



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.

# Genesys Authentication Private Edition Guide

[Configure Genesys Authentication](#)

---

## Contents

- [1 Add Java KeyStore support \(optional\)](#)
- [2 Configure a secret to access JFrog](#)
- [3 Override Helm chart values](#)
- [4 Configure Kubernetes](#)
  - [4.1 ConfigMaps](#)
  - [4.2 Secrets](#)
- [5 Configure security](#)

---

Learn how to configure Genesys Authentication.

### Related documentation:

- 
- 
- 

### RSS:

- [For private edition](#)

Complete the steps on this page to configure your Genesys Authentication deployment.

## Add Java KeyStore support (optional)

Complete the steps in this section to set up a Java KeyStore (JKS) if you need to configure Genesys Authentication to use JSON Web Token authentication. This method of authentication is currently used for WebRTC.

Create a keystore file:

```
keytool -keystore jksStorage.jks -genkey -alias gws-auth-key -storepass -keypass -keyalg RSA
```

Get the Base64 encoded key:

```
cat ./jksStorage.jks | base64
```

The result looks like this:

```
/u3+7QAAAAIAAAABAAAAAQAMZ3dzLWF1dGgta2V5AAABeRmB2Y4AAAUBMIIE/  
TA0BgorBgEEASoCEQBBAEggTpwQ05aw5CUYAsf4/IheBuNrLPPyZhUA+NWh3SG52HV3sVjV+p18vKp2k/  
q12I9NynoM6R/  
DW5bFfEWU1zx3cFXH2kNirRU0IbNZpa43N0royyF1GSdZFlwa8Kq8Xtp8ZBmiJdSb1n120DaTKGKv1cb5tsfdzkWs99QeTBGJypHMCdnBvdFB0N  
mMACTHk4R9yASsd7fljgNLSn0jhrz9FuxvYgp0VvExiq+sb5YrfbZjtTzZDzFV0u/  
2kWzASfZBSiyyxM0r3IhUPkMpIrg+UYkI0tgn/  
C3yR1wLr9HELpx8fCu610Rqp8hhp1yvL46K0c6eTa2JcRp06fmysf2EG0JagG7zNEJHlvtNnt3JpQV06xos2iWsFAtHq+9w8LwvCVbDzx/  
UHoCYenIdJ7SBv06mXgKisa3RDIi/y5x5/9T4brgCLUvwI4Z5Rf/oi2Zx5/lXjQXmBPLPAcUVHLr5PvNQUUx5NBr/  
ooioD7qka4ADF1/  
cx8I2bzqTi+U01fiFdMGRlNlCfcGDMI2h82JUeCswRYi4+dMDiSaGgC2MoL2susLxMYa5CTo9Vs0Y2k+6j8fhI04h8h0JxdXZ0DU630M0cDSUHX  
4IhiV3k7w40HYeXUeDvoNmfo/AriELZl+WgYETiXGsKzxmrsHrBKC0+aT098FwqdY9ACsM/  
7WoF2+9eftc7fa2jruutrRjmk0A/  
BaIqzboJLFiWaUUGV9gsexEmpGszikQsm0YSIRxY8BYF+SYLdehcfcsRRxDnhTaGNV8y2ZnwA61FNPAFps3gaFXeaYsUzLxTSi9m70HJJrUp7JD  
KFi90rEuAdhMJ+a+iQ21PBZ+iIwxb0y9xMReImoUtoqy6Epre3qM0S6MILLw2bVrxJYo38+hR5uzNdLbsUlpy0oorI1Hp8A/  
VEYtG9PDHEhhoqUamdUYUzkFDi9QZfyLIgi8Jc4G4PPrPKgMPqE7s16bJvoLavU58eHpdWo/Mb9UtdTx+L/  
SLuLCCE0Xce6M9YE1SyC2B3gd82zNqa81lx+QAY8IaSmX+C2nMz+UeXKngSEzguK6gXg9RwCs8pUavuLQ6uZGkJ+fhDBvDAFgD7hG1XdHs27XGS  
DT/KHRB7AHN5/  
vQpj6K0scxqmyPrgPY/+TseczEeaQLQ6MfjvXY+AAAAAQAFWC41MDkAAAN7MIIDdzCCA1+gAwIBAgIEYxhLHTANBgkqhkiG9w0BAQsFADBsMRAw  
esYcJNEqu1btJLwLvhXb6510yZnsmeNGP2BrNCPXZS6CBReMMKJaZr1CwJQxiSrGPHB/
```

