or other abnormal behavior. If such events occur, try the following steps:

1. Attempt to resubmit the message after a short duration, such as 30 seconds.
2. If the same error occurs again, use the alternative URL.
3. If you continue to experience problems, contact your Genesys account manager.

## SMSC API

Due to the connection-oriented nature of this protocol, your client should create at least one connection to each available SMSC instance from each of your client applications.

The list of available SMSC instances are:

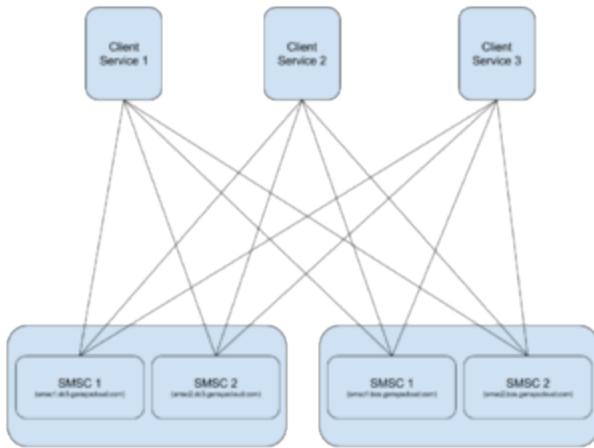
- [smc1.dc3.genesyscloud.com](https://smc1.dc3.genesyscloud.com)
- [smc2.dc3.genesyscloud.com](https://smc2.dc3.genesyscloud.com)
- [smc1.bos.genesyscloud.com](https://smc1.bos.genesyscloud.com)
- [smc2.bos.genesyscloud.com](https://smc2.bos.genesyscloud.com)

## General Guidelines

In all cases, follow this set of general guidelines:

- A client should bind into all listed SMSCs.
- When an SMSC is unavailable, the client should attempt to rebind. The time between these attempts should be greater than 30 seconds.
- A client should expect messages to be received from all active connections.
- No guarantee is given as to the bind used to send DRs/MOs to the client.
- Clients should not queue messages for inactive binds. Instead, any active binds should be used.

The diagram below shows the desired configuration:



**Client Configuration for SMSC DR**