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 Knowledge Center Deployment Guide

Knowledge Center Current

3/20/2023

Table of Contents

Genesys Knowledge Center Deployment Guide **4**
What is Genesys Knowledge Center? **6**
- Knowledge Center Components 10
- High-Level Architecture 14
- Terminology 17

Planning Your Deployment **18**
- Prerequisites 19
- Sizing Information 22
- Hardware Recommendations 23
- Software Configuration 26
- Multi-Tenancy 29

Installation and Deployment **30**
- Before you Begin 32
- Automatic Provisioning during installation 44
- Configuring the Knowledge Center Cluster Application 46
- Installing the Knowledge Center Server 51
- Installing the Knowledge Center CMS 69
  - Using CMS with Microsoft SQL Server 85
  - Using CMS with Oracle 87
  - Configuring CMS to Work with PostgreSQL 89
  - Configure Resource Access Point for Knowledge Center CMS Load-Balancer 90
- Installing the Workspace Desktop Edition Plugin 97

Post Installation and Deployment **107**
- Access Permissions 108
- Configure Reporting 114
  - Reporting REST API 125
- Configuration Options 131
  - Knowledge Center Cluster Configuration Options 132
  - Logging Configuration Options 143
- Configuring Resource Access Points 151
- Load-Balancing Configuration 152
- Security 155
  - Transport Layer Security (TLS) with Genesys Servers 156
  - Authentication 165
  - Cross Origin Resource Sharing (CORS) Filter 166

Translation service 170

IP Geolocation 174

UTF8 177

Supported Languages 178

Screening Rules and Standard Responses 180

Knowledge Center in Production **183**

Monitoring Knowledge Center 184

Viewing Metrics with JMX 186

Sample UI 191

Importing Data into the Knowledge Center Server 198

Upgrade Genesys Knowledge Center Server **208**

Genesys Knowledge Center Deployment Guide

Tip

The latest version of our documentation (titled “**Current**”) relates to release **9.0.x**.

What is Genesys Knowledge Center

Provides an overview of the Knowledge Center functionality and architecture:

What is Genesys Knowledge Center

Genesys Knowledge Center Components

High-level architecture

Terminology

Planning your Deployment

Describes major considerations while planning a deployment of your Knowledge Center cluster:

Prerequisites

Sizing Information

Hardware Recommendations

Software Configuration

Installation and Deployment

Step-by-step guide of Knowledge Center service deployment (see main page for full list):

Before You Begin

Configuring the Knowledge Center Cluster Application

Installing the Server

Installing the CMS

Post Installation and Deployment

Describes tuning options and additional functionalities to tune the Knowledge Center to your business needs:

Access Permissions

Configuration Options

Load Balancing Configuration

Security

Translation Service

Knowledge Center in Production

Tips & tricks on operating your Knowledge Center cluster in production:

Monitoring Knowledge Center

Sample UI

Importing Data into the Knowledge Center Server

What is Genesys Knowledge Center?

Genesys Knowledge Center allows you to make the best use of your enterprise knowledge by capturing, storing, and distributing it wherever it is needed. Let's take a closer look at the various capabilities of Knowledge Center and some corresponding use cases.

- Knowledge-assisted Channels
- Proactive Knowledge
- Knowledge Web Search

Knowledge-assisted Channels

With Knowledge Center, you can:

- Knowledge-enable channels by providing the right answers to customers in-channel to deflect interactions, leading to cost reduction and better customer service.
  - Knowledge-assisted Email form: Find applicable support articles based on email ticket submission and web form.
- Empower agents with context-appropriate knowledge in a unified desktop for faster resolution when agent-assisted service is needed.

Use Case: Knowledge-assisted Email

Basic Flow	Outcome 1	Outcome 2
1. Tracy clicks on an email web form to find out if GDemoTelecom has service in an area that she is moving to. 2. Tracy types *“Do you have service in Belmont, CA?”* in the subject line. 3. Tracy clicks out of the subject line to type the content in the message body. 4. An FAQ search is invoked.	Tracy is provided with the coverage map for Belmont, CA as a suggested answer. She provides feedback and closes the window.	Tracy ignores the FAQ search and types content in the message body since she has more questions. An email request is logged and placed in queue.

Note: This use case requires customization of Web Form with Knowledge Search API.

Use Case: Knowledge-assisted Social or SMS

Basic Flow	Outcome 1	Outcome 2
1. `@tibwizz` sends a Tweet (or SMS) *"looks like I will miss my connecting flight from LAX to SFO"* to `@blueskyairlines`. 2. Interaction is created and queued. 3. Orchestration script invokes Knowledge API to find answers on what to do when you miss connections.	Answer found. `@Blueskyairlines` auto-responds to `@tibwizz` *"Click here to schedule a call with our travel consultant to rebook"*.	Answer not found. Queue the message for agent.

Note: This use case requires customization of Orchestration logic.

Proactive Knowledge

- Combine Knowledge with Proactive Engagement to proactively provide suggested articles at the right moment.
- Provide knowledge-based assistance for agents if the customer asks for a human-assisted channel escalation.
- Reduce effort, reduce friction and channel escalation.

Use Case: Proactive Knowledge

Basic Flow	Outcome 1	Outcome 2	Outcome 3
1. Jurgen browses www.Gbank.com to research *College Savings Plan*. 2. He navigates to the page. 3. Web Engagement Rules can trigger knowledge article lookup to provide *knowledge nudges*.	Suggested Pages/Info Within the suggested articles section of the page, a few links are populated: • Starting a college savings plan • Transferring an existing college savings plan • College Savings Plan Calculator	Jurgen ignores the suggestions. No action taken.	Jurgen looks at suggestions, but still continues to browse. Proactively offer customers the ability to escalate to assisted service.

Note: This use case requires customization of Rules and Web Page logic.

Knowledge Web Search

Enable dynamic FAQ and channel deflection using natural language search and present knowledge articles to customers via the web.

Use Case: Contact Center Escalation

The following list of outcomes from examples on this page demonstrates how Knowledge Center allows customers to serve themselves if they want to, while providing them with easy ways to contact an agent if they cannot find what they are looking for:

- Outcome 3 in the Web Search and Proactive Knowledge examples
- Outcome 2 in the Knowledge-assisted Email example
- Outcome 3 in the Knowledge Assisted Chat example

Use Case: Web Search

Basic Flow	Outcome 1	Outcome 2	Outcome 3
1. John recently booked an Alaskan vacation for his family on Blue Sky Airlines. 2. John would like to know if he can gate check his baby's stroller and car seat. 3. John goes on www.blueskyairlines.com and in the search box types *"can I gate check my infant car seat and stroller?"*	One Question. One Answer. Knowledge Center finds the right answer in the FAQs and provides the answer to John.	Top 3 Answers. Knowledge Center also provides two other articles that contain information about gate checking guidelines.	John is not satisfied with the answers and says answer was not helpful. John is offered a choice of chat, email, or callback based on agent availability or hours of operation. Agent receiving John's request is presented with all the relevant information about John, his reservations, and the answers viewed by John so that he/she can quickly help John.

Note: This use case requires customization of Rules and web page logic.

Use Case: Fast access to content with auto-complete

Basic Flow	Outcome 1	Outcome 2
1. John goes online to the Blue Sky Airlines website. 2. He navigates the website and finds the page for *Traveling with an infant.* 3. After reviewing the page, John is not clear if he can gate check his stroller. 4. John notices a Search Bar at the top of the page and types *"can I gate check"* 5. Genesys Knowledge Center Auto-complete functionality provides suggestions like *"can I gate check my infant car seat?"*.	John finds the answers to the suggested questions helpful. He provides feedback and closes the window.	John has more questions. Create a chat interaction and place John in queue.

Use Case: Browsing though document categories

Basic Flow	Outcome
1. As John reads the knowledge article about gate checking his infant's car seat, he also notices a category link called *"Traveling with Infants"*. 2. John clicks on the link and now has access to four other articles: • Travel tips for parents traveling with infants • Baggage allowance for infants • Online check-in for parents traveling with kids	John now has all the information he needs. He answers *"Yes"* to the feedback question from the original article, which now ranks the article higher for subsequent searches. **Note:** Feedback is not available for browsed articles, since all feedback is directly related to a search query.

Knowledge Center Components

Before you start working with Genesys Knowledge Center, you might find it helpful to learn about its components:

- **Knowledge Center Server**—Combines indexing and natural language–based search capabilities to provide effective knowledge article retrieval from one or more knowledge bases.
- **Knowledge Center CMS**—Provides customers who do not have an existing Content Management System (CMS) with the ability to create and update their knowledge bases and push them to the Genesys Knowledge Center Server for indexing and search. This component also allows customers to import and edit knowledge articles from a file.
- **Knowledge Center Plugin for Workspace Desktop Edition**—Provides agents with access to knowledge events (searches, article views and feedback) related to the current customer and also allows them to search the knowledge base right from their desktop.

Knowledge Center Server

The Genesys Knowledge Center Server combines indexing and search capabilities that allow for effective knowledge retrieval over one or more knowledge bases.

Also, Genesys Knowledge Center Server provides the ability to use Named Entity Dictionaries to build a domain-specific thesaurus which, in turn, can be used as a Synonyms dictionary to expand the set of keywords when searching for documents. This provides greater efficiency of the search query formulated by words that are close in meaning to the subject of the search.

The Knowledge Center Server requires Elasticsearch 6.2 cluster to be set up and running.

Elasticsearch is a search server based on Lucene. It provides a distributed, multi-tenant–capable full-text search engine with a RESTful web interface and schema-free JSON documents. ElasticSearch is distributed, which means that indices can be divided into shards and each shard can have zero or more replicas. Each node hosts one or more shards, and acts as a coordinator to delegate operations to the correct shards.

Other Features of the Knowledge Center Server

- Knowledge Center Server exposes a REST API that can be used for both client and management functions.
- Knowledge Center Server is a cluster application, meaning that several nodes or servers can be grouped within a single cluster.
- Knowledge Center Server requires two application objects in Genesys Administrator:
    - One to describe the server itself (type = *Genesys Knowledge Center Server*)
    - Another for storing high-level options and knowledge base configurations, and for integrating the Knowledge Center server with other applications (type = *Application Cluster*)

- You can use third-party load-balancers above the cluster to organize your servers into a single pool, thereby providing a single point of entry for your users.
- Knowledge Center Server uses Genesys Roles to restrict access, and to authorize and authenticate users.

Knowledge Center CMS

The Knowledge Center Content Management System (CMS) serves several purposes:

- Creates, activates, and deactivates knowledge bases
- Creates, updates, and deletes questions and answers in a knowledge base
- Assigns categories to this content
- Imports historical information from the Knowledge Center Server

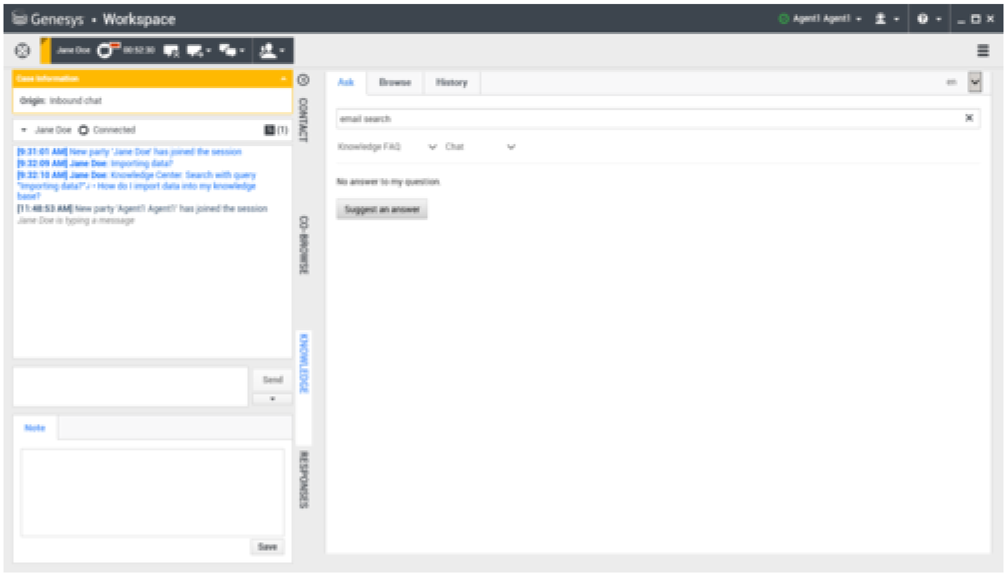
The CMS primarily interacts with the Knowledge Center Server when creating or updating index data.

Plugin for WDE

Your agents can use the Knowledge Center Plugin for Workspace Desktop Edition (WDE) to access Knowledge Center data from from their WDE worksession.

For example, if a customer escalates a question using a chat widget and the resulting interaction is routed to an agent, Knowledge Center can pre-populate a search based on the data that is attached to the chat interaction. When the interaction reaches the agent, he or she will see the customer's search history, so the customers needs can be met more quickly. In cases where the customer doesn't authorize automatic search-based access, the agent will also be able to search the customer's session history if the customer allows this during their chat.

The following images show a FAQ search and customer history, respectively.

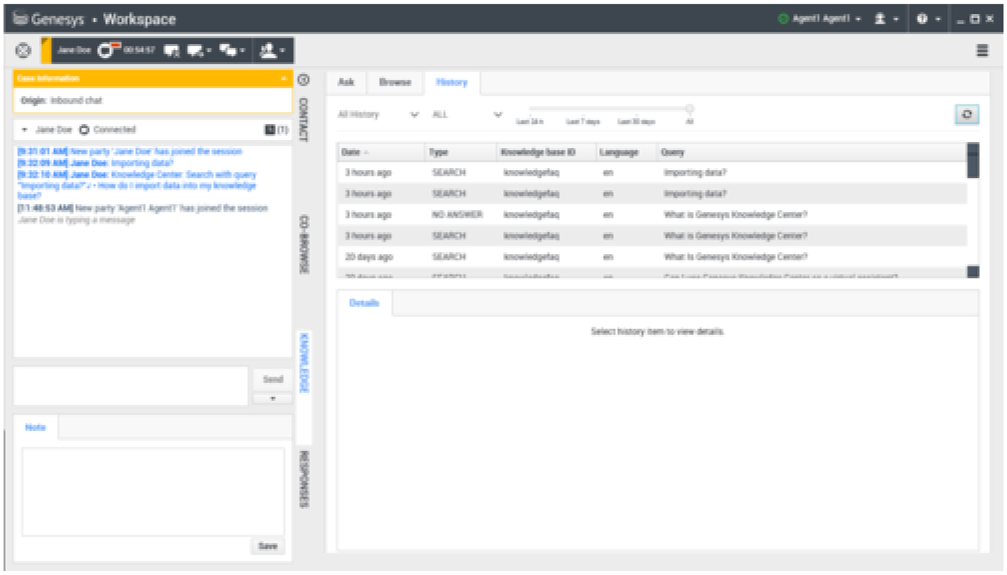


[9:31:01 AM] New party 'Jane Doe' has joined the session
[9:32:09 AM] Jane Doe: Importing data?
[9:32:10 AM] Jane Doe: Knowledge Center: Search with query "importing data?" ↓ • How do I import data into my knowledge base?
[11:48:53 AM] New party 'Agent1 Agent1' has joined the session
Jane Doe is typing a message

email search

No answer to my question.

FAQ Search



[9:31:01 AM] New party 'Jane Doe' has joined the session
[9:32:09 AM] Jane Doe: Importing data?
[9:32:10 AM] Jane Doe: Knowledge Center: Search with query "importing data?" ↓ • How do I import data into my knowledge base?
[11:48:53 AM] New party 'Agent1 Agent1' has joined the session
Jane Doe is typing a message

Date	Type	Knowledge base ID	Language	Query
3 hours ago	SEARCH	knowledgefaq	en	Importing data?
3 hours ago	SEARCH	knowledgefaq	en	Importing data?
3 hours ago	NO ANSWER	knowledgefaq	en	What is Genesys Knowledge Center?
3 hours ago	SEARCH	knowledgefaq	en	What is Genesys Knowledge Center?
20 days ago	SEARCH	knowledgefaq	en	What is Genesys Knowledge Center?

Select history item to view details.

Customer History

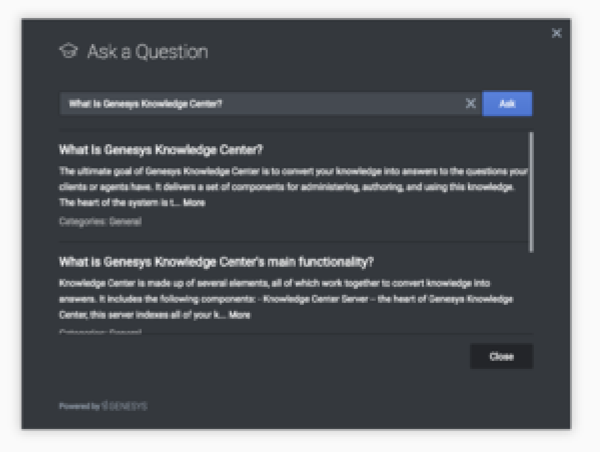
Integration with Genesys Solutions

Widgets

Knowledge Center functionality is pre-integrated into Genesys Widgets, as the part of Widgets framework. The following Knowledge Center related components are included:

- KnowledgeCenterService widget - provides API and events exposed by Knowledge Center within the Widgets framework.

- Search widget - allows a customer to address his question to the corporate knowledge. The UI appears within the page and customers can ask a question (search), review provided results, and provide feedback on whether the results addressed the problem.
- ChatDeflection widget - allows a customer to address a question while waiting for a customer service agent to join a live chat. ChatDeflection does not introduce a new UI, it simply adds additional functionality to the WebChat widget. ChatDeflection widget uses the KnowledgeCenterService widget to match a customer's question to the corporate knowledge base and comes up with the most relevant knowledge for that question. ChatDeflection stops any interactions with the customer as soon as the customer service agent joins the live chat session. The customer service agent who joins the session after the deflection attempt, now has some context of the customer issue ready for review, as well as the information on the suggested knowledge and the customer's interactions with it.



What is Genesys Knowledge Center?

What is Genesys Knowledge Center?

The ultimate goal of Genesys Knowledge Center is to convert your knowledge into answers to the questions your clients or agents have. It delivers a set of components for administering, authoring, and using this knowledge. The heart of the system is t... More

Categories: General

What is Genesys Knowledge Center's main functionality?

Knowledge Center is made up of several elements, all of which work together to convert knowledge into answers. It includes the following components: - Knowledge Center Server – the heart of Genesys Knowledge Center, this server indexes all of your k... More

Categories: General

Pulse

Important

Reporting functionality is not available in the 9.0 release of the product. Please contact customer care for further guidance.

Genesys Web Engagement

While it isn't exactly a component, we thought this would be a good place to mention that you can integrate Knowledge Center with Genesys Web Engagement. GWE helps you monitor, identify, and proactively engage web visitors in conversations that match your business objectives. And Knowledge Center can be used with GWE to provide proactive engagement capabilities.

For more information, see how to integrate Knowledge Center with Genesys Web Engagement.

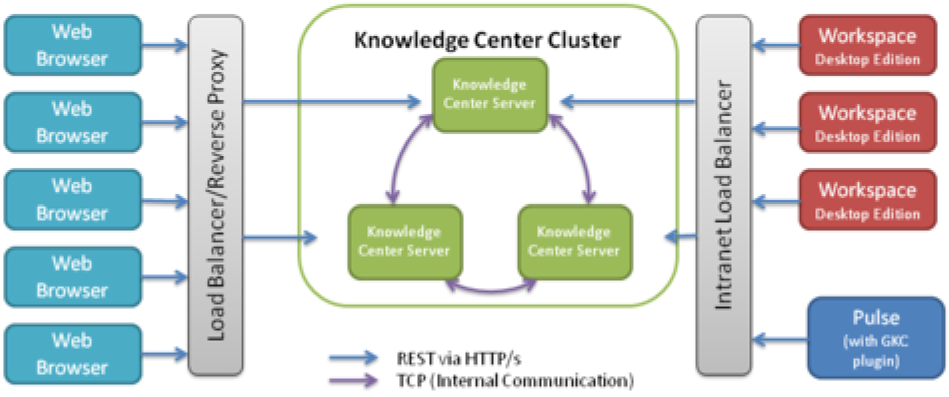
High-Level Architecture

Genesys Knowledge Center consist of several components:

- Genesys Knowledge Center Server
- Genesys Knowledge Center CMS
- Genesys Knowledge Center Plugin for Workspace Desktop Edition

Genesys Knowledge Center Server

Knowledge Center Server is the heart of the Genesys Knowledge Center solution. For purposes of load balancing and reliability, you can logically group your Knowledge Center Servers within a Knowledge Center Cluster. Each server in the cluster owns the same data and can be used to execute any desired queries against this data. These servers must be accessed by means of a properly configured load balancer that distributes the load among the server instances.



Knowledge Center High Level Architecture

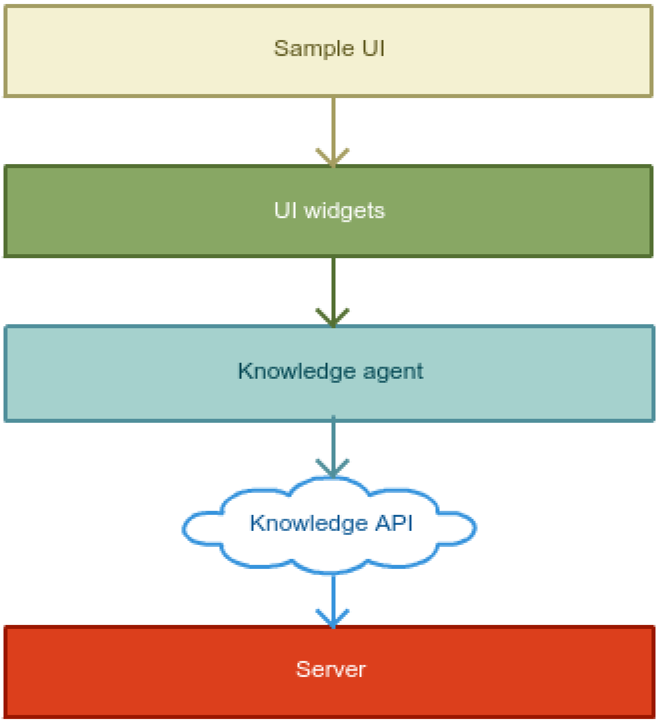
Genesys Knowledge Center Server provides several levels of integration, allowing you to access your knowledge wherever you need it—and in the way that best suits your needs. This includes a set of RESTful APIs that enables you to index data, query the server to find answers, and check usage information.

The Sample UI

The Sample UI is a JavaScript/HTML sample application that you can use as an example of how to integrate Knowledge Center into your corporate site. It runs in the visitors' browser and allows them to find answers to their questions in your corporate knowledge base.

The Sample UI offers all of the available levels of integration, allowing you to chose the one that best suits a particular need, whether it is:

- **The Knowledge API**—The RESTful web service that provides access to the Knowledge Center Server functionality
- **The Knowledge Agent**—A low-level JavaScript mapper that covers the Knowledge API and encapsulates Knowledge session management
- **The UI Widgets**—Basic and atomic UI elements covering different aspects of working with knowledge
- **The Sample UI**—An integrated sample application that implements fully functional access to the knowledge stored in Knowledge Center Server



Knowledge Center Sample UI

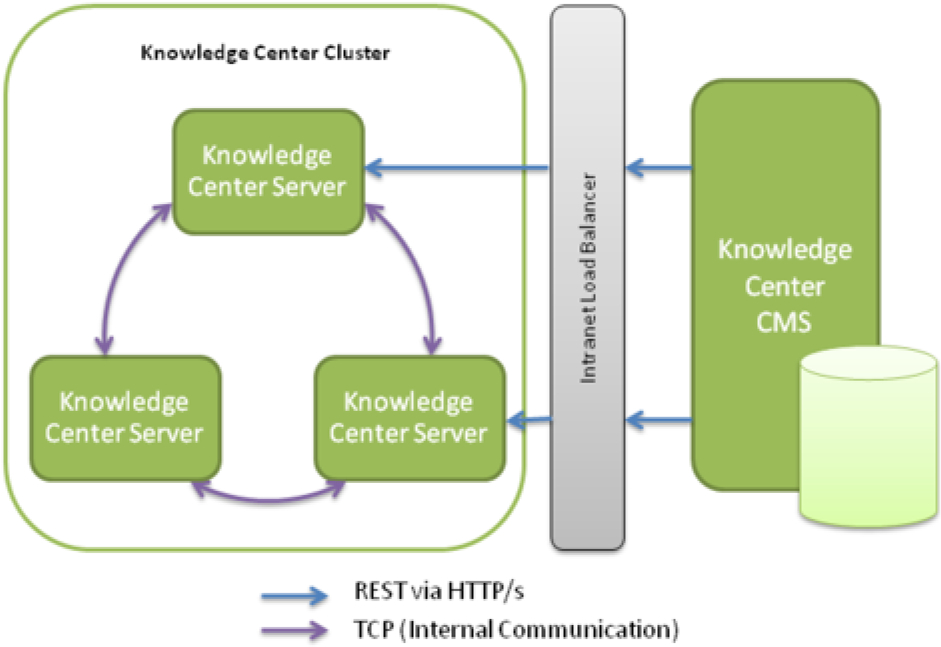
Genesys Knowledge Center CMS

The Genesys Knowledge Center CMS is an optional component that can be used to store company knowledge and allow role-based access for authoring and improvement. The CMS is seamlessly integrated with Knowledge Center Server using its public REST APIs and allows you to:

- Index authored information into the Knowledge Center Server to expose it for use by agent and customers

- Retrieve usage information from the Knowledge Center Server and use it to better understand customer needs and to improve your knowledge base

For more information, consult the Knowledge Center User's Guide.



Knowledge Center CMS Architecture

Genesys Knowledge Center Plugin for Workspace Desktop Edition

Genesys Knowledge Center comes with a plugin that allows it to be easily integrated into the Genesys environment:

- **The Plugin for Workspace Desktop Edition**—enriching standard agent workplace with the knowledge functionality and history of customer interaction with the knowledge

You can also integrate Knowledge Center with Genesys Web Engagement. This allows you to take actions based on the way your knowledge is used by the customer and agents.

Terminology

Term	Meaning
cluster	Set of the Knowledge Center Servers that are working together using the same knowledge.
knowledge base	Collection of your knowledge sharing same taxonomy (set of categories) and covering same domain/sub-domain.
node	One instance of the Genesys Knowledge Center Server.
replica	backup shard of data used to guarantee data redundancy.
shard	The way to divide your knowledge base on chunks that can be distributed between different servers.

Planning Your Deployment

This chapter helps you to plan the Knowledge Center deployment within your environment. It covers following topics:

- Terminology
- Prerequisites
- Multi-Tenancy
- Planning Your Cluster
- Hardware Recommendations
- Software Configuration

> **Important**
>
> The exact deployment architecture and solution size will vary depending on your hardware and your ability to fine-tune the deployed system to get the best performance on your equipment and with your particular user load. However, the estimates in the following topics may give you some basic ideas on how to size your deployment.

Prerequisites

OS Requirements

Knowledge Center Server

- OS Red Hat Enterprise Linux 7 (Intel EM64T)
- OS Windows Server 2012
- OS Windows Server 2016

Knowledge CMS

- OS Red Hat Enterprise Linux 7 (Intel EM64T)
- OS Windows Server 2012 (Intel EM64T)
- OS Windows Server 2016

Genesys Knowledge Center Plugin for Workspace Desktop Edition

- OS Windows Vista (Intel 32-bit)
- OS Windows 7 (Intel 32-bit, Intel EM64T)
- OS Windows Server 2012 (Intel EM64T)
- OS Windows Server 2016
- .Net framework 4.6.2 or higher

Genesys Knowledge Center Plugin for Pulse

- OS Red Hat Enterprise Linux 5 (Intel EM64T)
- OS Windows Server 2012 (Intel EM64T)
- OS Windows Server 2016

Web Browsers

- Google Chrome 34+
- Mozilla Firefox 54+

- Microsoft Internet Explorer 9, 10, 11
- Microsoft Edge
- Apple Safari 10+

Java Requirements

- OpenJDK

  Minimum version - Version 8

  Maximum version - Version 9

For OpenJDK 9 to work as expected, you must make the following changes in either Windows or Linux.

Windows

1. Open the `\server\launcher.ini` file.
2. Uncomment the following lines:

```
;--add-modules=java.xml.bind
 ;--add-modules=java.se.ee
 ;--add-modules=jdk.management
```

3. Open the `\cms\launcher.ini` file.
4. Uncomment the following lines:

```
;--add-modules=java.xml.bind
 ;--add-modules=java.se.ee
 ;--add-modules=jdk.management
```

Linux

1. Open the `\server\setenv.sh` file.
2. Uncomment the following lines:

```
JAVA_9_OPTS="--add-modules=java.xml.bind --add-modules=java.se.ee --add-
 modules=jdk.management"
```

3. Open the `\cms\setenv.sh` file.
4. Uncomment the following lines:

```
JAVA_9_OPTS="--add-modules=java.xml.bind --add-modules=java.se.ee --add-
 modules=jdk.management"
```

Elasticsearch Requirements

- Elasticsearch 6.2.3

Genesys Environment

- Genesys Framework 8.1–8.5
- Configuration Server (8.1.300.21 / 8.5.101.41)
- Genesys Administrator 8.5.210.10 or higher
- Workspace Desktop Edition 8.5.120.05 or higher
- Pulse 8.5.108.02 or higher

Sizing Information

> ### Important
> **Disclaimer:** This page contains information related to the 8.5.x release of the product. It will be updated soon to reflect the 9.0 release.

Before deploying the Genesys Knowledge Center solution to your production site, you must estimate the size of the solution that can handle the expected user load. Genesys recommends that you download the Sizing Calculator, an Excel workbook that you can use to help calculate the number of nodes required for your production deployment. **Note:** clicking the link will automatically start the download.

The process of estimation starts from input values, usually given in the terms of business operations (for example, number of knowledge bases, or number of sessions and questions per session). Using some math, and having in mind the workflow that is applied to the input traffic, you can then produce the expected load values in terms of requests per second. Applying these values to the experimentally produced measurements, you can estimate the size of the solution required to be deployed.

> ### Important
> The minimum number of the Knowledge Center Server nodes in Knowledge Center Cluster is 3. When doing the lab testing you can use 1 node configuration.
> A cluster with 2 nodes cannot be used in the lab or in a production deployment. Running a 2 node cluster might lead to data loss in a network outage between these nodes.

Hardware Recommendations

Important

Disclaimer: This page contains information related to the 8.5.x release of the product. It will be updated soon to reflect the 9.0 release.

Hardware you can use to deploy the Knowledge Center varies from the particular needs & conditions that you will use it in. Below is the set of recommendations and considerations that will help you to achieve a better understanding how the different components our your environment influence the Knowledge Center performance.

CPUs

Overall application is light on CPU when in comes to finding relevant knowledge to your search requests. This leads to lower dependency on CPU performance. Any modern processor with multiple cores will do the job. These days, two key parameters of the CPU are: speed and number of cores. In this case, you should choose a CPU with more cores than a slightly faster one. This allows the Knowledge Center to service concurrent requests more efficiently.

A modern CPU with 4 or 8 core CPUs is recommended.

Memory

This solution is designed to process tons of data and select only relevant data for each one of your queries. In this case, memory is one of the resources that is intensively used. When planning your host memory you need to ensure that RAM size will be enough to host all your running applications and some extra is left for the system to host the OS filesystem cache.

The absolute minimum of 8Gb RAM must not be crossed. It is recommended to use hosts with 16 Gb. With optimization and running multiple applications on the host, you may end up with 32 or 64 Gb hosts.

Important

In most cases it is recommended to plan your deployment with 50% of your memory allocated to the running application. The remaining 50% is used for the OS filesystem cache allowing for different software (including Genesys Knowledge Center) to work faster and minimizing disk operations.

Discs or Storage

Disks play a key role in the system performance as well. Being data-intensive and doing a lot of the read-write operations, Genesys Knowledge Center Server is highly dependent on the speed of the disk operations.

There are several common ways to improve performance of read-write intensive applications:

- Use the OS cache to minimize the number of read operations required (see recommendation above in the **Memory** section).
- Using faster disks; high-performance (15K) spinning disks are a good choice. Usage of SSD disks will burst the performance of your cluster even mlore.
- Using RAID 0 to improve the speed over any type of disk you are using (no need to go further with redundancy features of RAID, as data replication is the integral part of the solution itself).

The amount of disk space consumed by the Genesys Knowledge Center solution can be estimated using the Sizing Calculator.

> ### Important
> Avoid any types of the disk technologies that increase latency and throughput. An example of this solution would be the NAS.

Network

We recommend keeping all your nodes within a cluster in the same network, avoiding cross data center communication. Replication of the data between datacenter is a separate concern and deserves a separate solution.

The key parameters of the network you need to watch for are:

- latency: the Knowledge Center Cluster is the self-managing solution that distributes the load between all available nodes. By sending a request to one node of the cluster, your are employing all nodes (to the extent that it makes sense) to execute your request. Keeping the latency low will guarantee you the maximum speed of distributed execution.
- reliability: minimizing the number of disconnects in the system will guarantee that the Knowledge Center Cluster is fully concentrated on serving the request of your internal and external customers instead of doing house-keeping duties such as replacing dead nodes and relocating the data.
- bandwidth: being quite light in network communication during ordinary work (executing the searches), this solution can be demanding on the network bandwidth while indexing huge amounts of data or recovering from node failure.

Summary

Genesys Knowledge Center Server does not require any enormous hardware configuration to run on. A medium-sized box is the best option to run this application.

Another general recommendation is to keep your hardware set up as solid as possible:

- adding a high performance, huge RAM, SSD RAID 0 enabled server to the cluster of outdated servers will not provide any noticeable or stable performance improvement overall of the solution. The speed of newly-added servers are completely compromised by the old hardware that executes parts of the same requests making the overall response and performance to be almost unchanged.
- putting one server into a higher latency network segment can improve some access parameters in that particular segment but will result in overall system performance degradation.

The best shot for the deployment of the cluster is using similar hardware for all servers and putting them into similar network conditions. This will ensure the most balanced use of your resources.

> **Important**
>
> Please ensure that the disk's volume that you are using for search indexes has at least of 15% of the total volume of the disk in free space. We are recommending not to use huge volumes as it requires you to have a lot of free space. Genesys Knowledge Center Server is constantly monitoring the remaining free space on the disk and if it finds that there is less then 10% of your disk volume left, it might make a decision to relocate indexes on a different host.

Software Configuration

> Important
>
> **Disclaimer:** This page contains information related to the 8.5.x release of the product. It will be updated soon to reflect the 9.0 release.

JVM Settings

We recommended you run the most recent version of Java Virtual Machine. The minimum version supported is Java 1.8 64 bit. The recommended (default) memory settings for the Knowledge Center Server java process (Xms/Xms) is 4 Gb. Extending it to 16 Gb might be a good idea when using large amounts of data. Adding and extra 4 Gb of heap for the process recommended on the nodes that are used to execute history archiving.

> Important
>
> It is strongly advised to not set the Xmx larger than 30Gb.

Co-Locating On Same Host

We do not recommended co-locating two or more nodes of the Genesys Knowledge Center Server on the same host. Loosing the host due to hardware or network failure will result in two or more nodes being lost by the cluster. This will lead to massive network operations, potential loss of data (in the case where the number of replications is configured to 1) and even a complete outage of the cluster (for example, for clusters with 3 nodes).

Genesys Knowledge Center Server can be co-located on the same host with other Genesys or 3rd party solutions.

When co-locating please ensure that:

- The host is equipped with enough resources, especially RAM
- the solutions you are co-locating with are not causing any CPU spike when any other application on the host is blocked

Do not co-locate with other disks' read-write intensive solutions as it could easily overrun capabilities of your disk system.

Important

In most cases it is recommended to plan your deployment with 50% of your memory allocated to the running application. The remaining 50% is used for the OS filesystem cache allowing for different software (including Genesys Knowledge Center) to work faster and minimizing disk operations.

Genesys Knowledge Center Server/Cluster Configuration

Genesys Knowledge Center Server/Cluster is configured by default to enable smooth and high performance operations. Detailed information on every option exposed, valid values, and considerations behind the solutions are available on the Configurations Options page of the product documentation.

The section below provides additional information and recommendations.

Cluster Setup

The starting point of any cluster configuration is to create one application of the Application Cluster type and as many as needed applications of the Genesys Knowledge Center Server type in Genesys Administrator.

While doing this please ensure that you are creating the application only for the actual nodes of the Server that you will use. Having a spare application added to the cluster will mislead the cluster members while calculating the required number of nodes to be online and to enable cluster functionality.

Generally a cluster expects the N/2+1 node to be online to start servicing the clients (where N is the number of Genesys Knowledge Center Server applications connected to the cluster and is enabled).

For example, if you have configured 3 nodes in the Genesys Administrator and started just one, the started server will refuse any client's requests as it will treat the overall cluster as not started yet. The cluster will become functional only when the second node of The Genesys Knowledge Center Server joins the cluster.

In rare cases when you still need to run such a configuration there are several ways to enforce cluster functionality:

- Disable applications that you are not going to run (by unchecking the **Enable** checkbox in every such application in Genesys Administrator)
- Manually setting the **minimumMasterNodes** value option in the **index** section into a desired value (for example, 1 in the example below).

Important

We do not recommended using manual settings, especially manually defining the **minimumMasterNodes** option as any incorrect values could result in data corruption.

Tip

Running nodes needs to be restarted if you applying one of the listed below recommendations.

Internode Communication

When running a production cluster it is required to disable the multicast node discovery by setting it to *false* **enabled** option in **multicast** section of the cluster application object in the configuration. It is also a good idea to disable multicast in lab deployments.

Multicast may lead to incidental joining of the undesired node to the cluster that will trigger data relocations to rebalance the data between nodes.

Host On-Boarding

Having the majority of the configuration in common between all nodes in the cluster there are few parameters that must be configured to onboard the node on a particular host. An example of these parameters is the folder for log files that is configured in the **log** section of the Genesys Knowledge Center Server application.

The other configuration that you need to set properly is the location of the indexed knowledge that is configured in option **path.data** of **gms.yml** file.

Important

It is recommended to store your indexed knowledge on the fastest disk you have on the host. By default the data will be placed into the folder where you have installed Genesys Knowledge Center Server.
If you have two disks attached to the host (for example, one spinning and another SSD) you can reconfigure the application to store the data in the fastest disc (SSD) while using the spinning disc for the application binaries.

Multi-Tenancy

Knowledge Center 8.5.302.xx and earlier is a single tenant solution. This means that if you have a multi-tenant environment and you want to use the Knowledge Center application within several tenants, you need to deploy a separate cluster for every tenant where you plan to use the application.

Starting from 8.5.303.xx release of the product it supports multiple tenants within one cluster deployment. The list of the tenants needs to be explicitly set for the applications in cluster.

> ### Important
> Within one Knowledge Center cluster all Knowledge Center Server nodes and all Knowledge Center CMS nodes must be configured to have the same tenant(s) in the **Tenants** section.

Installation and Deployment

Task Summary: Genesys Knowledge Center

The following table outlines the task flow for installing Genesys Knowledge Center.