---

```
gpxKoAowLwL3V7wB2BHKDhrczQBPdvtsfBAzeqN/  
yRpdKZRAtu2LyGqRZKCgLSrwYenJFqR0d0eworbNmtIKXfQLiamE4KdhzQdPfnYBC7ZwtCIJUp9Va4LmCYD/  
IS0mVyfQ9Xql1rRNQLcVaewCKRM2ffBAkx98d3n79XUZDlj0zHh+79tCpheuuYfbMQqMCAwEAAaMhMB8wHQYDVR00BBYEFNtM8mIEb67VYot5tj  
Ta4y+B6JcdPjFtII6Pf5W0DDT0a3cHNMeukYn5lBnaMbIKqoxFT7nM7MD3DB+dISvMu8FtVwFwbPzXWhl+Aycuu9ETGlCoJqYfl+vmLyGjJVadcl  
YbN7be2QIJwmucIZzH7fkU90V+rmVZh19Bo8ixuIJG/vZTxmEBaDqmhiP4w=
```

Make note of the following values - you need them to configure JKS support in the Helm chart:

- Keystore filename
- Keystore password
- Key alias
- Key password
- Base64 encoded key

## Configure a secret to access JFrog

If you haven't done so already, create a secret for accessing the JFrog registry:

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

Now map the secret to the default service account:

```
kubectl secrets link default --for=pull
```

## 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 how to override Helm chart values, see [Overriding Helm chart values in the Setting up Genesys Multicloud CX Private Edition guide](#).

Parameters

| Parameter            | Description  | Valid values          | Default |
|----------------------|--|-----------------------|---------|
| gws-core-auth        | The gws-core-auth image version tag. For example, 100.0.003.3508.        | A valid image version | ""      |
| gws-core-environment | The gws-core-environment image version tag. For example, 100.0.003.1866. | A valid image version | ""      |
| gws-ui-auth          | The gws-ui-auth image version tag. For                                   | A valid image version | ""      |

| Parameter                   | Description   | Valid values                                | Default  |
|-----------------------------|---|---|--|
|                             | example,<br>100.0.003.1328.   |   |  |
| image.imagePullSecrets      | The secret Kubernetes uses to get credentials to pull images from the registry.                 | A valid secret                              | []   |
| image.pullPolicy            | Specifies when Kubernetes pulls images from the registry on start up.                           | IfNotPresent or Always                      | "IfNotPresent"                                   |
| image.registry              | Docker registry address   | A valid registry URL                        | ""   |
| consul.discovery_register   | Specifies whether services are registered in Consul.  | true or false                               | false  |
| consul.discovery_tenant_s   | Enables tenant discovery through Consul.  | true or false                               | true   |
| consul.enabled              | Enables a connection to Consul.   | true or false                               | false  |
| consul.host                 | The host of the local Consul agent.   | A valid URL                                 | "http://\$(K8_HOST_IP)"                          |
| consul.port                 | The port of the local Consul agent.   | A valid port                                | 8500   |
| consul.require_token        | Specifies whether Genesys Authentication reads the API token from a Kubernetes secret.          | true or false                               | false  |
| consul.secret.create        | Create or use an existing secret with the Consul API token.                                     | true or false                               | false  |
| consul.secret.name_override | The name of the Kubernetes secret for Consul.   | A valid secret name                         | nil  |
| consul.secret.token         | The API token to access Consul.   | A valid API token                           | nil  |
| ingress.enabled             | Enables external ingress for Genesys Authentication.  | true or false                               | true   |
| ingress.frontend            | The host that is used by external ingress.  | A valid host                                | "gauth.local"                                    |
| ingress.annotations.        | Annotations that are applied to external ingress. See the Kubernetes documentation for details. | A valid set of annotations as "name: value" | nginx.ingress.kubernetes.io/proxy-body-size: "0" |
| ingress.tls_enabled         | Enables Transport Layer   | true or false                               | true   |

