3. Trigger the installation with this command if you have created a copy of `values.yaml` file (for example, `config.yaml`) and updated the parameters in the copy.

   If you are using Helm 2, run this command:

   ```
   helm install <chart repo name>/<chart name>:version
   --name <release name> -f
   <path to config.yaml file>
   ```

   Make sure that `config.yaml` file has the same parameters as those in the `values.yaml` file. For list of configuration parameters, refer to Process Controller Helm Chart Configuration Parameters (on page 98).

   For example:

   ```
   helm install stable/eoc-sim-20:latest --name eoc20.1
   -f /tmp/config.yaml
   ```

   If you are using Helm 3, run this command:

   ```
   helm install <release name> <chart repo name>/
   <chart name>:version -f
   <path to config.yaml file>
   ```

   For example:

   ```
   helm install eoc20.1 stable/eoc-sim-20:latest
   -f /tmp/config.yaml
   ```

   Note:
   The release name must be given an appropriate value, such as `eoc20.1`.

15.2.3 Service Inventory Management Configuration Parameters

The following table lists the Helm chart configuration parameters of Service Inventory Management (SIM):

Service Inventory Management Global Parameters

Parameter		Default Value	Description
General			
affinity		{}	Node affinity is conceptually similar to nodeSelector. It allows you to constrain which nodes your pod is eligible to be scheduled on, based on labels on the node.
enabled		TRUE	Defines whether or not the helm-chart is enabled.
fullnameOverride		No default value	If nameOverride is set to true, this field defines the new service name. If nameOverride is false or unset this field is ignored and default service name is used

Parameter		Default Value	Description
localTest		false	This variable is for test environments only and does not need to be updated in production.
nameOverride		No default value	Set to true to override the servicename with the name provided in fullnameOverride.
nodeSelector		{}	This parameter is the simplest recommended form of node selection constraint. nodeSelector is a field of PodSpec. It specifies a map of key-value pairs. For the pod to be eligible to run on a node, the node must have each of the indicated key-value pairs as labels (it can have additional labels as well). The most common usage is one key-value pair.
podDisruptionBudget		`podDisruptionBudget:` `  maxUnavailable: 1`	The number of concurrent disruptions or pod evictions that the application experiences, allowing for higher availability while permitting the cluster administrator to manage the clusters nodes.
podDisruptionBudget.minAvailable			The number of application pods that must be available after an eviction. The **minAvailable** can be an absolute number or a percentage. Specify only one of **maxUnavailable** and **minAvailable** in a single **PodDisruptionBudget**.
podDisruptionBudget.maxUnavailable		1	The number of application pods that are unavailable after an eviction. The **maxUnavailable** can be either an absolute number or a percentage. Specify only one of **maxUnavailable** and **minAvailable** in a single **PodDisruptionBudget**.
replicaCount		1	This parameter contains the number of containers to be started.
sim.contextPath		/eoc	Defines context path of REST requests.

Parameter		Default Value	Description
sim.functionControlServerUrl		https://<licenseServer>:<port>/eoc	Defines URL of server from where the license key of SIM is fetched and verified. For information about license key, refer to EOC Licensing and Value Packages.
sim.resourceByValue		true	Defines to control whether a resource should be expanded by default for backward compatibility. The following are possible values: • true - Resource is always expanded irrespective of expand query parameters. • false - Resource is only expanded if expand query parameter contains supporting resource (supportingResource), otherwise resource is not expanded.
terminationDelayPeriodSeconds		15	The amount of time the pod waits to send a SIGTERM to the application. The delay is executed within the application preStop hook. This waiting time allows the application to not fail during a graceful shutdown because it gives time to Kubernetes to redirect requests to other pods.
terminationGracePeriodSeconds		60	Kubernetes waits for a specified time called the termination grace period. By default, this is 30 seconds. This happens in parallel to the preStop hook and the SIGTERM signal. If the grace period is over, and the application is trying to perform a graceful shutdown, Kubernetes sends a SIGKILL signal forcing the pod to terminate immediately.
tolerations		[]	Tolerations are applied to pods and allow (but do not require) the pods to schedule onto nodes with matching taints. Taints and tolerations work together to ensure that pods are not scheduled onto inappropriate nodes. One or more