Objective	Actions
1. Prepare your environment	1. Configure Languages 2. Setup RDBMS for CMS 3. Setup Elasticsearch cluster
2. Configure the Knowledge Center Cluster Application	1. Import the Knowledge Center Cluster Application Template 2. Create the Cluster Applications 3. Configure the Cluster Application
3. Install the Knowledge Center Server	1. Import the Knowledge Center Server Application Template 2. Create the Server Applications 3. Configure the Knowledge Center Server Application 4. Install Knowledge Center Server
4. Install the Knowledge Center CMS	1. Install the CMS 2. Configure Data Source (based on the selected provider): • (if using Microsoft Server as persistent storage), Configure the CMS to work with Microsoft SQL Server • (if using Oracle as persistent storage), Configure the CMS to work with Oracle • (if using PostgreSQL as persistent storage), Configure the CMS to work with PostgreSQL 3. Configure the CMS 4. Manage the Knowledge Base using CMS

Objective	Actions
5. Install the Workspace Desktop Edition Plugin	1. Install the Plugin for Workspace Desktop Edition 2. Configure the WDE Application to work with the WDE Plugin
6. Configure agent accounts	1. Grant access permission to content authors 2. Provide Knowledge Center Server Access to Agents 3. Provide Knowledge Center Workspace Desktop Edition Plugin Access to Agents
7. Configure Reporting	1. Enable and configure reporting within your Knowledge Center deployment

Before you Begin

This chapter describe the step(s) required to prepare your environment for the Knowledge Center installation. Preparation step(s) are:

- Define the languages used in your environment
- Chose and install RDBMS for Genesys Knowledge Center CMS
- Configure access to Elasticseach cluster for Genesys Knowledge Center Server

Configuring Languages

Overview

To operate the Genesys Knowledge Center solution you need to define and configure languages that will be used within your knowledge.

Knowledge Center requires:

- all supported languages to be defined in Configuration Server
- ISO codes to be defined in the Annex of the Language Attributes Values

Knowledge Center supports two types on languages:

- Language ("base" language)
- Regional language

Regional language is a version of the "base" Language that is used in a particular country.

The use of regional languages is recommended only in situations when knowledge documents can be different in the different countries using a same language (for example: knowledge documents which include local regulatory information or region-specific terminology, and so on).

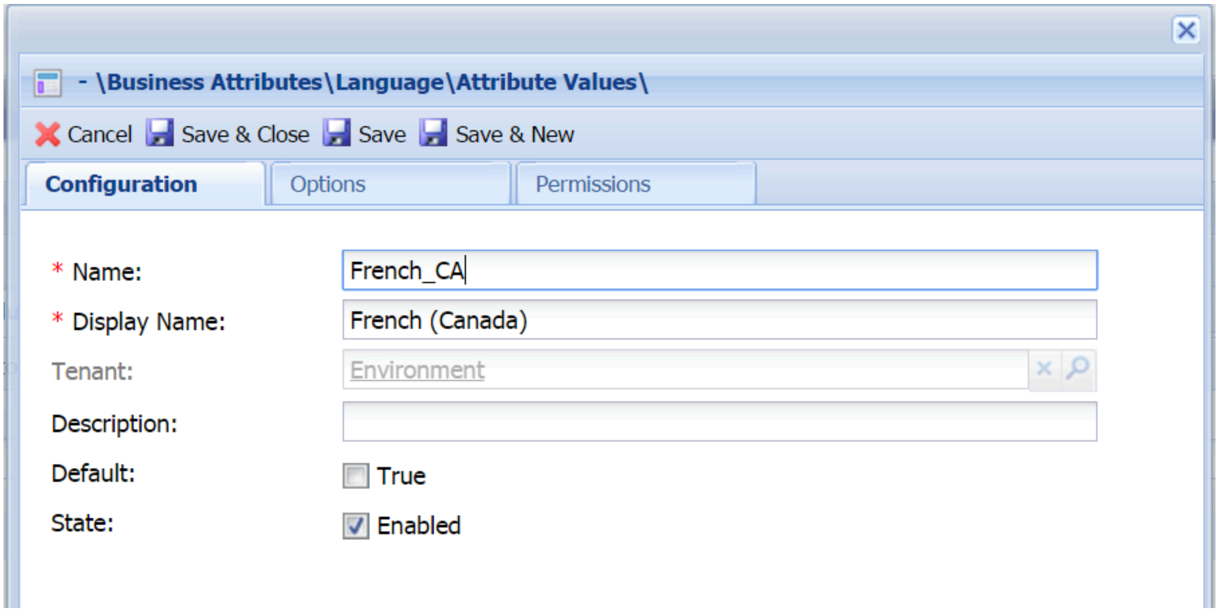
Regional language requires two ISO codes:

- language code (ISO 639-1)
- country code (ISO 3166-1 alpha-2 code)

How to configure a language

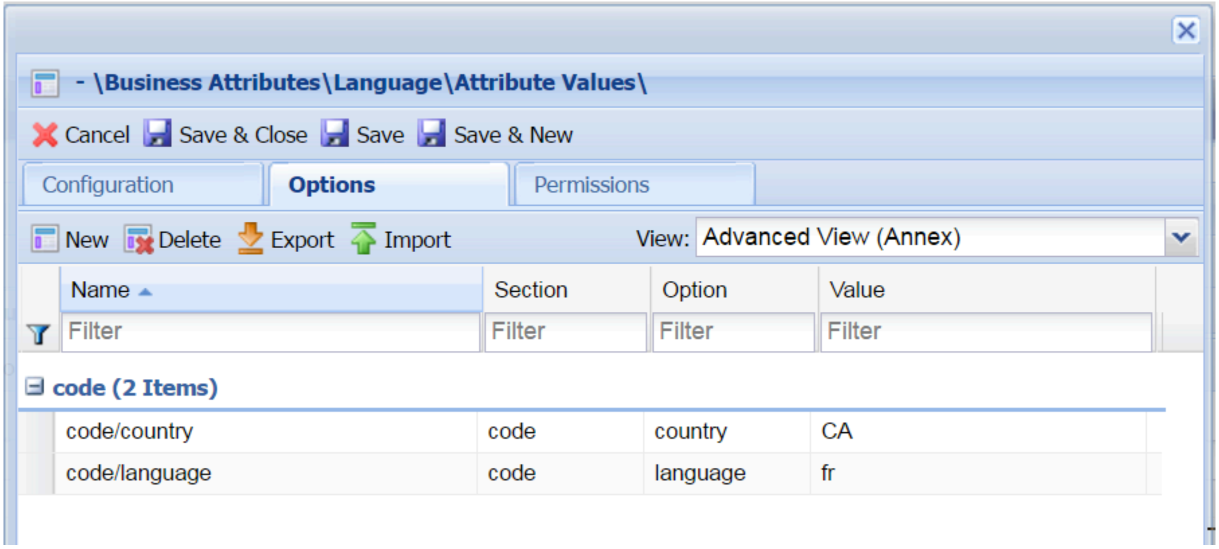
1. Open Genesys Administrator and navigate to **Provisioning** > **Routing/eServices** > **Business Attributes**.
2. Select **Language** business attribute

3. Click **Edit** button
4. Select **Attribute Values** tab
5. Click **New** button or select existing attribute value and press **Edit** button
6. On **Configuration** tab (skip this step if you are editing existing **Attributes Value**. For example, English which is created by default)
   a. Enter **Name**. For instance, French_CA
   b. Enter **Display Name**. For instance French (Canada)
   c. Ensure that **State** check is enabled



* Name:	French_CA
* Display Name:	French (Canada)
Tenant:	Environment
Description:	
Default:	☐ True
State:	☑ Enabled

7. Select **Options** tab:
   a. Press **New** button to add language code
   b. Enter "code" in **Section** field (eg. new section "code" should be created)
   c. Enter "language" in **Name** filed (eg. new option "name" should be created)
   d. Enter ISO 639-1 alpha-2 code that corresponds to desired language in **Value** field. For instance fr
   e. Press **OK** button
8. If you are adding regional language you also need to specify a region code:
   a. Press **New** button
   b. Enter code in **Section** field
   c. Enter country in **Name** filed
   d. Enter ISO 3166-1 alpha-2 code that corresponds to desired region/country in value filed. For instance CA
   e. Press **OK** button



View: Advanced View (Annex)

code (2 Items)

Name	Section	Option	Value
code/country	code	country	CA
code/language	code	language	fr

9. Press **Save & Close** button
   Note: You need to repeat this procedure for every language that you plan to use in your Knowledge Base.

Important

Please ensure that following rules are followed when you are adding Attribute Values to the Language Business Attribute:

- Languages should be create in the same tenant in which Knowlege Server and CMS applications will be configured.
- Every language needs to have language (mandatory) and country (if applicable) codes defined on options tab (languages w/o codes will be ignored)
- Ensure that all language/country combinations are unique (duplicate combinations will be ignored)
- Do not edit/change defined codes if they are used in the knowledge bases
- Language code needs to correspond to the ISO 639-1 alpha-2 code for the given language (http://www.iso.org/iso/home/standards/language_codes.htm)
- Country code needs to correspond to the ISO 3166-1 alpha-2 code for given language (http://www.iso.org/iso/country_codes)

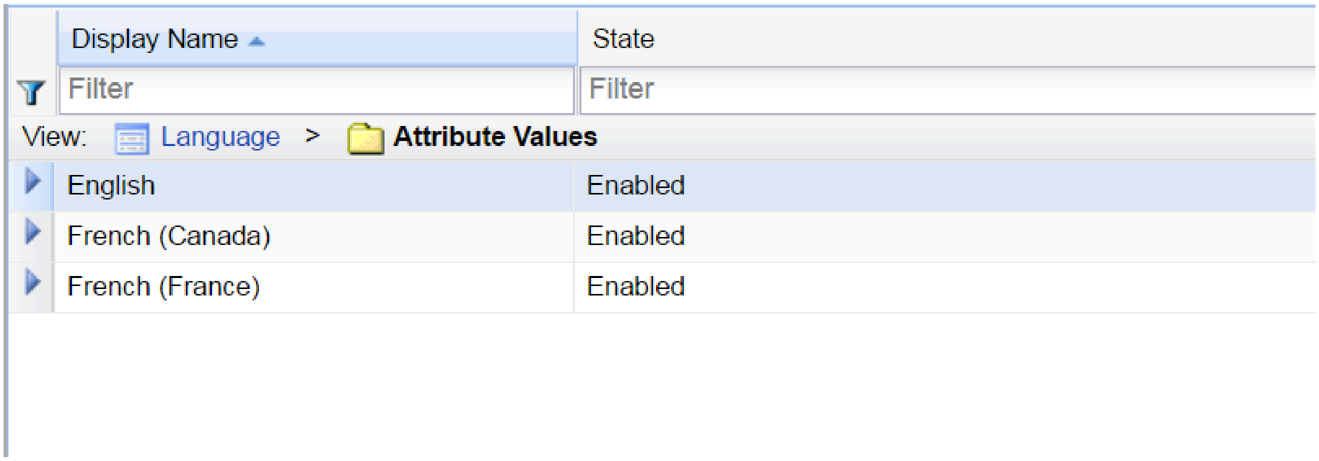
Example

If you wish to have following languages in your environment:

- English
- French (Canadian)

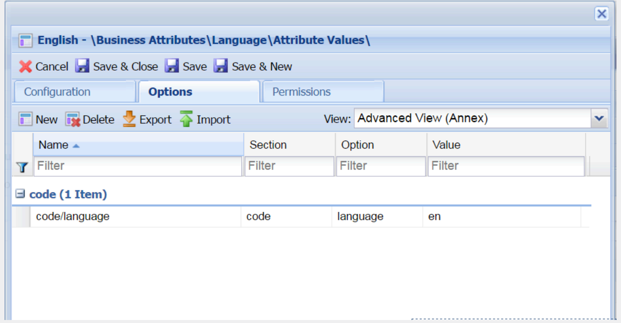
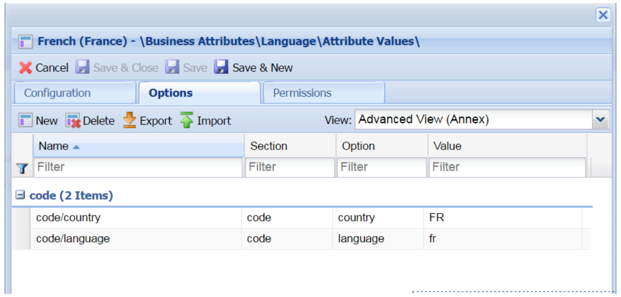
- French (France)

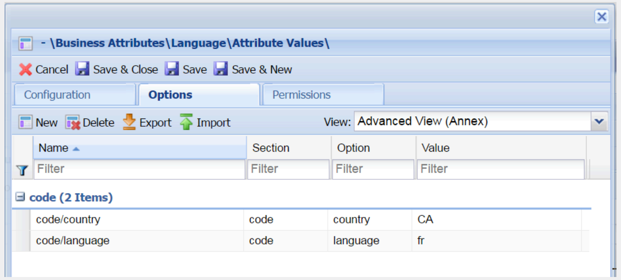
You will need to create 3 attribute values:



View: Language > **Attribute Values**

Display Name ▲	State
Filter	Filter
English	Enabled
French (Canada)	Enabled
French (France)	Enabled

Name	Display Name	Options
English	English	code/language=en  English - \Business Attributes\Language\Attribute Values\ Cancel Save & Close Save Save & New Configuration Options Permissions New Delete Export Import View: Advanced View (Annex) Name / Section / Option / Value code (1 Item) code/language / code / language / en
French_FR	French (France)	code/language=fr code/country=FR  French (France) - \Business Attributes\Language\Attribute Values\ Cancel Save & Close Save Save & New Configuration Options Permissions New Delete Export Import View: Advanced View (Annex) Name / Section / Option / Value code (2 Items) code/country / code / country / FR code/language / code / language / fr
French_CA	French (Canada)	code/language=fr code/country=CA

Name	Display Name	Options
		

View: Advanced View (Annex)

Name	Section	Option	Value
code (2 Items)			
code/country	code	country	CA
code/language	code	language	fr

Installing a Relational Database Management System

Knowledge Center CMS requires a Relational database management system (RDBMS) to be deployed and configured in order to store the knowledge data.

The following RDBMS providers are supported by Genesys Knowledge Center CMS:

- Microsoft SQL Server
- Oracle
- PostgreSQL

> **Important**
>
> Please check supported versions of RDBMS in the *Genesys Supported Operating Environment Reference Guide*.

Before proceeding with the installation of the Knowledge Center solution you need to:

1. Install RDBMS
2. Create a new dababase
3. Create a user that will be used by the Knowledge Center to access the database
4. Ensure that you are able to connect to the new database from the hosts that the Knowledge Center CMS nodes are running on
5. Create backups for the new database

Configure access to Elasticsearch

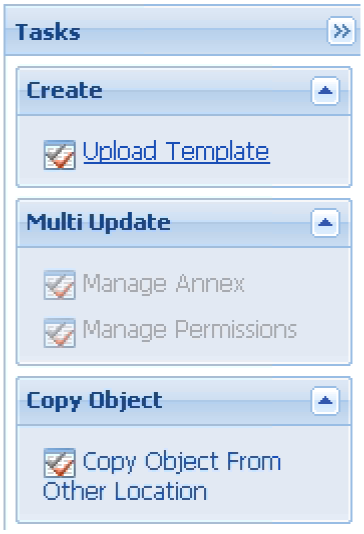
Knowledge Center Server requires Elasticsearch cluster to be deployed.

To use Elasticsearch culster by Knowledge Center Server you need to configure a Resource Access Point and connect it with the Knowledge Center Cluster application.

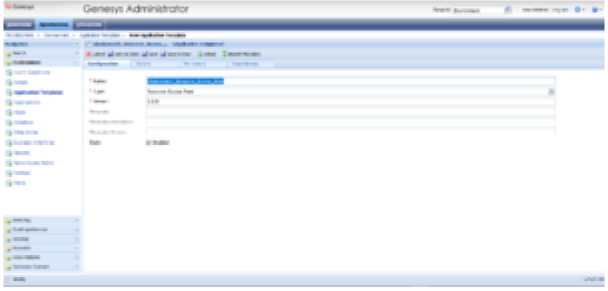
Importing the Elasticsearch Resource Access Point Template

Start

1. Open Genesys Administrator and navigate to **Provisioning > Environment > Application Templates**.
2. In the **Tasks** panel, click **Upload Template**.



3. Click **Add** and choose the application template (APD) file to import, then click **Add**.
4. Browse to the Elasticsearch_Resource_Access_Point.tpl file. Click **Open**.
   The New Application Template panel opens:



5. Click **Save & Close**.

End

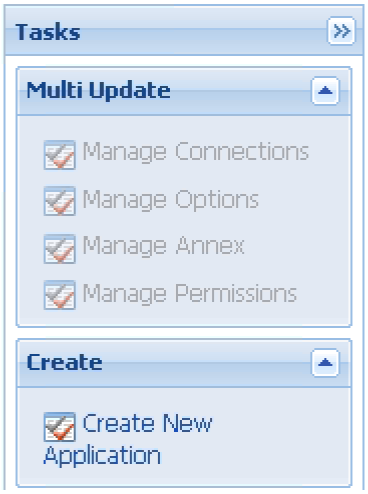
Creating the Elasticsearch Resource Access Point Application

Prerequisites

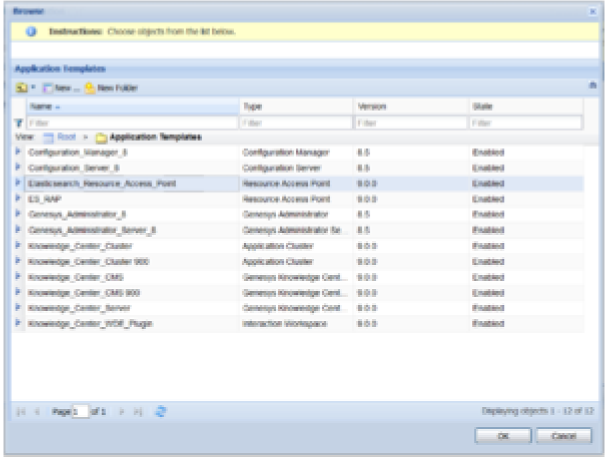
- You completed Importing the Elasticsearch Resource Access Point Template

Start

1. Open Genesys Administrator and navigate to **Provisioning > Environment > Applications**.
2. In the **Tasks** panel, click **Create New Application**.



3. In the **Select Application Template** panel, click **Browse for Template** and select the *Elasticsearch_Resource_Access_Point* template that you imported in Importing the Elasticsearch Resource Access Point Template. Click **OK**.

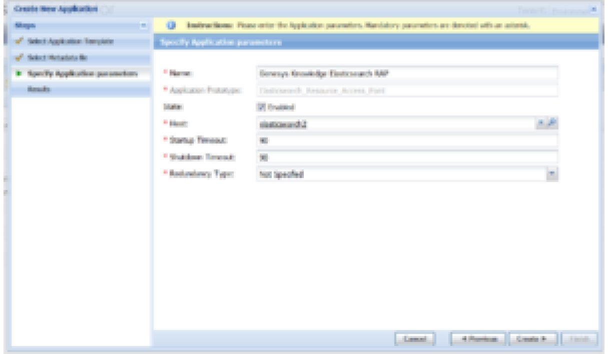

Browse
Instructions: Choose objects from the list below.
Application Templates
New ...
New Folder
View: Root > Application Templates
Page 1 of 1
OK
Cancel

Name	Type	Version	State
Configuration_Manager_8	Configuration Manager	8.5	Enabled
Configuration_Server_8	Configuration Server	8.5	Enabled
Elasticsearch_Resource_Access_Point	Resource Access Point	9.0.0	Enabled
ES_RAP	Resource Access Point	9.0.0	Enabled
Genesys_Administrator_8	Genesys Administrator	8.5	Enabled
Genesys_Administrator_Server_8	Genesys Administrator Se...	8.5	Enabled
Knowledge_Center_Cluster	Application Cluster	9.0.0	Enabled
Knowledge_Center_Cluster 900	Application Cluster	9.0.0	Enabled
Knowledge_Center_CMS	Genesys Knowledge Cent...	9.0.0	Enabled
Knowledge_Center_CMS 900	Genesys Knowledge Cent...	9.0.0	Enabled
Knowledge_Center_Server	Genesys Knowledge Cent...	9.0.0	Enabled
Knowledge_Center_WDE_Plugin	Interaction Workspace	9.0.0	Enabled

Displaying objects 1 - 12 of 12

4. The template is added to the **Select Application Template** panel. Click **Next**.
5. In the Select Metadata file panel:
   a. Click **Browse**
   b. Click **Add**
   c. Select the *Elasticsearch_Resource_Access_Point.xml* file
   d. Click **Open**
6. The metadata file is added to the **Select Metadata File** panel. Click **Next**.
7. In the **Specify Application Parameters** field:
   a. Enter a name for your application (for instance, "Genesys Knowledge Elasticsearch RAP")
   b. Make sure that **State** is enabled
   c. Select the **Host** on which the Access Point will reside

d. Click **Create**



Create New Application

Name: Genesys Knowledge Elasticsearch RAP

Application Prototype: Elasticsearch_Resource_Access_Point

State: ☑ Enabled

Host: elasticsearch2

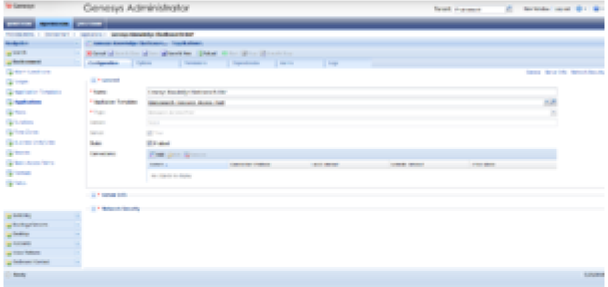
Startup Timeout: 90

Shutdown Timeout: 90

Redundancy Type: Not Specified

Steps
Select Application Template
Select Metadata file
Specify Application parameters
Results
Specify Application parameters
Cancel
◀ Previous
Create ▶
Finish

8. The Results panel opens.
9. Enable **Opens the Application details form after clicking 'Finish'** and click **Finish**. The Elasticsearch Resource Access Point application form opens and you can start configuring its properties.



End

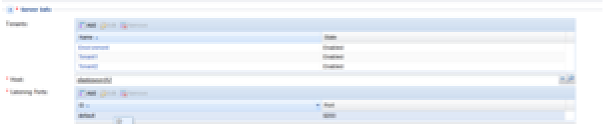
Configuring the Elasticsearch Resource Access Point Application

Prerequisites

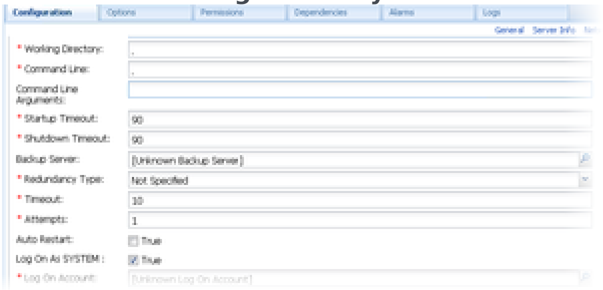
- You completed Creating the Elasticsearch Resource Access Point Application.

Start

1. If your Elasticsearch Resource Access Point application form is not open in Genesys Administrator, navigate to **Provisioning > Environment > Applications**. Select the application defined for the **Elasticsearch Resource Access Point** and click **Edit**.
2. Expand the **Server Info** pane.
3. In the **Tenant** section, click **Add** and select your tenant (for instance, **Environment**). Click **OK**. (Tenant should be same as the Genesys Application cluster previously created).
4. If your **Host** is not defined, click the lookup icon to browse to the hostname of your application, which should point to the host where you plan to locate your Elasticsearch node or Load-Balancer.
5. In the **Listening Ports** section, create the default port by clicking **Add**. The Port Info dialog opens.
   a. Enter the **Port** (for instance, 9200 [use value of http of your Elasticsearch]).
   b. Click **OK**. The default port appears in the list of **Listening ports**.

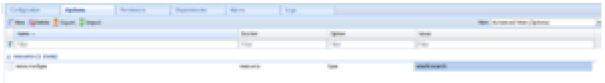


6. Ensure the **Working Directory** and **Command Line** fields contain a "." (period).



* Working Directory: .
* Command Line: .
Command Line Arguments:
* Startup Timeout: 90
* Shutdown Timeout: 90
Backup Server: [Unknown Backup Server]
* Redundancy Type: Not Specified
* Timeout: 10
* Attempts: 1
Auto Restart: □ True
Log On As SYSTEM : ☑ True
* Log On Account: [Unknown Log On Account]

7. Click **Save**.
8. The confirmation dialog for changing the application's port opens. Click **Yes**.
9. Select the **Options** tab.
   - Make sure the following options are set in the **[resource]** section:
     - **[resource]/type**=`elasticsearch`



10. Click **Save & Close**. If the confirmation dialog opens, click **Yes**.

End

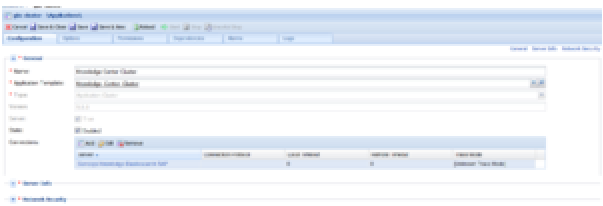
Configuring the Knowledge Center Cluster for Use with Elasticsearch RAP

Prerequisites

- You completed Configuring the Elasticsearch Resource Access Point Application.

Start

1. Navigate to **Provisioning > Environment > Applications**. Select the application defined for the Knowledge Center Cluster and click **Edit**.
2. In the **Connections** section of the **Configuration** tab, click **Add**. The Browse for applications panel opens. Select a Genesys application defined as a Elasticsearch Resource Access Point, then click **OK**.
3. Select the added connection to application, click **Edit** and ensure that the default connection port is selected as **ID**.
4. Click **Save & Close**. If the confirmation dialog opens, click **Yes**.



End

Automatic Provisioning during installation

During the installation of Genesys Knowledge Center Server and Genesys Knowledge Center CMS from the Installation Package, the Installation Wizard will automatically apply some minimal necessary provisioning actions for Configuration Server objects.

Provisioning during installation

The provisioning tool will take care of the following configuration details:

- Environment
  - create "selfservice" media type in Business Attributes
  - add language code to the English language
- Server or CMS application
  - check if application connected with Application Cluster object
  - define default ports (if they are not defined)
  - copy tenants from the cluster object (if they are not configured explicitly)
  - ensure that internal options are properly initialized

Provisioning tool

The provisioning tool is found in the following location:

- For Genesys Knowledge Center Server:

  ```
  <path to installation folder>\server\tools\provisioning
  ```
- For Genesys Knowledge Center CMS:

  ```
  <path to installation folder>\tools\provisioning
  ```

In this folder you will find logs with provisioning results in file `provisioning.log`

If everything is correct, the following results will appear (below is an example from Genesys Knowledge Center Server):

```
Provisioning script is started with the following arguments:
[--host, host, --port, 2020, --app, Knowledge_Center_Server, --user, user --password, pa, --
all, --product, server]
```

Command-line arguments, used for the connection to Configurations server and provided by Installation Wizard.

```
[4503] Connected to ConfigServer 'confserv' at host 'host', port 2020
```

Connection to Configuration Server.

```
Starting configuration thread
Configuration thread started.
Starting configuring application
Configuration init successfully completed.
```

Information messages.

```
Application [Knowledge_Center_Cluster] is configured to work with [2] tenant
```

Tool get cluster's tenants

```
Start provisioning of application [Knowledge_Center_Server] on CfgServer [host:2020]
Process LANGUAGE target ...
English in tenant 1 already has language defined [en]
English in tenant 101 already has language defined [en]
```

Check if, at minimum, the English language (with code en) was created in configured Tenants. If not, languages will be auto-configured. For more information, see Configuring Languages.

```
Process MEDIATYPE target ...
MediaType [selfservice] already exists in tenant 1. Leave it.
MediaType [selfservice] already exists in tenant 101. Leave it.
```

Check if `selfservice` media exists in configured Tenants. If not, `selfservice` Media Type is auto-created.

```
Process APPLICATION target ...
Knowledge_Center_Server_902 has the same tenants as the Cluster application
Knowledge_Center_Cluster_902
```

The tool then checks if the Cluster and Server applications have the same set of tenants.

```
Setting Knowledge_Center_Server_902/CFGKnowledgeCenter ports
[default] has been set already [5600]
[clustering] has been set already [9152]
[kibana] has been set already [5601]
```

Check if the necessary ports are configured in the application. If not, the port is auto-configured (in other words, a port is added and default values are set).

```
Provisioning script has finished work. Result: SUCCESS
```

End.

Limitations

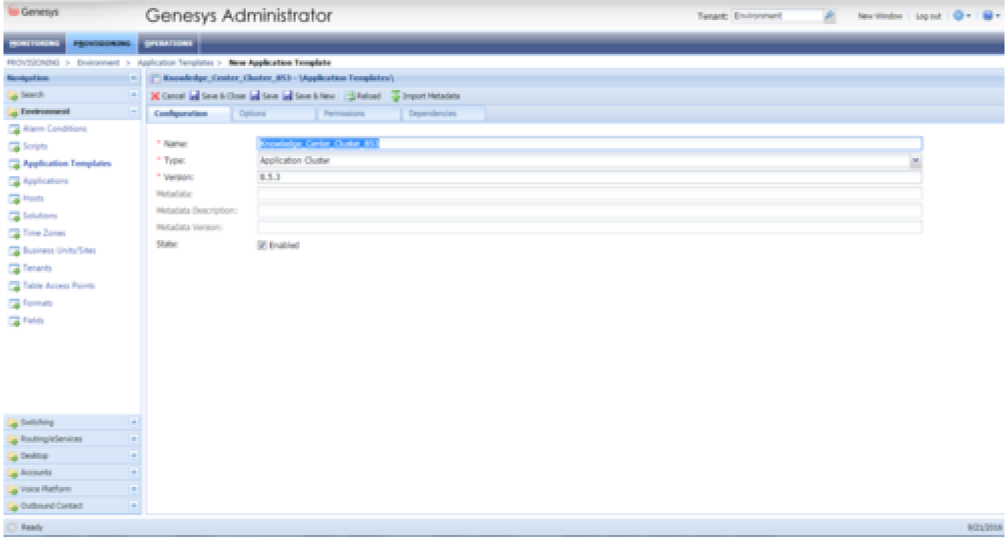
In IP mode, provisioning cannot interact with the Installation Package in any other way than returning an error code. This means that in a case of configuration issues we can write a report in the local folder, but cannot communicate to the user any errors or warnings in any other way than "failed IP installation".

Configuring the Knowledge Center Cluster Application

Carry out the procedures below, in order, to install and configure the Knowledge Center Cluster Application.

Import the Knowledge Center Cluster Application Template

1. Open Genesys Administrator and navigate to **Provisioning > Environment > Application Templates**.
2. In the **Tasks** panel, click **Upload Template**.
3. In the **Click 'Add' and choose application template (APD) file to import** window, click **Add**.
4. Browse to the *Knowledge_Center_Cluster.apd* file available in the templates directory of your installation CD.
5. Click open.
6. The **New Application Template** panel opens.



* Name: Knowledge_Center_Cluster_851

* Type: Application Cluster

* Version: 8.5.1

Metadata:

Metadata Description:

Metadata Version:

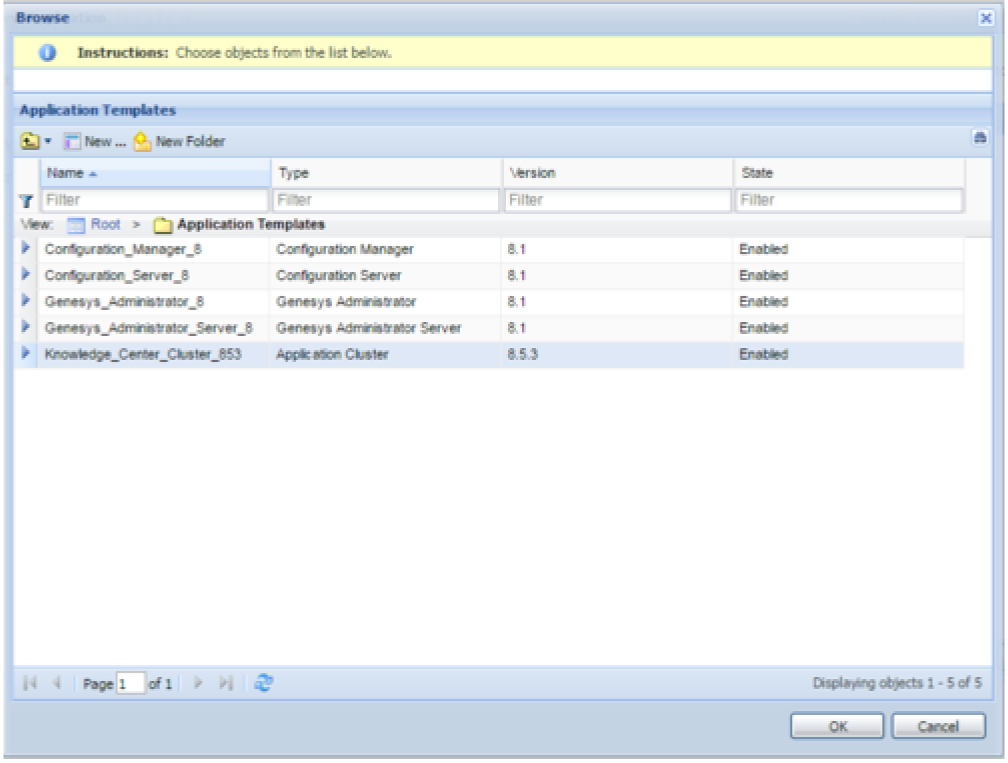
State: ☑ Enabled

New Application Template Panel

7. Click **Save and Close**.

Create Cluster Applications

1. Open Genesys Administrator and navigate to **Provisioning > Environment > Applications**.
2. In the **Tasks** panel, click **Create New Application**.
3. In the **Select Application Template** panel, click **Browse for Template** and select the Genesys Knowledge Center Cluster application template that you imported earlier. Click **OK**.



Instructions: Choose objects from the list below.

Application Templates

View: Root > **Application Templates**

Name	Type	Version	State
Filter	Filter	Filter	Filter
Configuration_Manager_8	Configuration Manager	8.1	Enabled
Configuration_Server_8	Configuration Server	8.1	Enabled
Genesys_Administrator_8	Genesys Administrator	8.1	Enabled
Genesys_Administrator_Server_8	Genesys Administrator Server	8.1	Enabled
Knowledge_Center_Cluster_853	Application Cluster	8.5.3	Enabled

Displaying objects 1 - 5 of 5

Selecting Knowledge Center Cluster Application Template

4. The template is added to the **Select Application Template** panel. Click **Next**.
5. In the Select Metadata file panel:

   a. Click **Browse**.

   b. Click **Add**.

   c. Select the *Knowledge_Center_Cluster.xml* file available in the templates directory of your installation CD.

   d. Click **Open**.

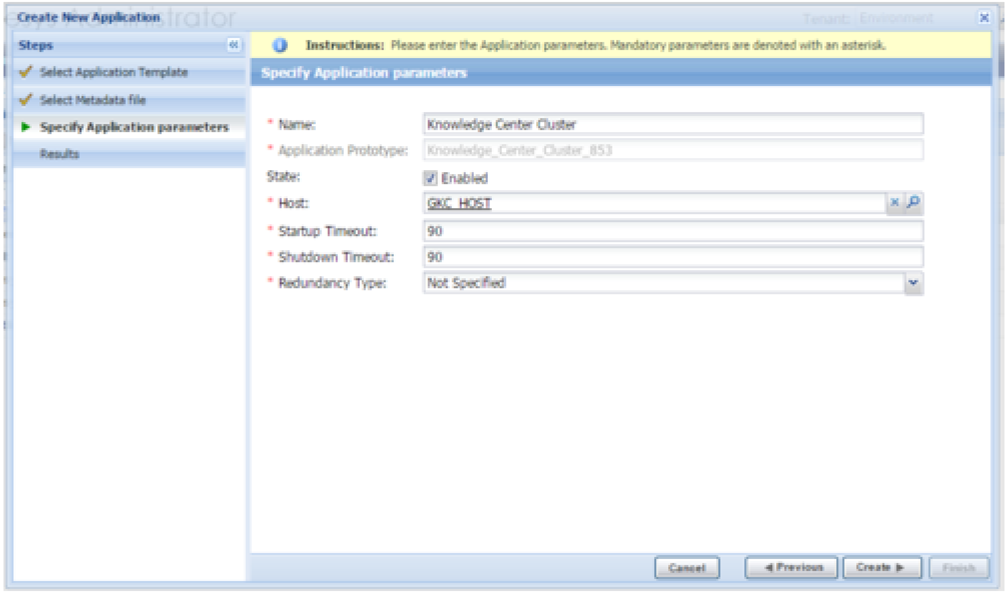
5. The metadata file is added to the **Select Metadata** file panel. Click **Next**.
6. In **Specify Application parameters**:

   a. Enter a name for your application. For instance, *Knowledge Center Cluster*.

   b. Ensure that **State** is checked.

   c. Select the **Host** on which the Knowledge Center Cluster load-balancer will reside.

d. Click **Create**.

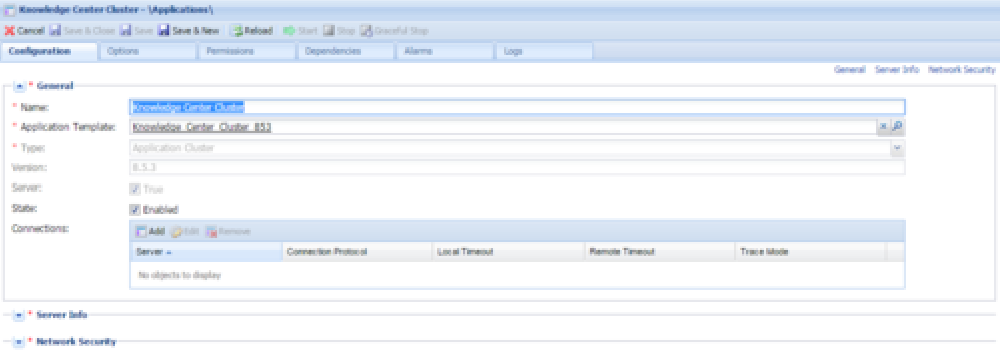


Instructions: Please enter the Application parameters. Mandatory parameters are denoted with an asterisk.

* Name:	Knowledge Center Cluster
* Application Prototype:	Knowledge_Center_Cluster_853
State:	☑ Enabled
* Host:	GKC_HOST
* Startup Timeout:	90
* Shutdown Timeout:	90
* Redundancy Type:	Not Specified

Specifying Knowledge Center Cluster Application Parameters

5. The **Results** panel opens.
6. Enable **Open the Application details form after clicking 'Finish'** and click **Finish**. The Knowledge Center Cluster application form opens and you can start configuring the Cluster application.



* Name:	Knowledge Center Cluster
* Application Template:	Knowledge_Center_Cluster_853
* Type:	Application Cluster
Version:	8.5.3
Server:	☑ True
State:	☑ Enabled
Connections:	

Server	Connection Protocol	Local Timeout	Remote Timeout	Trace Mode
No objects to display				

Configuring the Knowledge Center Cluster Application

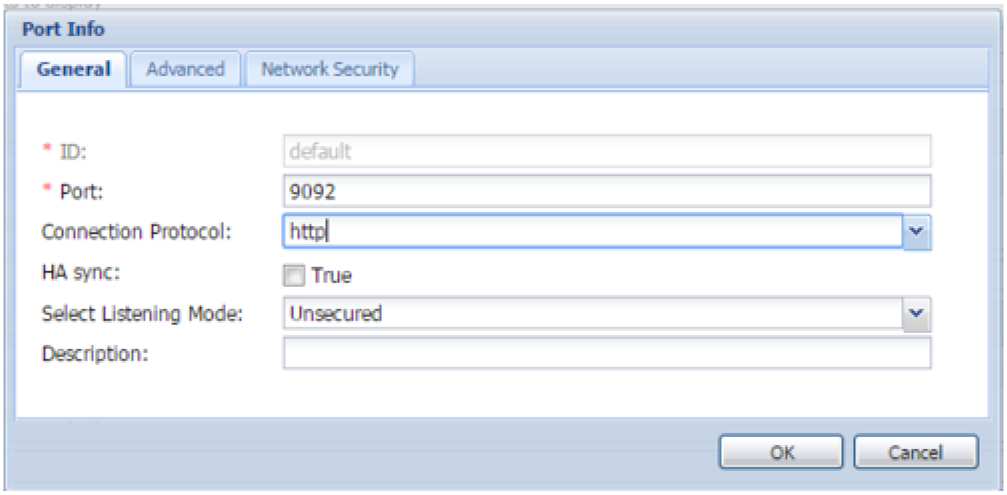
Configure the Cluster Application

1. If your Knowledge Center Cluster application form is not open in Genesys Administrator, navigate to **Provisioning > Environment > Applications**. Select the application defined for the Knowledge Center Cluster and click **Edit...**.
2. Expand the **Server Info** pane.
3. If your **Host** is not defined, click the lookup icon to browse to the host on which the Knowledge Center Cluster load-balancer will reside.