| Parameter   | Description  | Valid values                                | Default   |
|---|--|---|---|
|   | Security (TLS) on external ingress.  |   |   |
| ingress.tls   | The name of the secret for Secure Sockets Layer (SSL) certificates.  | A valid secret name                         | - hosts:<br>- gauth.local<br>secretName:<br>letsencrypt     |
| internal_ingress.enabled                            | Enables internal ingress for Genesys Authentication.   | true or false                               | true  |
| internal_ingress.frontend                           | The host that is used by internal ingress.   | A valid host                                | "gauth-int.local"   |
| internal_ingress.annotations                        | Annotations that are applied to internal ingress. See the Kubernetes documentation for details.                                    | A valid set of annotations as "name: value" | nginx.ingress.kubernetes.io/proxy-body-size: "0"            |
| internal_ingress.tls_enabled                        | Enables Transport Layer Security (TLS) on internal ingress.  | true or false                               | true  |
| internal_ingress.tls                                | The name of the secret for Secure Sockets Layer (SSL) certificates.  | A valid secret name                         | - hosts:<br>- gauth-int.local<br>secretName:<br>letsencrypt |
| monitoring.enabled                                  | Specifies whether to deploy Custom Resource Definitions (CRD) for ServiceMonitors to determine which services should be monitored. | true or false                               | false   |
| monitoring.interval                                 | The interval at which Prometheus scrapes metrics.  | A duration in seconds                       | "15s"   |
| monitoring.alarms                                   | Specifies whether to deploy CRD for PrometheusRules to define rules for alarms.  | true or false                               | false   |
| monitoring.alarmThresholds.redisKeys                | The threshold to trigger an alarm on the total number of keys in Redis.  | Number                                      | 5000000   |
| monitoring.alarmThresholds.redisMaxMemoryPercentage | The threshold to trigger an alarm for used Redis memory.   | Number                                      | 85  |
| monitoring.dashboards                               | Specifies whether to deploy ConfigMaps with  | true or false                               | false   |

| Parameter                  | Description   | Valid values  | Default   |
|----------------------------|---|---|---|
|                            | Grafana Dashboards.   |   |   |
| monitoring.pagerduty       | Enables alarms with a severity of CRITICAL.   | true or false   | true  |
| optional.affinity          | Specifies the affinity and anti-affinity for Genesys Authentication pods. See the Kubernetes documentation for details.                 | Object  | <pre> podAntiAffinity:   preferredDuringSchedulingIgnoredDuringExecution:     - podAffinityTerm:         labelSelector:           matchLabels:             gauth: '{{ .gauth }}'       app.kubernetes.io/name: '{{ include "auth.name" . }}'       app.kubernetes.io/instance: '{{ .Release.Name }}'       topologyKey: failure-domain.beta.kubernetes.io/zone       weight: 100 </pre> |
| optional.dnsConfig         | Specifies custom DNS settings for Genesys Authentication pods. See the Kubernetes documentation for details.                            | Object  | <pre> options: - name: ndots   value: "3" </pre>  |
| optional.dnsPolicy         | Specifies the DNS policy for Genesys Authentication pods. See the Kubernetes documentation for details.                                 | "Default", "ClusterFirst", "ClusterFirstWithHostNet", or "None" | "ClusterFirst"  |
| optional.nodeSelector      | The labels Kubernetes uses to assign pods to nodes. See the Kubernetes documentation for details.                                       | Object  | {}  |
| optional.priorityClassName | The class name Kubernetes uses to determine the priority of a pod relative to other pods. See the Kubernetes documentation for details. | A valid priority class name                                     | ""  |
| optional.securityContext   | Specifies the privilege and access control  | Object  | {}  |

