Genesys Authentication Private Edition Guide

Before you begin

5/23/2026

Contents

Find out what to do before deploying Genesys Authentication.

Related documentation:

-
-
-

RSS:

- For private edition

Download the Helm charts

Genesys Authentication in Genesys Multicloud CX private edition is made up of three containers, one for each of its components:

- gws-core-auth - Authentication API service
- gws-ui-auth - Authentication UI service
- gws-core-environment - Environment API service

The service also includes a Helm chart, which you must deploy to install all three containers for Genesys Authentication:

- gauth

See Helm charts and containers for Authentication, Login, and SSO for the Helm chart version you must download for your release.

To download the Helm chart, navigate to the **gauth** folder in the JFrog repository. See Downloading your Genesys Multicloud CX containers for details.

Third-party prerequisites

Install the prerequisite dependencies listed in the **Third-party services** table before you deploy Genesys Authentication.

Third-party services

Name	Version	Purpose	Notes
PostgreSQL	11.x	Relational database.	Genesys Authentication supports PostgreSQL

Name	Version	Purpose	Notes
			12.x.
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.	Redis must be in cluster mode.
Consul	1.13.x	Service discovery, service mesh, and key/value store.	
Ingress controller		HTTPS ingress controller.	
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.	
HTTPS certificates - cert-manager		Use with Let's Encrypt to provide free rotating TLS certificates for NGINX Ingress Controller.	
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.	
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.	
Command Line Interface		The command line interface tools to log in and work with the Kubernetes clusters.	

Storage requirements

Genesys Authentication uses PostgreSQL to store key/value pairs for the Authentication API and Environment API services. It uses Redis to cache data for the Authentication API service.

Network requirements

Ingress

Genesys Authentication supports both internal and external ingress with two ingress objects that are configured with the **ingress** and **internal_ingress** settings in the **values.yaml** file. See Configure Genesys Authentication for details about overriding Helm chart values.

- ingress - External ingress for UIs and external API clients. External ingress can be public.
- internal_ingress - Internal ingress for internal API clients. Internal ingress contains an extended list of API endpoints that are not available for external ingress. Internal ingress should not be public.

These ingress objects support Transport Layer Security (TLS) version 1.2. TLS is enabled by default and you can configure it by overriding the **ingress.tls** and **internal_ingress.tls** settings in **values.yaml**.

For example:

```
 ingress:
  enabled: true
  frontend: gauth.example.com
  tls_enabled: true
  tls:
    - hosts:
        - gauth.example.com
      secretName: gauth-example-com

internal_ingress:
  enabled: true
  frontend: gauth.int.example.com
  tls_enabled: true
  tls:
    - hosts:
        - gauth.int.example.com
      secretName: gauth-int-example-com
```

In the example above:

- **secretName** is the certificate and private key to use for TLS. The secret is a prerequisite and must be created before you deploy Genesys Authentication, unless you have Certificate ClusterIssuer installed and configured in Kubernetes Cluster. In this case, the secret is created by ClusterIssuer.
- **hosts** is a list of the fully qualified domain names that should use the certificate. The list must be the same as the value configured for **ingress.frontend** and **internal_ingress.frontend**.

Cookies

Genesys Authentication components use cookies to identify HTTP/HTTPS user sessions.

Browser requirements

The Authentication UI supports the web browsers listed in the **Browsers** table.

Browsers

Name	Version	Notes
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.
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	
Microsoft Edge Chromium	Current release	

Genesys dependencies

Genesys Authentication must be deployed before other Genesys Multicloud CX private edition services. To complete provisioning the service, you must first deploy Web Services and Applications and the Tenant Service. For a look at the high-level deployment order, see Order of services deployment.