Important

Knowledge Center Cluster serves as the entry point to all client requests sent to Knowledge Center Servers. The cluster application in Genesys Administrator needs to be configured to point to the host and port of the load balancer that will distribute these requests among your Knowledge Center Servers.

4. In the **Listening Ports** section, create the default port by clicking **Add**. The **Port Info** dialog opens.
   a. Enter the port number for the Knowledge Center Cluster load-balancer, for instance, *9092*.
   b. Choose *http* or "https" for the **Connection Protocol**.
   c. If you will be using a secure connection to the cluster, choose *Secured* for the **Select Listening Mode**.
   d. Click **OK**. The HTTP or HTTPS port with the default identifier appears in the list of **Listening ports**.

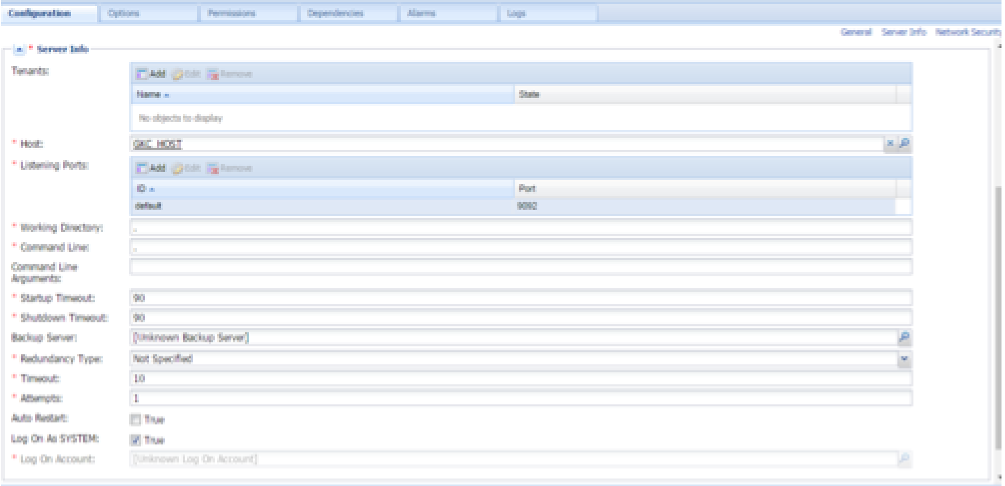


Port Info

* ID: default
* Port: 9092
Connection Protocol: http
HA sync: □ True
Select Listening Mode: Unsecured
Description:

Knowledge Center Cluster Port Information

   e. In the **Tenants** section, add a working tenant by clicking **Add**. Browse and choose the appropriate tenant in the pop-up dialog. Click Ok.
   f. Ensure the **Working Directory** and **Command Line** fields contain "." (period).



* Server Info

Tenants:

Name	State
No objects to display	

* Host: GKC_HOST

* Listening Ports:

ID	Port
default	9092

* Working Directory: .

* Command Line: .

Command Line Arguments:

* Startup Timeout: 90

* Shutdown Timeout: 90

Backup Server: [Unknown Backup Server]

* Redundancy Type: Not Specified

* Timeout: 10

* Attempts: 1

Auto Restart: □ True

Log On As SYSTEM: ☑ True

* Log On Account: [Unknown Log On Account]

Knowledge Center Cluster Server Information

5. Click **Save**.
6. The **Confirmation** dialog for changing the application's port opens. Click **Yes**.

Important

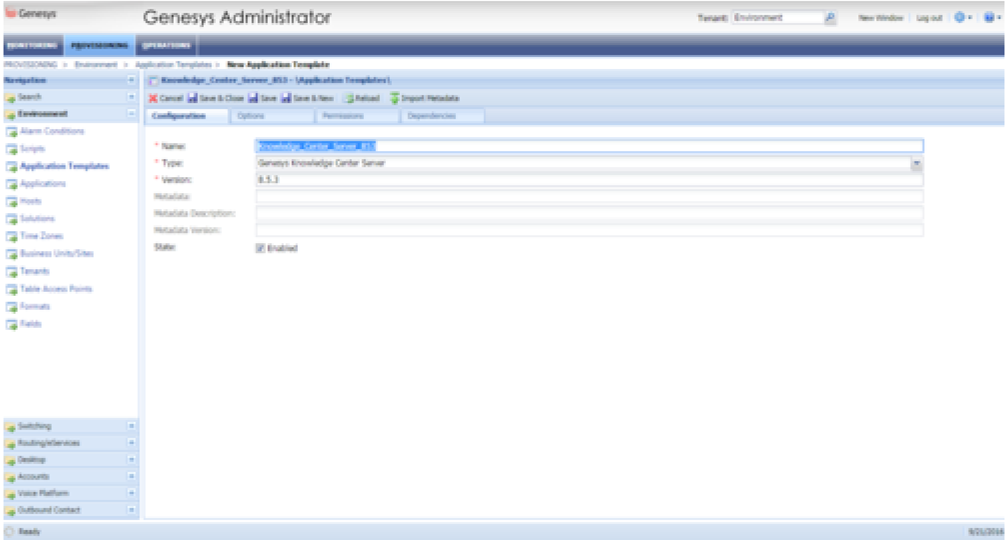
When configuring several Knowledge Center Clusters in one tenant, use the option "knowledgebaseFolder" found in the "general" section to separate the folders for your Knowledge Bases definitions in Scripts (for example, when setting different values for different clusters).

Installing the Knowledge Center Server

Import the Knowledge Center Server Application Template

Start

1. Open Genesys Administrator and navigate to **Provisioning > Environment > Application Templates**.
2. In the **Tasks** panel, click **Upload Template**.
3. In the **Click 'Add' and choose application template (APD) file to import** window, click **Add**.
4. Browse to the *Knowledge_Center_Server.apd* file available in the *templates* directory of your installation CD.
5. Click **Open**.
6. The **New Application Template** panel opens.



* Name: Knowledge_Center_Server_853

* Type: Genesys Knowledge Center Server

* Version: 8.5.3

Metadata:

Metadata Description:

Metadata Version:

State: ☑ Enabled

The Knowledge Center Server Application Template

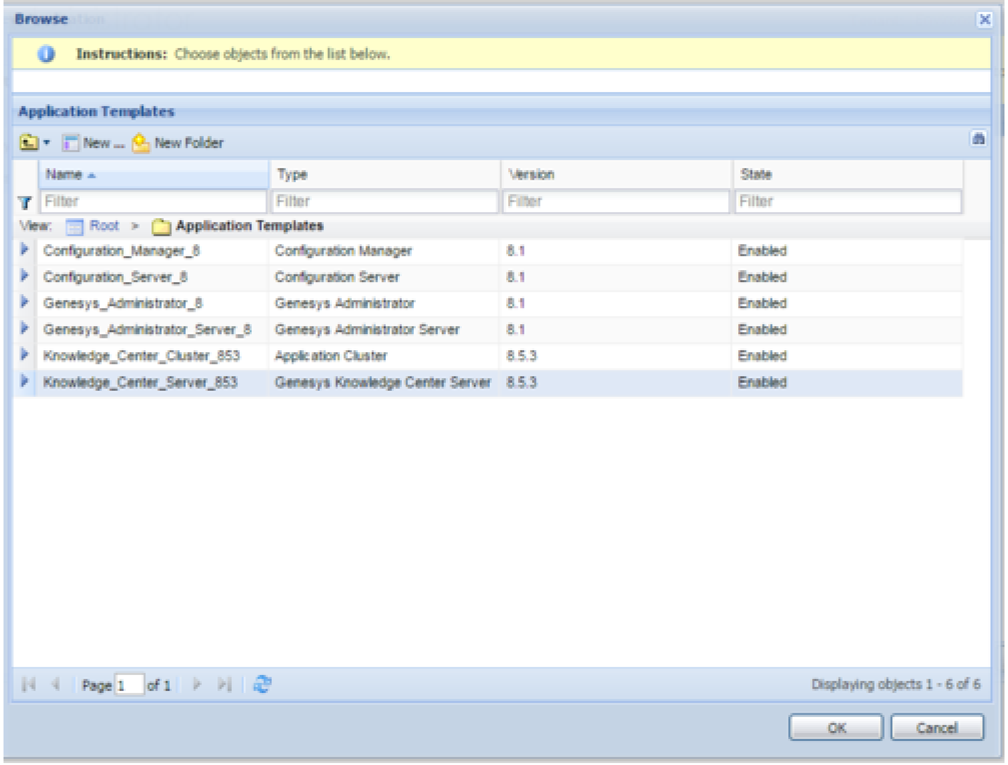
7. Click **Save and Close**.

End

Create Server applications

Start

1. Open Genesys Administrator and navigate to **Provisioning > Environment > Applications**.
2. In the **Tasks** panel, click **Create New Application**.
3. In the **Select Application Template** panel, click **Browse for Template** and select the Genesys Knowledge Center Server application template that you imported earlier. Click **OK**.



Instructions: Choose objects from the list below.

Application Templates

View: Root > Application Templates

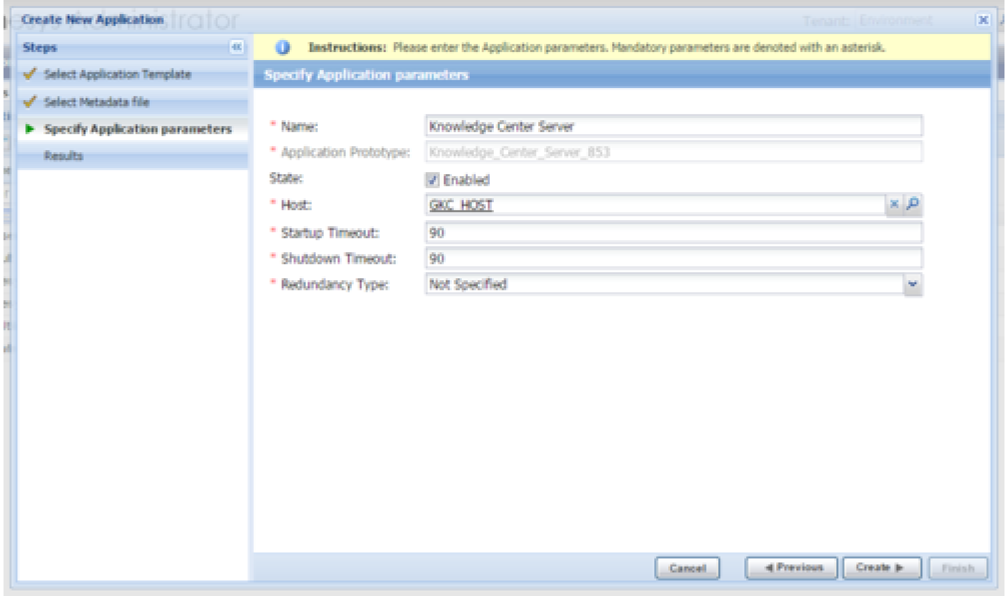
Name	Type	Version	State
Configuration_Manager_8	Configuration Manager	8.1	Enabled
Configuration_Server_8	Configuration Server	8.1	Enabled
Genesys_Administrator_8	Genesys Administrator	8.1	Enabled
Genesys_Administrator_Server_8	Genesys Administrator Server	8.1	Enabled
Knowledge_Center_Cluster_853	Application Cluster	8.5.3	Enabled
Knowledge_Center_Server_853	Genesys Knowledge Center Server	8.5.3	Enabled

Page 1 of 1

Displaying objects 1 - 6 of 6

Selecting the Knowledge Center Server Template

4. The template is added to the **Select Application Template** panel. Click **Next**.
5. In the **Select Metadata** file panel:
    a. Click **Browse**
    b. Click **Add**
    c. Select the *Knowledge_Center_Server.xml* file available in the templates directory of your installation CD.
    d. Click **Open**
6. The metadata file is added to the **Select Metadata** file panel. Click **Next**.
7. In **Specify Application parameters**:
    a. Enter a name for your application. For instance, *Knowledge Center Server*' .
    b. Enable the **State**
    c. Ensure that **State** checkbox is checked
    d. Select the **Host** on which the Knowledge Center Server will reside
    e. Click **Create**



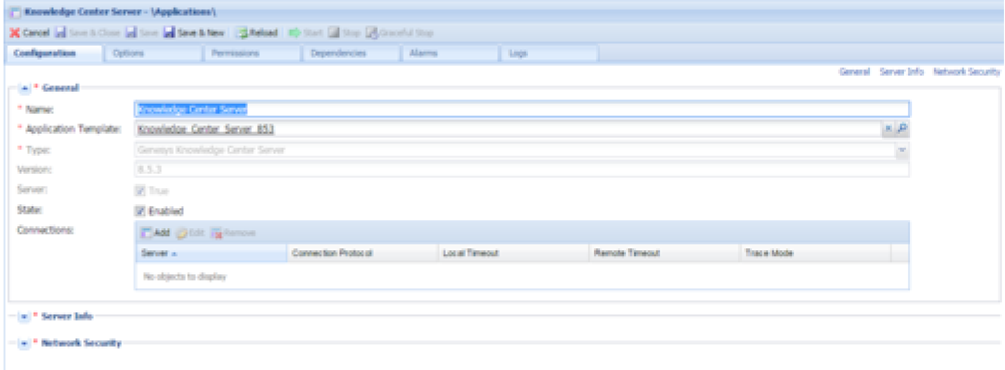
Instructions: Please enter the Application parameters. Mandatory parameters are denoted with an asterisk.

Specify Application parameters

* Name:	Knowledge Center Server
* Application Prototype:	Knowledge_Center_Server_853
State:	☑ Enabled
* Host:	GKC_HOST
* Startup Timeout:	90
* Shutdown Timeout:	90
* Redundancy Type:	Not Specified

Creating the Knowledge Center Server Application

6. The **Results** panel opens.
7. Enable **Open the Application details form after clicking Finish** and click **Finish**.
8. The Knowledge Center Server application form opens and you can start configuring the Knowledge Center Server application.



* General

* Name:	Knowledge Center Server
* Application Template:	Knowledge_Center_Server_853
* Type:	Genesys Knowledge Center Server
Version:	8.5.3
Server:	☑ True
State:	☑ Enabled
Connections:	

Server ▲	Connection Protocol	Local Timeout	Remote Timeout	Trace Mode
No objects to display				

Knowledge Center Server Application Details

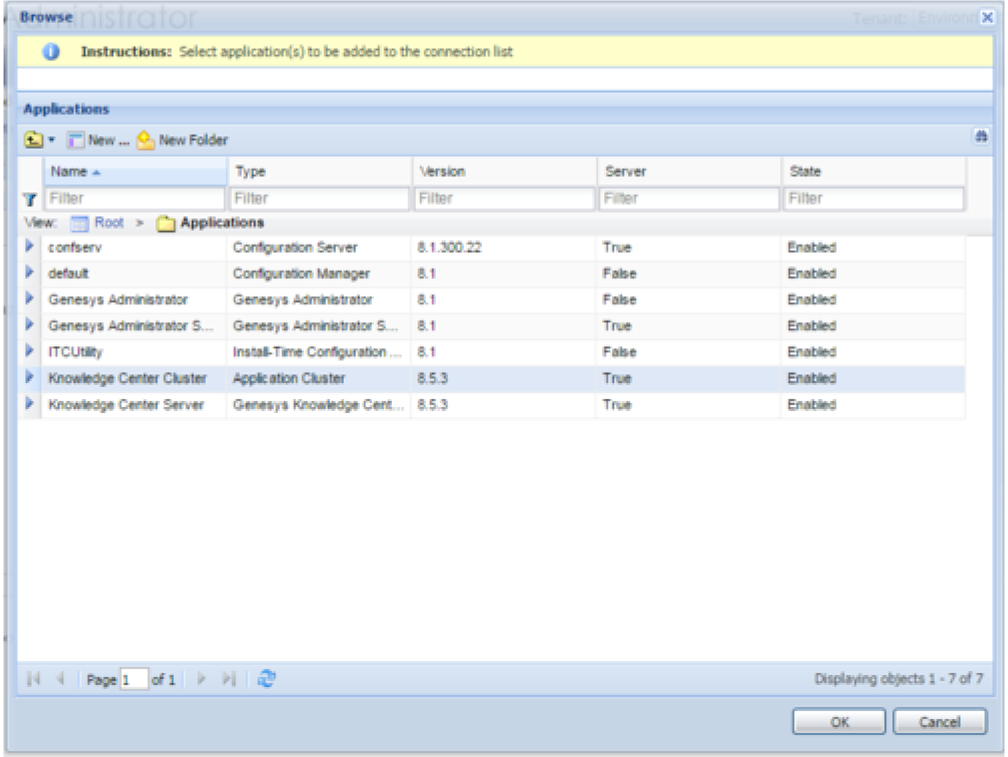
End

Configuring the Knowledge Center Server Application

Start

1. If your Knowledge Center Server application form is not open in Genesys Administrator, navigate to **Provisioning > Environment > Applications**. Select the application defined for the Knowledge Center Server and click **Edit...**.

2. In the **Connections** section of the **Configuration** tab, click **Add**. The **Browse for applications** panel opens. Select the Knowledge Center Cluster application, then click **OK**.



Instructions: Select application(s) to be added to the connection list

Applications

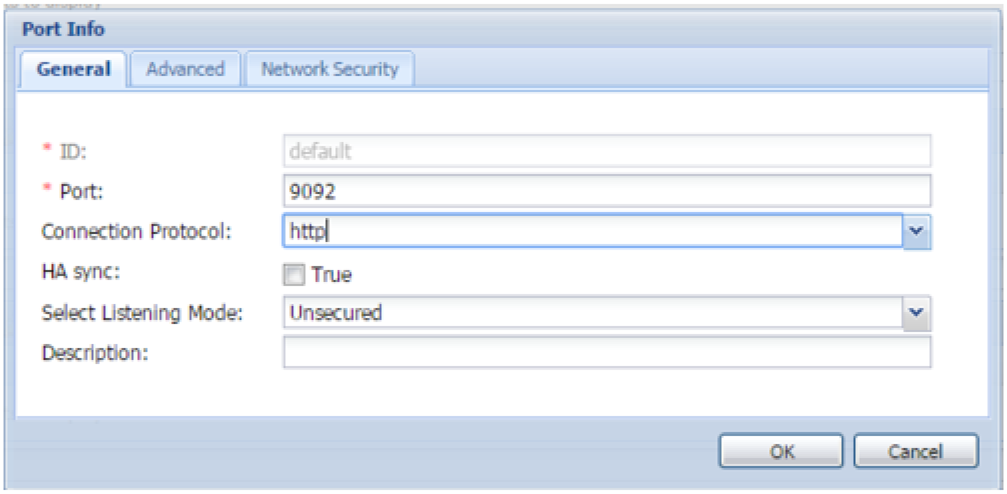
View: Root > **Applications**

Name	Type	Version	Server	State
confserv	Configuration Server	8.1.300.22	True	Enabled
default	Configuration Manager	8.1	False	Enabled
Genesys Administrator	Genesys Administrator	8.1	False	Enabled
Genesys Administrator S...	Genesys Administrator S...	8.1	True	Enabled
ITCUtility	Install-Time Configuration ...	8.1	False	Enabled
Knowledge Center Cluster	Application Cluster	8.5.3	True	Enabled
Knowledge Center Server	Genesys Knowledge Cent...	8.5.3	True	Enabled

Displaying objects 1 - 7 of 7

Selecting the Knowledge Center Cluster Application

3. Expand the **Server Info** pane.
4. If your **Host** is not defined, click the lookup icon to browse to the hostname of your application.
5. In the **Listening Ports** section, create the default port by clicking **Add**. The **Port Info** dialog opens.
    a. Enter the **Port**. For instance, *9092*. This should be the port number for the Knowledge Center Server instance.
    b. Choose *http* or *https* for the **Connection Protocol**.
    c. If you will be using a secure connection to the cluster, choose *Secured* for the **Select Listening Mode**.
    d. Click **OK**. The port with the default identifier appears in the list of **Listening ports**.



Port Info

* ID:	default
* Port:	9092
Connection Protocol:	http
HA sync:	□ True
Select Listening Mode:	Unsecured
Description:	

Knowledge Center Server Port Information

6. Add a port that will be used by Knowledge Center Server nodes to communicate with each other by clicking on the **Add** button and:

   a. Entering *clustering* in the ID field

   b. Entering the **Port**. For instance, 9152

   c. Clicking **OK**

   d. Ensure the **Working Directory** and **Command Line** fields contain "." (period).

   e. In the **Tenants** section, add a working tenant by clicking **Add**. Browse and choose the appropriate tenant in the pop-up dialog. Click Ok.

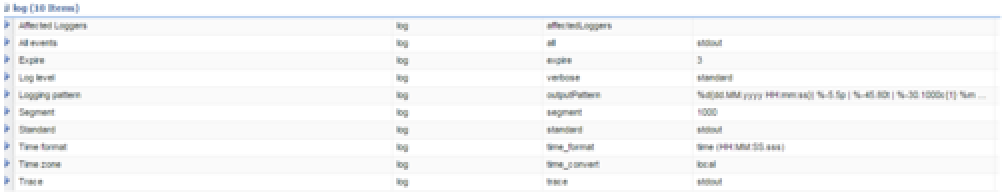
   f. If you are using Access Groups to assign privileges to agents:

      - Uncheck **Log On As System**
      - In **Log On Account** specify the user account that has the ability to view access groups (for example, user from the Super Administrators access group).
      - User should have access to the same tenant/tenants in which that Node is configured
      - User should belong to Administrator access group in Environment tenant or be granted "Read and Execute (RX)" and "Read Permissions (E)" permissions for Environment tenant, if the application configured not in the Environment tenant; user should belong to some Administrator Access Group in application's tenant/tenants

   g. Click **Save**.

   h. The Confirmation dialog for changing the application's port opens. Click **Yes**.

   i. (Optional) Select the Options tab. In the [log] section, the all option is set to stdout by default. Enter a filename if you wish to enable logging to a file. For example, you can enter stdout, *C:\Logs\Knowledge\Knowledge_server* to force the system to write logs both to the console and to a file.



log (10 Items)

Affected Loggers	log	affectedLoggers	
All events	log	all	stdout
Expire	log	expire	3
Log level	log	verbose	standard
Logging pattern	log	outputPattern	%d{dd.MM.yyyy HH:mm:ss} %-5.5p | %-45.60t | %-30.1000c{1} %m ...
Segment	log	segment	1000
Standard	log	standard	stdout
Time format	log	time_format	time (HH:MM:SS.sss)
Time zone	log	time_convert	local
Trace	log	trace	stdout

Knowledge Center Server Application Logging Options

End

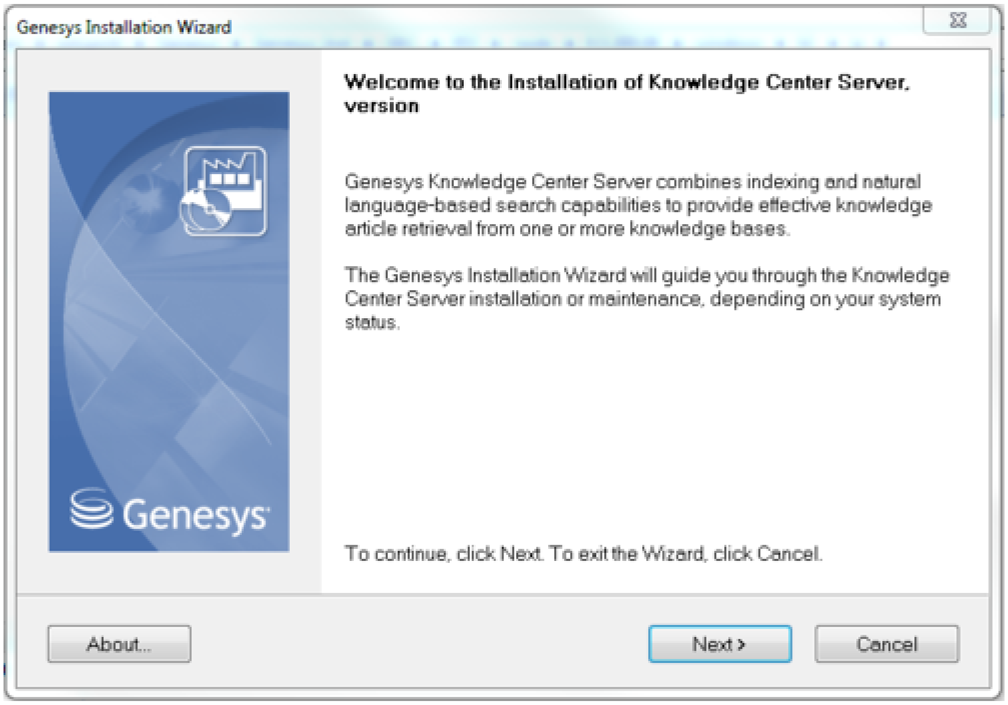
Installing Knowledge Center Server

Windows Installation Procedure

> **Important**
>
> From Knowledger Center Server version 8.5.302.04, you must install the Visual C++ Redistributable Packages run-time components which are required to run C++ applications on Windows.

Start

1. In your installation package, locate and double-click the *setup.exe* file. The Install Shield opens the welcome screen.



Genesys Installation Wizard

Welcome to the Installation of Knowledge Center Server, version

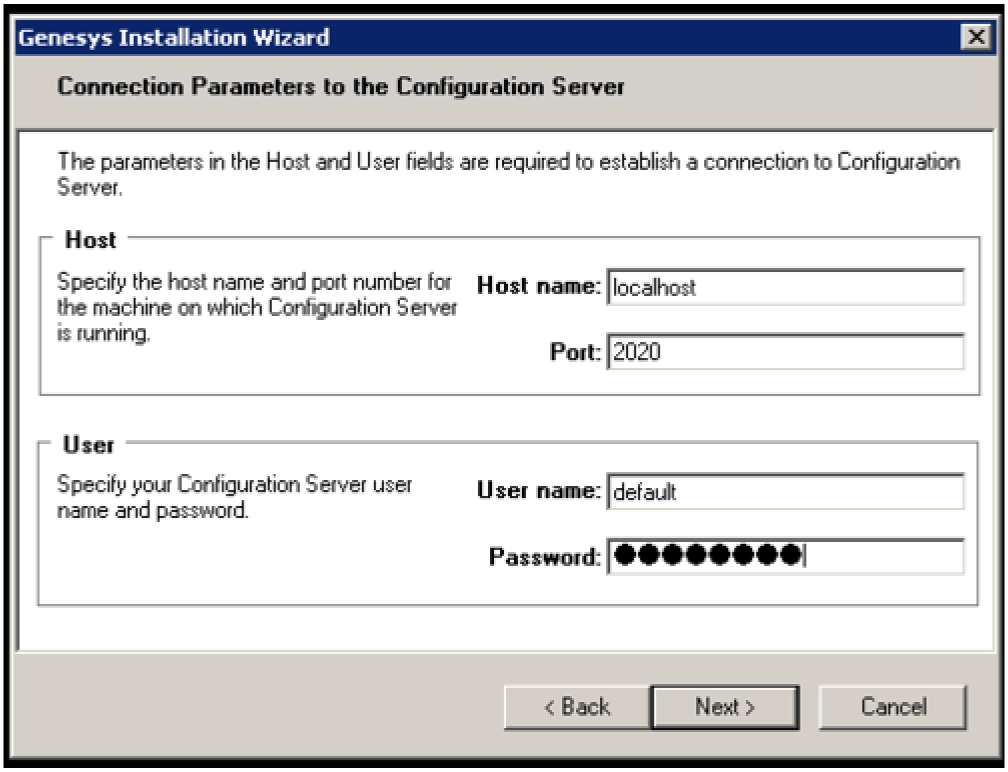
Genesys Knowledge Center Server combines indexing and natural language-based search capabilities to provide effective knowledge article retrieval from one or more knowledge bases.

The Genesys Installation Wizard will guide you through the Knowledge Center Server installation or maintenance, depending on your system status.

To continue, click Next. To exit the Wizard, click Cancel.

Knowledge Center Server Installation Window

2. Click **Next**. The **Connection Parameters to the Configuration Server** screen appears.



Genesys Installation Wizard

Connection Parameters to the Configuration Server

The parameters in the Host and User fields are required to establish a connection to Configuration Server.

Host

Specify the host name and port number for the machine on which Configuration Server is running.

Host name: localhost

Port: 2020

User

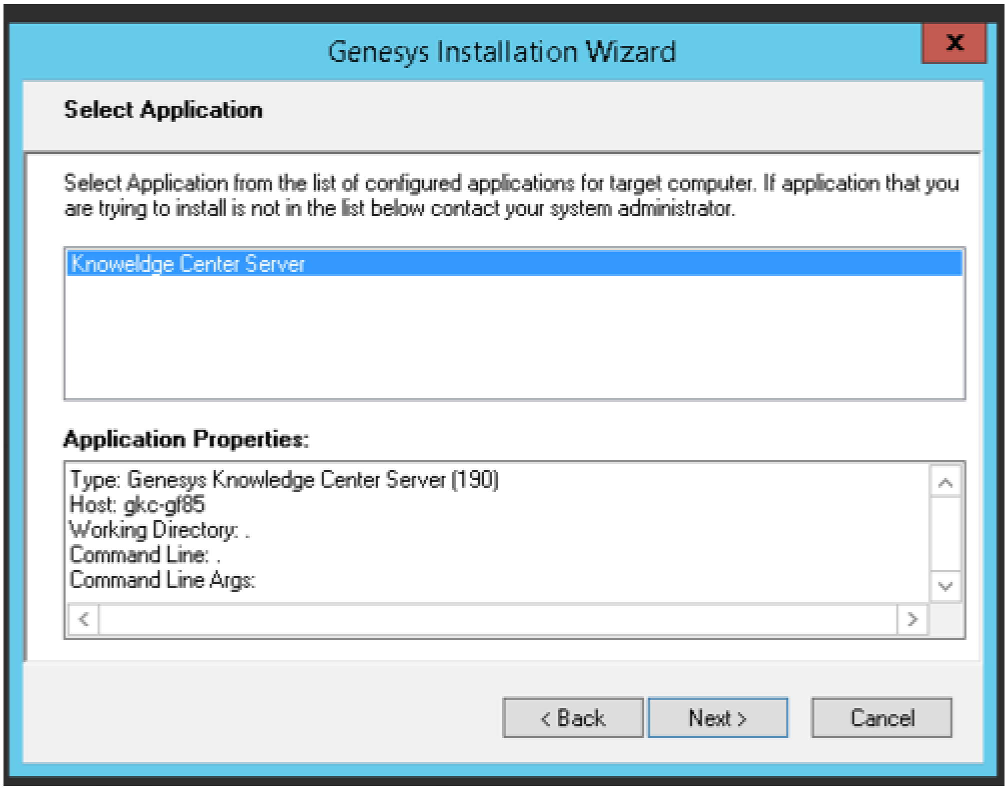
Specify your Configuration Server user name and password.

User name: default

Password: ●●●●●●●●

Knowledge Center Server Connection Parameters

3. Under **Host**, specify the host name and port number where Configuration Server is running. (This is the main listening port entered in the **Server Info** tab for Configuration Server.)
4. Under **User**, enter the user name and password for logging into Configuration Server.
5. Click **Next**. The **Select Application** screen appears.



Select Application from the list of configured applications for target computer. If application that you are trying to install is not in the list below contact your system administrator.

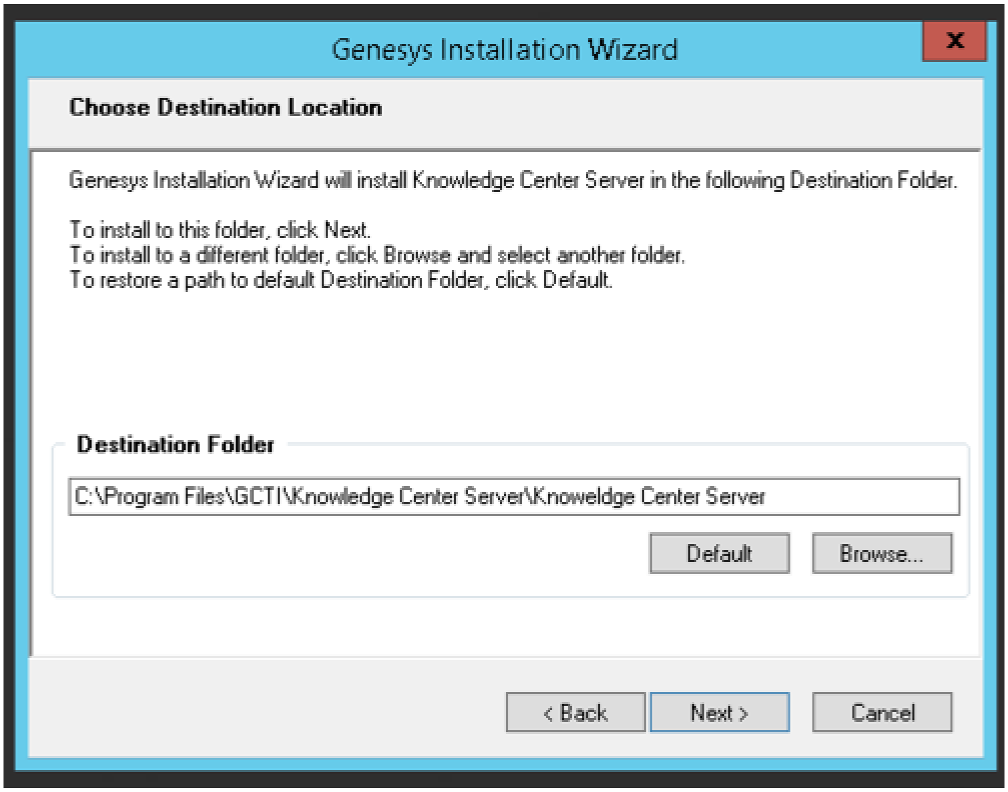
Knoweldge Center Server

Application Properties:

Type: Genesys Knowledge Center Server (190)
Host: gkc-gf85
Working Directory: .
Command Line: .
Command Line Args:

Selecting the Knowledge Center Server Application

6. Select the Knowledge Center Server application that you are installing. The **Application Properties** area shows the **Type**, **Host**, **Working Directory**, **Command Line executable**, and **Command Line Arguments** information previously entered in the **Server Info** and **Start Info** tabs of the selected Application object.
   Note: You might see "Reserved Application 6(190)" as the type under the application properties of the selected application. This happens when older versions of Configuration Server are used.
7. Click **Next**. The **Choose Destination Location** screen appears.



Genesys Installation Wizard will install Knowledge Center Server in the following Destination Folder.

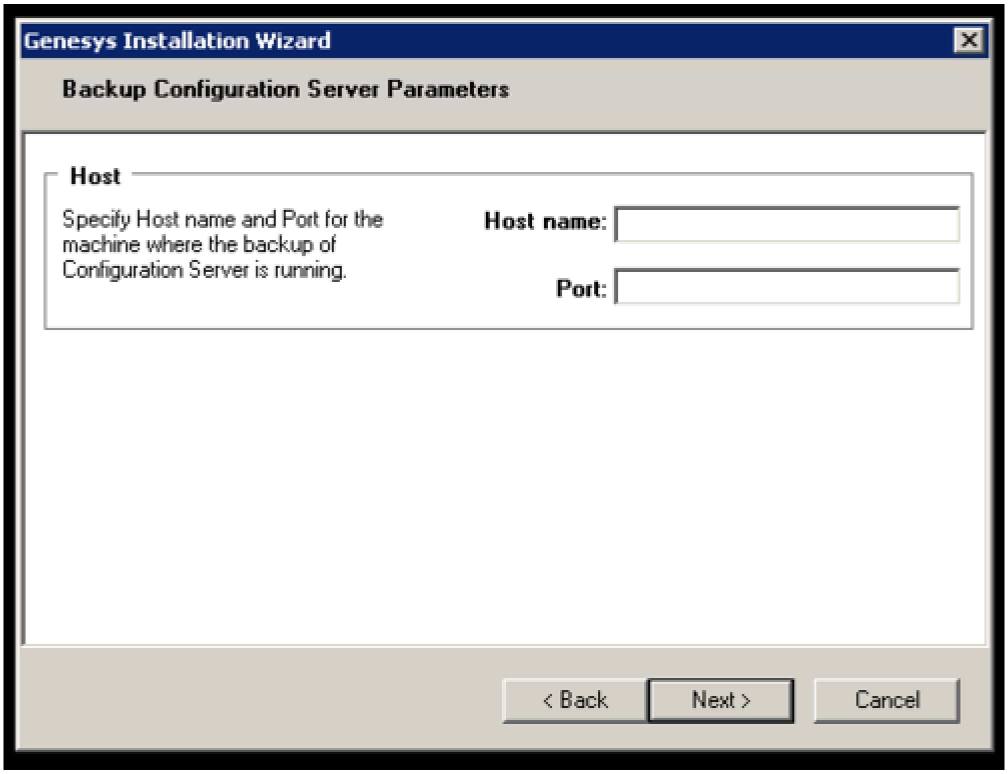
To install to this folder, click Next.
To install to a different folder, click Browse and select another folder.
To restore a path to default Destination Folder, click Default.

Destination Folder

C:\Program Files\GCTI\Knowledge Center Server\Knoweldge Center Server

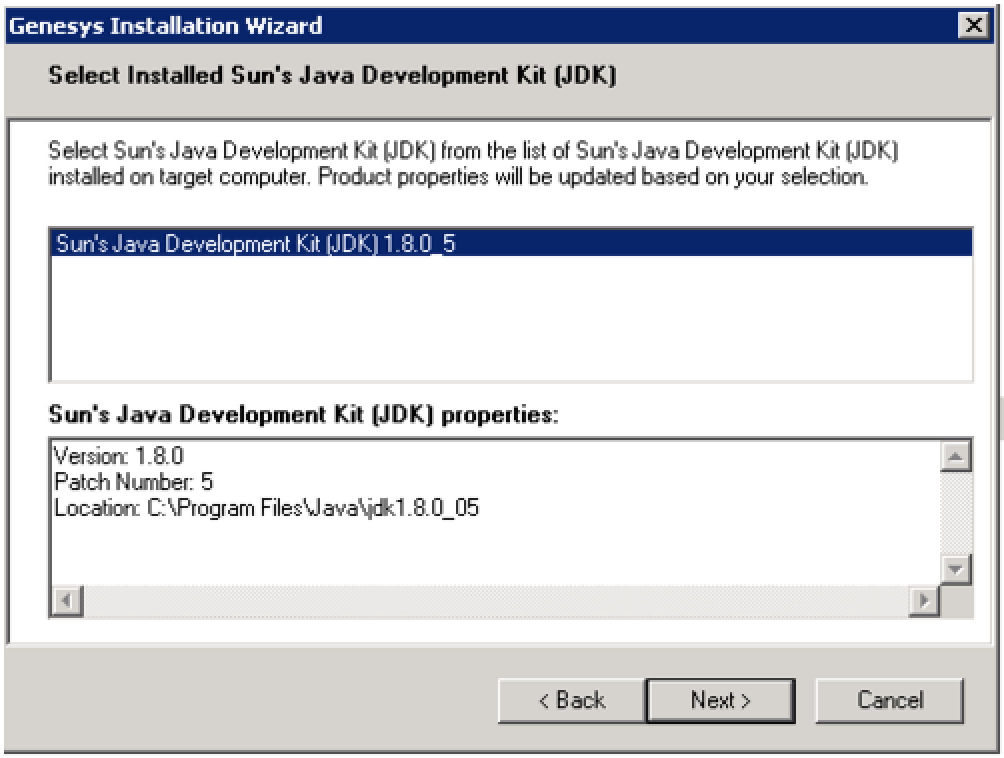
Choosing the Knowledge Center Server Installation Destination

8. Under **Destination Folder**, keep the default value or browse to the desired installation location.
9. Click **Next**. The **Backup Configuration Server Parameters** screen appears.


