



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.

# SIP Disaster Recovery

Desktop Operation

4/24/2025

---

## Contents

- 1 Desktop Operation
  - 1.1 Desktop Startup
  - 1.2 Detecting Site Failure
  - 1.3 Disaster Recovery Switchover Procedure

# Desktop Operation

## Desktop Startup

On startup, the desktop application must first connect to the Configuration Server Proxy at one of the sites. Since the preferred site for the agent is not known at this point, this connection can be to either site. If the desktop cannot connect to the first site attempted, it should attempt to connect to the other site. To connect to Configuration Server Proxy, AIL requires the following parameters:

- IP address and port of Config Server Proxy - from local configuration
- AIL Application name - from local configuration
- Username and password - supplied by agent on logging into the desktop

The desktop connects to the Config Server Proxy using the Application name to identify itself, and the user name and password to identify and authenticate the agent. After connecting to Configuration Server Proxy, the desktop application should obtain the name of the preferred site (site 1) and secondary site (site 2) AIL Application Objects for the agent from configuration data for the agent's Person object. The desktop should then read the configuration for the preferred site AIL Application Object, in order to obtain the IP address and port number of the preferred Configuration Server Proxy. If the preferred Configuration Server Proxy for the agent is not the one to which the desktop is currently connected, the desktop should re-connect to the Configuration Server Proxy at the preferred site, according to the Disaster Recovery Switchover procedure described below. The desktop application may cache the preferred site information to avoid the possibility of a switchover immediately after startup; however, on connecting to Configuration Server Proxy, it should always follow the procedure described above, in case the configuration has changed. Caching should not be used if hotel seating / hot seating is employed. The associated techniques are illustrated in the [code samples](#).

## Detecting Site Failure

This section recommends the procedures that the desktop application should follow to detect a failure of the site to which it is currently connected. The desktop application should follow the same procedures regardless of whether it is currently connected to the preferred site or secondary site. The associated techniques are illustrated in the [code samples](#). Genesys recommends that the desktop application create four listeners:

- A telephony service listener
- A configuration service listener
- A statistic service listener
- A listener to the DN of the agent's phone.

### **Telephony Service Listener**

The telephony service represents the status of the connection between this application and the primary/backup pair of SIP Servers. If the telephony service goes to an OFF status, this indicates that both the primary and the backup SIP Server are unavailable. When this occurs, AIL tries to reconnect to the current primary/backup SIP Servers. The retry interval is configured in the constructor for AilLoader.

If the telephony service does not return to an ON status within the site-timeout interval, the desktop application should treat the condition as a site failure, and initiate a Disaster Recovery switchover according to the procedure described below.

If site-timeout is not configured, or has a value of zero, the desktop should not perform a Disaster Recovery switchover based on the status of the telephony service listener.

### **Configuration Service Listener**

The configuration service represents the status of the connection between this application and the primary/backup pair of Configuration Servers. If the configuration service goes to an OFF status, this indicates that both the primary and the backup Configuration Servers are unavailable. When this occurs, AIL tries to reconnect to the current primary/backup Configuration Servers. The retry interval is configured in the constructor for AilLoader. Genesys recommends that the desktop application monitor the status of the configuration service. In the event that the service becomes unavailable, the desktop should warn the user and, if appropriate, generate alarms to upstream monitoring services, but should not initiate a Disaster Recovery switchover based solely on the status of this service.

### **Statistic Service Listener**

The statistic service represents the status of the connection between this application and the primary/backup pair of Stat Servers. If the statistic service goes to an OFF status, this indicates that both the primary and the backup Stat Server are unavailable. When this occurs, AIL tries to reconnect to the current primary/backup Stat Servers. The retry interval is configured in the constructor for AilLoader.

Genesys recommends that the desktop application monitor the status of the statistic service. In the event that the service becomes unavailable, the desktop should warn the user and, if appropriate, generate alarms to upstream monitoring services, but should not initiate a Disaster Recovery switchover based solely on the status of this service.

### **DN Listener**

The desktop application should utilize a DN Listener to detect EventAgentLogout events from SIP Server. There are several reasons why SIP Server can send EventAgentLogout:

- The agent logged out manually. The desktop application should take no further action.
- A supervisor forced a logout of the agent. The desktop application should take no further action. Genesys does not define a specific reason code for a supervisor forced logout, but recommends that, if possible, the customer's supervisor desktop assign a suitable reason code, and that the agent desktop check for that code.
- The associated SIP phone registration expired. In this case, the event data will contain the reason code `dr-force_logout`. If the desktop application does not have an embedded SIP endpoint, it should wait for the external endpoint to re-register. If the desktop application has an embedded SIP endpoint, it should wait for the endpoint to re-register or it should re-launch it if relevant. In either case, an `EventDNBackInService` event indicates successful re-registration.

If `site-sip-register-timeout` is configured with a non-zero value, and `EventDNBackInService` is not received within the time specified by `site-sip-register-timeout`, the desktop should initiate a Disaster Recovery switchover according to the procedure described below. If `site-sip-register-timeout` is not configured, or has a value of zero, the desktop should not perform a DR switchover based on the `dr-force_logout` reason code.

- SIP Server went into Graceful Shutdown mode. Graceful Shutdown mode is initiated through Genesys Administrator, and allows calls to be purged from SIP Server prior to shutting it down for maintenance

purposes. In this case, the event data will contain the reason code `graceful_shutdown_logout`. The desktop application should initiate a Disaster Recovery switchover according to the procedure described below.

## Disaster Recovery Switchover Procedure

To effect a site switchover, it is necessary to restart AIL with the parameters for the target site. Genesys recommends that the `killFactory()` function be used. This allows AIL to be restarted without having to restart the underlying JVM. To minimize the startup time, set the option `loading/on-demand` to true. Once the connection to the other site has been established, the desktop application should set up Telephony Service and DN listeners for that site, as described above. The associated techniques are illustrated in the [code samples](#).