Parameter		Default Value	Description
			taints are applied to a node. It indicates that the node should not accept any pods that do not tolerate the taints.
updateStrategy.type		RollingUpdate	Defines how to create, upgrade, or downgrade different versions of the application. It has two possible values: • **RollingUpdate**: New pods are added gradually, and old pods are terminated gradually. • **Recreate**: All old pods are terminated before any new pods are added.
updateStrategy.rollingUpdate.maxSurge		1	The maximum number of pods the deployment is allowed to create at one time. Specify as a whole number (example, 5) or as a percentage of the total required number of pods (example, 10%, always rounded up to the next whole number).
updateStrategy.rollingUpdate.maxUnavailable		1	The maximum number of pods that are allowed to be unavailable during the rollout. Like **MaxSurge**, it can be defined as an absolute number or a percentage.
Docker Image			
image.name		eric-eoc-process-sim	This parameter contains the Docker image to be used for running the installation container.
image.tag		latest	This parameter denotes the tag or build version for the Docker image.
image.pullPolicy		Always	This parameter governs when to download the Docker images on the node. Possible values: • Always • IfNotPresent
image.pullSecret		scmcred	Defines repository credentials.
image.registryUrl		armdocker.rnd.ericsson.se	Defines docker image repository URL.
image.repoPath		/proj-eoc/	Defines docker image repository sub-path.

Parameter		Default Value	Description
image.serviceCheckImage.repoPath		/proj-avm/	Service check image's repository path.
image.serviceCheckImage.name		eric-service-connectivity-check	Service check image's name.
image.serviceCheckImage.tag		2.0.0	Service check image's tag name.
Authentication and Security			
sim.security.enableAuthentication		TRUE	Enables or disables authentication enforcement. If set to true, the REST request is not granted without valid authorization token.
sim.security.securityProviderAddress		http://eric-eoc-iws:8080/eoc	The end point for EOC server issuing the authentication tokens.
sim.security.authRefreshPublickeyThreshold		15	Defines the minimum time authentication service should wait before attempting to refresh the public keys. This is to guard against using an invalid token and enforcing the public keys to be refreshed more than necessary. The value must be set in minutes.
sim.security.authRefreshPublickeySchedule		0 0/30 * * * *	Cron expression defines how often public keys are refreshed from the security provider address. For example: 0 0/30 * * * * It means refresh public keys after every 30 minutes starting from zero (0) minutes of any hour and any day.
sim.security.allowedOrigins		*	Defines to control the Cross Origin Resource Sharing (CORS). Comma-separated values are allowed for more than one origins. The default value is asterisk (*) that allows all origins.
sim.security.allowedHeaders		*	Defines allowed headers for CORS. Comma-separated values are allowed for more than one headers.

Parameter		Default Value	Description
			The default value is asterisk (*) that allows all headers.
sim.security.allowedMethods		*	Defines allowed methods for CORS. Comma-separated values are allowed for more than one methods. The default value is asterisk (*) that allows all methods.
Service Registry Adapter			
sim.srBaseUrl		No default value	Defines the URL of SR-enabled EOC server. For example: `https://<eoc_sr>:<port>/eoc`
sim.srDataBuffer-Limit		16MB	Controls the data buffer limit for SR response. If SR returns the response and response size is greater than defined memory buffer size, an error is thrown to increase the memory buffer size. The memory buffer size is defined in MB.
sim.srRead-Timeout		PT20s	Service Registry request read timeout.
sim.loopbackHttp-Headers		Content-Range	Indcates the acceptable customized headers values from SR configuration.
Ingress Settings			
externalSecurity.enabled		TRUE	This parameter is deprecated. The value does not affect or influence application startup and functionality in any way.
externalSecurity.certificateData		externaleoc-certs	This parameter is deprecated. The value does not affect or influence application startup and functionality in any way.
global.ingress.enabled		true	Enabled external access of the application.
global.ingress.controllerType		nginx	Ingress controller type. Supported options are nginx and iccr.
global.ingress.ingressClass-Name			Ingress class name indicating which Ingress controller instance is consuming the Ingress resource.
global.ingress.annotations		{}	General annotations that are shared by all Ingress resources. Default