Genesys Installation Wizard
Backup Configuration Server Parameters
Host
Specify Host name and Port for the machine where the backup of Configuration Server is running.
Host name:
Port:
< Back
Next >
Cancel

Knowledge Center Backup Config Server Parameters

10. If you have a backup Configuration Server, enter the **Host name** and **Port**.
11. Click **Next**. Choose the appropriate version of the Java JDK.
    Note: Knowledge Center Server requires Java 1.8 or higher.



Genesys Installation Wizard

Select Installed Sun's Java Development Kit (JDK)

Select Sun's Java Development Kit (JDK) from the list of Sun's Java Development Kit (JDK) installed on target computer. Product properties will be updated based on your selection.

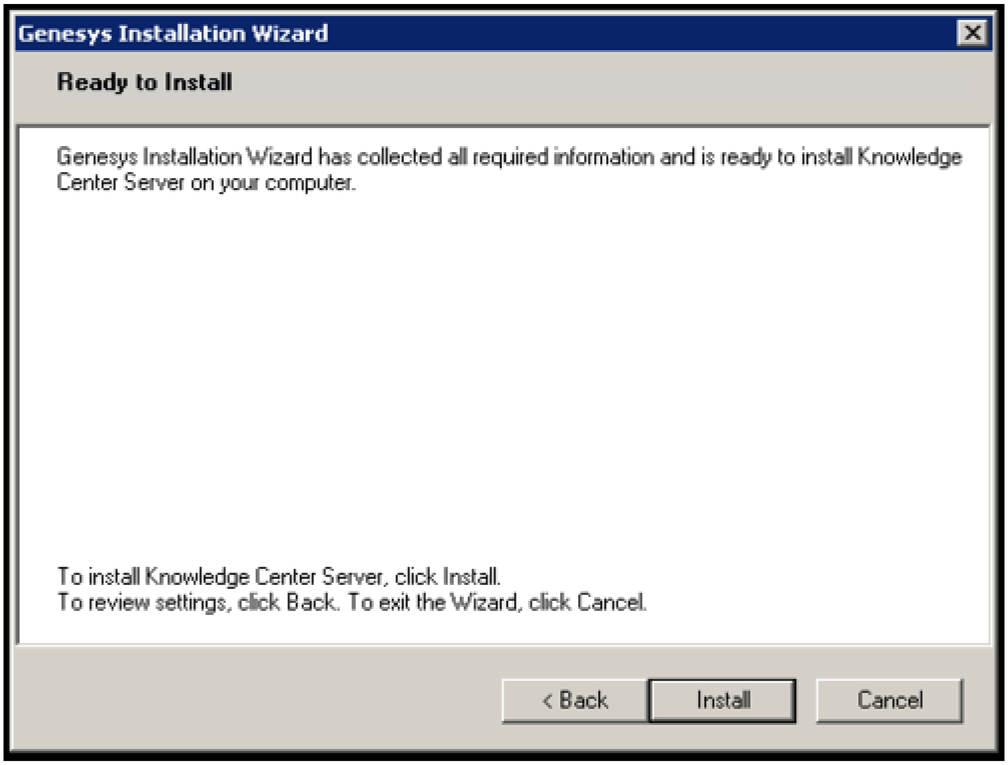
Sun's Java Development Kit (JDK) 1.8.0_5

Sun's Java Development Kit (JDK) properties:

Version: 1.8.0
Patch Number: 5
Location: C:\Program Files\Java\jdk1.8.0_05

Selecting the Knowledge Center Server Java Version

12. Click **Next**. The **Ready to Install** screen appears.



Genesys Installation Wizard

Ready to Install

Genesys Installation Wizard has collected all required information and is ready to install Knowledge Center Server on your computer.

To install Knowledge Center Server, click Install.
To review settings, click Back. To exit the Wizard, click Cancel.

Knowledge Center Server is Ready to Install

13. Click **Install**. The Genesys Installation Wizard indicates it is performing the requested operation. When through, the **Installation Complete** screen appears.
14. Click **Finish** to complete your installation.
15. Inspect the directory tree of your system to make sure that the files have been installed in the location that you intended.

End

Linux Installation Procedure

Start

1. Open a terminal in the Genesys Knowledge Center Server CD/DVD or the Genesys Knowledge Center Server installation package and run the install.sh file. The Genesys installation starts.
2. Enter the hostname of the host on which you are going to install.
3. Enter the connection information required to log in to the Configuration Server:
    a. Hostname—For instance, demosrv.genesyslab.com
    b. Listening port—For instance, 2020
    c. User name—For instance, demo
    d. Password
4. If you have a backup Configuration Server, enter the Host name and Port.
5. If the connection settings are successful, a list of keys and Genesys Knowledge Center Server applications is displayed.
6. Enter the key for the Genesys Knowledge Center Server application that you created previously on Configuration Server.
7. Enter the full path to your installation directory and confirm that it is correct.

If the installation is successful, the console displays the following message: *Installation of Genesys Knowledge Center Server, version 8.5.x has completed successfully.*

End

Installing multiple Server instances

To install multiple server instances you need to repeat following steps for every instance:

1. Create Server applications
2. Configuring the Knowledge Center Server Application
3. Installing Knowledge Center Server

Note: Knowledge Center Cluster Application is created just ones for all server instances working in the same cluster.

> **Important**
>
> It is advices to do not co-locate several Knowledge Center Server instances on the same host.

Geo-location database

- Database for Geo-IP Location (the way to translate client IP to its geographical location)
- On Windows, the path to */linguatools/geoip/GeoLite2-City.mmdb* can be changed in the *launcher.ini*' *file:* -DGEODB*.*
- On Linux, the path to */linguatools/geoip/GeoLite2-City.mmdb* can be changed in the '*setenv.sh* file under CUSTOM_JAVA_OPTS: *-DGEODB*.

Language Resources Configuration

- On Windows:
  - The path to */linguatools/freeling/data/* can be changed in the *launcher.ini* file: *-DFREELINGSHARE*.
  - The path to */linguatools/freeling/bin/* can be changed in the *launcher.ini* file: *-DFREELINGBIN*.
- On Linux:
  - The path to */linguatools/freeling/data/* can be changed in the *setenv.sh* file under CUSTOM_JAVA_OPTS:
    - *-DFREELINGSHARE* – Path to *Path to installation directory/linguatools/freeling/data*
    - *-DFREELINGBIN* – Path to *Path to installation directory/linguatools/freeling/bin*

Provide Knowledge Center Access to Agents

> **Tip**
>
> Access to a knowledge base may be limited by an agent's assigned skills (see Installing and Using the Administrator Plugin). Please add the appropriate skills so your agent may see the required knowledge bases (see Bulk Assignment of Skills to Agents for more information).

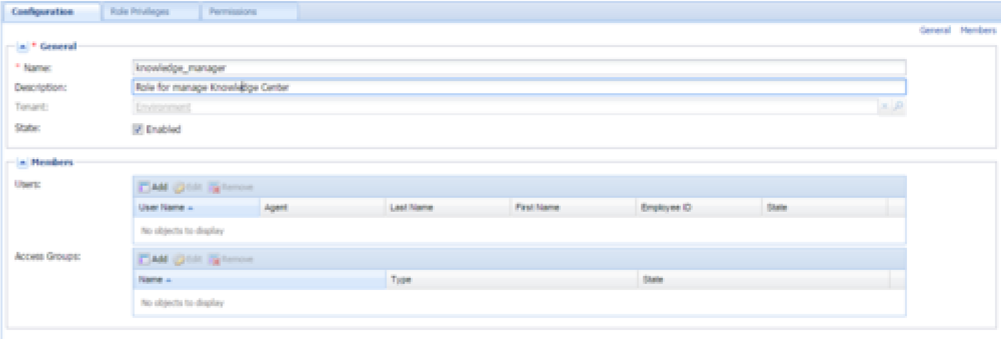
Genesys Knowledge Center supports the following privileges to restrict agent access:

- Allows agent to change data in a knowledge base (suggested for authors)
- Allows to bypass tenants restrictions (suggested for user configured in CMS for "Log On Account" in case of multi-tenant configuration)

To configure the appropriate privileges for an Agent:

Start

1. Go to **Provisioning > Accounts > Roles**.
2. In the taskbar, click **New** to create a new object.
3. Set the name of the role in the **General** section.



Name: knowledge_manager

Description: Role for manage Knowledge Center

Tenant: Environment

State: ☑ Enabled

Users:

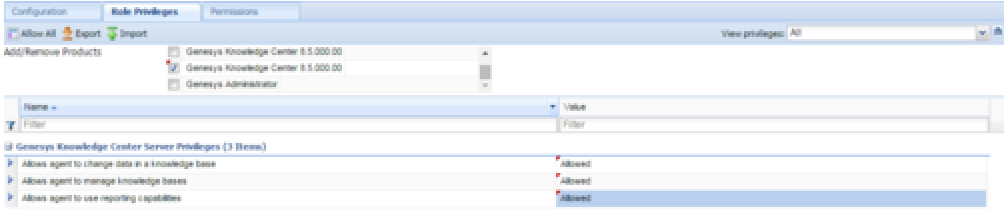
User Name	Agent	Last Name	First Name	Employee ID	State
No objects to display					

Access Groups:

Name	Type	State
No objects to display		

Knowledge Center Server Access Roles

4. Go to the **Role Privileges** tab and select the set of roles for Genesys Knowledge Center.
5. Open the list of privileges for Knowledge Center Server.
6. Set the appropriate privileges to **Allowed**.



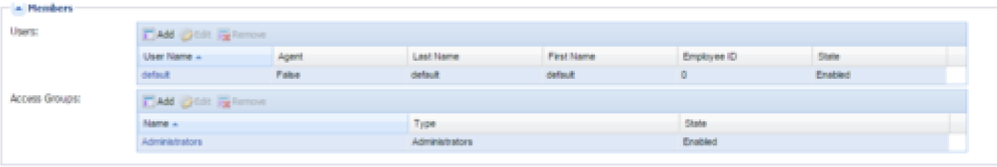
View privileges: All

Add/Remove Products:
□ Genesys Knowledge Center 8.5.000.00
☑ Genesys Knowledge Center 8.5.000.00
□ Genesys Administrator

Name	Value
Genesys Knowledge Center Server Privileges (3 Items)	
Allows agent to change data in a knowledge base	Allowed
Allows agent to manage knowledge bases	Allowed
Allows agent to use reporting capabilities	Allowed

Setting Knowledge Center Server Access Privileges

7. Go back to the **Configuration** tab.
8. In the **Members** section, add the appropriate Agent by clicking the **Add** button.



Users:

User Name	Agent	Last Name	First Name	Employee ID	State
default	False	default	default	0	Enabled

Access Groups:

Name	Type	State
Administrators	Administrators	Enabled

Knowledge Center Server Members Section

9. Save and Close.

End

Start and Stop Genesys Knowledge Center Server

Start the Server

Windows:

> ## Important
> You can start the Genesys Knowledge Center Server on Windows from:
>
> - Windows Services
> - The server.bat script
> - Genesys Administrator

Start

- You can start the server from Windows Services:
    1. Open Windows Services
    2. Select and start the Genesys Knowledge Center Server [Knowledge Center Server] service.
- You can use the provided server.bat script:
    1. Navigate to the Knowledge Center Server installation server directory and launch the Windows command console (cmd.exe).
    2. Open server directory
    3. Type and execute server.bat, without any parameters.

    > ## Important
    > You can use entry in the **Start > All Programs > Genesys Solutions > Knowledge Center Server [Knowledge Center Server]** menu to start the Server using server.bat

- You can start the server from Genesys Administrator:
    1. Navigate to PROVISIONING > Environment > Applications.
    2. Select the Knowledge Center Server.

3. Click Start applications in the Runtime panel.

End

The Genesys Knowledge Center Server is shown in Started status in Genesys Administrator.

Linux:

> Important
>
> You can start the Genesys Knowledge Center Server on Windows from:
>
> - The server.sh script
> - Genesys Administrator

Start

- You can use the provided server.sh script:
  1. Navigate to the Genesys Knowledge Center Server installation directory in the Unix command console.
  2. Go to server directory
  3. Type and execute server.sh, without any parameters.
- You can start the server from Genesys Administrator:
  1. Navigate to PROVISIONING > Environment > Applications.
  2. Select the Knowledge Center Server.
  3. Click Start applications in the Runtime panel.

End

The Genesys Knowledge Center Server is shown in Started status in Genesys Administrator.

After the Server start

After successful Server start you can use following URLs in your browser:

- http://<host>:<default_port>/gks-server - to access the Server REST API
- http://<host>:<default_port>/gks-sample-ui - to access Sample UI application shipped with product (**Note**: you need to load some data to be able to play with this application - reference on Quick Guide.)

Stop the Server

Windows:

> ### Important
> You can stop the Genesys Knowledge Center Server on Windows from:
>
> - Windows Services
> - Genesys Administrator
> - A console window

Start

- You can stop the server from Windows Services:
  1. Open Windows Services
  2. Select and stop the Knowledge Center Server service.
- You can stop the server from Genesys Administrator:
  1. Navigate to PROVISIONING > Environment > Applications.
  2. Select the Knowledge Center Server.
  3. Click Stop applications in the Runtime panel.
- If you previously started Genesys Knowledge Center Server in a console window, you can stop the server by closing the window or navigate to Genesys Knowledge Center Server installation directory in Windows console (cmd.exe), open server directory and execute comand: server.bat stop

End

The Genesys Knowledge Center Server is shown in Stopped status in Genesys Administrator.

Linux:

> ### Important
> You can stop the Genesys Knowledge Center Server on Linux from:
>
> - Genesys Administrator
> - A console window

Start

- can stop the server from Genesys Administrator:
    1. Navigate to PROVISIONING > Environment > Applications.
    2. Select the Knowledge Center Server.
    3. Click Stop applications in the Runtime panel.
- Or you can stop the server from the console window where it was started:
    1. Press Ctrl+C while the window is active.
    2. Type Y and press Enter.
- Or you could use provided script server.sh:
    1. Navigate to the Genesys Knowledge Center Server installation directory in the Unix command console.
    2. Go to server directory
    3. Type and execute server.sh with parameter "stop" (for example: server.sh stop)

End

The Genesys Knowledge Center Server is shown in Stopped status in Genesys Administrator.

Installing the Knowledge Center CMS

This chapter describes the process of installing and configuring Knowledge Center CMS that includes following steps:

- Importing the CMS Application Template
- Creating and configuring CMS Application in Genesys Administrator
- Configuring the Data Source
- Installing the CMS
- Granting your agents authoring privileges
- Starting/Stopping the installed CMS application

Before you proceed with these steps you need:

- Configure Knowledge Center Cluster application
- Select and install one of the Relational Database Management Systems (RDBMS) from the supported link
- Configure the load-balancer for access to CMS

Knowledge Center CMS support one of the following RDBMS as persistent storage:

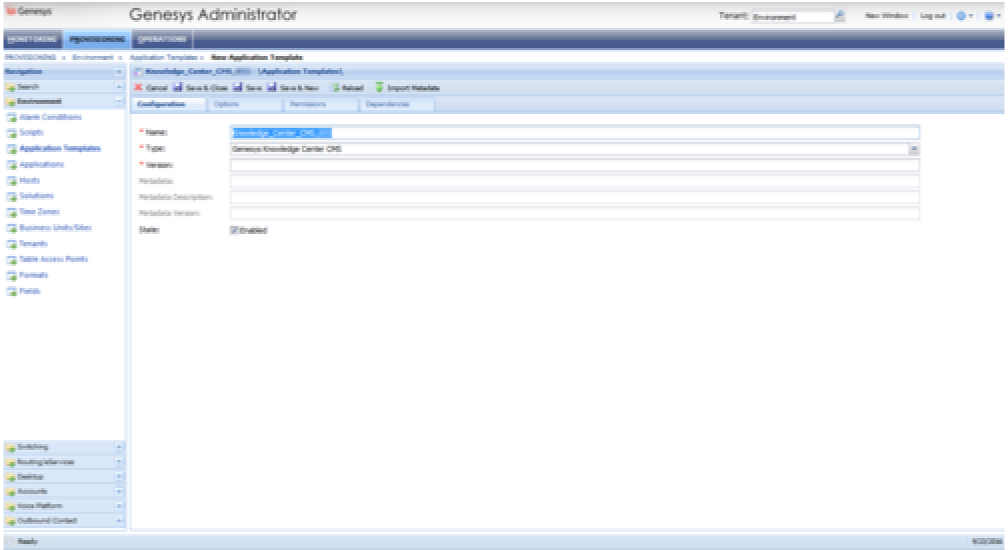
- Microsoft SQL Server 2012
- Oracle 11g
- PostgreSQL

Install the CMS

Import the CMS Application Template

Start

1. Open Genesys Administrator and navigate to **Provisioning > Environment > Application Templates**.
2. In the **Tasks** panel, click **Upload Template**.
3. In the **Click 'Add' and choose application template (APD) file to import** window, click **Add**.
4. Browse to the *Knowledge_Center_CMS.apd* file available in the templates directory of your installation CD. The **New Application Template** panel opens.



* Name: Knowledge_Center_CMS_

* Type: Genesys Knowledge Center CMS

* Version:

Metadata:

Metadata Description:

Metadata Version:

State: ☑ Enabled

The Knowledge Center CMS Application Template

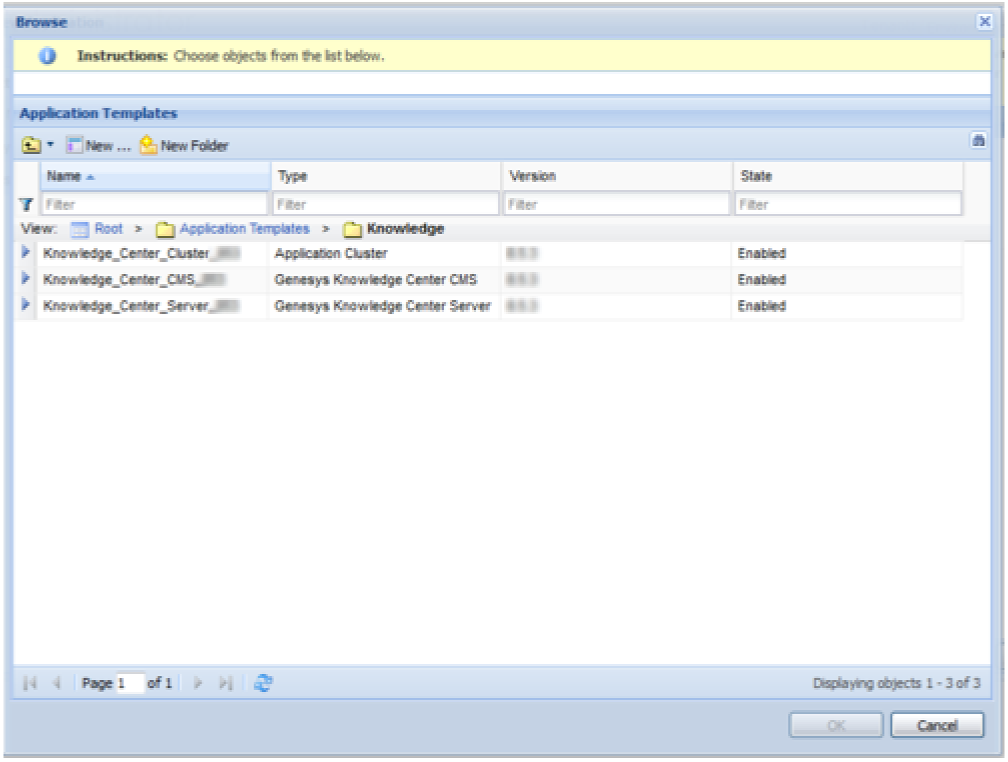
5. Click **Save and Close**.

End

Create CMS Applications

Start

1. Open Genesys Administrator and navigate to **Provisioning > Environment > Applications**.
2. In the **Tasks** panel, click **Create New Application**.
3. In the **Select Application Template** panel, click **Browse for Template** and select the Genesys Knowledge Center CMS application template that you imported earlier. Click **OK**.



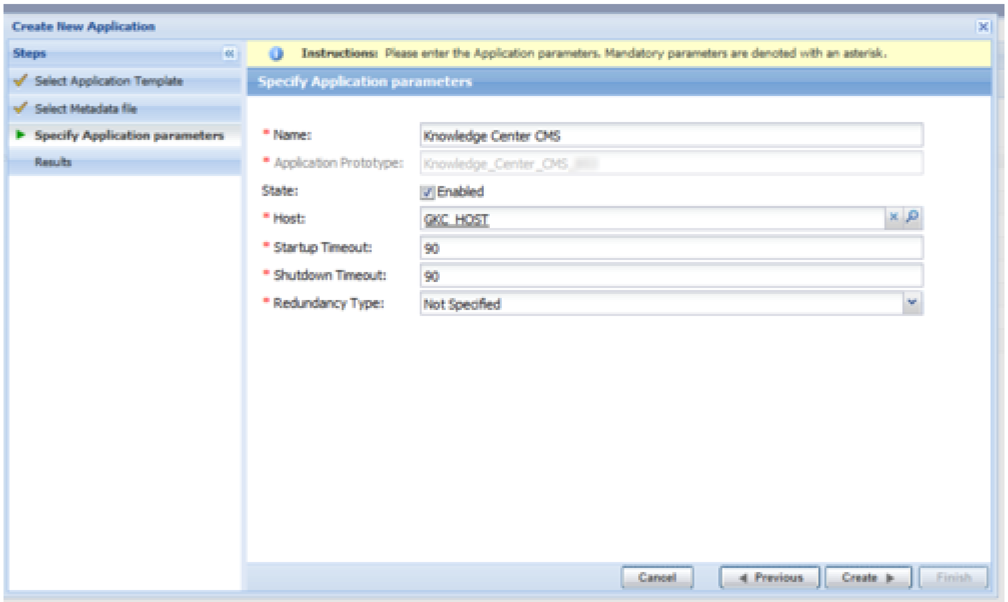
Instructions: Choose objects from the list below.

Name	Type	Version	State
Knowledge_Center_Cluster_[illegible]	Application Cluster	[illegible]	Enabled
Knowledge_Center_CMS_[illegible]	Genesys Knowledge Center CMS	[illegible]	Enabled
Knowledge_Center_Server_[illegible]	Genesys Knowledge Center Server	[illegible]	Enabled

Displaying objects 1 - 3 of 3

Selecting the Knowledge Center CMS Template

4. The template is added to the **Select Application Template** panel. Click **Next**.
5. In the **Select Metadata** file panel, click **Browse** and select the *Knowledge_Center_CMS.xml* file. Click **Open**.
6. The metadata file is added to the **Select Metadata** file panel. Click Next.
7. In **Specify the appropriate application parameters**:
    a. Enter a name for your application. For instance, *Knowledge Center CMS*.
    b. Enable the **State**.
    c. Select the Host on which the CMS will reside.
    d. Click **Create**.



Create New Application
Steps
✓ Select Application Template
✓ Select Metadata file
▶ Specify Application parameters
Results

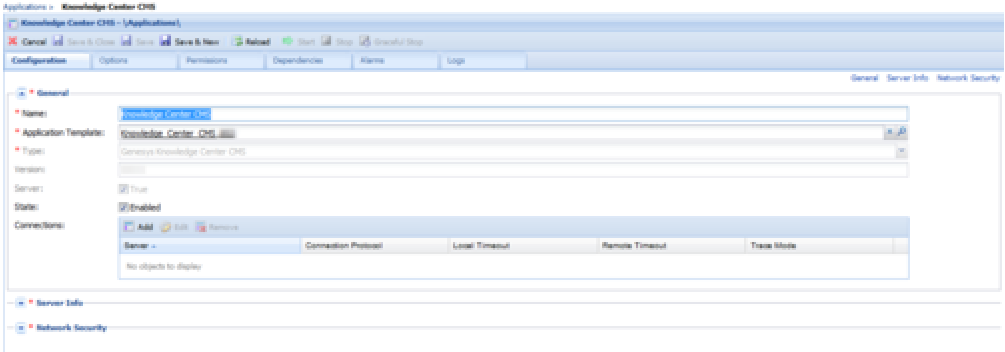
Instructions: Please enter the Application parameters. Mandatory parameters are denoted with an asterisk.

Specify Application parameters

* Name:	Knowledge Center CMS
* Application Prototype:	Knowledge_Center_CMS_[redacted]
State:	☑ Enabled
* Host:	GKC_HOST
* Startup Timeout:	90
* Shutdown Timeout:	90
* Redundancy Type:	Not Specified

Creating the Knowledge Center CMS Application

5. The **Results** panel opens.
6. Enable **Opens the Application details form after clicking 'Finish'** and click **Finish**. The Knowledge Center CMS application form opens and you can start configuring the CMS application.



* Name:	Knowledge Center CMS
* Application Template:	Knowledge_Center_CMS_[redacted]
* Type:	Genesys Knowledge Center CMS
Version:	[redacted]
Server:	☑ True
State:	☑ Enabled
Connections:	

Server	Connection Protocol	Local Timeout	Remote Timeout	Trace Mode
No objects to display				

Configuring the Knowledge Center CMS

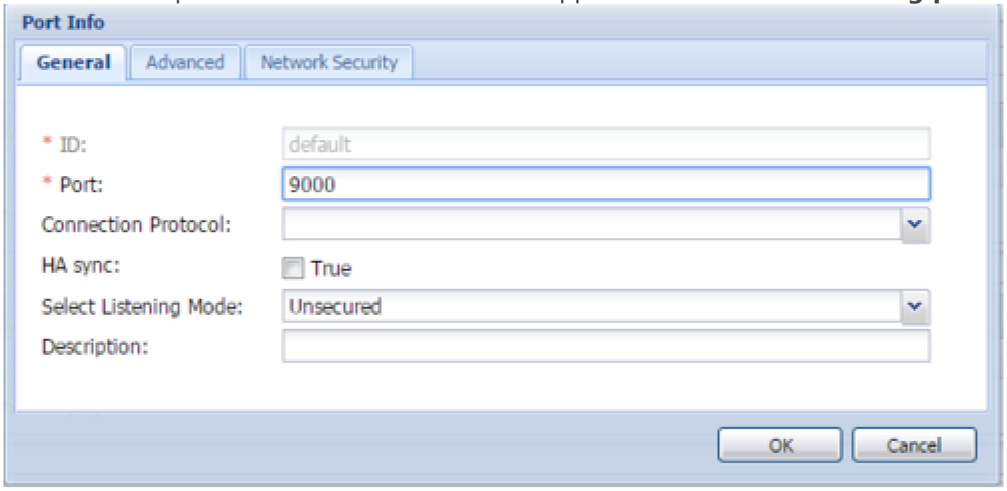
End

Configure the CMS Application

Start

1. If your Knowledge Center CMS application form is not open in Genesys Administrator, navigate to **Provisioning > Environment > Applications**. Select the application defined for the Knowledge Center CMS and click **Edit...**.
2. In the **Connections** section of the **Configuration** tab, click **Add**. The **Browse for applications** panel opens.
3. Select the Knowledge Center Cluster application, then click **OK**.

4. Expand the **Server Info** pane.
5. If your Host is not defined, click the lookup icon to browse to the hostname of your application.
6. In the **Listening Ports** section, create the default port by clicking **Add**. The **Port Info** dialog opens.
   a. Enter the **Port**. For instance, 9000.
   b. Choose *http* or "https" for the **Connection Protocol**.
   c. If you will be using a secure connection to the cluster, choose *Secured* for the **Select Listening Mode**.
   d. Click **OK**. The port with the default identifier appears in the list of **Listening ports**.

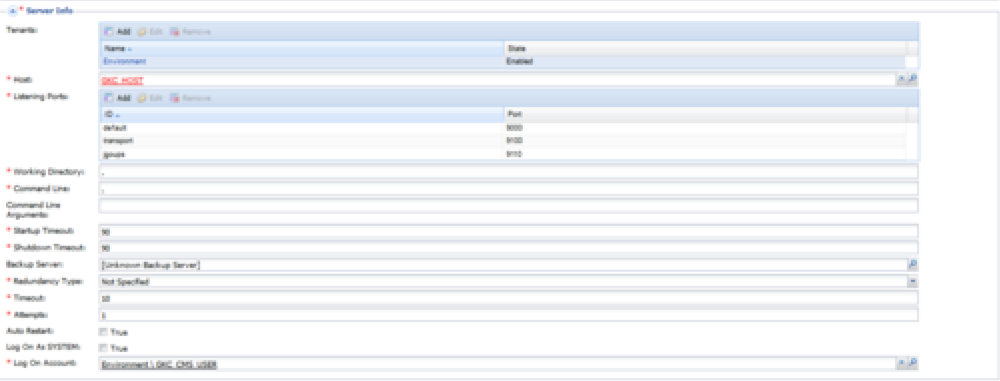


* ID: default
* Port: 9000
Connection Protocol:
HA sync: □ True
Select Listening Mode: Unsecured
Description:

Knowledge Center CMS Port Information

7. Add a port that will be used by Knowledge Center CMS nodes to communicate to each other by clicking on **Add** and:
   a. entering *clustering* in the **ID** field
   b. entering the **Port**. For instance, 9150.
   c. Clicking **OK**
8. In the **Tenants** section, add a working tenant by clicking **Add**. Browse and choose the appropriate tenant in the pop-up dialog. Click **OK**.
9. Uncheck **Log On As SYSTEM**.
10. In **Log On Account** specify the user account that:
    - has the ability to view access groups (this is required if you use access groups to set privileges for your agents)
    - has **Knowledge.AUTHOR** (Allows agent to change data in a knowledge base) privilege and **Knowledge.MULTITENANT** (Allows to bypass tenants restrictions) in case multi-tenant configuration (required for scheduled synchronization)
    - User should have access to the same tenant/tenants in which that CMS is configured
    - User should be granted "Read and Execute (RX)" and "Read Permissions (E)" permissions for Environment tenant, if the application configured not in the Environment tenant; user should belong to Administrators Access Group in CMS tenants (required for scheduled synchronization)

14. Click **Save**.
15. The **Confirmation** dialog for changing the application's port opens. Click **Yes**.



* Server Info

Tenants:

Name	State
Environment	Enabled

* Host: GKC_HOST

* Listening Ports:

ID	Port
default	9000
transport	9100
[illegible]	9110

* Working Directory: .

* Command Line: .

Command Line Arguments:

* Startup Timeout: 90

* Shutdown Timeout: 90

Backup Server: [Unknown Backup Server]

* Redundancy Type: Not Specified

* Timeout: 10

* Attempts: 1

Auto Restart: □ True

Log On As SYSTEM: □ True

* Log On Account: Environment\GKC_CMS_USER

Knowledge Center CMS Information

16. Go to **Application Cluster** application, open **Options** tab. In section cms.general set valid URL to CMS or CMS cluster load balancer in externalURL option (for example, http://<cms host>:<CMS default port>/gks-cms).

End

Configure Data Source

Knowledge Center CMS requires persistent storage to be configured to store all the authored content. Please follow one of the instructions to set up storage of your choice:

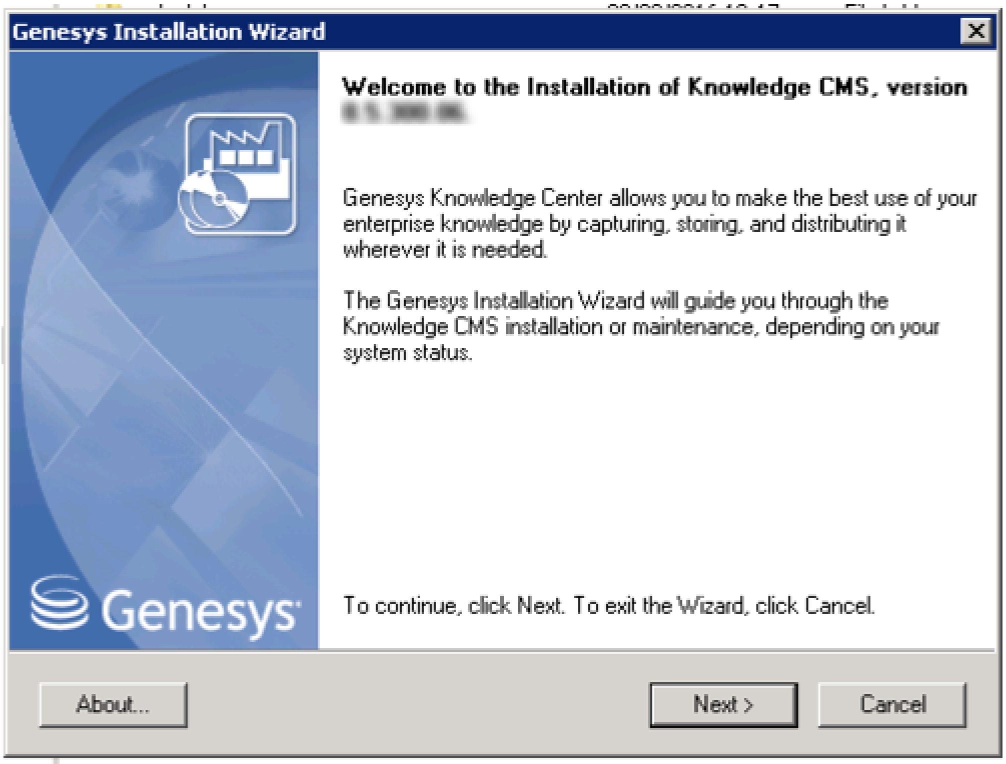
- Microsoft SQL Server - Using CMS with Microsoft SQL Server
- Oracle - Using CMS with Oracle
- PostgreSQL - Using CMS with PostgreSQL

Installing the CMS

Windows Installation Procedure

Start

1. In your installation package, locate and double-click the *setup.exe* file. The Install Shield opens the welcome screen.



Genesys Installation Wizard

Welcome to the Installation of Knowledge CMS, version [redacted]

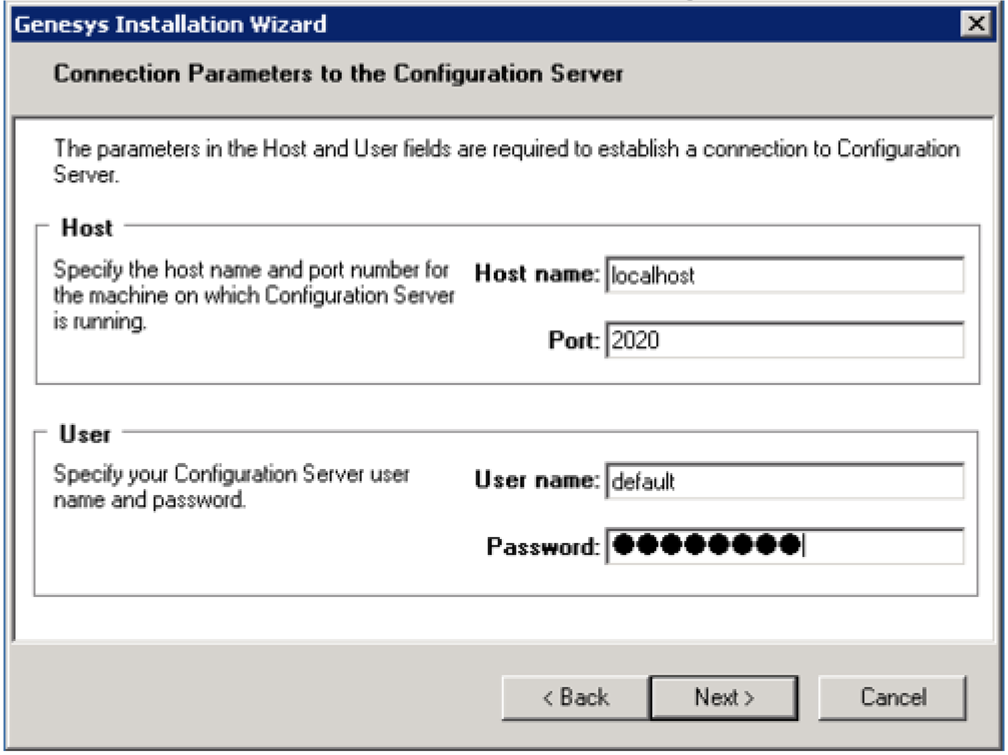
Genesys Knowledge Center allows you to make the best use of your enterprise knowledge by capturing, storing, and distributing it wherever it is needed.

The Genesys Installation Wizard will guide you through the Knowledge CMS installation or maintenance, depending on your system status.

To continue, click Next. To exit the Wizard, click Cancel.

Knowledge Center CMS installation Window

2. Click **Next**. The **Connection Parameters to the Configuration Server** screen appears.



Genesys Installation Wizard

Connection Parameters to the Configuration Server

The parameters in the Host and User fields are required to establish a connection to Configuration Server.

Host

Specify the host name and port number for the machine on which Configuration Server is running.

Host name: localhost

Port: 2020

User

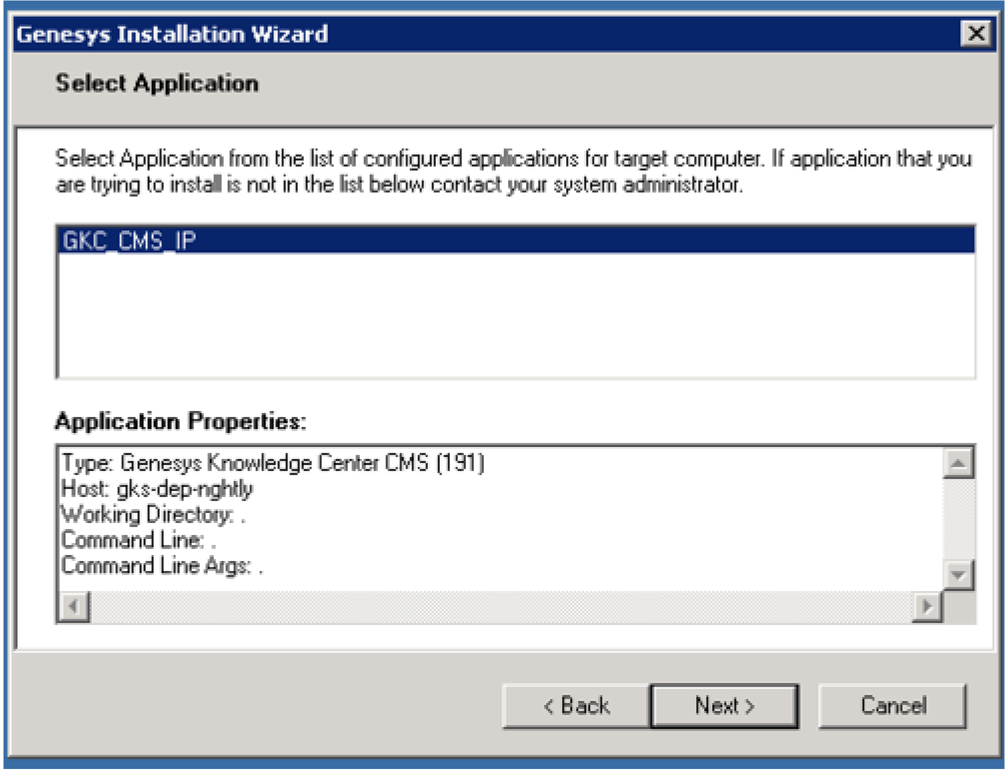
Specify your Configuration Server user name and password.

