



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.

Setting up Genesys Multicloud CX Private Edition

Software requirements

Contents

- 1 Private edition general prerequisites
 - 1.1 Licensing requirements
- 2 Third-party dependencies for Genesys Multicloud CX services
- 3 Permissions
 - 3.1 Consul

Prerequisite software and third-party dependencies required for the Genesys Multicloud CX private edition environment.

Related documentation:

-
-

RSS:

- [For private edition](#)

This article covers the following sections:

- The prerequisites required for the private edition environment
- The third-party dependencies required for the Genesys Multicloud CX services.

You must first set up the private edition environment with the supported Kubernetes distribution, Helm, contact center components, and so on. In the Kubernetes clusters, deploy the third-party dependencies such as Consul, Redis, Kafka, and so on, that are necessary for the Genesys Multicloud CX services to function. Once you have the private edition environment with the required third-party dependencies deployed, you can proceed with deploying the Genesys Multicloud CX services.

Private edition general prerequisites

The private edition general prerequisites are:

- Domain Name System (DNS)
- Helm 3.0+
- Ingress Controller
 - NGINX Ingress Controller (Google Kubernetes Engine)
- JFrog Edge Artifactory account
- Kubernetes 1.25
- Kubernetes secrets
- Session Border Controller (SBC)
- Web Application Firewall (WAF) - optional, but recommended.

Licensing requirements

Genesys Multicloud CX private edition services (release 100.x and above) do not require any

technical licenses or activation files for deployment or operation in any environment that contains only Genesys software. However, software or services provided by vendors other than Genesys might require licenses or activation files. Any licenses or activation files required for third-party software or services that are resold by Genesys and/or are embedded in Genesys services will be issued separately according to the terms outlined in your contract and services order. It is your responsibility to acquire licenses for software or services that you obtain from other vendors.

Third-party dependencies for Genesys Multicloud CX services

Genesys Multicloud CX services require specific third-party dependencies for its functioning, for example, Redis (an in-memory caching software). You can install these third-party dependencies in a different namespace or outside the cluster provided the namespace has direct network access to these services.

Important

Deploying and maintaining the third-party dependencies is your responsibility. For more information on your responsibilities and how Genesys supports the deployment process, see [Understanding responsibilities](#).

See the table below for details about the Genesys supported third-party dependencies.

Name	Version	Purpose	Mandatory?	Private edition services
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.	Yes	All Genesys services
An SMTP relay		Facilitates email communications in an environment where GCXI reports or voicemails are sent as emails to contact center personnel. Genesys	No	<ul style="list-style-type: none">• Genesys Customer Experience Insights• Voice Microservices

Name	Version	Purpose	Mandatory?	Private edition services
		recommends PostFix, but you can use any SMTP relay that supports standard mail libraries.		
Command Line Interface		The command line interface tools to log in and work with the Kubernetes clusters.	No	<ul style="list-style-type: none"> • Genesys Authentication • Genesys Web Services and Applications • AI Connector • Digital Channels • GIM Config Adapter • GIM • GIM Stream Processor • WebRTC Gateway Service
HTTPS certificates - cert-manager		Use with Let's Encrypt to provide free rotating TLS certificates for NGINX Ingress Controller.	Optional	<ul style="list-style-type: none"> • Genesys Authentication • Genesys Web Services and Applications • AI Connector • Digital Channels
HTTPS certificates - Let's Encrypt		Use with cert-manager to provide free rotating TLS certificates for NGINX Ingress Controller. Note: Let's Encrypt is a suite-wide requirement if you choose an Ingress Controller that needs it.	No	<ul style="list-style-type: none"> • Genesys Authentication • Genesys Web Services and Applications • AI Connector • Digital Channels
Ingress controller		HTTPS ingress controller.	Yes	<ul style="list-style-type: none"> • Genesys Authentication • Genesys Web Services and Applications • AI Connector

Name	Version	Purpose	Mandatory?	Private edition services
				<ul style="list-style-type: none"> Digital Channels Universal Contact Service
Load balancer		<p>VPC ingress.</p> <p>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.</p>	Yes	<ul style="list-style-type: none"> Genesys Authentication Designer Genesys Web Services and Applications AI Connector Digital Channels Intelligent Workload Distribution CX Contact Genesys Customer Experience Insights Genesys Pulse Universal Contact Service WebRTC Gateway Service
Object storage		<p>Persistent or shared data storage, such as Amazon S3, Azure Blob Storage, or Google Cloud Storage.</p>	No	<ul style="list-style-type: none"> GIM Config Adapter GIM GIM Stream Processor
Kafka	2.x	Message bus.	Yes	<ul style="list-style-type: none"> Interaction Server GIM Config Adapter GIM GIM Stream Processor Tenant Service Event Stream Voice Microservices
Keda	2.0	<p>Custom metrics for scaling. Use of Keda or HPA is configurable through Helm charts.</p>	No	<ul style="list-style-type: none"> WebRTC Gateway Service

Name	Version	Purpose	Mandatory?	Private edition services
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.	Yes	<ul style="list-style-type: none"> • Genesys Authentication • Designer • Genesys Web Services and Applications • Interaction Server • Genesys Engagement Service • AI Connector • Digital Channels • Email • Intelligent Workload Distribution • CX Contact • Genesys Pulse • Tenant Service • Event Stream • Voice Microservices
Consul	1.13.x	Service discovery, service mesh, and key/value store.	Yes	<ul style="list-style-type: none"> • Genesys Authentication • Genesys Web Services and Applications • Genesys Engagement Service • Tenant Service • Voice Microservices
Elasticsearch	7.x	Used for text searching and indexing. Deployed per service that needs Elasticsearch during runtime.	Yes	<ul style="list-style-type: none"> • Designer • Genesys Web Services and Applications • Intelligent Workload Distribution • CX Contact • Universal Contact Service
MS SQL Server	2016 or later	Relational database. Required only		<ul style="list-style-type: none"> • Genesys Voice Platform

Name	Version	Purpose	Mandatory?	Private edition services
		for GVP.		
PostgreSQL	11.x	Relational database.	Yes	<ul style="list-style-type: none"> • Genesys Authentication • Genesys Voice Platform • Genesys Web Services and Applications • Interaction Server • Genesys Engagement Service • AI Connector • Digital Channels • IWD Data Mart • Intelligent Workload Distribution • CX Contact • GIM • Genesys Pulse • Tenant Service • Universal Contact Service

For information on troubleshooting third-party services, refer to [Troubleshooting Third-Party Services](#) in our public repository.

Permissions

Security context parameters in the Helm charts specify the users authorized to access the pods and containers for the respective services. By default, the Helm charts specify the user, group, and file-service group IDs as 500:500:500.

Consul

- Consul and Consul Service Mesh are required.
- Consul requires privileged containers; so the cluster-administrator must have permissions to install mutating hooks, configure kube-dns, and access Kubernetes APIs.

In an early implementation, private edition required the use of a custom SCC called **genesys-restricted** to control permissions associated with the **genesys** user (500) specified by the services. The **genesys-restricted** SCC has now been deprecated.

Arbitrary UIDs

To use arbitrary UIDs, override the Helm chart values so that no specific IDs are defined for users and groups.