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 (CX Contact) Private Edition Guide

Configure CX Contact

2/5/2026

Contents

Learn how to configure CX Contact.

Related documentation:

-
-
-
-

RSS:

- For private edition

Override Helm chart values

You can specify parameters for the deployment by overriding Helm chart values in the **values.yaml** file. See the Parameters table for a full list of overridable values.

For more information about Helm chart values, see Overriding Helm chart values.

Parameter	Description
configserver.user_name, user_password	Defines the system username and password for CX Contact.
redis.nodes	Provides a valid URI to Redis.
redis.password	Provides a valid auth password for Redis.
elasticsearch.host	Provides a valid URI to Elasticsearch.
gws.client_id	The name of the GWS service client that will be created (if it doesn't exist) and the secret that will be placed in the k8s secrets repository.
gws.client_secret	The client that will be created with this secret string. If a GWS client with this name already exists, you'll need to enter the secret here.
gws.frontend_host, frontend_port	The SSO GAuth URI where CX Contact redirects during log in.
core.auth, environment	The internal URI to core services that is required for further provisioning. You can see, in our example GAuth is installed in namespace "gauth"
platform.ocs, configration, .. etc.	The internal URI to the platform's GWS services. You can see, in our example GWS is installed in namespace "gws"
ingress.cxc_frontend	Creates a URI that is used by Ingress to route external incoming requests to CX Contact (Web UI and API).

Parameter	Description
internal_ingress.cxc_backend	Creates the URI that is used by Ingress to route internal incoming requests to CX Contact (API for OCS, GWS, Designer, etc)
storage.size	Defines the appropriate size for the permanent storage, depending on the daily volume of interactions, etc.
storage.storageClassName	Picks the existing Storage Class, which is described in this document earlier.

Configure Kubernetes

Preconfiguring Kubernetes ConfigMaps and create a default secret when you are preparing the cluster resources.

Configure security

When configuring CX Contact, you must set the connectivity to the Compliance Data Provider (CDP).

> ### Tip
>
> Before attempting to connect to CDP Next Generation (NG), you'll need the access ID and Secret. To obtain these credentials, contact Genesys Customer Care.

As of 9.0.025.xx, CX Contact uses CDP NG by default. The following Helm chart settings control the CDP NG connectivity:

```
cxcontact:
  compliance_data:
    cdp_ng:
      url: "https://api.usw2.pure.cloud/api/v2/outbound/compliancedata"
      gcloud_auth: "https://login.usw2.pure.cloud/oauth/token"
      gcloud_id:
      gcloud_secret:
    # LIST_BUILDER_DATA_EMBEDDED_BASEPATH
    embedded_basepath: "/list_builder/data/ng_init_data"
    rule_set:
      areacode: "AU,CA,GB,NZ,US"
      geo: "AU,CA,GB,NZ,US"
      postal: "CA,GB,US"
      dnc: "GB,US"
```

> ### Important

> The **gcloud_id** and **gcloud_secret** parameters are required, but do not have default values.

You can use the following parameters to switch to legacy CDP:

```
cxcontact:
  compliance_data:
    cdp_ng:
      url: false
      gcloud_auth: false
      gcloud_id: false
      gcloud_secret: false
    # LIST_BUILDER_DATA_EMBEDDED_BASEPATH
    embedded_basepath: "/list_builder/data/init_data"
```

Security Context

The security context settings define the privilege and access control settings for pods and containers.

By default, the user and group IDs are set in the **values.yaml** file as `500:500:500`, meaning the **genesys** user. For example:

```
securityContext:
    runAsNonRoot: true
    runAsUser: 500
    runAsGroup: 500
    fsGroup: 500
```

TLS authentication

TLS 1.2 connectivity is required for all connections to databases (Redis, PostgreSQL, and Elasticsearch) and connections must be authenticated using credentials.