| Parameter                       | Description  | Valid values   | Default  |
|---------------------------------|--|--|--|
|                                 | settings Genesys Authentication pods. See Configure security for details.  |  |  |
| optional.strategy               | Specifies details for the rolling update strategy Genesys Authentication uses to upgrade its containers. See the Kubernetes documentation for details.         | Object   | <pre>type: RollingUpdate rollingUpdate:   maxSurge: 10   maxUnavailable: 0</pre>   |
| optional.tolerations            | The tolerations Kubernetes uses for advanced pod scheduling. See the Kubernetes documentation for details.   | Object   | []   |
| podDisruptionBudget.create      | Specifies whether to create a PodDisruptionBudget. See the Kubernetes documentation for details.   | true or false  | false  |
| podDisruptionBudget.spec        | Specifies the details of your PodDisruptionBudget. See the Kubernetes documentation for details.   | A valid spec that defines a value for either minAvailable or maxUnavailable. Do not specify .spec.selector because it is calculated by Helm. | minAvailable: 2  |
| pod_autoscaler.auth.enabled     | Enables the Horizontal Pod Autoscaler for the Authentication Service. See the Kubernetes documentation for details.  | true or false  | false  |
| pod_autoscaler.auth.maxReplicas | Specifies the maximum number of Authentication Service replicas the Horizontal Pod Autoscaler controller will scale.   | Number   | 10   |
| pod_autoscaler.auth.metrics     | Specifies resource metrics the Horizontal Pod Autoscaler controller uses to scale Authentication Service pods up or down. See the Kubernetes documentation for | Object   | <pre>- type: Resource   resource:     name: cpu     target:       type:         Utilization         averageUtilizati</pre> |

| Parameter                              | Description  | Valid values          | Default   |
|--|--|-----------------------|---|
|  | details.   |                       | on: 350%  |
| pod_autoscaler.environment.enabled     | Enables the Horizontal Pod Autoscaler for the Environment Service. See the Kubernetes documentation for details.   | true or false         | false   |
| pod_autoscaler.environment.maxReplicas | Specifies the maximum number of Environment Service replicas the Horizontal Pod Autoscaler controller will scale.  | Number                | 10  |
| pod_autoscaler.environment.metrics     | Specifies resource metrics the Horizontal Pod Autoscaler controller uses to scale Environment Service pods up or down. See the Kubernetes documentation for details. | Object                | - type: Resource<br>resource:<br>name: cpu<br>target:<br>type:<br>Utilization<br>averageUtilization: 350% |
| postgres.deploy                        | Specifies whether to deploy PostgreSQL. Set this option for lab environments only.   | true or false         | false   |
| postgres.image                         | Specifies the Docker image to use in the lab environment if postgres.deploy=true.  | A Docker image        | "postgres:11-alpine"  |
| postgres.configmap.create              | Specifies whether Genesys Authentication creates a ConfigMap with PostgreSQL connection parameters. If the value is false, you must create the ConfigMap manually.   | true or false         | false   |
| postgres.configmap.name_override       | The name of the ConfigMap.   | A value name          | nil   |
| postgres.db                            | The name of the PostgreSQL database from Create a PostgreSQL database and user.  | A valid database name | nil   |
| postgres.host                          | The host of the PostgreSQL instance.   | A valid host          | nil   |
| postgres.port                          | The port of the  | A valid port          | nil   |