User name: default

Password: ●●●●●●●●

Knowledge Center CMS Connection Parameters

3. Under **Host**, specify the host name and port number where Configuration Server is running. (This is the main listening port entered in the **Server Info** tab for Configuration Server.)
4. Under **User**, enter the user name and password for logging in to Configuration Server.
5. Click **Next**. The **Select Application** screen appears.
6. Select the Knowledge Center CMS that you are installing. The **Application Properties** area shows the **Type**, **Host**, **Working Directory**, **Command Line executable**, and **Command Line Arguments** information previously entered in the **Server Info** and **Start Info** tabs of the selected application object.



Select Application from the list of configured applications for target computer. If application that you are trying to install is not in the list below contact your system administrator.

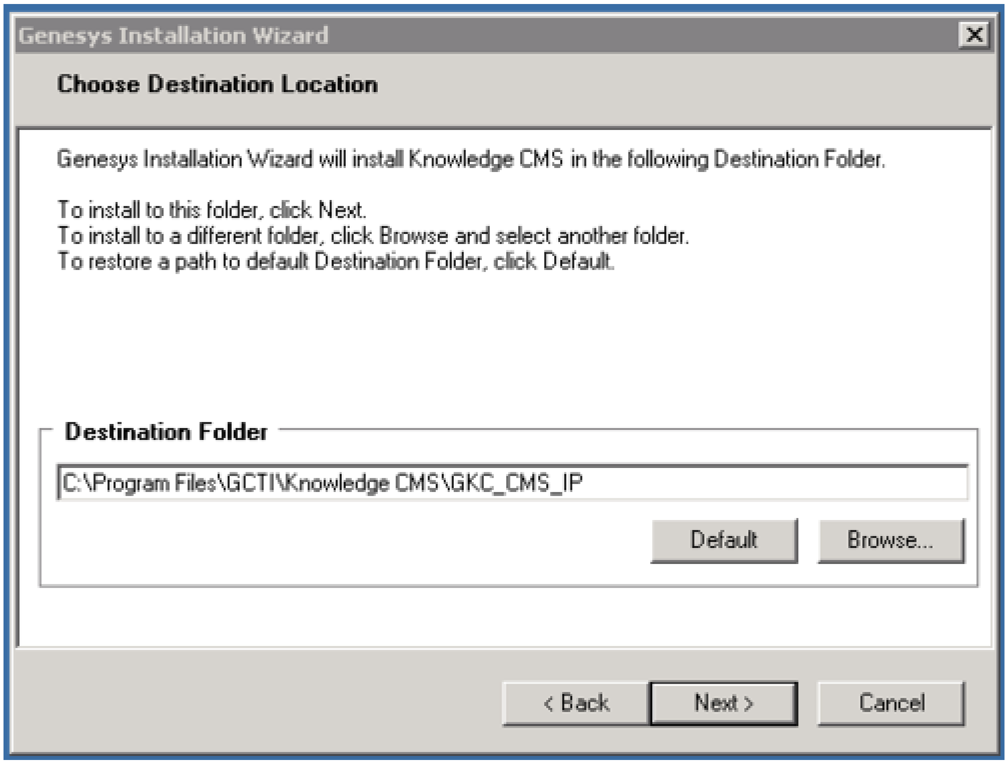
GKC_CMS_IP

Application Properties:

Type: Genesys Knowledge Center CMS (191)
Host: gks-dep-nghtly
Working Directory: .
Command Line: .
Command Line Args: .

Selecting the Knowledge Center CMS Application

7. Click **Next**. The **Choose Destination Location** screen appears.
8. Under **Destination Folder**, keep the default value or browse for the desired installation location.



Choose Destination Location

Genesys Installation Wizard will install Knowledge CMS in the following Destination Folder.

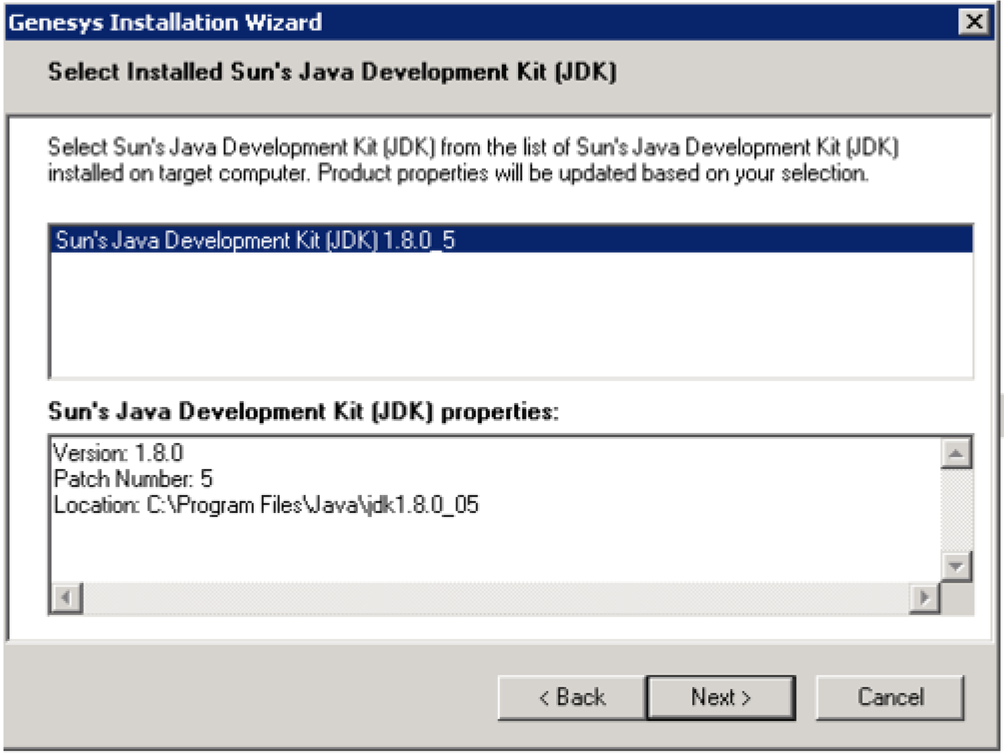
To install to this folder, click Next.
To install to a different folder, click Browse and select another folder.
To restore a path to default Destination Folder, click Default.

Destination Folder

C:\Program Files\GCTI\Knowledge CMS\GKC_CMS_IP

Choosing the Knowledge Center CMS Installation Destination

9. Click **Next**. Choose the appropriate version of the Java JDK.
   Note: Knowledge Center Server requires Java 1.8 or higher.



Select Installed Sun's Java Development Kit (JDK)

Select Sun's Java Development Kit (JDK) from the list of Sun's Java Development Kit (JDK) installed on target computer. Product properties will be updated based on your selection.

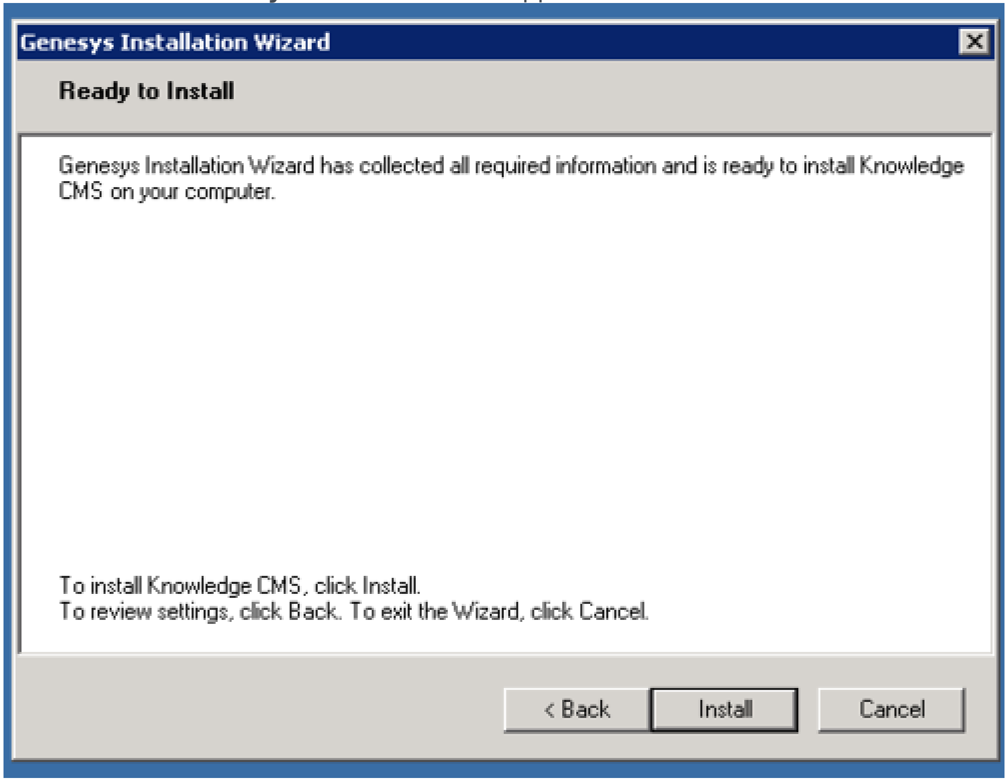
Sun's Java Development Kit (JDK) 1.8.0_5

Sun's Java Development Kit (JDK) properties:

Version: 1.8.0
Patch Number: 5
Location: C:\Program Files\Java\jdk1.8.0_05

Selecting the Knowledge Center CMS Java Version

10. Click **Next**. The **Ready to Install** screen appears.



Genesys Installation Wizard has collected all required information and is ready to install Knowledge CMS on your computer.

To install Knowledge CMS, click Install.
To review settings, click Back. To exit the Wizard, click Cancel.

Knowledge Center Knowledge Center is Ready to Install

11. Click **Install**. The Genesys Installation Wizard indicates it is performing the requested operation for the Genesys Knowledge Center CMS. When through, the **Installation Complete** screen appears.
12. Click **Finish** to complete your installation.
13. Inspect the directory tree of your system to make sure that the files have been installed in the location that you intended.

End

Linux Installation Procedure

Start

1. Open a terminal in the CMS installation package, and run the *install.sh* file. The Genesys installation starts.
2. Enter the hostname of the host on which you are going to install.
3. Enter the connection information required to log in to the Configuration Server:
   a. **Hostname**—For instance, *demosrv.genesyslab.com*
   b. **Listening port**—For instance, *2020*
   c. **User name**—For instance, *demo*
   d. **Password**

4. If you have a backup Configuration Server, enter the Host name and Port.
5. If the connection settings are successful, a list of keys and Knowledge Center CMS applications is displayed.
6. Enter the key for the Knowledge Center CMS application that you created previously in Configuration Server.
7. Enter the full path to your installation directory and confirm that it is correct.
8. If the installation is successful, the console displays the following message:
Installation of Genesys Knowledge CMS has completed successfully.

End

Installing multiple CMS instances

To install multiple CMS instances you need to repeat following steps for every instance:

1. Create CMS applications
2. Configuring the Knowledge Center CMS Application
3. Installing Knowledge Center CMS

Note: Knowledge Center Cluster Application is created just ones for all CMS instances working in the same cluster.

Granting Agents Authoring Privileges

Genesys Knowledge Center supports the following privileges to restrict agent access:

- Administrator (allows a user to carry out Administrator tasks such as creating and editing Knowledge bases)
- Approver (allows a user to Approve and Publish documents)
- Category Author (allows a user to create and update categories)
- Document Author (allows a user to create and update documents)
- Multitenant user (allows a user to work with data in all tenants in the CMS)

Important

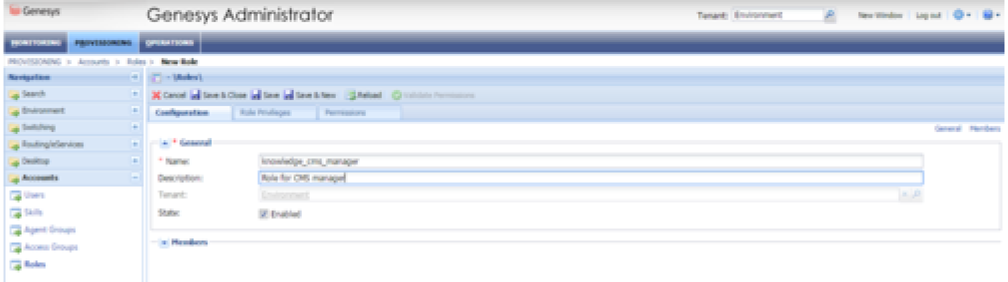
Only agents who have both Document Author and Category Author privileges can successfully import data from XML files into CMS.
To publish document from CMS to Knowledge Server agent also should have "Allows

> agent to change data in a knowledge base" privilege on Knowledge Server (link to Provide Knowledge Center Access to Agents in Server installation page)

To configure the appropriate privileges for an agent:

Start

1. Go to **Provisioning > Accounts > Roles.**
2. In the taskbar, click **New** to create a new object.
3. Set the name of the role in the **General** section.



* General

* Name: knowledge_cms_manager

Description: Role for CMS manager

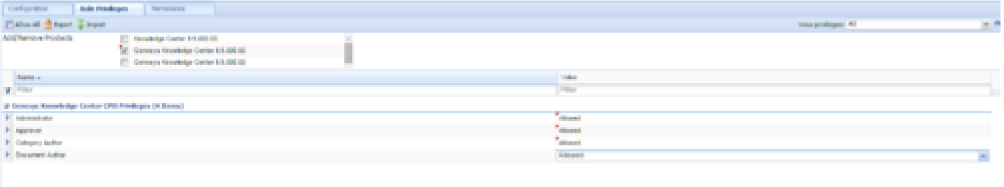
Tenant: Environment

State: ☑ Enabled

Members

Knowledge Center CMS Access Roles

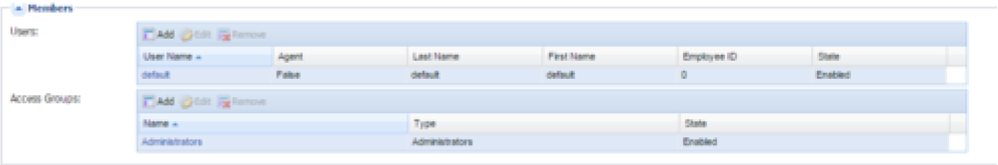
4. Go to the **Role Privileges** tab and select the set of roles for Genesys Knowledge Center.
5. Open the Genesys Knowledge Center CMS privileges list.
6. Set the appropriate privileges to **Allowed**.



Name	Value
Genesys Knowledge Center CMS Privileges (4 Items)	
Administrator	Allowed
Approver	Allowed
Category Author	Allowed
Document Author	Allowed

Setting Knowledge Center CMS Access Privileges

7. Go back to the **Configuration** tab.
8. In the **Members Section**, add the appropriate Agent by clicking the **Add** button.



Users:

User Name	Agent	Last Name	First Name	Employee ID	State
default	False	default	default	0	Enabled

Access Groups:

Name	Type	State
Administrators	Administrators	Enabled

Knowledge Center CMS Members Section

9. Save and Close.

End

Start and Stop Genesys Knowledge Center CMS

Start the CMS

Windows:

> **Important**
>
> You can start the Genesys Knowledge Center CMS on Windows from:
>
> - Windows Services
> - the server.bat script
> - Genesys Administrator

Start

- You can start the server from Windows Services.
  1. Open Windows Services
  2. Select and start the Genesys Knowledge Center CMS [Knowledge Center CMS] service.
- You can use the provided server.bat script.
  1. Navigate to the Knowledge Center CMS installation server directory and launch the Windows command console (cmd.exe).
  2. Open server directory
  3. Type and execute server.bat, without any parameters.

  > **Important**
  >
  > You can use entry in the Start > All Programs > Genesys Solutions > Knowledge Center CMS [Knowledge Center CMS] menu to start the Server using server.bat

- You can start the server from Genesys Administrator.
  1. Navigate to PROVISIONING > Environment > Applications.
  2. Select the Knowledge Center CMS
  3. Click Start applications in the Runtime panel.

End

The Genesys Knowledge Center CMS is shown in Started status in Genesys Administrator.

Linux:

> ### Important
> You can start the Genesys Knowledge Center CMS on Windows from:
>
> - the server.sh script
> - Genesys Administrator

Start

- You can use the provided server.sh script.
  1. Navigate to the Genesys Knowledge Center CMS installation directory in the Unix command console.
  2. Go to server directory
  3. Type and execute server.sh, without any parameters.
- You can start the server from Genesys Administrator
  1. Navigate to **PROVISIONING** > **Environment** > **Applications**.
  2. Select the Knowledge Center CMS.
  3. Click **Start applications** in the **Runtime** panel.

End
The Genesys Knowledge Center CMS is shown in Started status in Genesys Administrator.

After the CMS start

After successful CMS start you can use following URLs in your browser:

- http://<cms host>:<CMS default port>/gks-cms - to access the CMS user interface

Stop the CMS

Windows:

> ### Important
> You can stop the Genesys Knowledge Center CMS on Windows from:
>
> - Windows Services
> - Genesys Administrator

> - A console window

Start

- You can stop the server from Windows Services.
  1. Open Windows Services
  2. Select and stop the Knowledge Center CMS service.
- You can stop the server from Genesys Administrator.
  1. Navigate to **PROVISIONING** > **Environment** > **Applications**.
  2. Select the Knowledge Center CMS.
  3. Click **Stop applications** in the **Runtime** panel.
- If you previously started Genesys Knowledge Center CMS in a console window, you can stop the server by closing the window or navigate to Genesys Knowledge Center CMS installation directory in Windows console (cmd.exe), open server directory and execute command: server.bat stop

End
The Genesys Knowledge Center CMS is shown in Stopped status in Genesys Administrator.

Linux:

> ### Important
> You can stop the Genesys Knowledge Center CMS on Linux from:
>
> - Genesys Administrator
> - A console window

Start

- You can stop the server from Genesys Administrator.
  1. Navigate to **PROVISIONING** > **Environment** > **Applications**.
  2. Select the Knowledge Center CMS.
  3. Click **Stop applications** in the **Runtime** panel.
- Or you can stop the server from the console window where it was started.
  1. Press Ctrl+C while the window is active.
  2. Type Y and press Enter.

- Or you could use provided script server.sh:
    1. Navigate to the Genesys Knowledge Center CMS installation directory in the Unix command console.
    2. Go to server directory
    3. Type and execute server.sh with parameter "stop" (for example: server.sh stop)

End
The Genesys Knowledge Center CMS is shown in Stopped status in Genesys Administrator.

Using CMS with Microsoft SQL Server

Prerequisites

- Create new database in Microsoft SQL Server
- Create user account to access the database

Configuring CMS

1. Open Genesys Administrator and navigate to **Provisioning > Environment > Applications**
2. Select the application defined for the Knowledge Center Cluster and click **Edit**
3. From the **Options** tab in the **cms.cluster** section, set the following options:
   a. set option **type** to value **mssql**

      > ### Important
      > if you are using version 8.5.300.xx, please type **jdbc** instead of **mssql**

   b. set **dbConnectionUrl** to JDBC connection string for connection to MS SQL Server following the format:
      `jdbc:sqlserver://<host_of_MSSQL_Server>:<port_of_MSSQL_Server, 1433 by default>;databaseName=<CMS_DB_name>`

   c. **dbUsername** - set to the username that needs to be used to login to MS SQL Server

   d. **dbPassword** - set to the password for db account

   e. **dbDriverClass** - set to **net.sourceforge.jtds.jdbc.Driver**

> ### Important
> Description of options in cms.cluster section can be found in Configuration Options.

If you are installing Knowledge Center CMS 8.5.302.xx or earlier, you need to download and place **Microsoft SQL Server JDBC driver** on every CMS host:

1. Open in your browser https://sourceforge.net/projects/jtds/files/jtds/1.2.7/

2. Download **jtds-1.2.7-dist.zip** (Oracle account is needed)
3. Unpack downloaded archive
4. Place **jtds-1.2.7.jar** into **<CMS_installation_folder>/lib/ext**

> ### Important
> The driver must be added to the installation folder of every CMS node in your deployment.
> Starting from the 8.5.303.xx release of the product, drivers are embedded into the CMS's IP.

Using CMS with Oracle

> **Important**
>
> Oracle 11g supported from version 8.5.302.xx of the product.

Prerequisites

- Create new database in Oracle 11g
- Create user account to access the database

Configuring CMS

1. Open Genesys Administrator and navigate to **Provisioning > Environment > Applications**
2. Select the application defined for the Knowledge Center Cluster and click **Edit**
3. From the **Options** tab in the **cms.cluster** section, set the following options:
    a. set option **type** to value **oracle**
    b. set dbConnectionUrl to JDBC connection string for connection to Oracle following the format: `jdbc:oracle:thin:@<host_with_Oracle>:<port_of_Oracle, 1521 by default>:<CMS_DB_SID>` or `jdbc:oracle:thin:@//<host_with_Oracle>:<port_of_Oracle, 1521 by default>/<Service Name>`
    c. **dbUsername** - set to the username that needs to be used to login to Oracle
    d. **dbPassword** - set to the password for db account
    e. dbDriverClass - set to **oracle.jdbc.driver.OracleDriver**

> **Important**
>
> Description of options in cms.cluster section can be found in Configuration Options.

If you are installing Knowledge Center CMS 8.5.302.xx, you need to download and place **Oracle JDBC driver** on every CMS host:

1. Open in your browser http://www.oracle.com/technetwork/apps-tech/jdbc-112010-090769.html
2. Accept the license
3. Download **ojdbc6.jar** (Oracle account is needed)
4. Place **ojdbc6.jar** into **<CMS_installation_folder>/lib/ext**

> Important
>
> The driver must be added to the installation folder of every CMS node in your deployment.
> Starting from the 8.5.303.xx release of the product, drivers are embedded into the CMS's IP.

Configuring CMS to Work with PostgreSQL

> **Important**
>
> PostgreSQL is supported starting from 8.5.304.xx release of the Genesys Knowledge CMS Please use the latest stable version of PostgreSQL.

Prerequisites

- Create new database in PostgreSQL
- Create user account to access the database

Configuring CMS

1. Configure database properties in the Genesys Knowledge Center Cluster application.
2. Open Genesys Administrator and navigate to **Provisioning > Environment > Applications**.
3. Select the application defined for the Knowledge Center Cluster and click **Edit**.
4. From the **Options** tab in the **`cms.cluster`** section, set the following options:
   - for option **type** set **postgre** value.
   - **dbConnectionUrl** - to JDBC connection string for connection to PostreSQL Server following the format:

     ```
     jdbc:postgresql://<host_of_PostgreSQL>:<port_of_PostgreSQL>/<CMS_DB_name>
     ```
   - **dbUsername** - set to the username that needs to be used to login to PostgreSQL.
   - **dbPassword** - set to the password for db account.

   Note: Description of options in `cms.cluster` section can be found in Configuration Options.

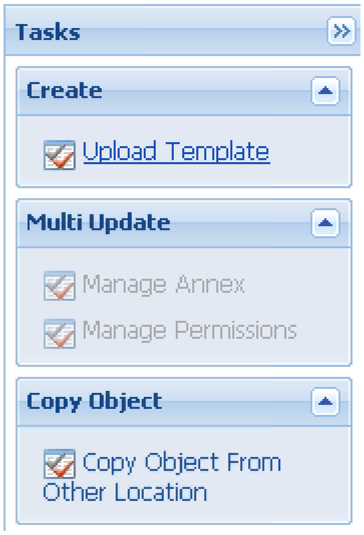
Configure Resource Access Point for Knowledge Center CMS Load-Balancer

If you plan to use several instances of Knowledge Center CMS or use it with Universal Constance Server for Standard Responses you'll need to set up an external Load-Balancer and/or configure a Resource Access Point (RAP).

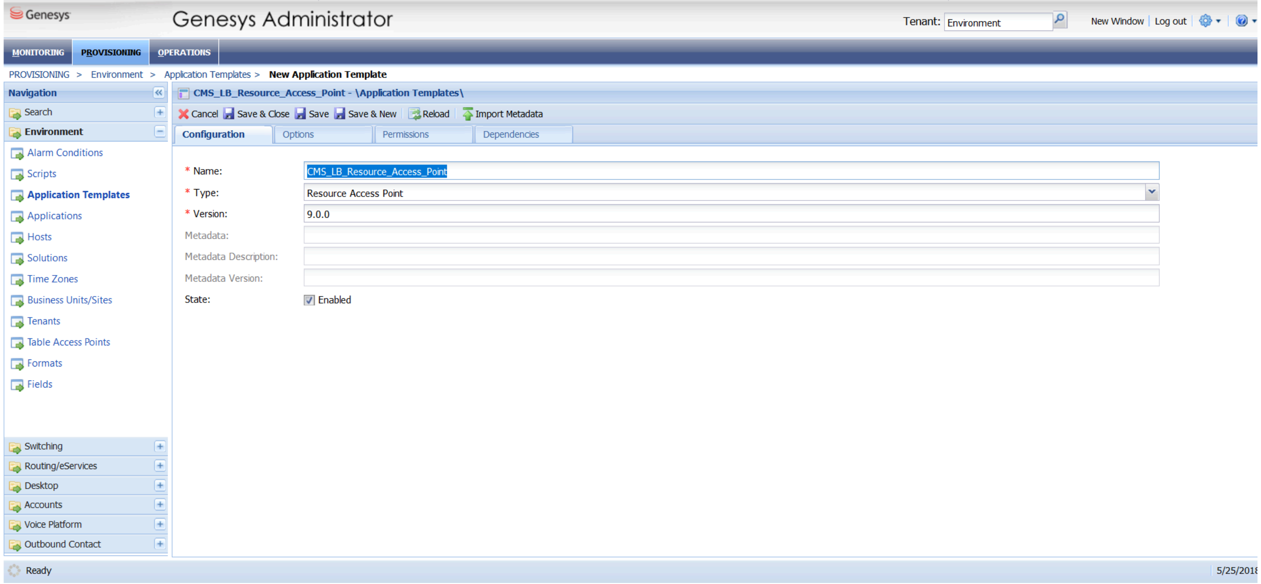
Importing the Load-Balancer Resource Access Point Template

Start

1. Open Genesys Administrator and navigate to **Provisioning** > **Environment** > **Application Templates**.
2. In the **Tasks** panel, click **Upload Template**.



3. Click **Add** and choose application template (APD) file to import window, click **Add**.
4. Browse to the CMS_LB_Resource_Access_Point.apd file. Click **Open**.
   The New Application Template panel opens:



* Name: CMS_LB_Resource_Access_Point
* Type: Resource Access Point
* Version: 9.0.0
Metadata:
Metadata Description:
Metadata Version:
State: ☑ Enabled

5. Click **Save & Close**.

End

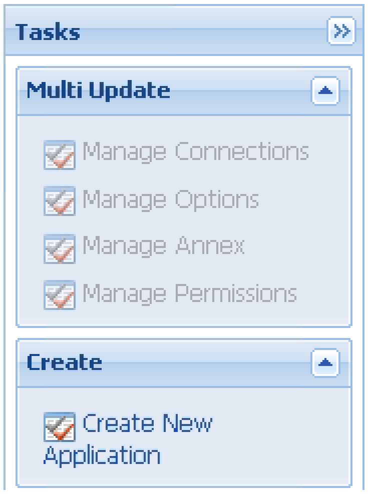
Creating the Load-Balancer Resource Access Point Application

Prerequisites

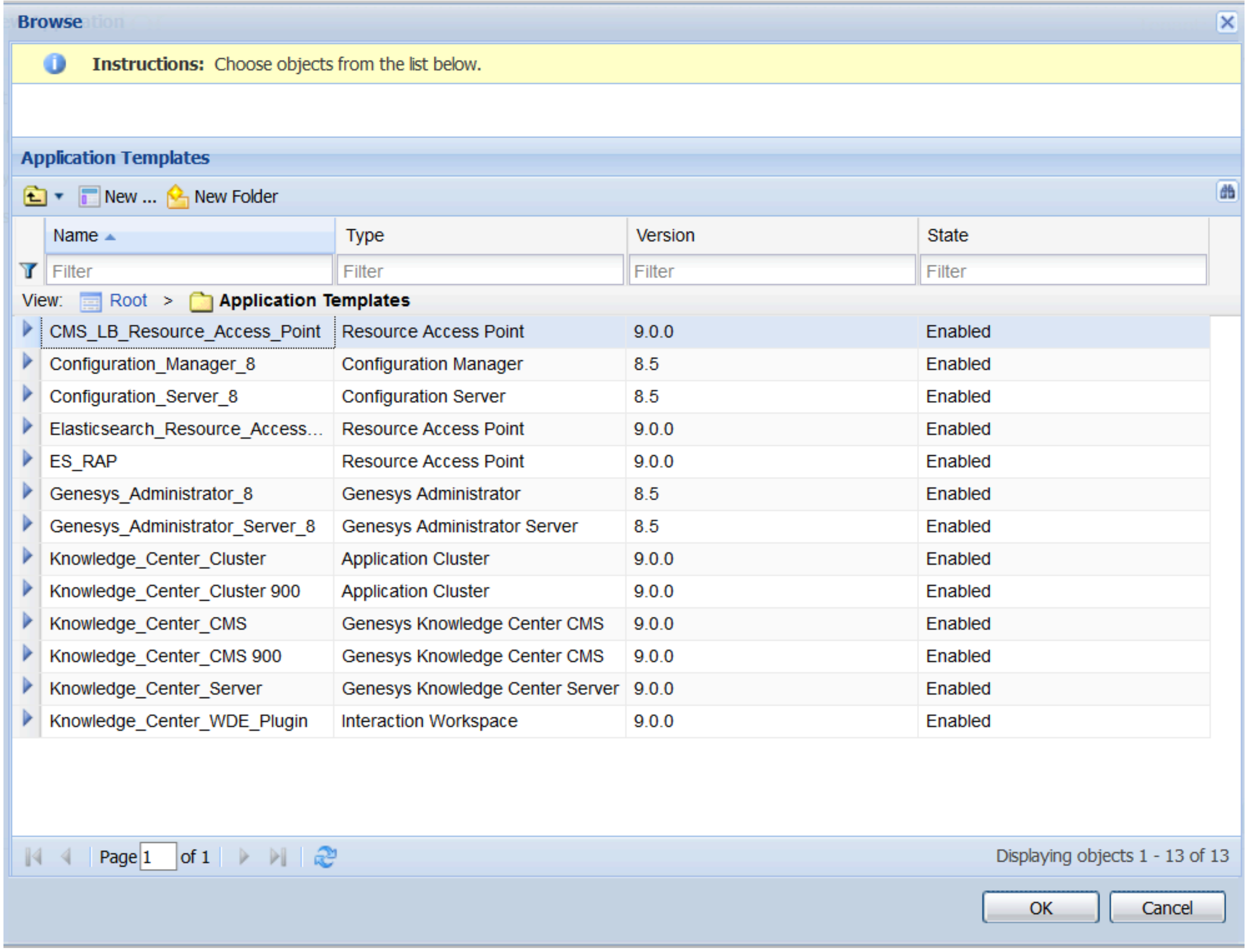
- You completed Importing the Load-Balancer Resource Access Point Template.

Start

1. Open Genesys Administrator and navigate to **Provisioning** > **Environment** > **Applications**.
2. In the **Tasks** panel, click **Create New Application**.



3. In the **Select Application Template** panel, click **Browse for Template** and select the CMS_LB_Resource_Access_Point template that you imported in Importing the Load-Balancer Resource Access Point Template. Click **OK**.



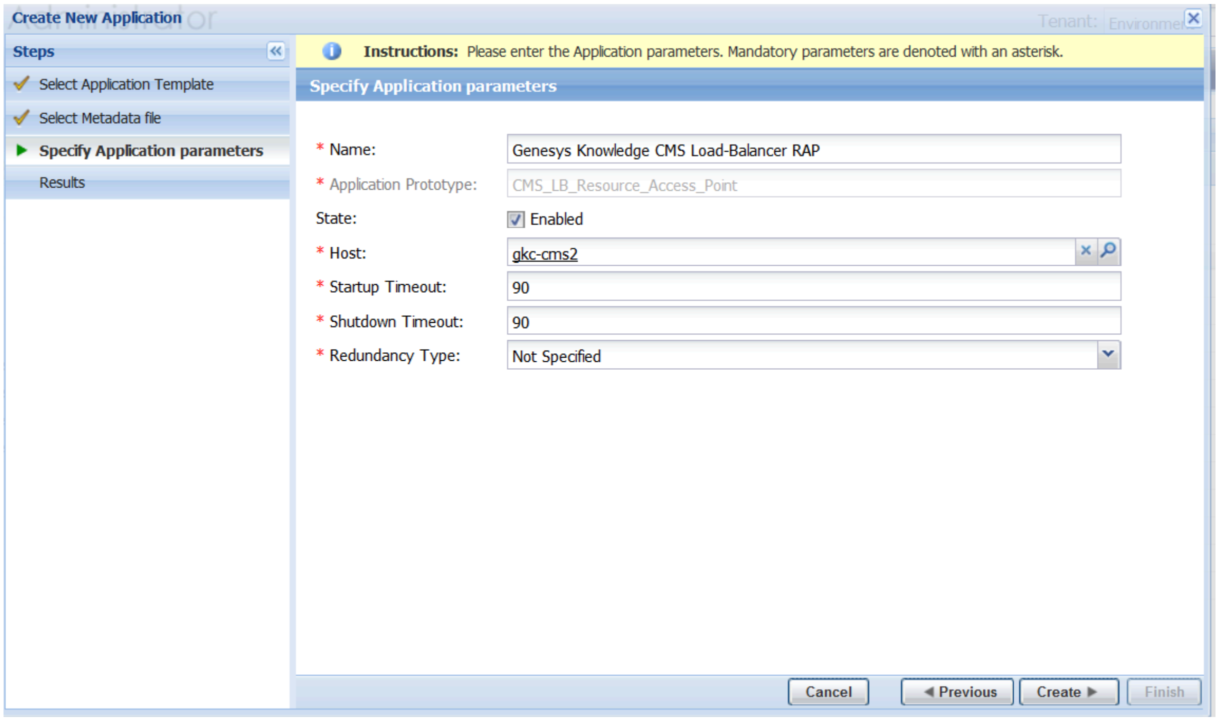
Instructions: Choose objects from the list below.

Name	Type	Version	State
CMS_LB_Resource_Access_Point	Resource Access Point	9.0.0	Enabled
Configuration_Manager_8	Configuration Manager	8.5	Enabled
Configuration_Server_8	Configuration Server	8.5	Enabled
Elasticsearch_Resource_Access...	Resource Access Point	9.0.0	Enabled
ES_RAP	Resource Access Point	9.0.0	Enabled
Genesys_Administrator_8	Genesys Administrator	8.5	Enabled
Genesys_Administrator_Server_8	Genesys Administrator Server	8.5	Enabled
Knowledge_Center_Cluster	Application Cluster	9.0.0	Enabled
Knowledge_Center_Cluster 900	Application Cluster	9.0.0	Enabled
Knowledge_Center_CMS	Genesys Knowledge Center CMS	9.0.0	Enabled
Knowledge_Center_CMS 900	Genesys Knowledge Center CMS	9.0.0	Enabled
Knowledge_Center_Server	Genesys Knowledge Center Server	9.0.0	Enabled
Knowledge_Center_WDE_Plugin	Interaction Workspace	9.0.0	Enabled

Displaying objects 1 - 13 of 13

4. The template is added to the **Select Application Template** panel. Click **Next**.

5. In the **Select Metadata** file panel,
    a. click **Browse**
    b. click **Add**
    c. select the CMS_LB_Resource_Access_Point.xml file
    d. Click **Open**
6. The metadata file is added to the Select Metadata file panel. Click **Next**.
7. In **Specify Application** parameters:
    a. Enter a name for your application. For instance, "Genesys Knowledge CMS Load-Balancer RAP"
    b. Make sure that **State** is enabled
    c. Select the **Host** on which the Access Point will reside
    d. Click **Create**

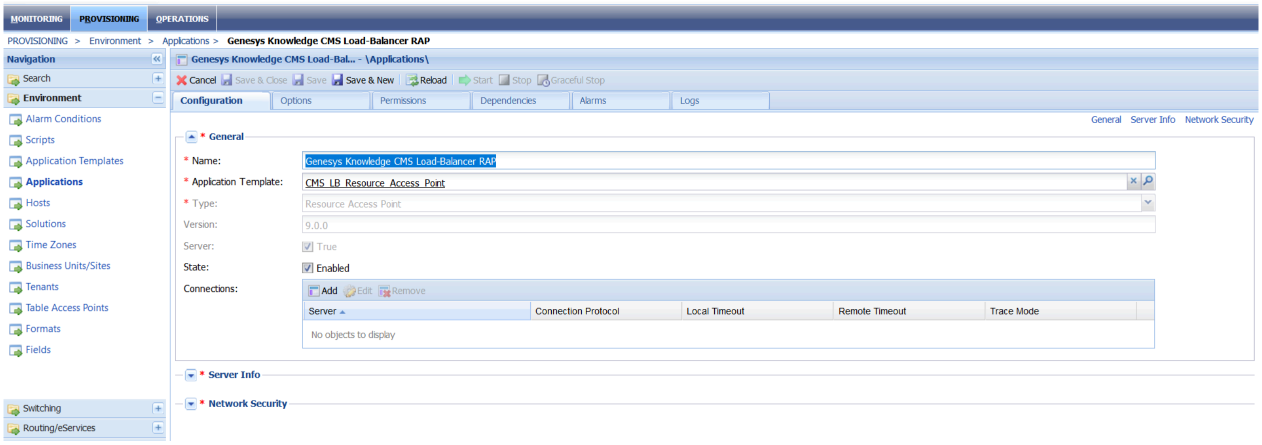


Instructions: Please enter the Application parameters. Mandatory parameters are denoted with an asterisk.

Specify Application parameters

* Name:	Genesys Knowledge CMS Load-Balancer RAP
* Application Prototype:	CMS_LB_Resource_Access_Point
State:	☑ Enabled
* Host:	gkc-cms2
* Startup Timeout:	90
* Shutdown Timeout:	90
* Redundancy Type:	Not Specified

8. The **Results** panel opens.
9. Enable Opens the Application details form after clicking 'Finish' and click **Finish**. The Load-Balancer Resource Access Point application form opens and you can start configuring its properties.



* Name: Genesys Knowledge CMS Load-Balancer RAP

* Application Template: CMS_LB_Resource_Access_Point

* Type: Resource Access Point

Version: 9.0.0

Server: ☑ True

State: ☑ Enabled

Connections: Add Edit Remove

Server	Connection Protocol	Local Timeout	Remote Timeout	Trace Mode
No objects to display				

End

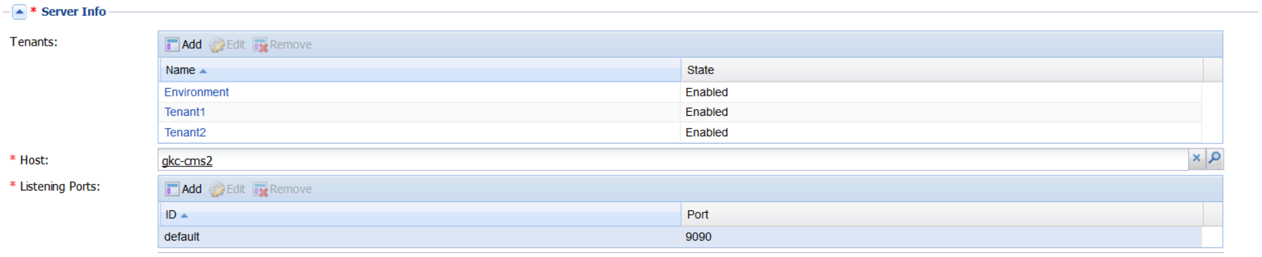
Configuring the Load-Balancer Resource Access Point Application

Prerequisites

- You completed Creating the Load-Balancer Resource Access Point Application.

