# Genesys Customer Experience Insights Private Edition Guide

## Before you begin deploying GCXI

2/10/2026

# Contents

Find out what to do before deploying Genesys Customer Experience Insights (GCXI).

**Related documentation:**
- 
- 
- 
- 

**RSS:**
- For private edition

## Limitations and assumptions

GCXI can provide meaningful reports only if Genesys Info Mart and Reporting and Analytics Aggregates (RAA) are deployed and available. Deploy GCXI only after Genesys Info Mart and RAA.

## Download the Helm charts

For more information about how to download the Helm charts in Jfrog Edge, see the suite-level documentation: Downloading your Genesys Multicloud CX containers

To learn what Helm chart version you must download for your release, see Helm charts and containers for Genesys Customer Experience Insights

**GCXI Containers**

- GCXI Helm chart uses the following containers.
    - **gcxi** - main GCXI container, runs as a StatefulSet. This container is roughly 12 GB; ensure that you have enough space to allocate it.
    - **gcxi-control** - supplementary container, used for initial installation of GCXI, and for clean-up.

**GCXI Helm Chart** Download the latest yaml files from the repository, or examine the attached files: Sample GCXI yaml files

## Third-party prerequisites

For more information about setting up your Genesys Multicloud CX private edition platform, including Kubernetes, Helm, and other prerequisites, see Software requirements.

Third-party services

| Name | Version | Purpose | Notes |
|---|---|---|---|
| A container image registry and Helm chart repository | | Used for downloading Genesys containers and Helm charts into the customer's repository to support a CI/CD pipeline. You can use any Docker OCI compliant registry. | |
| PostgreSQL 12 | 12 | Relational database (Genesys Customer Experience Insights meta requires this version) | Version 12 is required. |
| MicroStrategy | | Genesys Customer Experience Insights provides this software but requires replacement of MicroStrategy 3rd party keys. | |
| 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. | |
| An SMTP relay | | Facilitates email communications in an environment where GCXI reports or voicemails are sent as emails to contact center personnel. Genesys recommends PostFix, but you can use any SMTP relay that supports standard mail libraries. | |

# Storage requirements

GCXI installation requires a set of local Persistent Volumes (PVs). Kubernetes *local* volumes are directories on the host with specific properties: https://kubernetes.io/docs/concepts/storage/volumes/#local

Example usage: https://zhimin-wen.medium.com/local-volume-provision-242affd5efe2

Kubernetes provides a powerful volume plugin system, which enables Kubernetes workloads to use a wide variety of block and file storage to persist data.

You can use the GCXI Helm chart to set up your own PVs, or you can configure PV Dynamic Provisioning in your cluster so that Kubernetes automatically creates PVs.

## Volumes Design

GCXI installation uses the following PVC:

| Mount Name | Mount Path (inside container) | Description | Access Type | Approximate Size | Default Mount Point on Host (You can change the mount point using values.) The local provisioner requires that the specified directory pre-exists on your host. | Must be Shared across Nodes? | Required Node Label (applies to default Local PV setup) |
|---|---|---|---|---|---|---|---|
| gcxi-backup | /genesys/gcxi_shared/backup | Backup files Used by control container / jobs. | RWX | Depends on backup frequency. 5 GB+ | /genesys/gcxi/backup You can override this setting using Values.gcxi.local.pv.backup.path | Only in multiple concurrent installs scenarios. | gcxi/local-pv-gcxi-backup = "true" |
| gcxi-log | /mnt/log | MSTR logs Used by main container. The GCXI Helm chart allows log volumes of legacy hostPath | RWX | Depends on rotation scheme. 5 GB+ | /mnt/log/gcxi subPathExpr: $(POD_NAME) You can override this setting using | Not necessarily. | gcxi/local-pv-gcxi-log = "true" If you are using hostPath volumes for logs, you don't need |

| Mount Name | Mount Path (inside container) | Description | Access Type | Approximate Size | Default Mount Point on Host (You can change the mount point using values.) The local provisioner requires that the specified directory pre-exists on your host. | Must be Shared across Nodes? | Required Node Label (applies to default Local PV setup) |
|---|---|---|---|---|---|---|---|
| | | type. This scenario is the default and used in examples in this document. | | | Values.gcxi.local.pv.log.path | | node label. |
| gcxi-postgres | /var/lib/postgresql/data (if using Postgres in container) or disk space in Postgres RDBMS | Meta DB volume Used by Postgres container, if deployed. | RWO | Depends on usage. 10 GB+ | /genesys/gcxi/shared You can override this setting using Values.gcxi.local.pv.postgres.path | Yes, unless you tie the Postgres container to some particular node | gcxi/local-pv-postgres-data = "true" |
| gcxi-share | /genesys/gcxi_share | MSTR shared caches and cubes Used by main container. | RWX | Depends on usage. 5 GB+ | /genesys/gcxi/data subPathExpr: $(POD_NAME) You can override this setting using Values.gcxi.local.pv.share.path | Yes. | gcxi/local-pv-gcxi-share = "true" |