| Parameter                     | Description  | Valid values                                | Default           |
|-------------------------------|--|---|-------------------|
|                               | PostgreSQL instance.   |   |                   |
| postgres.username             | The username to access the PostgreSQL database from Create a PostgreSQL database and user.   | A valid username                            | nil               |
| postgres.password             | The password to access the PostgreSQL database from Create a PostgreSQL database and user.   | A valid password                            | nil               |
| postgres.secret.create        | Specifies whether to create a Kubernetes secret with user credentials for PostgreSQL. If this value is false, you must create the secret manually. | true or false                               | false             |
| postgres.secret.name_override | The name of the PostgreSQL secret.   | A valid name                                | nil               |
| redis.cluster_nodes           | The Redis nodes in your cluster. For example, "redis-cluster1:7000,redis-cluster2:7002".   | A comma-separated list of "host:port" pairs | nil               |
| redis.configmap.create        | Specifies whether to create a ConfigMap with connection parameters for Redis. If this value is false, you must create the ConfigMap manually.      | true or false                               | false             |
| redis.configmap.name_override | The name of the Redis ConfigMap.   | A valid name                                | nil               |
| redis.deploy                  | Specifies whether to deploy a Redis cluster. Set this option for lab environments only.  | true or false                               | false             |
| redis.image                   | Specifies the Docker image to use in the lab environment if <code>redis.deploy=true</code> .   | A Docker image                              | "redis:5-stretch" |
| redis.password                | The Redis password.  | A valid password                            | nil               |
| redis.password_required       | Specifies whether Genesys Authentication should read the Redis password from a Kubernetes secret.  | true or false                               | false             |
| redis.secret.create           | Specifies whether to create a Kubernetes secret with Redis   | true or false                               | false             |

| Parameter                           | Description  | Valid values  | Default   |
|-------------------------------------|--|---|-----------|
|                                     | password. If this value is false, you must create the secret manually.   |   |           |
| redis.secret.name_override          | The name of the Redis secret.  | A valid name  | nil       |
| redis.use_tls                       | Enable or disable a TLS connection to the Redis cluster.   | true or false                                       | false     |
| serviceAccount.create               | Specifies whether to create a service account.   | true or false                                       | false     |
| serviceAccount.name                 | The name of the service account to use.  | A service account name                              | ""        |
| serviceAccount.annotations          | Annotations to add to the service account. See the Kubernetes documentation for details.                         | A valid set of labels as "name: value"              | {}        |
| services.initContainers             | Optional init containers to add to Genesys Authentication deployments.   | Object  | {}        |
| services.location                   | Location of the deployment. For example, "/USW1".  | A valid location.                                   | "/"       |
| services.replicas                   | The number of Genesys Authentication pod replicas to deploy.   | Number  | 3         |
| services.db.init                    | Enable automatic updates for the database schema.  | true or false                                       | true      |
| services.db.poolCheckoutTimeout     | The database pool timeout.   | Number  | 3000      |
| services.db.poolSize                | The database pool size.  | Number  | 3         |
| services.auth.loglevel              | Specifies the log level for the Authentication Service.  | INFO, DEBUG, WARN                                   | DEBUG     |
| services.db.ssl                     | Enable or disable an SSL connection to PostgreSQL. See the PostgreSQL documentation for details about SSL modes. | disable, prefer, require, verify-ca, or verify-full | "disable" |
| services.auth.deploymentAnnotations | Annotations for Authentication Service deployment objects. See the Kubernetes documentation for                  | A valid set of annotations as "name: value"         | {}        |