Start

1. If your Load-Balancer Resource Access Point application form is not open in Genesys Administrator, navigate to **Provisioning** > **Environment** > **Applications**. Select the application defined for the Load-Balancer Resource Access Point and click **Edit**.
2. Expand the **Server Info** pane.
3. In the **Tenant** section, click **Add** and select your tenant. For instance, Environment. Click **OK**. (Tenant should be same as for previously created Genesys Application cluster <link to chapter about installing Cluster>)
4. If your **Host** is not defined, click the lookup icon to browse to the hostname of your application, which should point to the host where you plan to locate your external Load-Balancer or CMS server.
5. In the **Listening Ports** section, create the default port by clicking **Add**. The Port Info dialog opens.
    a. Enter the **Port**. For instance, 9090 (use value of http port of your external Load-Balancer or CMS server).
    b. Click **OK**. The **default** port appears in the list of **Listening** ports.



* Server Info

Tenants:

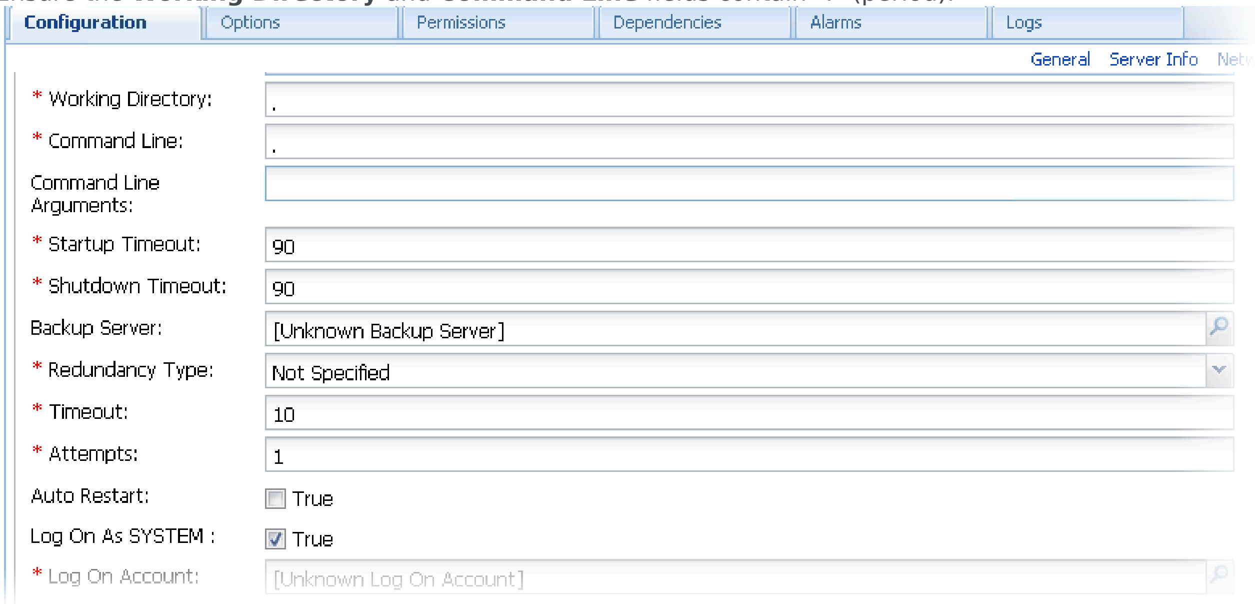
Name	State
Environment	Enabled
Tenant1	Enabled
Tenant2	Enabled

* Host: gkc-cms2

* Listening Ports:

ID	Port
default	9090

6. Ensure the **Working Directory** and **Command Line** fields contain "." (period).



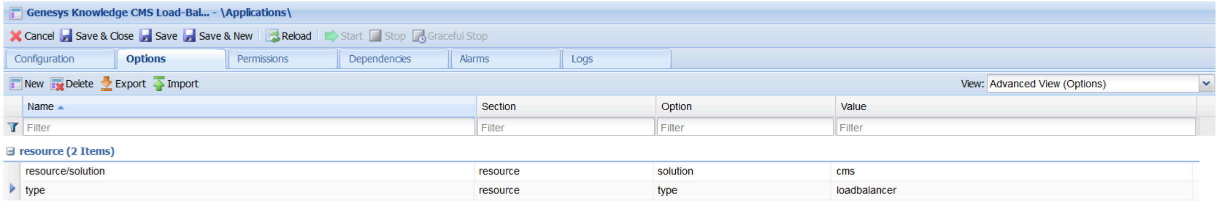
* Working Directory:	.
* Command Line:	.
Command Line Arguments:	
* Startup Timeout:	90
* Shutdown Timeout:	90
Backup Server:	[Unknown Backup Server]
* Redundancy Type:	Not Specified
* Timeout:	10
* Attempts:	1
Auto Restart:	□ True
Log On As SYSTEM :	☑ True
* Log On Account:	[Unknown Log On Account]

7. Click **Save**.

8. The **Confirmation** dialog for changing the application's port opens. Click **Yes**.

9. Select the **Options** tab.

   - Make sure the following options are set in the **[resource]** section:
     - **[resource]/type**=`loadbalancer`
     - **[resource]/solution**=`cms`



Genesys Knowledge CMS Load-Bal... - \Applications\

View: Advanced View (Options)

Name	Section	Option	Value
Filter	Filter	Filter	Filter
resource (2 Items)			
resource/solution	resource	solution	cms
type	resource	type	loadbalancer

10. Click **Save & Close**. If the **Confirmation** dialog opens, click **Yes**.

End

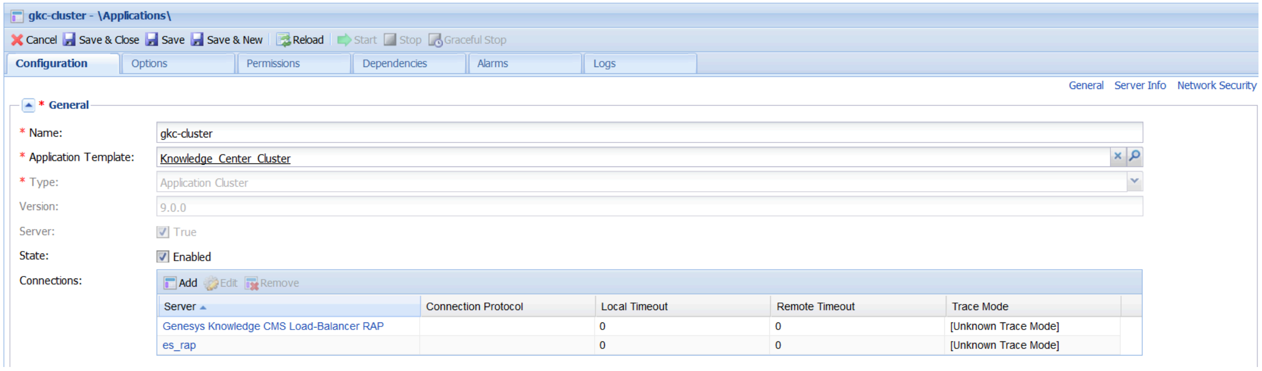
Configuring the Knowledge Center Cluster for Use with Load-Balancer

Prerequisites

- You completed Configuring the Load-Balancer Resource Access Point Application.

Start

1. Navigate to **Provisioning** > **Environment** > **Applications**. Select the application defined for the Knowledge Center Cluster and click **Edit**.
2. In the **Connections** section of the **Configuration** tab, click **Add**. The Browse for applications panel opens. Select a Genesys application defined as a Load-Balancer Resource Access Point, then click **OK**.
3. Select added connection to application, click **Edit** and ensure that the default connection port selected as ID
4. Click **Save & Close**. If the **Confirmation** dialog opens, click **Yes**



* Name: gkc-cluster

* Application Template: Knowledge_Center_Cluster

* Type: Application Cluster

Version: 9.0.0

Server: ☑ True

State: ☑ Enabled

Connections:

Add Edit Remove

Server ▲	Connection Protocol	Local Timeout	Remote Timeout	Trace Mode
Genesys Knowledge CMS Load-Balancer RAP		0	0	[Unknown Trace Mode]
es_rap		0	0	[Unknown Trace Mode]

End

Installing the Workspace Desktop Edition Plugin

Installing the Plugin for Workspace Desktop Edition

Agents can use the Knowledge Center Plugin for Workspace Desktop Edition (WDE) to access knowledge-related information right from their desktop. For example, if a customer asks a question using a chat widget and the corresponding interaction is routed to an agent, Knowledge Center can execute a pre-populated search based on data attached to the new interaction, as well as displaying the customer's search history and providing the agent with full access to the knowledge base access. And if the customer has not authorized during their search, the agent can link their session history to that customer's ID to access their full history while working with the interaction. To use this plugin complete the procedures below, in order.

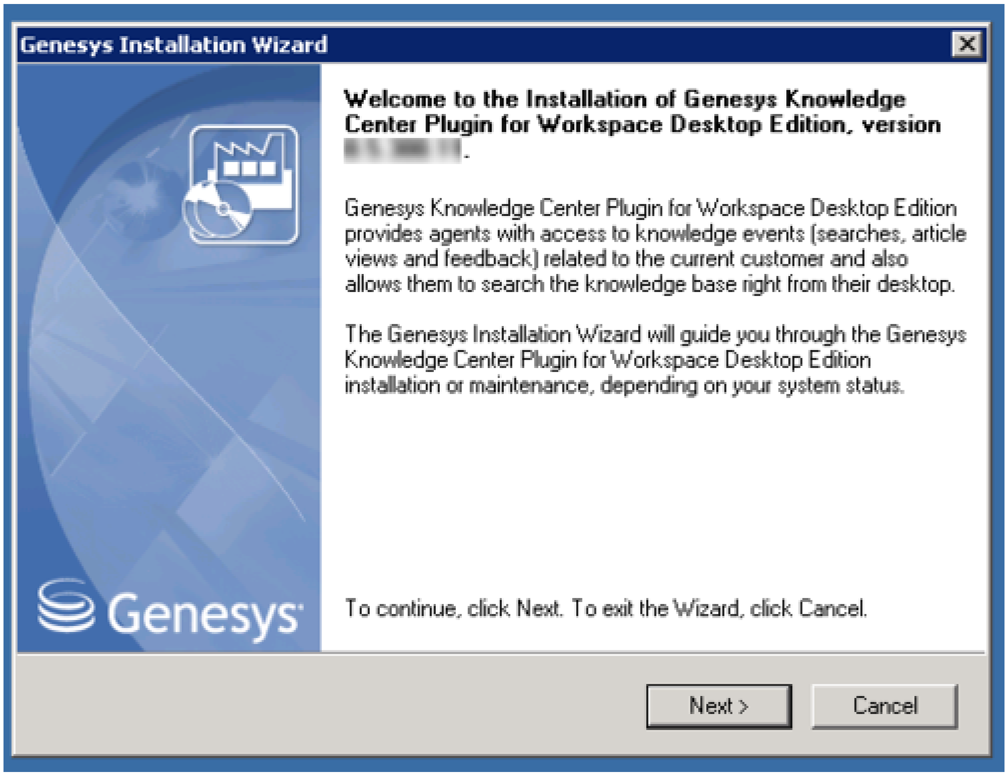
Installing the Plugin for Workspace Desktop Edition

Prerequisites

Workspace Desktop Edition must be installed and configured to work with voice or media interactions.

Start

1. In your installation package, locate and double-click the **setup.exe** file. The Install Shield opens the welcome screen.



Welcome to the Installation of Genesys Knowledge Center Plugin for Workspace Desktop Edition, version [redacted].

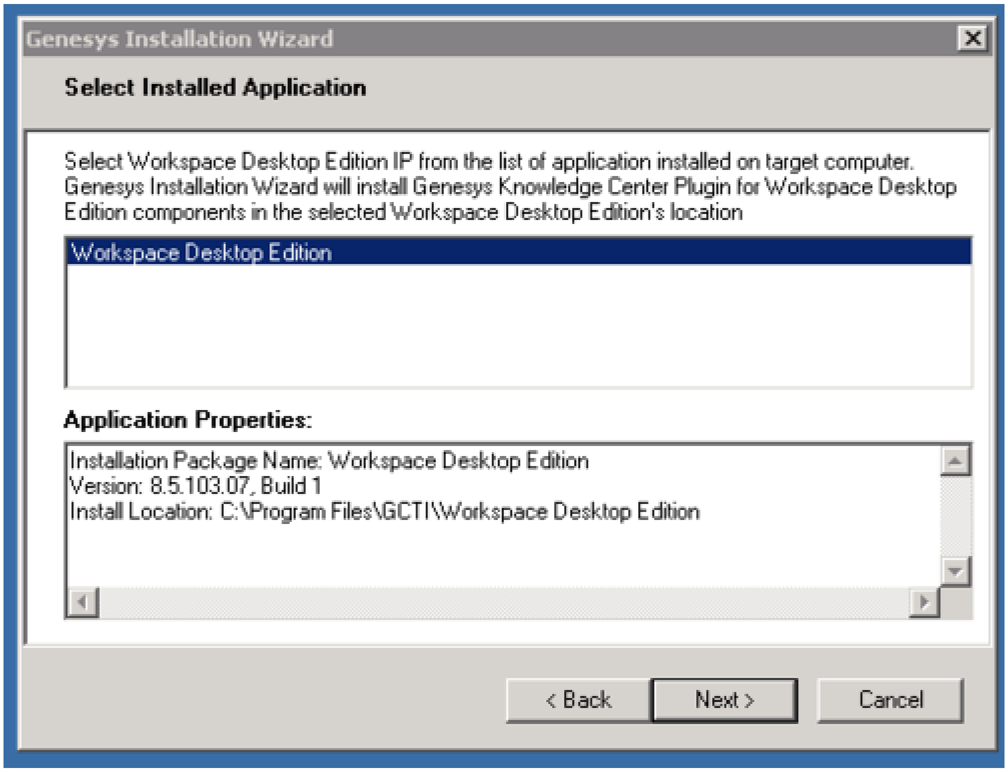
Genesys Knowledge Center Plugin for Workspace Desktop Edition provides agents with access to knowledge events (searches, article views and feedback) related to the current customer and also allows them to search the knowledge base right from their desktop.

The Genesys Installation Wizard will guide you through the Genesys Knowledge Center Plugin for Workspace Desktop Edition installation or maintenance, depending on your system status.

To continue, click Next. To exit the Wizard, click Cancel.

Knowledge Center WDE Plugin—Install Shield Screen

2. Click **Next**. The **Select Installed Application** screen appears.
3. Select the installed Workspace Desktop Edition Application for which you want to install the plugin. The **Application Properties** area shows the **Type**, **Host**, **Working Directory**, **Command Line executable**, and **Command Line Arguments** information previously entered in the Server Info and Start Info tabs of the selected Application object.



Select Installed Application

Select Workspace Desktop Edition IP from the list of application installed on target computer. Genesys Installation Wizard will install Genesys Knowledge Center Plugin for Workspace Desktop Edition components in the selected Workspace Desktop Edition's location

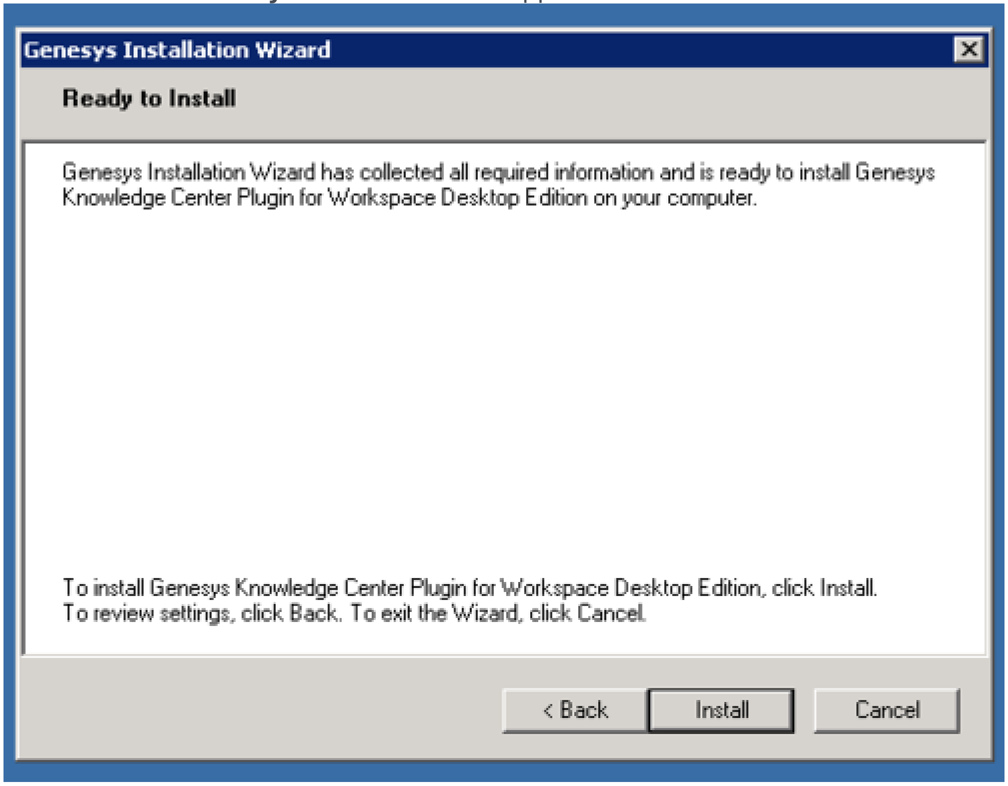
Workspace Desktop Edition

Application Properties:

Installation Package Name: Workspace Desktop Edition
Version: 8.5.103.07, Build 1
Install Location: C:\Program Files\GCTI\Workspace Desktop Edition

Select Installed Workspace Desktop Edition Application

4. Click **Next**. The **Ready to Install** screen appears.



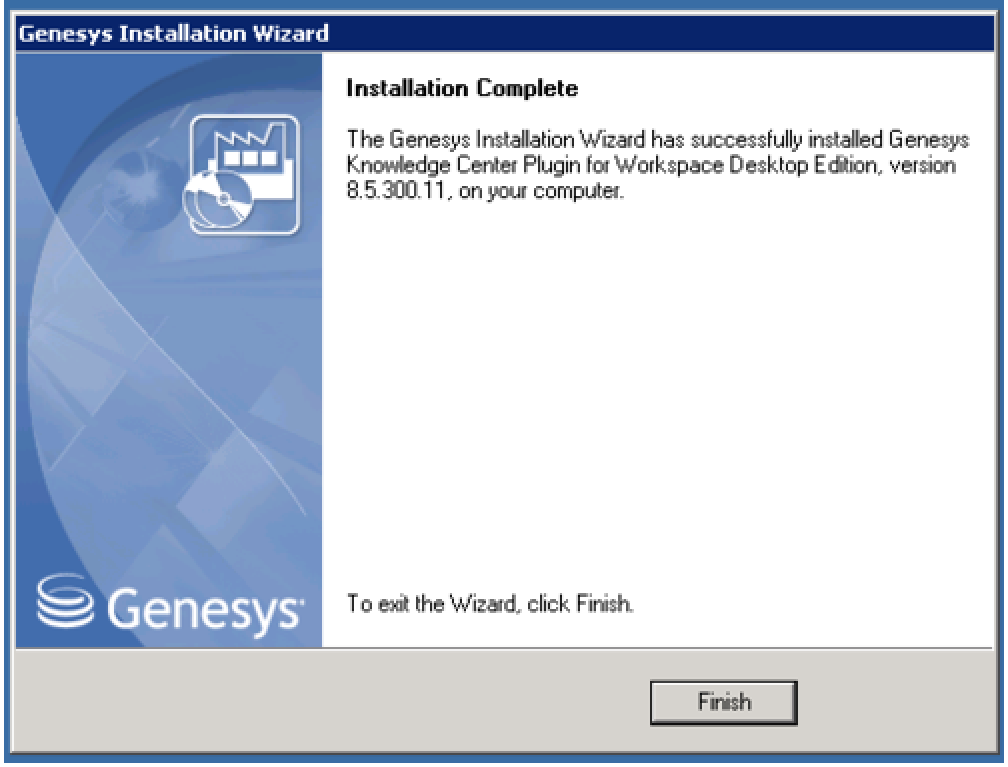
Ready to Install

Genesys Installation Wizard has collected all required information and is ready to install Genesys Knowledge Center Plugin for Workspace Desktop Edition on your computer.

To install Genesys Knowledge Center Plugin for Workspace Desktop Edition, click Install.
To review settings, click Back. To exit the Wizard, click Cancel.

Knowledge Center WDE Plugin—Ready to Install

5. Click **Install**. The Genesys Installation Wizard indicates it is performing the requested operation for Backend Server. When through, the **Installation Complete** screen appears.



Genesys Installation Wizard

Installation Complete

The Genesys Installation Wizard has successfully installed Genesys Knowledge Center Plugin for Workspace Desktop Edition, version 8.5.300.11, on your computer.

To exit the Wizard, click Finish.

Knowledge Center WDE Plugin—Installation Complete

6. Click **Finish** to complete your installation.
7. Inspect the directory tree of your system to make sure that the following files have been installed in the location that you intended:

- *GWEInstallationFolder\Genesyslab.Desktop.Modules.Knowledge.dll*
- *GWEInstallationFolder\Genesyslab.Desktop.Modules.Knowledge.module-config*
- *GWEInstallationFolder\Genesyslab.Desktop.Modules.Knowledge.pdb*
- *GWEInstallationFolder\Newtonsoft.Json.dll*
- *GWEInstallationFolder\RestSharp.dll*
- *GWEInstallationFolder\System.Net.Http.Formatting.dll*
- *GWEInstallationFolder\Language\Genesyslab.Desktop.Modules.Knowledge.en-US.xml*

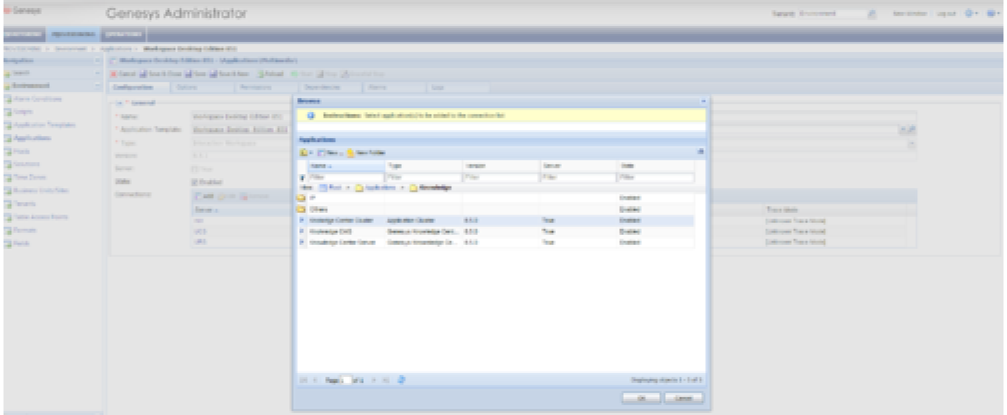
End

Configuring the WDE Application to work with the WDE Plugin

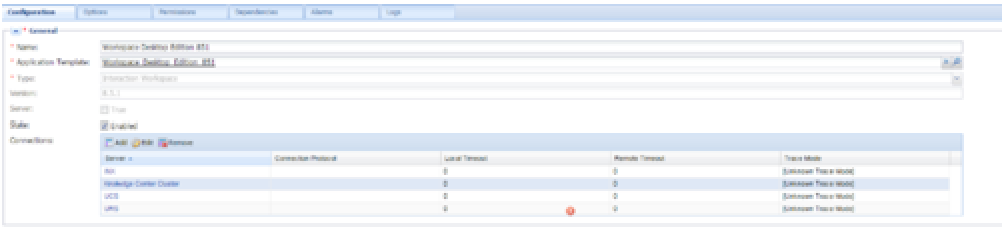
> **Important**
>
> To run the WDE plugin correctly, the local storage must be enabled in Internet Explorer on the host with the WDE client application. To verify this, open **Settings** > **Internet Options** then click the **Advanced** tab > **Security**. Confirm that “Enable DOM-Storage” is checked. If it is not, click the check box and then save your updated settings.

Add the Knowledge Center Cluster to Your WDE Connections

1. If your Workspace Desktop Edition application form is not open in Genesys Administrator, navigate to **Provisioning > Environment > Applications**. Select the application defined for the Workspace Desktop Edition and click **Edit...**.
2. In the **Connections** section of the **Configuration** tab, click **Add**. The **Browse for applications** panel opens. Select the **Knowledge Center Cluster application**, then click **OK**.



Knowledge Center WDE Plugin—Browse for applications 1



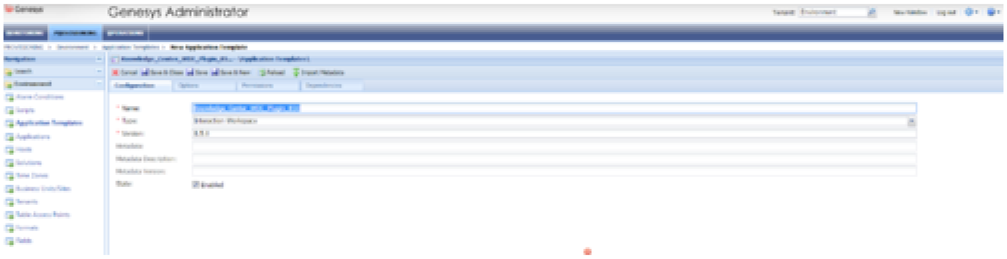
Knowledge Center WDE Plugin—Browse for applications 2

Add Knowledge Center Options to Your WDE Application

To use the Knowledge Center Plugin for WDE, you need to add some options to your WDE application so that it can gather knowledge-related information from incoming interactions. You can add these options to the the **interaction-workspace** section of the WDE application.

Start

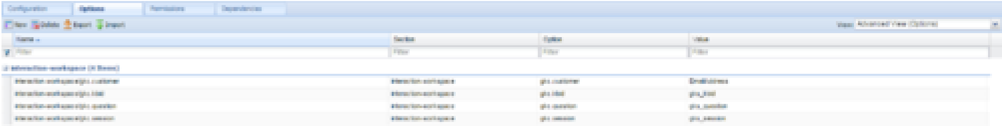
1. Import the template with the additional options:
    1. Open Genesys Administrator and navigate to **Provisioning > Environment > Application Templates**.
    2. In the **Tasks** panel, click **Upload Template**.
    3. In the *Click 'Add' and choose application template (APD) file to import* window, click **Add**.
    4. Choose the application template (APD) file from the import window and click **Add**.
    5. Browse to the *Knowledge_Center_WDE_Plugin.apd* file available in the templates directory of your installation CD. The **New Application Template** panel opens.



Knowledge Center WDE Plugin—New Application Template panel

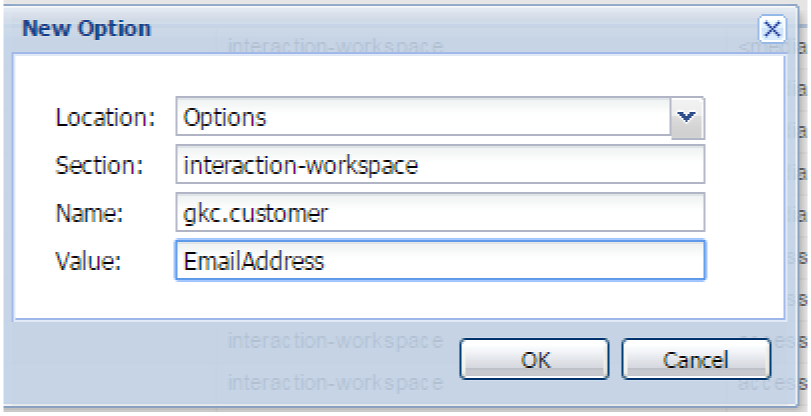
    6. Click **Save and Close**

2. Open the **Options** tab of the uploaded application and review the new options.



Knowledge Center WDE Plugin—Options tab of uploaded application

3. Navigate to **Provisioning > Environment > Applications**. Select the application defined for Workspace Desktop Edition and click **Edit...**.
4. Open the **Options** tab.
5. Add the plugin options to the **interaction-workspace** section using the **New** button.



Location: Options

Section: interaction-workspace

Name: gkc.customer

Value: EmailAddress

Knowledge Center WDE Plugin—Add plugin options

End

The Knowledge Center Plugin for WDE uses the following additional options:

Section	Option	Default value	Allowed values	Description	Takes effect
interaction-workspace	gkc.question	gks_question	any valid user data key	Interaction user data key that contains search query that will be pre-populated in Desktop	Next agent session
interaction-workspace	gkc.kbid	gks_kbid	any valid user data key	Interaction user data key containing the knowledge base Id to search knowledge in	Next agent session
interaction-workspace	gkc.customer	EmailAddress	any valid user data key	Interaction user data key that contains customer identification (for example email address of the customer)	Next agent session
interaction-workspace	gkc.session	gks_session	any valid user data key	User data key that contains knowledge session Id associated with the interaction	Next agent session
interaction-workspace	gkc.language	gks_lang, Language	comma-separated list of valid user	Interaction user data key that contains	Next agent session

Section	Option	Default value	Allowed values	Description	Takes effect
			data keys	language of interaction This option can contain a comma-separated ordered list of keys. for example "gks_lang, Language"; in the case of several keys in the attached data, the first key in the list is used	
interaction-workspace	gkc.country	Country	any valid user data key	Interaction user data key that contains a region of interaction (used for multi-regional languages, for example en_US, en_UK)	Next agent session
interaction-workspace	gkc.spellcheck	false	true false	Enables or disables spell check correction of the searched query	Next agent session
interaction-workspace	gkc.send-document	false	true false	Allows agents to push a link to the document into the chat session transcript by clicking the **Send Document** button	Next agent session
interaction-workspace	gkc.extended-filters-view	false	true false	Allows you to display type labels for custom attributes in an applied filter **Introduced in: 9.0.001.04**	Next agent session

Providing Knowledge Center Access to Agents

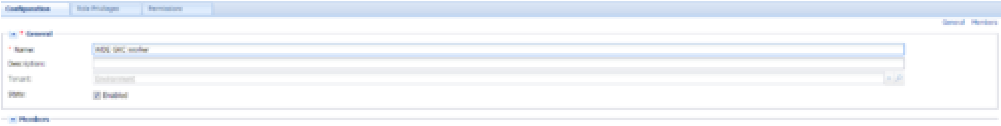
Genesys Knowledge Center supports the following privilege in order to restrict Agent access:

- **Knowledge.WORKER** — Enables access to the Genesys Knowledge Center tab in WDE
- **Knowledge.AUTHOR** — Enables ability to suggest new knowledge to knowledge bases.

To configure the appropriate role for an agent:

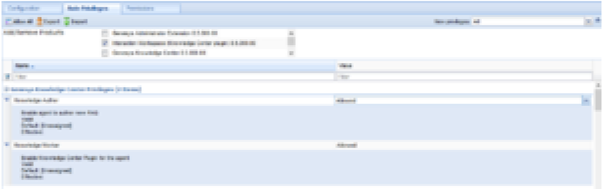
Start

1. Go to **Provisioning > Environment > Application Templates**.
2. Select the application template defined for Workspace Desktop Edition and click **Edit...**.
3. Click **Import Metadata**.
4. Click **Add** and select the *Knowledge_Center_WDE_Plugin.xml* file.
5. Click **Open**.
6. Information from the metadata file will be added to the template and the appropriate privilege will be added into the framework.
7. Save and Close.
8. Go to **Provisioning > Accounts > Roles**.
9. In the taskbar click **New** to create a new object.
10. Set the name of the role in the **General** section.



Knowledge Center WDE Plugin—Set Role Names

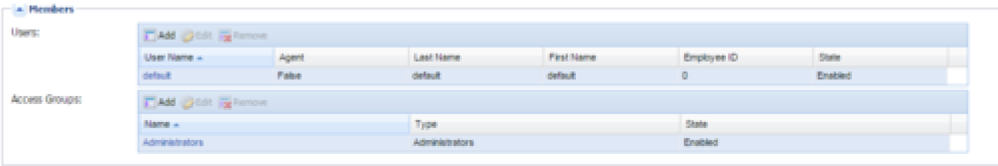
11. Go to the **Role Privileges** tab, and select the set of roles for Genesys Knowledge Center.
12. Open the WDE Knowledge Center Plugin privileges list and select the **Genesys Knowledge Center Privileges** section.
13. Create the appropriate privileges as allowed.



Knowledge Center WDE Plugin—Create Privileges

14. Go back to the **Configuration** tab.

15. Add the appropriate Agent to the **Members** section by clicking the **Add** button.



Users:

User Name	Agent	Last Name	First Name	Employee ID	State
default	False	default	default	0	Enabled

Access Groups:

Name	Type	State
Administrators	Administrators	Enabled

Knowledge Center WDE Plugin—Members Section

16. Save and Close.

End

Post Installation and Deployment

This chapter provides you with information on what to do after you've deployed the Knowledge Center within your environment. It covers following topics:

- Access Permissions
- Configuration Options
- Load-Balancing Configuration
- Security
- Geo Location
- UTF8
- Supported Languages
- Translation Service

Access Permissions

Overview

Before starting up with Knowledge Center you need to:

- Define access rules for every knowledge base you have created
- Set up permissions for your knowledge team
- Set up access to knowledge for your agents

Knowledge Center leverages privileges and skills to define desired access level:

- Privileges used to grant access to functional capabilities such as authoring ability, approval rights, ability to work with knowledge in Workspace or ability to suggest content. Privileges assigned to roles that you can assign to your personnel.
- Skills allow you define knowledge areas that an agent or author can access. Skills are highly dynamic and allow you to provide additional knowledge while you assign areas of responsibilities to your agents.

Let's review these tasks a bit closer in the following sections.

Access permissions

Restricting access to Knowledge

To restrict access to the knowledge you need to define these restrictions for a knowledge base. All documents within knowledge base will follow the defined restrictions.

A knowledge base can be restricted–

for viewing:

- Public (Anyone) - its content is accessible to all agents and customers
- Private (Agent Only) - its content is accessible to agents only
- Private with skill restriction (Skilled agent) - content of the knowledge base is accessible to an agent with specific skills

for authoring:

- Any Author - any agent that is granted author privilege can create/update knowledge documents
- Authors with skill restriction - only agents that are granted author privilege and have one of the selected skills can create/update knowledge documents

Skill-based access allows you dynamically manage access to the knowledge along with managing the distribution of the customer's interactions. That ensures that there are no additional actions required when you assign an agent to a new area.

For example, say you have a knowledge base with restricted access for agents who have the skill "technical support", and the same skill is used for routing interactions to your group of agents. Adding the agent to the group by assigning him the "technical support" skill will automatically give him access to the proper knowledge bases.

Setting up Knowledge Team

The next task is to grant access to the CMS and knowledge bases to the members of your authoring team. CMS allows the following privileges to be granted:

- Administrator - allowed to manage knowledge bases (create new, modify and delete)
- Author: Categories - gives content author ability to create new categories, and modify and delete existing ones
- Author: Documents - gives content author ability to create new documents, and modify and delete existing ones
- Approver - designated for content managers who validate and approve created documents and categories

At least one of the above privileges are required to be able to work with CMS.

Also, content authors and managers need to be assigned proper skills to get access to the private knowledge bases with skill restrictions. **Note:** Administrators have access to any knowledge base, no matter the skill restrictions applied.

Granting access to agents

Agents follow the same concept. They require *privileges* to get access to functionality and *skills* for getting access to private knowledge bases with skill restrictions.

An agent can be assigned following privileges:

- Knowledge Worker - allows access to Knowledge Center functionality in the Workspace
- Knowledge Author - allows agent to suggest knowledge content from the Workspace

Also, agents need to be assigned proper skills to get access to the private knowledge bases with skill restrictions.

Configuration Procedures

Knowledge Center Privileges

Knowledge Center supports following privileges

Privilege	Product	Description	Since
Knowledge.AUTHOR	Knowledge Center Server	Allows changing data in a knowledge base. This privilege is required for agents that are running data synchronization from Genesys Knowledge Center CMS or third-party sources.	9.0.0
Knowledge.MULTITENANT	Knowledge Center Server	Allows to bypass tenants restrictions while importing data into knowledge bases. Important Required only for the multi-tenant deployments. Will not affect other privileges or access rights except authoring.	9.0.0
Knowledge.CanAccessPublic	Knowledge Center Server	Allows agents to access public knowledge bases. Used if the Cluster option privilege.can-access-public in section search is set to false	9.0.0
Knowledge.CMS.Document.Author	Knowledge Center CMS	Gives content author ability to create new documents, and modify and delete existing ones	9.0.0
Knowledge.CMS.Category.Author	Knowledge Center CMS	Gives content author ability to create new categories, and modify and delete existing ones	9.0.0
Knowledge.CMS.Approver	Knowledge Center CMS	Designated for content managers who validate and approve created documents and categories	9.0.0
Knowledge.CMS.Administrator	Knowledge Center CMS	Allowed to manage knowledge bases (create new, modify and delete)	9.0.0
Knowledge.CMS.Multitenant	Knowledge Center CMS	Allows bypassing tenant restrictions while working through API	9.0.0
Knowledge.Worker	Workspace Desktop Edition	Enable the Knowledge Center Plugin for the agent	9.0.0
Knowledge.Author	Workspace Desktop Edition	Allows agent to propose new knowledge documents from	9.0.0

Privilege	Product	Description	Since
		Workspace	

Privileges for typical Roles

The table below shows examples of typical roles and privileges required for them:

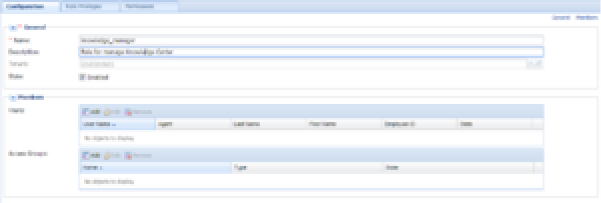
Role	Description	Privileges
CMS Administrator	• Manages Knowledge Bases • Sets up publishing schedules • Doing maintenance procedures with knowledge	• Knowledge.CMS.Administrator (CMS) • Knowledge.AUTHOR (Server)
Knowledge Manager	• Approves content produced by authors • Publish knowledge documents to be used by agents and customer	• Knowledge.CMS.Approver (CMS) • Knowledge.AUTHOR (Server)
Knowledge Author	• Creates knowledge documents • Creates knowledge categories • Reviews usage feedback and update knowledge content	• Knowledge.CMS.Document.Author (CMS) • Knowledge.CMS.Category.Author (CMS)
Agent	• Handles customers' interactions • Access to public Knowledge bases for this agent is allowed (while disabled in general)	• Knowledge.Worker (WDE) • Knowledge.Author (WDE) • Knowledge.CanAccessPublic (Server)

Assigning a Privilege

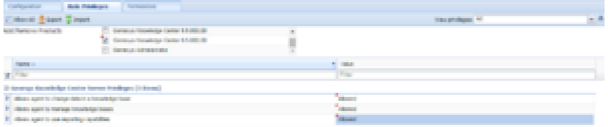
To configure the appropriate privileges for an Agent:

Start

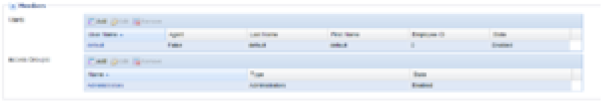
1. Go to **Provisioning** > **Accounts** > Roles.
2. In the taskbar, click **New** to create a new object.
3. Set the name of the role in the **General** section.