Parameter		Default Value	Description
			annotations for NGINX are already provided. It can be left empty.
global.ingress.hostname			The Fully Qualified Domain Name (FQDN).
global.ingress.tls.enabled		false	Enables TLS in Ingress.
global.ingress.existingSecret		extingress-certs	The secret name containing external certificates.
global.ingress.responseTimeout		"60"	Response timeout from the backend connection to ECM. Increase this timeout if ICCR is timing out its connection to ECM.
ingress.enabled		true	Set to false to disable Ingress addressing.
ingress.annotations		{}	General annotations for the SIM ingress resources. Default annotations for NGINX are already provided. It can be left empty.
ingress.*		tls-hosts: ingress-nginx	Allowed host names and external certificates, if required, at the Ingress level. The tls.secretName must not be changed.
ingress.hosts		host: ingress-nginx paths: /	This parameter represents an array of FQDN and path for Ingress routing. • The default paths are automatically computed by the product and only additional Ingress paths need to be specified in this section. • The default host FQDN (ingress-nginx) must match the Ingress controller LB service IP. Ingress-nginx is an example.
loadbalancer.enabled		FALSE	Sets the service addressing type to LoadBalancer. If both loadbalances and ingress are enabled, then ClusterIP address is used.
service.type		NodePort	If Ingress.enabled is set to false, this defines the addressing mode used by the service. Possible values are: • NodePort • LoadBalancer

Parameter		Default Value	Description
			• ClusterIP
service.port		8443	Defines the internal HTTP port exposed by the service.
Logging Configuration			
logging.logLevel		error	Defines the application's log level for diagnostic needs. The following log levels are available and are case-insensitive: • OFF This setting indicates that logging is off. • ERROR This setting allows for error-level logging. • WARN This setting denotes warning-level logging. • INFO This setting represents information-level logging. • DEBUG This setting indicates debug-level logging. • TRACE This setting allows for trace-level logging.
logging.enable-Collection		FALSE	Defines to enable or disable collections of application run logs.
logging.runLogs		/var/log/eoc/sim/RunLogs	Defines path to store application run logs on associated Kubernetes worked.
logging.outputs		**`file`**	Sets the value for the log output. The supported values are **`stdout`** and **`file`**. When **`stdout`** is selected, the logs are redirected to **`stdout`**. When **`file`** is selected, the logs are persisted to the Kubernetes node using `hostPaths`. **Note:** Select **`file`** if using the ADP logging solution.

Parameter		Default Value	Description
logging.persistInSyslog.enabled		FALSE	Allows enabling or disabling container log persistence to a remote syslog server.
logging.persistInSyslog.syslogServer		syslog	Contains the hostname of the remote syslog server where the logs are to be persisted.
logging.persistInSyslog.syslogPort		514	Specifies the port number of the remote syslog server.
logging.persistInSyslog.syslogFormat		RFC3164	Indicates the format of the syslog message.
logging.persistInSyslog.syslogFacility		user-level	Indicates the syslog facility.
logging.logcfgMounted		false	Defines which logging configuration should be used for log format. The following are possible options: • true - Uses custom logback.xml configuration. • false - Uses default ADP JSON configuration.
logging.bannerMode		off	Defines whether to print default banner on log output. The following are possible options: • `CONSOLE` - Print the banner to System.out. • `LOG` - Print the banner to the log file. • `OFF` - Disable printing of the banner.
External Repository URL for href The version in example URLs is provided based on the earlier product release for href parameters. When configuring the following parameters, make sure the version in URL is aligned with the current product release.			
sim.serviceSpecificationBaseUrl		No default value	Defines URL of Commercial Browsing microservice for service specification. For example for Commercial Browsing: http://<pob_host>:<port>/pob/discovery/v1/serviceSpecification/
sim.placeBaseUrl		No default value	Defines URL of Integrated Workstation (IWS) or Customer Profile Repository (CPR) server for location.

Parameter		Default Value	Description
			For example for IWS: http://<iws_host>:<port>/eoc/uws/v1/location/
sim.relatedParty-BaseUrl		No default value	Defines URL of IWS or CPR server for customer. Example: For IWS: http://<iws_host>:<port>/eoc/uws/v2/customer/ For CPR: http://<cpr_host>:<port>/customerManagement/v1/party/ For external system customer resource URI: http://<host>:<port>/<relativePath>
Resource Configuration			
resourceLimits.xmsPercent		50	Sets initial heap size as a percentage of total memory.
resourceLimits.xmxPercent		50	Sets maximum heap size as a percentage of total memory.
resources.limits.cpu		1000m	Maximum use of CPU resource allowed by the API.
resources.limits.memory		2000Mi	Maximum use of memory resource allowed by the API.
resources.requests.cpu		800m	Minimum requested CPU resource by the API.
resources.requests.memory		1600Mi	Maximum requested memory resource by the API.

Note:
For authorization profile, a default `AuthorizationProfile.json` file has been added in the Helm-chart folder of this microservice. If required, you can modify the default file to add or remove privileges. After deployment, the file is automatically mounted to the `/opt/authorization/` folder inside the container. For information about Service Inventory Management privileges, refer to Service Inventory Management Privileges (on page 252).