| Parameter   | Description  | Valid values                     | Default   |
|---|--|----------------------------------|---|
|   | details.   |                                  |   |
| services.auth.env.GWS_AUTH_SECURITY_HTTP_SCHEME_HEADER_NAME | The name of the header with protocol. This value can be used when HTTPS is terminated by the load balancer.  | A valid header name              | "X-Forwarded-Proto"   |
| services.auth.env.GWS_AUTH_timeouts_request TimeoutMs       | The Authentication Service request timeout.  | A value in milliseconds          | 30000   |
| services.auth.env.JAVA_TOOL_OPTIONS                         | Specifies JVM arguments to set in the JAVA_TOOL_OPTIONS environment variable.  | Valid JVM arguments              | "-XX:+PrintFlagsFinal<br>-XX:+UseG1GC<br>-Dfile.encoding=UTF-8<br>-XX:+ExitOnOutOfMemoryError<br>-XX:MaxRAMPercentage=80.0" |
| services.auth.env.GWS_AUTH_logging_level_com_genesys_gws_v3 | Specifies the log level for the Authentication Service.  | INFO, DEBUG, WARN                | DEBUG   |
| services.auth.env.GWS_AUTH_http_headers_frame_options       | Specifies the value of the X-Frame-Options HTTP response header.   | SAMEORIGIN, DENY, DISABLE, ALLOW | ALLOW   |
| services.auth.jks.enabled                                   | Specifies whether Genesys Authentication uses Java KeyStore. See Add JKS support for details. This value must be set to true for Security Assertion Markup Language single sign-on (SAML SSO) functionality. | true or false                    | false   |
| services.auth.jks.keyAliases                                | The name of the key alias in the keystore used by the Authentication Service. This value comes from Add JKS support.   | A valid key alias                | nil   |
| services.auth.jks.keyPassword                               | The keystore password from Add JKS support.  | A valid keystore password        | nil   |
| services.auth.jks.keyStore                                  | The name of the Java keystore file from Add JKS support.   | A valid keystore name            | "jksStorage.jks"  |
| services.auth.jks.keyStorePassword                          | The keystore password from Add JKS support.  | A valid keystore password        | nil   |
| services.auth.jks.secret.create                             | Specifies whether to create a new secret with the keystore file content and keystore credentials.  | true or false                    | true  |

| Parameter                              | Description   | Valid values                                | Default  |
|--|---|---|--|
| services.auth.jks.keyStoreFileData     | The Base64 encoded key value from Add JKS support.  | A valid key                                 | nil  |
| services.auth.jks.secret.name          | A Kubernetes secret name with the keystore credentials and content.   | A valid secret name                         | nil  |
| services.auth.jks.sso.enabled          | Specifies whether to enable SAML SSO functionality.   | true or false                               | false  |
| services.auth.livenessProbe            | Specifies parameters for the livenessProbe. See the Kubernetes documentation for details.                       | Object                                      | <pre> livenessProbe:   httpGet:     path: /health     port: management   initialDelaySeconds: 120   periodSeconds: 10   successThreshold: 1   timeoutSeconds: 3   failureThreshold: 3 </pre> |
| services.auth.readinessProbe           | Specifies parameters for the readinessProbe. See the Kubernetes documentation for details.                      | Object                                      | <pre> readinessProbe:   httpGet:     path: /health     port: management   initialDelaySeconds: 30   timeoutSeconds: 3   periodSeconds: 10 </pre>   |
| services.auth.replicas                 | The number of Authentication Service pod replicas to deploy. This value overrides services.replicas.            | Number                                      | nil  |
| services.auth.resources                | The requests and limits for Authentication Service pod resources. See the Kubernetes documentation for details. | Object                                      | <pre> requests:   cpu: 500m   memory: 4Gi limits:   cpu: "4"   memory: 6Gi </pre>  |
| services.auth.serviceAnnotations       | Annotations for Authentication Service service objects. See the Kubernetes documentation for details.           | A valid set of annotations as "name: value" | {}   |
| services.auth_ui.deploymentAnnotations | Annotations for Authentication UI deployment objects. See the Kubernetes documentation for                      | A valid set of annotations as "name: value" | {}   |