4. Go to the **Role Privileges** tab and select the set of roles for Genesys Knowledge Center.
5. Open the list of privileges for Knowledge Center Server.
6. Set the appropriate privileges to **Allowed**.



7. Go back to the **Configuration** tab.
8. In the **Members** section, add the appropriate agent by clicking the **Add** button.



9. Save and Close.

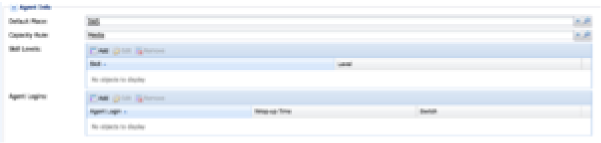
End

Assignining Skills

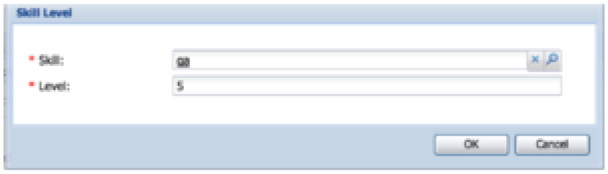
To configure the appropriate skills for an Agent:

Start

1. Go to **Provisioning** > **Accounts** > **Users**.
2. Select **Agent** from the table
3. Click **Edit...** button
4. Expand Agent Info panel
5. Click **Add...** in the **Skills Level** section



6. In the **Skills Level** dialog:



* Skill: qa
* Level: 5

- select the skill
- enter the skill level
- click OK

7. Save and Close.

End

Configure Reporting

> **Important**
>
> Reporting functionality is available starting from version 9.0.001.xx

Knowledge Center Server packages contain the following reporting modules:

- Kibana-based discovery dashboards: allows you to discover different insights of your knowledge data usage
- Predefined Templates and Datasource for native Pulse widgets

This chapter describes how to enable and configure this functionality within your Knowledge Center deployment.

Prerequisites

For Pulse widgets, it is required you use Pulse 8.5.108.02 or higher.

For Kibana dashboards, it is required to use ElasticSearch 6.2.3 version, 6.2.x is supported but not recommended.

Restrictions

Note the following restrictions related to the reporting functionality:

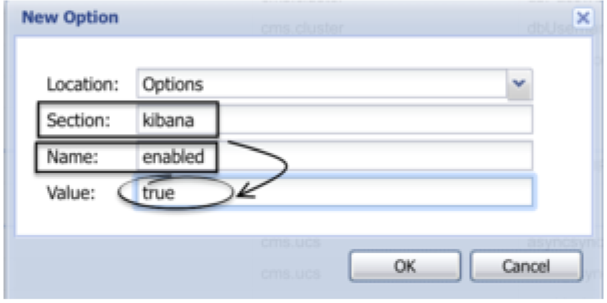
- The basic authentication feature of the Knowledge Center Server must be disabled to allow Pulse to use Knowledge Center data source for widgets (only for versions of 9.0.001.xx family).
- You cannot run two or more nodes of Knowledge Center Server on the same host with reporting functionality enabled (only for versions of 9.0.001.xx family).
- HTTPs for Kibana supported if security proxy enabled (from version 9.0.003.06), or via secured Load-Balancer on top of Genesys Knowledge Cluster (from version 9.0.004.x).
- Taking into account that Pulse is single tenant and does not support Cloud configuration, in multi-tenant environments, each tenant must have its own dedicated Pulse for reporting.
- If you are deploying several Knowledge Center Clusters within one environment, each independent Knowledge Center cluster must have its own dedicated Pulse for reporting.
- In case of standalone Pulse, the base URL should be set as "/gax". For example, set "root_url=/gax" in ./conf/pulse.properties for Pulse installation (only for versions of 9.0.001.xx and 9.0.002.xx family).

Configuration

By enabling the reporting functionality you have to enable the Kibana process that is started and controlled by the Knowledge Center Server on each server Knowledge Center Server runs (Kibana exposes discovery dashboards for Knowledge Center).

To enable reporting functionality in Genesys Knowledge Center you must follow the steps described below:

1. Open Genesys Administrator and navigate to **Provisioning > Environment > Applications**
2. Select the application defined for the Knowledge Center Cluster and click **Edit**
3. From the **Options** tab in the **kibana** section, set the following option:
   - option **enabled** to value **true**

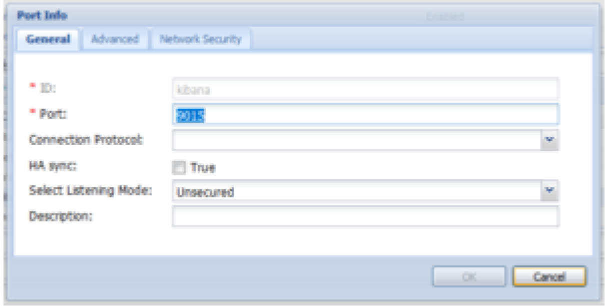


Location: Options
Section: kibana
Name: enabled
Value: true

4. Click **Save**

By default, Kibana is enabled and Knowledge Center Server uses port 5601 to expose the Kibana application. As of version **9.0.002.09** you can configure a custom port for Kibana on the Knowledge Server node:

1. Open Genesys Administrator and navigate to **Provisioning > Environment > Applications**.
2. Select the application defined for the Knowledge Center Server node application and click **Edit**.
3. Expand the **Server Info** pane.
4. In the **Listening Ports** section, select the port with the name "kibana" and click **Edit**. The Port Info dialog opens.
5. Change the **Port** value and click **OK**.

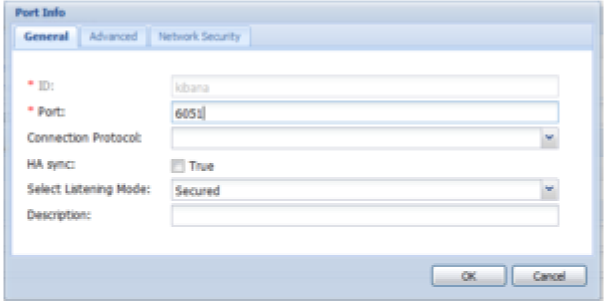


* ID: kibana
* Port: 2015
Connection Protocol:
HA sync: □ True
Select Listening Mode: Unsecured
Description:

6. Save your changes.

As of version **9.0.004.x**, to correctly import Kibana URLs into Pulse during Tenant Provisioning, you should create a port with the name "kibana" in the Genesys Knowledge Center Cluster application:

1. Open Genesys Administrator and navigate to **Provisioning > Environment > Applications**.
2. Select the application defined for the Knowledge Center Cluster application and click **Edit**.
3. Expand the **Server Info** pane.
4. In the **Listening Ports** section, create a port with name "Kibana" by clicking **Add**. The Port Info dialog opens.
   a. Enter the port number for the load-balancer configured for Kibana; for instance, 6051.
   b. If you are using a secure connection to Kibana Load-balancer, choose **Secured** under **Select Listening Mode**.
   c. Click **OK**. The HTTP or HTTPS port with the "Kibana" identifier appears in the list of **Listening ports**.



Port Info

* ID: kibana
* Port: 6051
Connection Protocol:
HA sync: □ True
Select Listening Mode: Secured
Description:

5. Save your changes.

Important

- The new configuration is applied to newly started nodes or restarted nodes.
- To ensure proper load balancing of requests between Kibana nodes embedded into Knowledge Center Servers you must configure the load balancer to distribute new sessions evenly between started nodes.
- Kibana load balancer must run on the same *host* as Knowledge Center Server load balancer.
- If Kibana Security proxy is configured, you cannot configure the "Kibana" port in the Knowledge Cluster Application. In this case, the "default" port will be used to access Kibana.

Kibana security

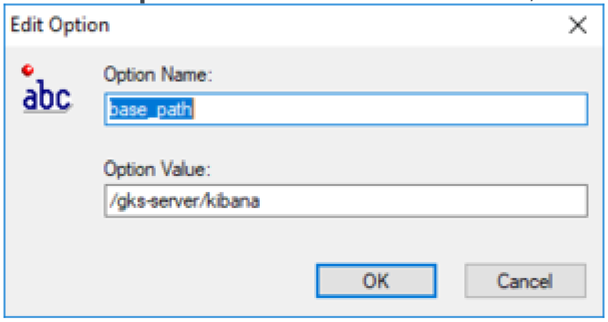
Important

Available as of version 9.0.003.06.

By default you can access the Reporting Dashboard in Kibana using the "kibana" port and host configured in the Knowledge Server Application. This behavior does expose the ability to modify and delete data via the DevTools console or Kibana API. To restrict the processing of any data modification requests, you need to enable the Kibana security proxy.

To enable restricted access to Kibana with proxy to protect the data from modification, follow these steps:

1. Open Genesys Administrator and navigate to **Provisioning > Environment > Applications**.
2. Select the application defined for the Knowledge Center Cluster and click **Edit**.
3. From the **Options** tab in the kibana section, set the following options:



Option Name: base_path

Option Value: /gks-server/kibana

4. Click **Save**.

Important

After configuring the proxy you must restart all instances of Knowledge Center Server before doing any further activities against reporting.

If you want to close the access with proxy to Kibana which was already configured and provisioned, you must:

1. Call tenant provisioning API.
2. Remove all GK* widgets from Pulse (If they were already previously created) and create them again using updated GK* templates.

> **Important**
>
> If the Kibana security proxy is configured and a connection to the node configured as "secured" then access to Kibana will also be via secured connection via the "default" Server port.

Configuring external Kibana

> **Important**
>
> Configuring Kibana has been possible as of version 9.0.006.08.

By default reporting is provided using the embedded Kibana version 6.2.3. You can install an external Kibana instance (https://www.elastic.co/kibana) and configure the Knowledge Server to show which dashboard is not embedded.

To enable reporting in external Kibana, follow these steps:

1. Install and configure external Kibana (https://www.elastic.co/start).
2. Open the Kibana configuration file (that is, kibana.yml), and add or change the following option: server.basePath: "/gks-server/kibana"
3. Configure Kibana to use the same Elasticsearch used by the Genesys Knowledge Center.

> **Important**
>
> You should use the same Kibana version that is used for your Elasticsearch instances.

Access the **Option of Knowledge Center Cluster** application and set the following options in the **Kibana** section:

- **base_path** = /gks-server/kibana.
- **host** = set the external Kibana's hostname or IP address (for example - kibana.demo.com or 192.168.10.10).
- **port** = set the external Kibana's port (for example - 5601).

After you apply this configuration, run the Knowledge Server Cluster and the external Kibana.

Click the following link to access the Kibana: <GKC Server host or access>:<GKC server port>/gks-server/kibana/app/kibana.

Important

- Access to the external Kibana will only be available via a secured proxy within the GKC Server. The secured proxy will redirect Kibana calls to a real external Kibana instance.
- If you use external Kibana - no need to configure Kibana port in GKC Server nodes applications or in GKC Cluster application. For external Kibana this port could be removed from configuration.

Pulse templates auto-provisioning

Important

Pulse templates auto-provisioning available only for versions of 9.0.001.xx family.

To configure Pulse templates auto-provisioning you must specify the pulse URL and credentials used during provisioning. From the host Knowledge Center Server installed:

1. Locate the **<installation_folder>/server** folder:
   Windows:
   - Open the **launcher.ini** configuration file
   - Locate the following lines:

   ```
   -Dreporting.pulse.url=http://host:port
    -Dreporting.pulse.user=default
    -Dreporting.pulse.password=password
   ```

   Linux:
   - Open **setenv.sh** file
   - Locate line starting from CUSTOM_JAVA_OPTS and containing:

   ```
   -Dreporting.pulse.url=http://host:port -Dreporting.pulse.user=default
    -Dreporting.pulse.password=password
   ```
2. Change **host:port** to the actual host port of Pulse or its load balancer
3. Change **default** to the user name you wish to use during provisioning
4. Change the **password** to the password for this user account
5. **Save** changes
6. Restart Knowledge Center Node (Pulse should be running)

Troubleshooting

"*No default index pattern*" message

If you see "No default index pattern" message in Kibana you need to execute following steps:

1. Stop Knowledge Center Server
2. Delete the **.kibana** index in Elasticsearch by executing following command:

   ```
   curl --request DELETE --url http://<ES Host>:<ES Port>/.kibana
   ```

3. Start Knowledge Center Server

When the Knowledge Center Server re-initializes after start, the Kibana definitions help to resolve the problem.

"*Error: EPERM: operation not permitted, open '.babelcache.json*'" message

If you see message "Error: EPERM: operation not permitted, open '.babelcache.json'" in logs of the Knowledge Center Server you must execute following steps:

1. Navigate to the **<installation_folder>/server/kibana/optimize** folder (the one the error message refers to)
2. Using administrative permissions, delete file **.babelcache.json**
3. Start Knowledge Center Server

Tenant Provisioning

> **Important**
>
> To make reporting more controllable and stable, auto-provisioning was removed in version 9.0.002.09. Now, if you need the reporting feature, you can enable and configure it using API.

Tenant Provisioning includes generation and importing visualization metadata into Pulse and Kibana. You can skip them with next application option under `reporting` section.

Section	Option	Value	Description
reporting	kibana.provision	true or false	Enable or disable Kibana metadata provision. By default, is is set to `true`.
reporting	pulse.provision	true or false	Enable or disable widget templates import into Pulse. By default it is set

Section	Option	Value	Description
			to `true`.

To perform a tenant provision, you need to execute a **Reporting Provision API** request:

For v.9.0.002.09

```
request POST
--url http://<Knowledge Cluster Host>:<Knowledge Cluster Port>/gks-server/reporting/v1/
provision
--header 'content-type: application/json'
--header 'ContactCenterID: <Id of working Tenant>'
--data
'{
    "pulseUrl" : "http://<Pulse Host>:<Pulse Port>",
    "pulseUser": "<Pulse User>",
    "pulsePassword": "<Pulse User Password>",
    "kibanaTenantName": "<Custom name for working tenant>"
}'
```

For versions v.9.0.003 and higher

PulseUrl should be used in the format `http://<Pulse Host>:<Pulse Port>/<Pulse base URL>` this is because when using Pulse in GAX you use the URL format `http://<Pulse Host>:<Pulse Port>/gax`. Standalone Pulse however, by default, is configured in the URL as `http://<Pulse Host>:<Pulse Port>/pulse`.

Provisioning request for v.9.0.003 and higher should look like:

```
request POST
--url http://<Knowledge Cluster Host>:<Knowledge Cluster Port>/gks-server/reporting/v1/
provision
--header 'content-type: application/json'
--header 'ContactCenterID: <Id of working Tenant>'
--data
'{
    "pulseUrl" : "http://<Pulse Host>:<Pulse Port>/<Pulse base URL>",
    "pulseUser": "<Pulse User>",
    "pulsePassword": "<Pulse User Password>",
    "kibanaTenantName": "<Custom name for working tenant>"
}'
```

When the provision is done correctly, you can expect the following response:

```
{ "status": {
        "code": 200,
        "message": "Ok" },
    "data": {
        "provisionLog": {
            "log": [
                "Kibana Provision - DONE",
                "Pulse Provision - DONE"]
} } }
```

Example (v9.0.002.09)

```
curl --request POST \
--url http://localhost:9010/gks-server/reporting/v1/provision \
--header 'content-type: application/json' \
--header 'ContactCenterID: a906b47e-e641-4216-96e5-05c827725ecd' \
--data '{
    "pulseUrl" : "http://demosrv:8081",
    "pulseUser": "default",
    "pulsePassword": "password",
    "kibanaTenantName": "Genesys Tenant"
}'
```

Example (v9.0.003 and higher)

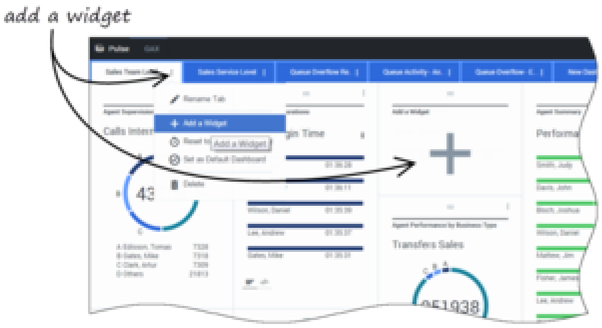
```
curl --request POST
--url http://localhost:9010/gks-server/reporting/v1/provision
--header 'content-type: application/json'
--header 'ContactCenterID: a906b47e-e641-4216-96e5-05c827725ecd'
--data '{
    "pulseUrl" : "http://demosrv:8081/pulse",
    "pulseUser": "default",
    "pulsePassword": "password",
    "kibanaTenantName": "Genesys Tenant"
}'
```

Adding Knowledge Widgets in Pulse

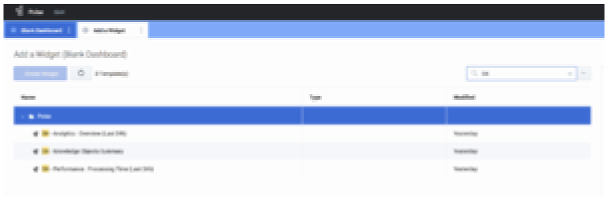
> **Important**
>
> To see data on minimized widgets, **Pull Collector** must be configured and running for Pulse.

1. There are two ways you can add a report to your dashboard or wallboard:
    - Click the more icon (⋮) in the right corner and click **Add a Widget**.
    - On empty dashboards and wallboards, click the **Add a Widget** icon.

   Genesys Pulse opens a report builder to guide you.



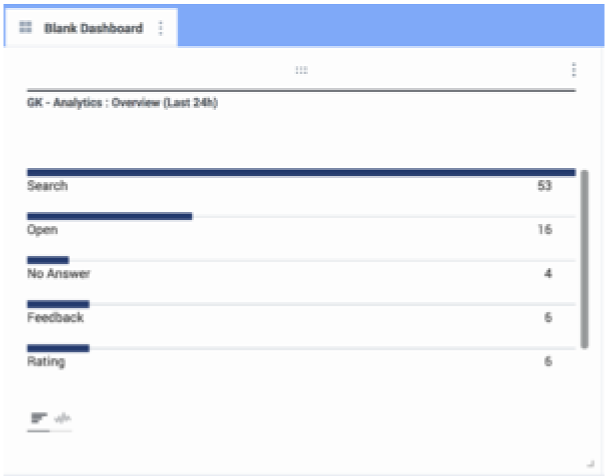
To quickly locate Knowledge Center widgets in the search bar of the "Add a Widget" window, type "GK" and it will filter Knowledge Center widgets:



Important

- If widgets are not shown, it means that they have not yet been provisioned
- In versions of 9.0.001.xx family Knowledge Center provisions widget templates automatically as soon as:
  - kibana/enabled options are set to **true**
  - **reporting.pulse.*** variables are properly set
  - Knowledge Center Server node with proper settings is re-started
- Please investigate log files for errors if you do not see provisioned Pulse templates after these steps are completed

2. Select one of the widgets:
   - **GK - Analytics: Overview (Last 24h)** - provides summary statistics on knowledge usage events (such as search requests, feedback, 5-star rating, comments, and other) over last 24 hours. Expanded view for this widget displays the Kibana dashboard allowing you to discover details of knowledge events.
   - **GK - Knowledge Objects Summary** - provides you a summary of indexed knowledge (number of knowledge bases, documents, categories, and others), Expanded view for this widget displays the Kibana dashboard allowing you to explore indexed knowledge documents.
   - **GK - Performance: Processing Time (Last 24h)** - provides you request processing performance metrics allowing you to monitor solution performance. Expanded view for this widget displays the Kibana dashboard with detailed performance information.
3. Click the **Create Widget** button
4. Select the **Objects** and **Statistics** that you want to use in your report
5. Click the **Display Options** tab to define how you want to display your report, such as:
   - Widget Title
   - Widget Type
   - Size
   - Headline Type & Object
6. Click **Create Widget** and the newly added widget will appear on the dashboard:


Blank Dashboard
GK - Analytics : Overview (Last 24h)
Search
53
Open
16
No Answer
4
Feedback
6
Rating
6

Reporting REST API

Important

Available since v9.0.002.09

Overview

This page describes Genesys Knowledge Reporting REST API.

Reporting Provisioning

Provides provision functionality for Pulse and Kibana metadata.

1. Check Kibana index. Create and configure it with appropriate mapping if it does not exist.
2. **Kibana provisioning:**
   1. Generates dashboards and visualisations metadata files
   2. Patch metadata with requested TenantId/ContactCenterID
   3. Import metadata into ElasticSearch Kibana index
3. **Pulse provisioning:**
   1. Generates Pulse templates
   2. Import Pulse generated templates into Pulse

You can skip Kibana and Pulse provisioning with following application options under the `reporting` section:

Section	Option	Value	Description
reporting	kibana.provision	true or false	Enable or disable Kibana metadata provision. By default, is is set to `true`.
reporting	pulse.provision	true or false	Enable or disable widget templates import into Pulse. By default it is set to `true`.

HTTP Description

<table>
<tr><th colspan="2">Request</th></tr>
<tr><td><b>Method</b></td><td>POST</td></tr>
<tr><td><b>URI</b></td><td>/reporting/v1/provision</td></tr>
<tr><td><b>Content-type</b></td><td>application/json</td></tr>
<tr><td><b>Body</b></td><td>JSON Object with next fields
<table>
<tr><th>Field</th><th>Value</th><th>Mandatory</th><th>Description</th><th>Example</th></tr>
<tr><td>"pulseUrl"</td><td>URL
http://<pulse host="">:<pulse port=""> for v.9.0.002.09 http://<pulse host="">:<pulse port="">/<Pulse base URL> for v.9.0.003.xx</td><td>yes
in the case of Pulse Provisioning being enabled, see <b>Reporting Provisioning</b> section.</td><td>URL to Pulse server, where generated dashboards will be imported.</td><td>"http://demosrv:8040" for v.9.0.002.09 or "http://demosrv:8040/pulse" for v.9.0.003.xx</td></tr>
<tr><td>"pulseUser"</td><td>String</td><td>yes
in the case of Pulse Provisioning being enabled, see <b>Reporting Provisioning</b> section.</td><td>Pulse user username. Required to have permissions to write data to Pulse.</td><td>"default"</td></tr>
<tr><td>"pulsePassword"</td><td>String</td><td>yes
in the case of Pulse Provisioning being enabled, see <b>Reporting Provisioning</b> section.</td><td>Pulse user password</td><td>"password"</td></tr>
<tr><td>"kibanaTenantName"</td><td>String</td><td>no</td><td>Custom</td><td>"Example</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Value</th><th>Mandatory</th><th>Description</th><th>Example</th></tr>
<tr><td></td><td></td><td></td><td>name for Description section of Dashboards and Visualizations. If not specified, <code>ContactCenterID</code> value is taken.</td><td>Tenant Name"</td></tr>
</table>
</td></tr>
<tr><td><b>Headers</b></td><td>
<table>
<tr><th>Name</th><th>Value</th><th>Mandatory</th><th>Description</th></tr>
<tr><td>ContactCenterID</td><td>UUID</td><td>no</td><td>If specified, contains Contact Center ID.
If not specified, works like "on-prem" installation.</td></tr>
</table>
</td></tr>
<tr><td colspan="2"><b>Response</b></td></tr>
<tr><td><b>Content-type</b></td><td>application/json</td></tr>
<tr><td><b>HTTP codes</b></td><td>
<pre>
200 - OK

Provision was success.

Response Body Example

{
   "status": {
     "code": 200,
</pre>
</td></tr>
</table>

```
    "message": "Ok"
  },
  "data": {
    "provisionLog": {
      "log": [
        "Kibana Provision - DONE",
        "Pulse Provision - DONE"
      ]
    }
  }
}


400 - Required request body field is missing

In the case if required parameter is missed

Response Body Example

{
  "status": {
    "code": 651,
    "message": "Field [pulseUser] is required. String type. For
example [default]"
  }
}

500 - General server error

Provision was failed on any step described steps aboe. Response
body includes related error message.

Response Body Example

{
  "status": {
    "code": 500,
    "message": "Unable to import Pulse templates on the
initialization phase :Failed to connect http://demosrv:8081"
  }
```

	}

Configuration Options

For information on 9.0+ Knowledge Center Configuration Options, please see the links below.

> **Important**
>
> Knowledge Center Server and Knowledge Center CMS have the same options as Knowledge Center Cluster.

- Knowledge Center Cluster Configuration Options
- Logging Configuration Options

Knowledge Center Cluster Configuration Options

Section:

- **cross-origin**
- **cms.cluster**
- **cms.general**
- **translation**
- **general**
- **index**
- **reporting**
- **search**
- **configuration**
- **security**
- **kibana**
- **agent-can-see**

Option	Name	Description	Value
Section: cross-origin			
CORS Filter Configuration	allowedOrigins	A comma separated list of origins (for example, instrumented web sites) allowed to access the Knowledge Center. If an allowed origin contains one or more "*" characters (for example http://*.domain.com) then "*" characters are converted to ".*". Characters "." are converted to "\.". Thus obtained allowed origin can be interpreted as a regular expression.	**Default value:** "*" **Value Type:**string **Changes Take Effect:** At start/restart
Section: cms.cluster Configuration of the Knowledge Center CMS Cluster.			

Database connection URL	dbConnectionUrl	Database connection string for the selected persistent storage.
		Examples:
		for Microsoft SQL:
		`jdbc:sqlserver://[host of MS SQL server]:[port of MS SQL server; 1433 by default];databaseName=[CMS DB name]`
		for Oracle:
		`jdbc:oracle:thin:[userName]/[password]@[host of Oracle DB]:[port of Oracle DB; 1521 by default]:[SID. for example ORCL]` or `jdbc:oracle:thin:@//[host of Oracle DB]:[port of Oracle DB; 1521 by default]/[Service Name]`
		for PostgreSQL:
		`jdbc:postgresql://[host of PostreSQL server]:[port of`
			Default value: <empty>
			Value Type:string
			Changes Take Effect: At start/restart

Option	Name	Description	Value
		`PostreSQL server; 5432 by default]/[CMS DB name]`	
Database user password	dbPassword	Password for user for access JDBC database.	**Default value:** <empty> **Value Type:**string **Changes Take Effect:** At start/restart
Database user name	dbUsername	Name of user for access JDBC database.	**Default value:** <empty> **Value Type:**string **Changes Take Effect:** At start/restart
Storage type	type	Type of persistent storage provider used for Knowledge Center CMS repository.	**Default value:** mssql **Value Type:**enumerated type **Valid values:** **[+] mssql** Microsoft SQL Server **[+] oracle** Oracle **[+] postgre** PostgreSQL **Changes Take Effect:** At start/restart
Section: cms.general			

Option	Name	Description	Value
Connection to CMS load balancer	externalURL	Public URL that is used to access the CMS directly or via load balancer (like http://<cms host>:<CMS default port>/gks-cms). This URL will be used to build the link on the attachments in knowledge documents.	**Default value:** <empty> **Value Type:**string **Changes Take Effect:** Immediately
Approval flow default value	approvalFlow.default	(Introduced in 9.0.003) Default value for approval flow in knowledge bases.	**Default value:** standard **Value Type:** enumerated type **Valid Values:** standard, simple **Changes Take Effect:** at start/restart
Named entities synchronization delay	ne.synchro.delay	(Introduced in 9.0.004.xx) Delay for named entities synchronization from CMS to GKS in minutes.	**Default value:** 30 **Value Type:** integer **Valid values:** any positive integer **Changes Take Effect:** At start/restart
Section: translation			
API key	key	Translation service API key. Key is provided by translation provider and required as part of request authentication to API.	**Default value:** <empty> **Value Type:**string **Changes Take Effect:** Immediately
Translation service	type	Defines translation service provider used by Knowledge Center CMS.	**Default value:** none **Value Type:**enumerated type **Valid values:** **[+] none** None **[+] google**

Option	Name	Description	Value
			Google Could Translation API **[+] microsoft** Microsoft Translator Text API **[+] yandex** Yandex.Translate **Changes Take Effect:** At start/ restart
Section: general			
Time to live for session	sessionTtl	Specifies the length of time that the server will store session information while no activities are carried out.	**Default value:** 8h **Value Type:**regular expression [^[0-9]*(ms|m|h|d|w)] **Valid values:** number + unit, for example, 1d or 3m. Supported units: d (days), m (minutes), h (hours), or w(weeks) **Changes Take Effect:** Immediately
Folder name for knowledge bases	knowledgebaseFolder	Name for folder in \"Script\" in Tenant in Configuration for storing Knowledge Base definitions for particular Knowledge Center Cluster.	**Default value:** knowledge **Value Type:**regular expression [^[a-zA-Z0-9_]*$] **Valid values:** Any non-empty alpha-numeric string **Changes Take Effect:** After restart
Section: index			
Number of replicas in historical index	historyNumberOfReplicas	Number of copies of historical index. Copies of index help to improve read	**Default value:** 1

Option	Name	Description	Value
		performance and tolerate lost data nodes. On the other hand they consume your disc space.	**Value Type:**integer **Changes Take Effect:** Immediately
Number of shards in historical index	historyNumberOfShards	Number of shard (parts) that each historical index is divided into. Please follow Elasticsearch recommendations and projected load to estimate number of shards required.	**Default value:** 1 **Value Type:**integer **Valid values:** Any integer greater than 1 and less than 10 inclusively. Takes effect for new indexes only, settings of existing historical indexes will not be changed. **Changes Take Effect:** Immediately
Index namespace	namespace	Namespace constant used as the prefix in the name of Elasticsearch indexes to ensure no naming conflict will arise while using the same Elasticsearch cluster for other tasks (including 2 independent Knowledge Center clusters)",	**Default value:** default **Value Type:**regular expression [^[a-zA-Z0-9_]*$] **Valid values:** Any alpha-numeric string **Changes Take Effect:** After restart
History segment format	historySegmentFormat	History segment format as Java date	**Default value:** yyyy-MM **Value Type:** string **Changes Take Effect:** Immediately
Section: reporting			
IP geo location mode	geo	Determine the precision of IP geo location algorithm.	**Default value:** CITY **Value Type:**enumerated type **Valid values:** **[+] OFF** Disabled **[+] CITY**

Option	Name	Description	Value
			Customer's city **[+] IP** Customer's IP Address **[+] COUNTRY** Customer's country **Changes Take Effect:** Immediately
Time to live	ttl	Specifies the length of time that records will be stored in the history.	**Default value:** 365d **Value Type:**regular expression [^[0-9]*(ms|m|h|d|w)] **Valid values:** number + unit, for example, 1d or 3m. Supported units: d (days), m (minutes), h (hours), or w(weeks) **Changes Take Effect:** Immediately
Kibana provisioning	kibana.provision	Enable Kibana provisioning with dashboards and visualization.	**Default value:** true **Value Type:** Boolean **Changes Take Effect:** At start/restart
Overwrite Pulse Templates	pulse.provision	Enable Pulse provisioning with predefined templates.	**Default value:** true **Value Type:** Boolean **Changes Take Effect:** At start/restart
Section: search			

Option	Name	Description	Value
Using NLP at analysis	useNlp	Enables/disables NLP processing against indexing data and search queries	**Default value:** true **Value Type:** Boolean **Changes Take Effect:** At start/restart
Number of documents in result	numberOfAnswers	Number of documents returned as the result of search operation (if other not specified directly in request)	**Default value:** 6 **Value Type:**integer **Valid values:** Any integer greater than `0` **Changes Take Effect:** Immediately
Trending period	trendingPeriod	Number of the days from now that is document usage is analyzed for to show trending knowledge documents (the documents having most attention during the recent period).	**Default value:** 10 **Value Type:**integer **Changes Take Effect:** Immediately
Access to public knowledge	privilege.can-access-public	Enables/disables access to public knowledge for agents (authorized user). If set to true, agents able to access both public and private knowledge bases. If set to false, all agents have access to private knowledge bases only unless agent is granted special privilege"	**Default value:** true **Value Type:**Boolean **Changes Take Effect:** Immediately
Words per minute rate	wordsPerMin	Default words per minute rate that is used as basis in reading time calculation.	**Default value:** 160 **Value Type:**integer **Valid values:** Any integer greater than `0` **Changes Take Effect:** Immediately
Section: configuration			
Applying NED modifications interval	reindexNedInterval	(Introduced in 9.0.004.xx) Defines time between operations of applying modifications of NED for improving search.	**Default Value:** 120s **Value Type:** regular expression [^[0-9]*(s|m|h|d)] **Changes Take Effect:** Immediately

Option	Name	Description	Value
Feedback classification interval	feedbackClassificationInterval	(Introduced in 9.0.004.xx) Defines time interval between operations of classifying feedback information.	**Default Value:** 1d **Value Type:** regular expression [^[0-9]*(s|m|h|d)] **Valid Values:** any positive integer plus h, m, s or d to indicate hours, minutes, second or days **Changes Take Effect:** Immediately
Update document rating interval	updateRatingInterval	(Introduced in 9.0.004.xx) Defines time interval for performing document rating update.	**Default Value:** 1h **Value Type:** regular expression [^[0-9]*(s|m|h|d)] **Valid Values:** any positive integer plus h, m, s or d to indicate hours, minutes, second or days **Changes Take Effect:** Immediately
Agent refresh interval	usersRefreshInterval	Defines the time interval in which information about agents is cached in memory. The larger the interval, the fewer the requests sent to configuration server, but it will take more time (up to specified interval) to get recently updated information from Configuration Server.	**Default value:** 120s **Value Type:** regular expression [^[0-9]*(s|m|h|d)] **Valid values:** any positive integer plus h, m, s or d to indicate hours, minutes, second or days **Changes Take Effect:** Immediately
Business attributes refresh interval	attributesRefreshInterval	Defines time interval that information about business attributes (languages, media type) is cached in memory. The larger the interval, the fewer the requests sent to configuration server, but it will take more time (up to specified interval) to get recently updated information from Configuration Server.	**Default value:** 120s **Value Type:** regular expression [^[0-9]*(s|m|h|d)] **Valid values:** any positive integer plus h, m, s or d to indicate hours, minutes, second or days **Changes Take Effect:** Immediately
Skills refresh interval	skillsRefreshInterval	Defines time interval that information about skills is cached in	**Default value:** 120s

Option	Name	Description	Value
		memory. The larger the interval, the fewer the requests sent to configuration server, but it will take more time (up to specified interval) to get recently updated information from Configuration Server.	**Value Type:** regular expression [^[0-9]*(s|m|h|d)] **Valid values:** any positive integer plus h, m, s or d to indicate hours, minutes, second or days **Changes Take Effect:** Immediately
Section: security			
Authorization scheme	auth-scheme	Specifies the HTTP authentication scheme used to secure REST API requests to the Knowledge Server. With the Basic scheme, clients must be authenticated with a user ID and password. Applies to: Genesys Knowledge Center Server	**Default value:** none **Value Type:**enumerated type **Valid values:** **[+] basic** Basic Authorization **[+] none** Disabled **Changes Take Effect:** Immediately
Password	password	The user password used in authentication for the REST API. Applies to: Genesys Knowledge Center Server.	**Default value:** <empty> **Value Type:**string **Changes Take Effect:** Immediately
User ID	user-id	The user identifier (login) used in authentication for the REST API. Applies to: Genesys Knowledge Center Server.	**Default value:** <empty> **Value Type:**string **Changes Take Effect:** Immediately

Option	Name	Description	Value
Section: kibana			
Enable/disable Kibana	enabled	Configuration of Kibana component	**Default value:** false **Value Type:** Boolean **Changes Take Effect:** Immediately
Path to kibana proxy	base_path	Path to mount Kibana for running it behind a proxy. It is important to enter exactly the value of "/gks-server/kibana" with no tailing slash. Exactly at this point knowledge server exposes its entry point for proxying kibana.	**Default value:** "" **Value to enable proxy** "/gks-server/kibana" **Changes Take Effect:** Immediately
Kibana protected (internal) host	host	Specifies the host to which GKS will redirect Kibana proxy calls. IP addresses and host names are both valid values.	**Default value:** 0.0.0.0 **Recommended value:** Hostname or IP address of Kibana instanse **Changes Take Effect:** At start/restart
Enable/disable connection to external Kibana	external	Enabling or disabling use of external Kibana for reporting.	**Default value:** false **Value Type:** Boolean **Changes Take Effect:** At start/restart
Port of external Kibana instance.	port	Specifies the port to which GKS will redirect Kibana proxy calls.	**Default value:** 5601 **Recommended value:** valid port of external Kibana instanse **Changes Take Effect:** At start/restart
Section: agent-can-see			
Access to the query history from the Knowledge Center WDE Plug-in.	history	Enables/disables access to conversation history. If set to true, agents are able to access the history from the Agent UI.	**Default value:** true **Value Type:** Boolean **Changes Take Effect:** At start/restart

Logging Configuration Options

Overview

This page explains the options that are used to configure application logging.

It is recommended you define log configuration in the Knowledge Center Cluster Application so it can be used by all Knowledge Center Server and Knowledge Center CMS nodes connected to the cluster.

> **Important**
>
> The file path defined in the `log` section of the Knowledge Center Cluster Application must be valid for every node within this cluster. It is recommended to use a relative path.

There are two sections in the configuration that allow you to configure log system behavior:

- `log` - defined logging system common options
- `log-extended` - enables extended logging for certain sub-systems of the application

> **Important**
>
> - We do not recommend you change the settings in the `log-extended` section unless you are advised to do so by Genesys Technical Support.
> - The `log-extended` section might be used when collecting information for an incident investigation.
> - Please ensure that values in this section are reverted to original values during production use of the product.

Genesys Knowledge Center allows you to change log options for a particular node of the Knowledge Center Server or Knowledge Center CMS by defining log configuration options in the **Application** object of this particular node.

> **Important**
>
> We do not recommend you define a separate configuration for individual nodes unless you have a specific reason to do so (for example, you were advised by a Genesys

> Technical Support representative).