# Preparing the environment

To prepare your environment, complete the following steps:

1. To log in to the cluster, run the following command:

- For AKS:

    ```
    az aks get-credentials --resource-group  --name
    ```

- For GKE:

    ```
    gcloud container clusters get-credentials gke1
    ```

- For OpenShift:

    ```
    oc login --token  --server
    ```

    - To check the cluster version on OpenShift deployments, run the following command:

        ```
        oc get clusterversion
        ```

2. To create a new project, run the following command:
   GKE or AKS:

   1. Edit the **create-gcxi-namespace.json**, adding the following values:

      ```
      {
        "apiVersion": "v1",
        "kind": "Namespace",
        "metadata": {
          "name": "gcxi",
          "labels": {
            "name": "gcxi"
          }
        }
      }
      ```

   2. To apply the changes, run the following command:

      ```
      kubectl apply -f apply create-gcxi-namespace.json
      ```

      OpenShift:

      ```
      oc new-project gcxi
      ```

3. For GKE or AKS, to confirm namespace creation, run the following command:

   ```
   kubectl describe namespace gcxi
   ```

4. Create a secret for docker-registry to pull images from the Genesys JFrog repository:

   ```
   kubectl create secret docker-registry  --docker-server= --docker-username= --docker-
    password= --docker-email= -n gim
   ```

5. Create the file **values-test.yaml**, and populate it with appropriate override values. For a simple deployment using PostgreSQL inside the container, you must include PersistentVolumes named **gcxi-log-pv**, **gcxi-backup-pv**, **gcxi-share-pv**, and **gcxi-postgres-pv**. You must override **GCXI_GIM_DB** with the name of your Genesys Info Mart data source.

# Network requirements

## Ingress

Ingress annotations are supported in the **values.yaml** file (see line 317). Genesys recommends session stickiness, to improve user experience.

```
ingress:
    # http path and annotations may be overriden for external and internal access separately
    annotations:
      kubernetes.io/ingress.class: "nginx"
      nginx.ingress.kubernetes.io/affinity: cookie
      nginx.ingress.kubernetes.io/affinity-mode: persistent
      nginx.ingress.kubernetes.io/proxy-body-size: "50m"
      nginx.ingress.kubernetes.io/proxy-buffer-size: "8k"
      nginx.ingress.kubernetes.io/ssl-redirect: "false"
    domain:
    external:
      annotations:
      host:
      tls:
        enabled: false
        secretName:
    internal:
      annotations:
      host:
      tls:
        enabled: false
        secretName:
    path: /
```

Allowlisting is required for GCXI.

## WAF Rules

WAF rules are defined in the **variables.tf** file (see line 245).

## SMTP

The GCXI container and Helm chart support the environment variable `EMAIL_SERVER`.

## TLS

The GCXI container does not serve TLS natively. Ensure that your environment is configured to use proxy with HTTPS offload.

# Browser requirements

MicroStrategy Web is the user interface most often used for accessing, managing, and running the Genesys CX Insights reports. MicroStrategy Web certifies the latest versions, at the time of release, for the following web browsers:

- Apple Safari
- Google Chrome (Windows and iOS)
- Microsoft Edge
- Microsoft Internet Explorer (Versions 9 and 10 are supported, but not certified)
- Mozilla Firefox

To view updated information about supported browsers, see the MicroStrategy ReadMe.

Browsers

| Name | Version | Notes |
|------|---------|-------|
| Firefox | Current release or one version previous | Genesys also supports the current ESR release. Genesys supports the transitional ESR release only during the time period in which the new ESR release is tested and certified. For more information, see Firefox ESR release cycle. Firefox updates itself automatically. Versions of Firefox are only an issue if your IT department restricts automatic updates. |
| Microsoft Edge (Legacy) | Current release | |
| Chrome | Current release or one version previous | Chrome updates itself automatically. Versions of Chrome are only an issue if your IT department restricts automatic updates. |

# Genesys dependencies

GCXI requires the following services:

- Reporting and Analytics Aggregates (RAA) is required to aggregate Genesys Info Mart data.
- Genesys Info Mart and / or Intelligent Workload Distribution (IWD) Data Mart. GCXI can run without these services, but cannot produce meaningful output without them.
- GWS Auth/Environment service
- Genesys Platform Authentication thru Config Server (GAuth). Alternatively, GCXI includes a native internal login, which you can use to authorize users, instead of GAuth. This document assumes you are

using GAuth (the recommended solution), which gives ConfigServer users access to GCXI.

- GWS client id/client secret

## GDPR support

GCXI can store Personal Identifiable Information (PII) in logs, history files, and in reports (in scenarios where customers include PII data in reports). Genesys recommends that you do not capture PII in reports. If you do capture PII, it is your responsibility to remove any such report data within 21 days or less, if required by General Data Protection Regulation (GDPR) standards.

For more information and relevant procedures, see: Genesys CX Insights Support for GDPR and the suite-level **Link to come** documentation.