| Parameter   | Description  | Valid values                                | Default   |
|---|--|---|---|
|   | details.   |   |   |
| services.auth_ui.env.GWS_NGINX_ENABLE_MAPPING                 | Use Consul to discover Auth Service  |   | "false"   |
| services.auth_ui.livenessProbe                                | Specifies parameters for the livenessProbe. See the Kubernetes documentation for details.                  | Object                                      | {}  |
| services.auth_ui.readinessProbe                               | Specifies parameters for the readinessProbe. See the Kubernetes documentation for details.                 | Object                                      | {}  |
| services.auth_ui.replicas                                     | The number of Authentication UI pod replicas to deploy. This value overrides services.replicas.            | Number                                      | nil   |
| services.auth_ui.resources                                    | The requests and limits for Authentication UI pod resources. See the Kubernetes documentation for details. | Object                                      | requests:<br>cpu: 100m<br>memory: 500Mi<br>limits:<br>cpu: 500m<br>memory: 1Gi  |
| services.auth_ui.serviceAnnotations                           | Annotations for Authentication UI service objects. See the Kubernetes documentation for details.           | A valid set of annotations as "name: value" | {}  |
| services.environment.logging_level                            | Specifies the log level for the Environment Service.   | INFO, DEBUG, WARN                           | INFO  |
| services.environment.deploymentAnnotations                    | Annotations for Environment Service deployment objects. See the Kubernetes documentation for details.      | A valid set of annotations as "name: value" | {}  |
| services.environment.env.JAVA_TOOL_OPTIONS                    | Specifies JVM arguments to set in the JAVA_TOOL_OPTIONS environment variable.                              | Valid JVM arguments                         | "-XX:+PrintFlagsFinal<br>-XX:+UseG1GC<br>-Dfile.encoding=UTF-8<br>-XX:+ExitOnOutOfMemoryError<br>-XX:MaxRAMPercentage=80.0" |
| services.environment.env.GWS_ENVIRONMENT_LOGGING_LEVEL_CONFIG | Specifies the log level for the Environment Service.   | INFO, DEBUG, WARN                           | INFO  |

| Parameter                               | Description   | Valid values                                | Default  |
|---|---|---|--|
| sys_gws_v3                              |   |   |  |
| services.environment.force_writable     | Ignore the Data Center topology in a single-region deployment.  | true or false                               | true   |
| services.environment.livenessProbe      | Specifies parameters for the livenessProbe. See the Kubernetes documentation for details.   | Object                                      | <pre>livenessProbe:   httpGet:     path: /health     port: management   initialDelaySeconds: 120   periodSeconds: 10   successThreshold: 1   timeoutSeconds: 3   failureThreshold: 3</pre> |
| services.environment.readinessProbe     | Specifies parameters for the readinessProbe. See the Kubernetes documentation for details.  | Object                                      | <pre>readinessProbe:   httpGet:     path: /health     port: management   initialDelaySeconds: 30   timeoutSeconds: 3   periodSeconds: 10</pre>   |
| services.environment.replicas           | The number of Environment Service pod replicas. This value overrides services.replicas.   | Number                                      | nil  |
| services.environment.resources          | The requests and limits for Environment Service pod resources. See the Kubernetes documentation for details.  | Object                                      | <pre>requests:   cpu: 500m   memory: 4Gi limits:   cpu: "4"   memory: 6Gi</pre>  |
| services.environment.serviceAnnotations | Annotations for Authentication Service service objects. See the Kubernetes documentation for details.   | A valid set of annotations as "name: value" | {}   |
| services.secret.admin_password          | Encrypted password of the operational user. The password should be encrypted with bcrypt hashing with any number of rounds. You can generate an encrypted password on the following site: <a href="https://www.javainuse.com">https://www.javainuse.com</a> | A valid password                            | nil  |

