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.

Outbound Contact Deployment Guide

Outbound Contact and HTTP Server

4/2/2025

Contents

Outbound Contact and HTTP Server

OCS supports communication with OCS clients, such as GVP using HTTP requests and responses. This enables an HTTP client to send requests to update records over HTTP or HTTPS.

Starting with release 8.1.516.04, OCS supports custom security-related headers sent by the OCS HTTP Server in HTTP responses. The Application-level option **http-custom-headers** allows you to specify custom headers sent in OCS HTTP Server responses. The following HTTP headers are supported:

- X-Frame-Options: SAMEORIGIN
- X-XSS-Protection: 1; mode=block
- X-Content-Type-Options: nosniff
- Content-Security-Policy: script-src 'self'; object-src 'self'
- Strict-Transport-Security: max-age=31536000; includeSubDomains

Configuring HTTP/HTTPS

To configure HTTP support, see the procedure Configuring OCS for HTTP.

Support for HTTPS

OCS supports communication over HTTPS, or strictly speaking, HTTP over Transport Layer Security (TLS) connection, using a Genesys TLS implementation.

For a detailed description of a Genesys TLS implementation, see the Protection of Data in Transit in the *Genesys Security Deployment Guide*.

For the installation procedure of Genesys Security Pack on UNIX, see the Installing Genesys Security Pack in the *Genesys Security Deployment Guide*. On Windows platforms, support for SSL/TLS is integrated into the operating system.

How Outbound Contact Uses HTTP/HTTPS

The HTTP server-side interface in OCS, HTTP Proxy, is a gateway between HTTP version 1.1 and outbound protocols (the Desktop protocol and the Third Party protocol).

At its startup, when OCS determines that an HTTP port is configured, it automatically starts HTTP Proxy. As the end user, you do not need to start this child process manually.

In OCS, this HTTP Proxy translates:

- HTTP requests into OCS proprietary protocols.
- OCS proprietary protocols responses into HTTP responses.

HTTP Proxy supports UTF-8 encoding. OCS sends the value of the encoding option value to HTTP

Proxy, which can transcode (or convert) the JSON body of HTTP requests or responses (such as `AddRecord` and `PreviewRecord` events, or pre-dial validation requests) according to the value specified. If no value is specified, no conversion takes place.

At OCS startup, OCS starts HTTP Proxy, and HTTP Proxy opens the associated port that is configured in the OCS application object. If HTTP Proxy cannot open the port, it shuts down. If HTTP Proxy terminates unexpectedly, OCS tries to restart it after the Reconnect Timeout expires. This Reconnection Timeout is specified on the OCS Configuration tab/Server Info section (in Genesys Administrator).

Previously, HTTP Proxy did not have its own log and passed log messages to OCS, which logged them into the OCS log file. Starting with version 8.1.504.14, OCS writes all HTTP Proxy-related activity traces to a separate HTTP Proxy log. This log file is stored in the same location as the OCS log, but has the suffix **_HTTPPRX** added to the filename.

Note:	Be aware that using NMAP or similar port scanners can cause OCS to close HTTP ports.

Configuring OCS for HTTP

Purpose

- To configure the OCS application object to communicate with clients using HTTP requests/responses.

Start

1. In Genesys Administrator, go to Provisioning > Environment > Applications and double-click your OCS application object.
2. Configure a separate listener port on the Configuration tab/Server Info section with the Connection Protocol set to `http`.

End

Configuration Changes

Dynamic changes to this port are not supported. As a result, any such changes are not communicated to an HTTP Proxy that is already running. However, any HTTP Proxy started that is after that port change will reflect the change.

HTTP terminates if the HTTP listener port is removed from the OCS Configuration tab/Server Info section or if the connection is lost between OCS and HTTP Proxy.

Primary and Backup OCS and HTTP Proxy

If you have configured primary and backup OCS applications, the primary instance starts an associated HTTP Proxy and opens a listening port. The backup OCS only starts HTTP Proxy and opens a listening port when it is switched into primary mode.