



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

Before you begin

7/27/2024

Contents

- 1 Limitations and assumptions
 - 1.1 Prerequisites
 - 1.2 Optional tasks
- 2 Download the Helm charts
- 3 Third-party prerequisites
- 4 Storage requirements
- 5 Network requirements
 - 5.1 Single namespace
 - 5.2 External connections
 - 5.3 Ingress
 - 5.4 Ingress SSL
 - 5.5 Logging
 - 5.6 Monitoring
- 6 Browser requirements
- 7 Genesys dependencies
- 8 GDPR support

Find out what to do before deploying CX Contact.

Related documentation:

-
-
-
-

RSS:

- [For private edition](#)

Limitations and assumptions

There are no limitations. Before you begin deploying the CX Contact service, it is assumed that the following prerequisites and optional task, if needed, are completed:

Prerequisites

- A Kubernetes cluster is ready for deployment of CX Contact.
- The Kubectl and Helm command line tools are on your computer.
- You have connectivity to target cluster, the proper kubectl context to work with the cluster, and your user has administrative permissions to deploy CX Contact to the defined namespace.

Optional tasks

- **SFTP Server**—Install an SFTP Server with basic authentication for optional input and output data. SFTP Server is used when automation capabilities are required.
- **CDP NG access credentials**—As of CX Contact 9.0.025, Compliance Data Provider Next Generation (CDP NG) is used as a CDP by default. Before attempting to connect to CDP NG, obtain the necessary access credentials (ID and Secret) from Genesys Customer Care.
- **Bitnami repository**—If you choose to deploy dedicated Redis and Elasticsearch for CX Contact, add the Bitnami repository to install Redis and Elasticsearch using the following command:
helm repo add bitnami <https://charts.bitnami.com/bitnami>

After you've completed the mandatory tasks, check the Third-party prerequisites.

Download the Helm charts

For information about how to download the Helm charts, see [Downloading your Genesys Multicloud CX containers](#).

See Helm charts and containers for CX Contact for the Helm chart version you must download for your release.

CX Contact is the only service that runs in the CX Contact Docker container. The Helm charts included with the CX Contact release provision CX Contact and any Kubernetes infrastructure necessary for CX Contact to run.

Third-party prerequisites

Set up Elasticsearch and Redis services as standalone services or installed in a single Kubernetes cluster.

For information about setting up your Genesys Multicloud CX private edition platform, see [Software requirements](#).

Third-party services

Name	Version	Purpose	Notes
Elasticsearch	7.x	Used for text searching and indexing. Deployed per service that needs Elasticsearch during runtime.	CX Contact supports Elasticsearch 6.3 and later releases.
Redis	6.x	Used for caching. Only distributions of Redis that support Redis cluster mode are supported, however, some services may not support cluster mode.	CX Contact supports Redis 4.0 (5.0 and later releases recommended), clustered with persistence in Production.
Load balancer		VPC ingress. For NGINX Ingress Controller, a single regional Google external network LB with a static IP and wildcard DNS entry will pass HTTPS traffic to NGINX Ingress Controller which will terminate SSL traffic and will be setup as part of the platform setup.	
PostgreSQL	11.x	Relational database.	Relational database.
A container image registry and Helm chart		Used for downloading Genesys containers and	

Name	Version	Purpose	Notes
repository		Helm charts into the customer's repository to support a CI/CD pipeline. You can use any Docker OCI compliant registry.	

Storage requirements

CX Contact requires shared persistent storage and an associated storage class created by the cluster administrator. The Helm chart creates the ReadWriteMany (RWX) Persistent Volume Claim (PVC) that is used to store and share data with multiple CX Contact components.

The minimal recommended PVC size is 100GB.

Network requirements

This topic describes network requirements and recommendations for CX Contact in private edition deployments:

Single namespace

Deploy CX Contact in a single namespace to prevent ingress/egress traffic from going through additional hops, due to firewalls, load balancers, or other network layers that introduce network latencies and overhead. Do not hardcode the namespace. You can override it by using the Helm file/values (provided during the Helm install command **standard --namespace= argument**), if necessary.

External connections

For information about external connections from the Kubernetes cluster to other systems, see Architecture. External connections also include:

- Compliance Data Provider (AWS)
- SFTP Servers

Ingress

The CX Contact UI requires Session Stickiness. Use **ingress-nginx** as the ingress controller (see github.com).

Important

The CX Contact Helm chart contains default annotations for session stickiness only for **ingress-nginx**. If you are using a different ingress controller, refer to its documentation for session stickiness configuration.

Ingress SSL

If you are using Chrome 80 or later, the **SameSite** cookie must have the **Secure** flag (see Chromium Blog). Therefore, Genesys recommends that you configure a valid SSL certificate on ingress.

Logging

Log rotation is required so that logs do not consume all of the available storage on the node.

Kubernetes is currently not responsible for rotating logs. Log rotation can be handled by the **docker json-file log driver** by setting the **max-file** and **max-size** options.

For effective troubleshooting, the engineering team should provide **stdout logs** of the pods (using the command **kubectrl logs**). As a result, log retention is not very aggressive (see JSON file logging driver). For example:

```
{
  "log-driver": "json-file",
  "log-opts": {
    "max-size": "100m",
    "max-file": "3"
  }
}
```

For on-site debugging purposes, CX Contact logs can be collected and stored in Elasticsearch. (For example, EFK stack. See medium.com).

Monitoring

CX Contact provides metrics that can be consumed by Prometheus and Grafana. It is recommended to have the **Prometheus Operator** (see github.com) installed in the cluster. CX Contact Helm chart supports the creation of **CustomResourceDefinitions** that can be consumed by the Prometheus Operator.

For more information about monitoring, see [Observability in Outbound \(CX Contact\)](#).

Browser requirements

Browsers

Name	Version	Notes
Chrome	Current release or one version	Chrome updates itself

Name	Version	Notes
	previous	automatically. Versions of Chrome are only an issue if your IT department restricts automatic updates. The latest version of Chrome must be used as the CX Contact UI browser.
Microsoft Edge (Legacy)	Current release	Starting from CX Contact release 9.0.026.04, Edge Chromium browser 2020

Genesys dependencies

CX Contact components operate with Genesys core services (v8.5 or v8.1) in the back end. All voice-processing components (Voice Microservice and shared services, such as GVP), and the GWS and Genesys Authentication services (mentioned below) must be deployed and running before deploying the CX Contact service. See Order of services deployment.

The following Genesys services and components are required:

- GWS
- Genesys Authentication Service
- Tenant Service
- Voice Microservice
- Multi-tenant Configuration Server

Nexus is optional.

GDPR support

CX Contact does not support GDPR.