| Parameter  | Description  | Valid values   | Default                              |
|--|--|--|--------------------------------------|
|  | om/onlineBcrypt  |  |                                      |
| services.secret.admin_username                               | The username of an operational user.   | Any valid username. For example, opsAdmin, clientAdmin, ops.                     | nil                                  |
| services.secret.client_id                                    | The ID of an encrypted client secret.  | Any valid client ID. For example, external_api_client, nexus_client, authclient. | nil                                  |
| services.secret.client_secret                                | The encrypted client secret. The client secret should be encrypted with bcrypt hashing with any number of rounds. You can generate an encrypted client secret on the following site: <a href="https://www.javainuse.com/onlineBcrypt">https://www.javainuse.com/onlineBcrypt</a> | A valid client secret  | nil                                  |
| services.secret.create                                       | Specifies whether to create the Kubernetes secret with the credentials of the operational user and client ID.  | true or false  | true                                 |
| services.secret.name_override                                | The name of the secret.  | A valid name   | nil                                  |
| services.secrets.secretProviderClassNames.admin_user         | The name of the secretProviderClass with the operational user credentials.   | A valid class name   | "keyvault-gauth-admin-user"          |
| services.secrets.secretProviderClassNames.client_credentials | The name of the secretProviderClass with the client credentials.   | A valid class name   | "keyvault-gauth-client-credentials"  |
| services.secrets.secretProviderClassNames.consul_token       | The name of the secretProviderClass with the Consul token.   | A valid class name   | "keyvault-consul-consul-gauth-token" |
| services.secrets.secretProviderClassNames.jks_credentials    | The name of the secretProviderClass with the JKS credentials.  | A valid class name   | "keyvault-gauth-jks-credentials"     |
| services.secrets.secretProviderClassNames.jks_keyvault       | The name of the secretProviderClass with the JKS keystore.   | A valid class name   | "keyvault-gauth-jks-keyvault"        |
| services.secrets.secretProviderClassNames.pg_user            | The name of the secretProviderClass with PostgreSQL credentials.   | A valid class name   | "keyvault-gauth-pg-user"             |
| services.secrets.secretProviderClassNames.redis_password     | The name of the secretProviderClass with the Redis password.   | A valid class name   | "keyvault-gauth-redis-password"      |
| services.secrets.useSecret                                   | Specifies whether to   | true or false  | false                                |

| Parameter                 | Description  | Valid values  | Default |
|---------------------------|--|---|---------|
| etProviderClass           | read secrets from the secretProviderClass instead of Kubernetes secrets.   |   |         |
| topologySpreadConstraints | In Kubernetes, topology spread constraints are used to control how Pods are spread across the cluster among failure-domains such as regions, zones, nodes, and other user-defined topology domains. This helps to achieve high-availability as well as efficient resource utilization. | Valid topology spread constraints settings. See the Kubernetes documentation for details. | {}      |

## Configure Kubernetes

The sections below provide more information about configuring Kubernetes.

### ConfigMaps

Genesys Authentication includes separate ConfigMaps for PostgreSQL and Redis configuration.

#### PostgreSQL - configmap-pg.yaml

```

{{- if or .Values.postgres.configmap.create .Values.postgres.deploy }}
apiVersion: v1
kind: ConfigMap
metadata:
  name: {{ include "configmap.postgres" . }}
  namespace: {{ .Release.Namespace | quote }}
  labels:
    {{- include "gauth.labels" . | nindent 4 }}
  gauth: postgres
data:
  db: {{ required "Missing required parameter 'postgres.password'" .Values.postgres.db | quote }}
  host: {{ default ( include "name.postgres" . ) .Values.postgres.host | quote }}
  port: {{ default ( include "port.postgres.service" . ) .Values.postgres.port | quote }}
{{- end }}

```

#### Redis - configmap-redis.yaml

```

{{ if or .Values.redis.configmap.create .Values.redis.deploy }}
apiVersion: v1
kind: ConfigMap
metadata:
  name: {{ include "configmap.redis" . }}
  namespace: {{ .Release.Namespace | quote }}
  labels:

```

---

```
    {{- include "gauth.labels" . | nindent 4 }}
    gauth: redis
data:
  cluster_nodes: {{ default ( include "service.redis" . ) .Values.redis.cluster_nodes |
quote}}
  {{end}}
```

## Secrets

The following Genesys Authentication services artifacts are stored as Kubernetes secrets:

- Administrator user credentials for the Authentication API and Environment API services.
- OAuth 20 client IDs and client secrets for the Authentication API and Environment API services.
- PostgreSQL database credentials for the Environment API service.
- PostgreSQL database credentials for the Authentication API service.
- Java keystore password for Authentication API service.
- Credentials for access to a password-protected Redis (Access Key) for the Authentication API service.

## Configure security

To learn more about how security is configured for private edition, be sure to read the Permissions topic in the *Setting up Genesys Multicloud CX Private Edition* guide.

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.

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