Log section

Option	Name	Description	Value
Section: log Logging options.			
All events	all	Specifies the outputs to which an application sends all log events. The log output types must be separated by a comma when more than one output is configured. For example: `all = stdout, logfile`	**Default value:** stdout **Value Type:**string **Valid values:** stdout, stderr, network, [filename] **Changes Take Effect:** Immediately
Standard	standard	Specifies the outputs to which an application sends the log events of the Standard level. The log output types must be separated by a comma when more than one output is configured. For example: `standard = stderr, network`	**Default value:** stdout **Value Type:**string **Valid values:** stdout, stderr, network, [filename] **Changes Take Effect:** Immediately
Trace	trace	Specifies the outputs to which an application sends the log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels). The log outputs must be separated by a comma when more than one output is configured. For example:`trace = stderr, network`	**Default value:** stdout **Value Type:**string **Valid values:** stdout, stderr, network, [filename] **Changes Take Effect:** Immediately
Debug	debug	Specifies the outputs to which an application sends the log events of	**Default value:** stdout

Option	Name	Description	Value
		the Debug level and higher (that is, log events of the Standard, Interaction, Trace and Debug levels). The log outputs must be separated by a comma when more than one output is configured. For example: `debug = stderr, network`	**Value Type:**string **Valid values:** stdout, stderr, network, [filename] **Changes Take Effect:** Immediately
Verbose	verbose	Determines whether a log output is created. If it is, specifies the minimum level of log events generated. The log events levels, starting with the highest priority level, are Standard, Interaction, Trace, and Debug.	Default value: standard **Value Type:**chooseMultiple **Valid values:** all > debug | trace | interaction | standard | none **Changes Take Effect:** Immediately
Logging pattern	outputPattern	Specifies the output pattern that logs is formated to. Log4j/Log4j2 pattern format must be used.	Default value: %d{dd.MM.yyyy HH:mm:ss}> %-5.5p | %-45.80t | %-30.1000c{1} %m %ex%n **Value Type:**string **Changes Take Effect:** Immediately
Log compression	compressMethod	Specified method that will be used for archiving log files.	**Default value:** <empty> **Value Type:**enumerated type **Valid values:**

Option	Name	Description	Value
			[+] None None **[+] gzip** GZIP **[+] zip** ZIP **Changes Take Effect:** Immediately
Segment	segment	Specifies whether there is a segmentation limit for a log file. If there is, sets the mode of measurement, along with the maximum size. If the current log segment exceeds the size set by this option, the file is closed and a new one is created. This option is ignored if log output is not configured to be sent to a log file.	Default value: 100 MB **Value Type:**regular expression [^(?i)(false>(\d+) (kb|mb|hr))$] **Valid values:** false | <number>[KB] | <number> MB | <number> hr **Changes Take Effect:** Immediately
Expire	expire	Determines whether log files expire. If they do, sets the measurement for determining when they expire, along with the maximum number of files (segments) or days before the files are removed. This option is ignored if log output is not configured to be sent to a log file.	Default value: 10 **Value Type:**regular expression [^(?i)(false>(\d+) day|(\d+))$] **Valid values:** false | <number>[file] (1-1000) | <number> day (1-100)

Option	Name	Description	Value
			Changes Take Effect: Immediately
Time zone	timeConvert	Specifies the system in which an application calculates the log record time when generating a log file. The time is converted from the time in seconds since "00:00:00 UTC, January 1, 1970".	**Default value:** local **Value Type:**enumerated type **Valid values:** **[+] local** The time of log record generation is expressed as a local time, based on the time zone and any seasonal adjustments. Time zone information of the application's host computer is used. **[+] utc** The time of log record generation is expressed as Coordinated Universal Time (UTC). **Changes Take Effect:** Immediately
Time format	timeFormat	Specifies how to represent, in a log file, the time when an application generates log records. A log record's time field in the ISO 8601 format looks like this: "2001-07-24T04:58:10.123".	**Default value:** time **Value Type:**enumerated type **Valid values:** **[+] time** The time string is formatted according to

Option	Name	Description	Value
			"HH:MM:SS.sss" (hours, minutes, seconds, and milliseconds) format. **[+] locale** The time string is formatted according to the system's locale. **[+] iso8601** The date in the time string is formatted according to the ISO 8601 format. Fractional seconds are given in milliseconds. **Changes Take Effect:** Immediately
Message format	message-format	Specifies the format of log record headers that an application uses when writing logs in the log file. Using compressed log record headers improves application performance and reduces the log file's size.	**Default value:** custom **Value Type:**enumerated type **Valid values:** **[+] short** An application uses compressed headers when writing log records in its log file. **[+] medium** An application uses medium size headers when writing log records in its log file. **[+] full**

Option	Name	Description	Value
			An application uses complete headers when writing log records in its log file. **[+] shortcsv** An application uses compressed headers with comma delimiter when writing log records in its log file. **[+] shorttsv** An application uses compressed headers with tab char delimiter when writing log records in its log file. **[+] shortdsv** An application uses compressed headers with 'messageHeaderDelimiter' delimiter when writing log records in its log file. **[+] custom** Custom message format, specified in 'customMessageFormat' option. **Changes Take Effect:** Immediately

Configuring Resource Access Points

Genesys Knowledge Center requires two types of Resource Access Points to be configured:

- Elasticsearch Resource Access Point - used by the Knowledge Center Server to access the Elasticsearch cluster
- CMS Resource Access Point - used by Genesys components (for example, Universal Contact Server 9.1) to access the Knowledge Center CMS nodes within a cluster

Elasticsearch Resource Access Point Configuration Options

In section **resource**:

- option **type** must be set to value "elasticsearch".

For more information see Configure access to Elasticsearch.

CMS Resource Access Point Configuration Options

CMS Resource Access Point must have following options configured:

In section **resource**

- option **type** must be set to value "loadbalancer".
- option **solution** must be set to value "cms".

Load-Balancing Configuration

Deploying a Cluster

> **Important**
>
> Whenever you deploy a Knowledge Center Server instance, you must configure a Knowledge Center Cluster, even if you only plan on having one server.

Knowledge Center Cluster stores all of the settings and data that are shared by each of the Knowledge Center Server instances that reside within it. This makes it pretty easy to add additional servers as your knowledge needs grow.

Knowledge Center Cluster also serves as the entry point to all client requests sent to Knowledge Center Servers. The cluster application in Genesys Administrator needs to be configured to point to the host and port of the load balancer that will distribute these requests among your Knowledge Center Servers.

> **Important**
>
> If you only have one server deployed in your cluster, you can configure the cluster application to point directly to the host and port of that server.

Configuring Your Load-Balancer Solution

Let's take a look at how you might configure your load balancer to distribute requests between servers. This sample uses an Apache load balancer.

> **Important**
>
> Genesys recommends that you use a round-robin approach to balancing for Knowledge Center Server. If want to use a cluster of Knowledge Center CMS instances you'll need to use a sticky session strategy for load-balancing in order to keep authorized user on the same node.

> **Important**
>
> If you need more information about load balancing in a Genesys environment, the Genesys Web Engagement Load Balancing page provides some useful background information.

Prerequisites

- Several Knowledge Center Servers/Knowledge Center CMS should be installed. These servers will be used as cluster nodes (node1, node2, node3, and so on)
- You must have a Genesys Administrator application type Application Cluster
- An application created for each Knowledge Center Servers/Knowledge Center CMS in cluster
- All Knowledge Center Server/Knowledge Center CMS applications should be connected to the application cluster

Start

1. Install Nginx HTTP and reverse proxy server (https://nginx.org/en/). The port and host of the installed load balancer should be used in the Application Cluster application in Genesys Administrator.
2. Configure nginx as the load-balancer for your cluster. See below for an example of configuring from a nginx.conf file.
   - Pay close attention to the `upstream cluster_nodes` section; here you can add a list of nodes and then select the balancing method.
   - For Knowledge Center Servers, we recommend using `least_conn` balancing method (http://nginx.org/en/docs/http/ngx_http_upstream_module.html#least_conn)
   - For Knowledge Center CMS, we recommend using `ip_hash` (http://nginx.org/en/docs/http/ngx_http_upstream_module.html#ip_hash)
3. Restart nginx, then restart all of your nodes.
4. All requests that are sent to nginx will be distributed to your cluster nodes.

```
user nginx;
worker_processes 1;

error_log /var/log/nginx/error.log warn;
pid /var/run/nginx.pid;

events {
    worker_connections 1024;
}

http {
    include /etc/nginx/mime.types;
    default_type application/octet-stream;

    log_format main '$remote_addr - $remote_user [$time_local] "$request" '
                    '$status $body_bytes_sent "$http_referer" '
                    '"$http_user_agent" "$http_x_forwarded_for"';

    access_log /var/log/nginx/access.log main;
    sendfile on;
    #tcp_nopush on;

    keepalive_timeout 65;

    #gzip on;

    include /etc/nginx/conf.d/*.conf;

    server {
        listen 9999;
        underscores_in_headers on;
        location / {
        proxy_pass http://cluster_nodes;
        }
    }

    upstream cluster_nodes {
        ip_hash;

        server gkc-node-1:9010;
        server gkc-node-1:9010;
    }

}
```

End

Here are couple of sample requests:

- Request to a specific node: http://host_node_1:port_node_1/gks-sample-ui
- Request to the cluster, which will be distributed to any appropriate node: http://host_load_balacer:port_load_balancer/gks-sample-ui

Security

Genesys is committed to offering products and solutions with a high level of security. Opening Application Programming Interface (API) access on the web requires a secure transmission. Genesys Knowledge Center does not compromise the security level of the enterprise network.

Genesys Knowledge Center adheres to the standards described in the Open Web Application Security Project (OWASP) Top 10 — see the OWASP website for details about the Top 10 — and has adopted several methods of ensuring security, for example:

- Errors are logged locally to prevent information leakage through API requests.
- User sessions have a timeout option.
- Cross Site Request Forgery Protection

The following topics discuss issues that you may wish to consider when deploying the Genesys Knowledge Center, depending on your enterprise network architecture.

> ### Important
> Genesys performs security testing with OWASP Zed Attack Proxy (ZAProxy) to make sure the Genesys Knowledge Center solution is invincible to known attacks.

Genesys Knowledge Center includes additional security configurations that can be used with your Knowledge Center installation:

- Transport Layer Security (TLS) with Genesys Server — Configure TLS for connection between Knowledge Center servers and other Genesys server.
- Authentication — Enable authentication for the Knowledge Center Server and the CMS.
- Cross Origin Resource Sharing (CORS) filter — Configure web resources that are allowed to access Knowledge Center APIs

Transport Layer Security (TLS) with Genesys Servers

Genesys Knowledge Center Server and Genesys Knowledge Center CMS supports the Transport Layer Security (TLS) protocol to secure data exchanged with other Genesys components. For details about TLS, see the Genesys Security Deployment Guide.

Configure TLS between Genesys Knowledge Center Server and Genesys Knowledge Center CMS

If Genesys Knowledge Center Server or Load-Balancer have been used for Servers Cluster configured to run in TLS mode, you'll need to ensure that its root certificate has been added to the trusted store of JDK/JRE used by Genesys Knowledge Center CMS. Without this CMS it will not possible to establish a connection with Knowledge Center Server for background operations.

Configuring TLS for Genesys Servers

To configure the TLS parameters for Genesys servers, see Introduction to Genesys Transport Layer Security.

Configuring TLS Options

For connections with other Genesys servers, configure **Connections** of the Knowledge Center Cluster (8.5.1+) application through secure ports. The Genesys Knowledge Center Server or CMS nodes includes the following TLS-related configuration options in its security section.

Parameter Name	Acceptable Values	Purpose
tls	Boolean value. Possible values are "1"/"0", "yes"/"no", "on"/"off", "true"/"false". Example: • "tls=1"	Client: 1 - perform TLS handshake immediately after connecting to server. 0 – do not turn on TLS immediately but autodetect can still work.
provider	"PEM", "MSCAPI", "PKCS11" Not case-sensitive. Example: • "provider=MSCAPI"	Explicit selection of security provider to be used. For example, MSCAPI and PKCS11 providers can contain all other parameters in their internal database. This parameter allow configuration of TLS through security provider

Parameter Name	Acceptable Values	Purpose
		tools.
certificate	PEM provider: path to a X.509 certificate file in PEM format. Path can use both forward and backward slash characters. MSCAPI provider: thumbprint of a certificate – string with hexadecimal SHA-1 hash code of the certificate. Whitespace characters are allowed anywhere within the string. PKCS11 provider: this parameter is ignored. Examples: • "certificate= C:\certs\client-cert-3-cert.pem" • "certificate=A4 7E A6 E4 7D 45 6A A6 2F 15 BE 89 FD 46 F0 EE 82 1A 58 B9"	Specifies location of X.509 certificate to be used by application. MSCAPI provider keeps certificates in internal database and can identify them by hash code; so called thumbprint. In Java, PKCS#11 provider does not allow selection of the certificate; it must be configured using provider tools. **Note:** When using autodetect (upgrade) TLS connection, this option MUST be specified in application configuration, otherwise Configuration Server would return empty TLS parameters even if other options are set.
certificate-key	PEM provider: path to a PKCS#8 private key file without password protection in PEM format. Path can use both forward and backward slash characters. • MSCAPI provider: this parameter is ignored; key is taken from the entry identified by "certificate" field. • PKCS11 provider: this parameter is ignored. Examples: • "certificate-key= C:\certs\client-cert-3-key.pem"	Specifies location of PKCS#8 private key to be used in pair with the certificate by application. MSCAPI provider keeps private keys paired with certificates in internal database. In Java, PKCS#11 provider does not allow selection of the private key; it must be configured using provider tools.
trusted-ca	PEM provider: path to a X.509 certificate file in PEM format. Path can use both forward and backward slash characters. MSCAPI provider: thumbprint of a certificate – string with hexadecimal SHA-1 hash code of the certificate. Whitespace characters are allowed anywhere within the string. PKCS11 provider: this parameter is ignored. Examples: • "trusted-ca= C:\certs\ca.pem"	Specifies location of a X.509 certificate to be used by application to validate remote party certificates. The certificate is designated as Trusted Certification Authority certificate and application will only trust remote party certificates signed with the CA certificate. MSCAPI provider keeps CA certificates in internal database and can identify them by hash code; so called thumbprint. In Java, PKCS#11 provider does not allow selection of the CA certificate; it must be configured using provider tools.

Parameter Name	Acceptable Values	Purpose
	• "trusted-ca=A4 7E A6 E4 7D 45 6A A6 2F 15 BE 89 FD 46 F0 EE 82 1A 58 B9"	
tls-mutual	Boolean value. Possible values are "1"/"0", "yes"/"no", "on"/"off", "true"/"false". Example: • "tls-mutual=1"	Has meaning only for server application. Client applications ignore this value. When turned on, server will require connecting clients to present their certificates and validate the certificates the same way as client applications do.
tls-crl	All providers: path to a Certificate Revocation List file in PEM format. Path can use both forward and backward slash characters. Example: • "tls-crl= C:\certs\crl.pem"	Applications will use CRL during certificate validation process to check if the (seemingly valid) certificate was revoked by CA. This option is useful to stop usage of leaked certificates by unauthorized parties.
tls-target-name-check	"host" or none. Not case-sensitive. Example: • "tls-target-name-check=host"	When set to "host", enables matching of certificate's Alternative Subject Name or Subject fields against expected host name. PSDK supports DNS names and IP addresses as expected host names.
cipher-list	String consisting of space-separated cipher suit names. Information on cipher names can be found online. Example: • "cipher-list= TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA"	Used to calculate enabled cipher suites. Only ciphers present in both the cipher suites supported by security provider and the cipher-list parameter will be valid.
fips140-enabled	Boolean value. Possible values are "1"/"0", "yes"/"no", "on"/"off", "true"/"false". Example: • "fips140-enabled=1"	PSDK Java: when set to true, effectively is the same as setting "provider=PKCS11" since only PKCS11 provider can support FIPS-140. If set to true while using other provider type, PSDK will throw exception.
sec-protocol	String value. Possible values are "SSLv23", "SSLv3", "TLSv1", "TLSv11", "TLSv12".	Starting with PSDK release 8.5.1, an application can specify the exact protocol to send and accept secure connection

Parameter Name	Acceptable Values	Purpose
	Example: • "sec-protocol=TLSv1"	requests on one or more of its connections.

See Configuring Trusted Stores below for details about configuration for a specific type of store (PEM, JKS, MSCAPI).

Configuring Trusted Stores

PEM Trusted Store

PEM stands for "Privacy Enhanced Mail", a 1993 IETF proposal for securing email using public-key cryptography. That proposal defined the PEM file format for certificates as one containing a Base64-encoded X.509 certificate in specific binary representation with additional metadata headers.

PEM certificate trusted store works with CA certificate from an X.509 PEM file. It is a recommended trusted store to work on Linux systems.

Complete the steps below to work with the PEM certificate trusted store:

Start

1. Configure TLS for Genesys servers to use certificates signed by CA certificate **certificateCA.crt**.
2. Place the trusted CA certificate in PEM format on the Genesys Knowledge Center Server application host. To convert a certificate of another format to .pem format you can use the OpenSSL tool. For example:
    - Convert a DER file (.crt .cer .der) to PEM:
      ```
      openssl x509 -inform der -in certificateCA.crt -out certificateCA.pem
      ```
    - Convert a PKCS#12 file (.pfx .p12) containing a private key and certificates to PEM:
      ```
      openssl pkcs12 -in certificateCA.pfx -out certificateCA.pem -nodes
      ```

      You can add **-nocerts** to only output the private key or add **-nokeys** to only output the certificates.
3. In Genesys Administrator, navigate to **Provisioning > Environment > Applications** and open your Knowledge Center Server application.
4. Click the **Options** tab and navigate to the security section.
5. Set the **trusted-ca-type** option to PEM.
6. Set the **trusted-ca** option to the path and file name for your trusted CA in PEM format on the Genesys Knowledge Center Server application host.
7. Click **Save & Close**.

End

JKS Trusted Store

A Java KeyStore (JKS) is a repository of security certificates used, for instance, in SSL/TLS encryption. The Java Development Kit provides a tool named keytool to manipulate the keystore.

Complete the steps below to work with the JKS certificate trusted store:

Start

1. Configure TLS for Genesys servers to use certificates signed by CA certificate **certificateCA.crt**.
2. Import the CA certificate to an existing Java keystore using keytool:
    - Run the `keytool` command with option `-alias` set to `root`:
      ```
      keytool -import -trustcacerts -alias root -file certificateCa.crt -keystore
       /path/to/keysore/keystore.jks
      ```
    - Enter the keystore password in command line prompt - for example:
      ```
      Enter keystore password: somepassword
      ```
3. In Genesys Administrator, navigate to **Provisioning > Environment > Applications** and open your Knowledge Center Server application.
4. Click the **Options** tab and navigate to the security section.
5. Set the **trusted-ca-type** option to JKS.
6. Set the **trusted-ca** option to the path and file name for your JKS trusted storage type on the Genesys Knowledge Center Server application host.
7. Set the **trusted-pwd** option to the password defined for your keystore in Step 2.
8. Click **Save & Close**.

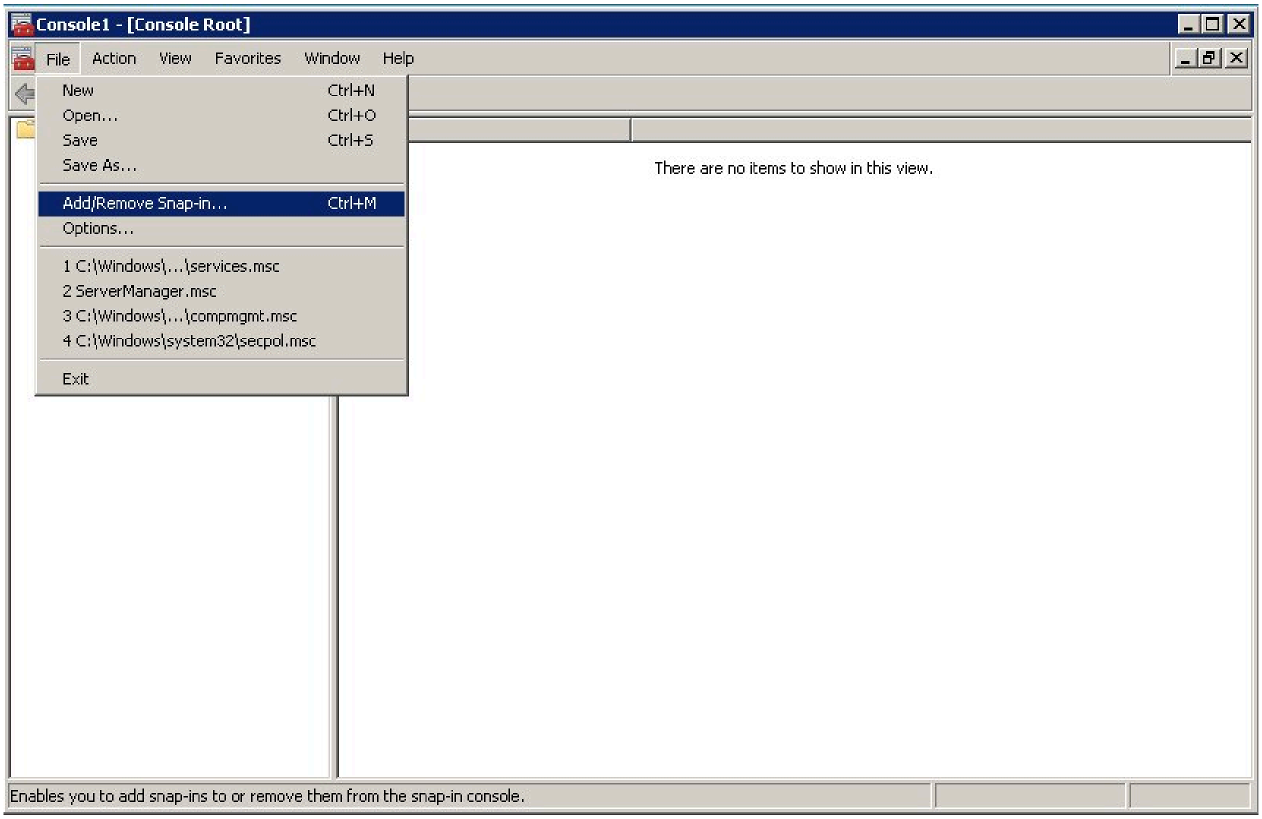
End

MSCAPI Trusted Store

Complete the steps below to work with the MSCAPI certificate trusted store:

Start

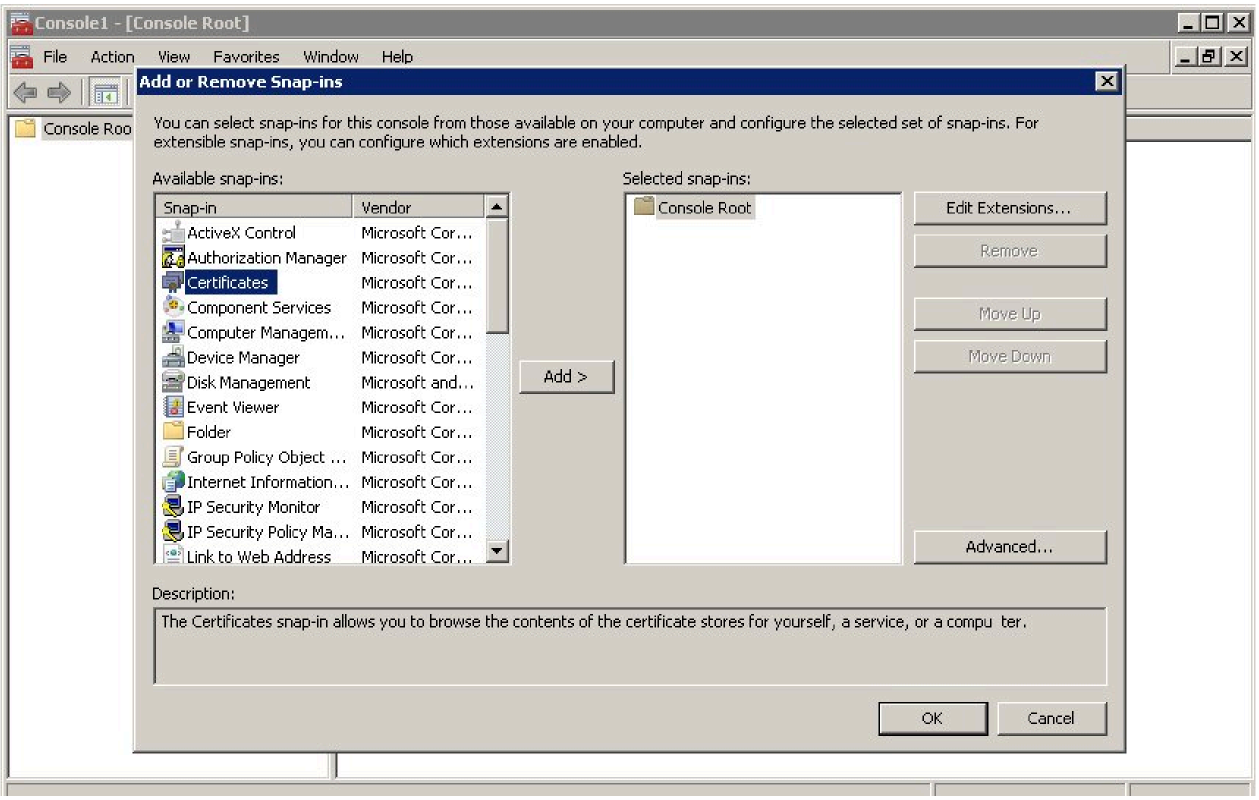
1. Configure and tune TLS for Genesys servers to use certificates signed by the same CA.
2. If the Knowledge Center Server is running on a different host, copy the trusted CA certificate to this host.
3. Import the CA certificate to WCS via Certificates Snap-in on the Knowledge Center Server host by launching the MMC console. Enter `mmc` at the command line.
4. Select **File > Add/Remove Snap-in...** from the main menu.


Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Windows\...\services.msc
2 ServerManager.msc
3 C:\Windows\...\compmgmt.msc
4 C:\Windows\system32\secpol.msc
Exit

There are no items to show in this view.

Enables you to add snap-ins to or remove them from the snap-in console.

5. Select **Certificates** from the list of available snap-ins and click **Add**.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
Internet Information...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy Ma...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

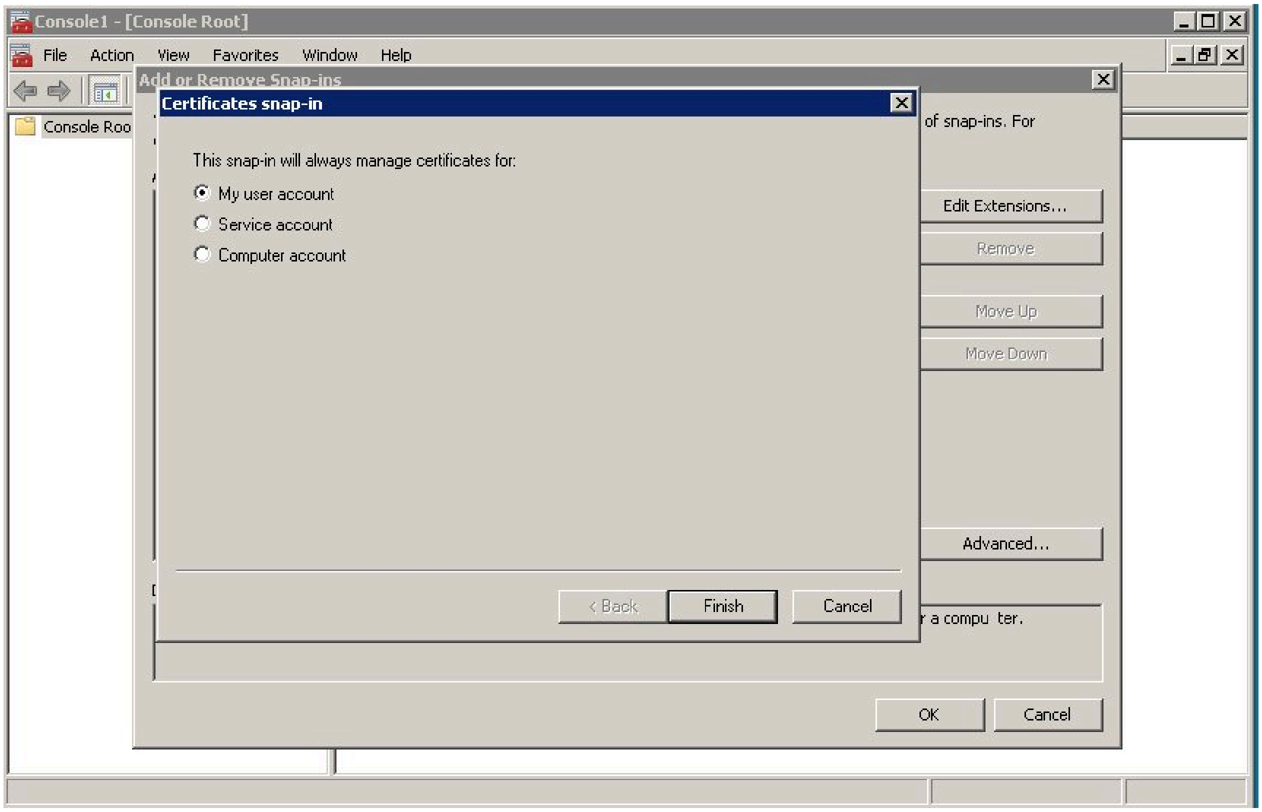
Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a compu ter.

6. Select the account to manage certificates for and click **Finish**. It is important to place certificates under the correct Windows account. Some applications are run as services under the Local Service or System account, while others are run under user accounts. The account chosen in MMC must be the same as the account used by the application which certificates are configured for, otherwise the application will not be able to access this WCS storage.



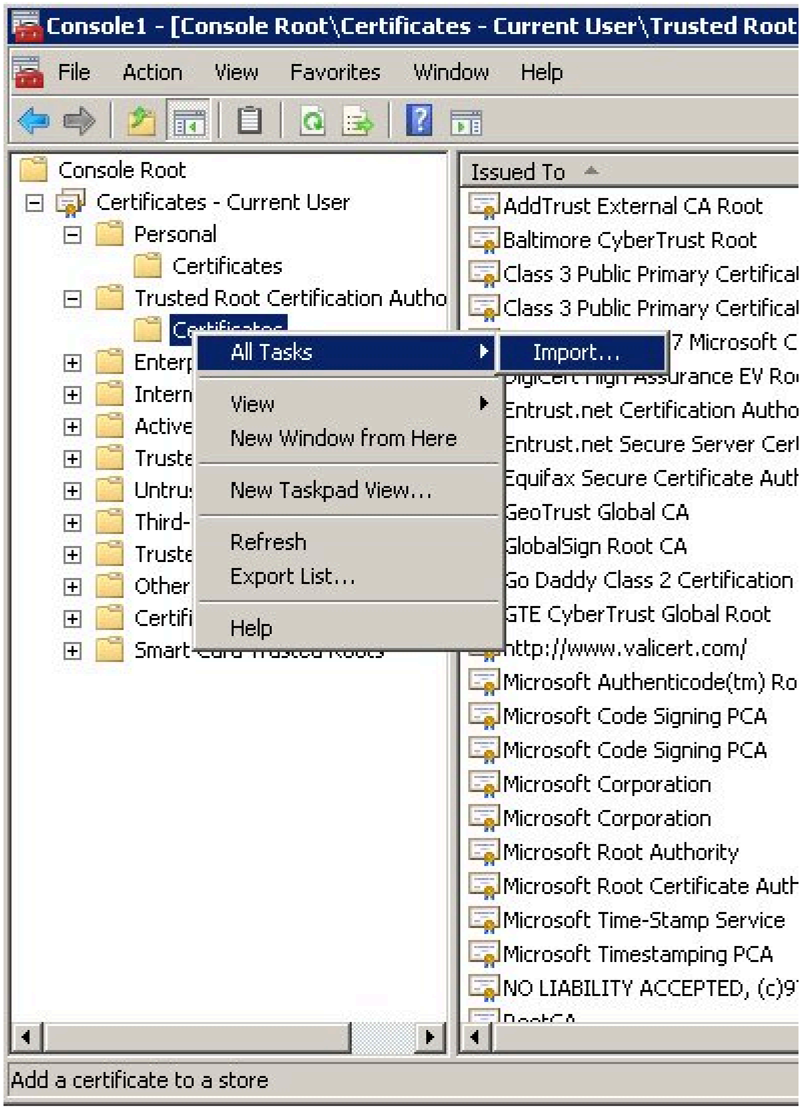
This snap-in will always manage certificates for:

● My user account

○ Service account

○ Computer account

7. Click **OK**.
8. Import a certificate. Right-click the "Trusted Root Certification Authorities/Certificates" folder and choose `All Tasks > Import...` from the context menu. Follow the steps presented by the Certificate Import Wizard. Oonce finished the imported certificate appears in the certificates list.


Console1 - [Console Root\Certificates - Current User\Trusted Root
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Autho
Certificates
Enterp
Intern
Active
Truste
Untru
Third-
Truste
Other
Certifi
Smart Card Trusted Roots
All Tasks
Import...
View
New Window from Here
New Taskpad View...
Refresh
Export List...
Help
Issued To
AddTrust External CA Root
Baltimore CyberTrust Root
Class 3 Public Primary Certifica
Class 3 Public Primary Certifica
7 Microsoft C
DigiCert High Assurance EV Roo
Entrust.net Certification Autho
Entrust.net Secure Server Cer
Equifax Secure Certificate Auth
GeoTrust Global CA
GlobalSign Root CA
Go Daddy Class 2 Certification
GTE CyberTrust Global Root
http://www.valicert.com/
Microsoft Authenticode(tm) Ro
Microsoft Code Signing PCA
Microsoft Code Signing PCA
Microsoft Corporation
Microsoft Corporation
Microsoft Root Authority
Microsoft Root Certificate Auth
Microsoft Time-Stamp Service
Microsoft Timestamping PCA
NO LIABILITY ACCEPTED, (c)97
RootCA

Add a certificate to a store

9. In Genesys Administrator, navigate to **Provisioning > Environment > Applications** and open your Knowledge Center Server application.
10. Click the **Options** tab and navigate to the security section.
11. Set the **trusted-ca-type** option to MSCAP.
12. Click **Save & Close**.

End

Authentication

You can enable secure communications with the Management and Reporting REST APIs by completing the procedures below to implement authentication. If you do enable authentication, then all API clients must use the authentication scheme and credentials. Three common clients of the API are the Genesys Knowledge Center Plugin for Administrator, Genesys Knowledge Center Plugin for Workspace Desktop Edition and Genesys Knowledge Center CMS.

Configuring Authentication in Genesys Knowledge Center

Complete the steps below to enable authentication for the Management and Reporting REST APIs.

Start

1. In Genesys Administrator, navigate to **Provisioning > Environment > Applications**, select the Knowledge Center Cluster application, and click **Edit...**.
2. Click the **Options** tab and scroll down to the **[security]** section.
3. Set the following options:
   - auth-scheme
   - user-id
   - password
4. Click **Save & Close**.

End

Cross Origin Resource Sharing (CORS) Filter

What is CORS?

Since the browser Same Origin Policy prevents a web page from making an XMLHttpRequest to another domain, the Genesys Knowledge Center supports Cross Origin Resource Sharing (CORS) to allow the web application to interact with the Knowledge Center APIs across domains.

For a simple request — one that uses either GET or POST and whose body is text/plain — the request is sent with an extra header called Origin. The Origin header contains the origin URI (scheme, domain name or address, and port, as per RFC 6454) of the requesting page so that the server can easily determine whether or not it should serve a response. An example Origin header might look like this:

`Origin:` http://www.genesys.com:8080

If the server decides that the request should be allowed, it either sends an Access-Control-Allow-Origin header echoing back the same origin that was sent or '*' if it is a public resource.

For example:

`Access-Control-Allow-Origin:` http://www.genesys.com:8080

If this header is missing, or the value of this header does not match the value of Origin header, then the browser disallows the request. If all is well, then the browser processes the response.

For general information and background on CORS, see Cross-Origin Resource Sharing.

Configuring CORS Filter

Knowledge Center supports the CORS pre-flight OPTIONS requests.

Types of requests:

- A CORS request is an HTTP request that includes an `Origin` header.
- A CORS-preflight request is a CORS request that checks to see if the CORS protocol is understood. It uses `OPTIONS` as method.

Allowed-Origins

To set up Cross-Origin Resource Sharing, make sure you set the `allowedOrigins` option in the `cross-origin` section of Knowledge Center Cluster application. Knowledge Center will use the provided list of domains to validate the `Origin` header of the request and respond with `Access-Control-Allow-Origin` in response.

> **Important**
>
> By default `cross-origin/allowedOrigins` is set to ***** which makes it possible to use Knowledge Center APIs from any web resource. Before going into production mode, the default value of this option MUST be updated with the most precise list of origins in which API access is allowed.

`allowedOrigins` option must be set as a comma-separated list of allowed domains. For example:

```
allowedOrigins=http://*.genesys.com,http://*.genesyslab.com
```

Other CORS options

All options are collected in section `cross-origin` (default), however the name of this section can be changed. **Note:** Genesys Knowledge Center has two application servers, while CMS and every other application have their own section: `gks.cross-origin` and `cms.cross-origin`.

Option	Description	Default value
skipCheckControlRequestHeaders	Allow pass **CROSS** preflight request with out check Access-Control-Request-Headers.	false **for Genesys Knowledge Center:** true
preflightMaxAge	The number of seconds that preflight requests can be cached by the client.	1800 seconds, or 30 minutes **for Genesys Knowledge Center:** 3600 seconds, or 60 minutes
passBlockedRequestToChain	Allow pass next chain if this request is **CROSS** request but not allowed by origin, method, or header.	true
exposedHeaders	A whitelist of additional response headers to be exposed to the browser tab beyond the default headers.	Cache-Control,Content-Language,Content-Type,Expires,Last-Modified,Pragma **for Genesys Knowledge Center:** gkc_agentId,gkc_apiClientId,gkc_apiClientMediaType, gkc_customerId,gkc_interactionId,gkc_sessionId, ContactCenterID,Authorization,contentType
enable	Boolean value that allows `cross-origin` filter.	true
emptyAllowedFor	A comma-separated list of requested URLs that are allowed to access this server application in the case when there is no	.* (any request)

Option	Description	Default value
	Origin and **Referer**. This option is affected if `allowOrigin` does not contain "*" (any origin).	
disableHttpOptionsRequest	Boolean value that disables the **OPTIONS** http request if it is `true`. If it is `false` we cannot use preflight requests.	false
checkReferer	Boolean value; will answer **Referrer** canonized to **Origin** instead of **Origin** for use with native **CrossOrigin** check. If this option is enabled: • Origin present and Referrer present and both are valid (filter recognizes them as allowed for CrossOrigin), so CrossOrigin headers are added to response. • Origin absent and Referrer present and valid, so CrossOrigin headers are added to response. • Origin present and Referrer present and one of them is invalid, so CrossOrigin headers are not added to response.	true
chainPreflight	If `true`, preflight requests are chained to their target resource for normal handling (as an **OPTION** request). Otherwise the filter responds to the preflight.	true
allowedOrigins	A comma-separated list of origins (for example, instrumented web sites) allowed to access this server application. If an allowed origin contains one or more "*" characters (for example http://*.domain.com) this can be interpreted as a regular expression.	"*" (any origin)
allowedMethods	a comma-separated list of **HTTP** methods that are allowed to be used when accessing the resources (for preflight requests).	GET,POST,HEAD **for Genesys Knowledge Center:** GET,POST,HEAD,PUT,DELETE, ATCH
allowedHeaders	a comma separated list of **HTTP** headers that are allowed to be	X-Requested-With,Content-Type,Accept,Origin

Option	Description	Default value
	specified when accessing the resources (for preflight requests).	**for Genesys Knowledge Center:** gkc_agentId,gkc_apiClientId,gkc_apiClientMediaType, gkc_customerId,gkc_interactionId,gkc_sessionId, ContactCenterID,Authorization,contentType,Content-Type
allowCredentials	A boolean indicating if the resource allows requests with credentials.	false **for Genesys Knowledge Center:** true

For morel information and background on CORS and response headers, see Cross Origin Resource Sharing Standard.

Translation service

> **Important**
>
> Usage of translation service will result in the document content being transferred to the 3rd-party translation provider. By enabling this feature you authorize your authors to perform such operations with the pre-configured translation service. Usage of translation service will result in the service fee according to the pricing policy of the translation provided and configured.

What is translation service?

Knowledge Center can use 3rd-party translation APIs to enable authors with a capability to automatically translate the content of knowledge documents from one language to another.

Authors can translate the whole document or just particular fields of the document. Automated translation allows using state-of-the-art Neural Machine Translation (NMT) to simplify an authors work by avoiding routine translation done by computer. The Author is able to review and edit pre-translated content before saving.

Supported Translation APIs

Knowledge Center supports following Translation APIs:

- Cloud Translation API
- Microsoft Translator Text API
- Yandex.Translate API

Configuring Translation Service

The Administrator is able to configure the translation service for the Knowledge Center cluster by setting following option:

1. In the section translation set option **Translation Service** (type) to one of the following values:
   - none - translation service is disabled (default value)
   - google - Cloud Translation API
   - microsoft - Microsoft Translator Text API

- yandex - Yandex.Translate API

2. In the section translation, set option **API Key** (key) to the value of API key provided by the selected translation provider.

Getting API key

Important

This chapter provides sample steps to get API Key from one of the supported translation providers. Please always refer to the documentation of the selected provider to get up-to-date information on configuration on API keys and pricing.

Warning

Usage of Translation API will result in changes on your account according to pricing policy of the selected provider.

Each of the providers of text translation functionality has its own way of obtaining the API key:

Google

1	Set up Google cloud project	1. Sign in at Google cloud console 2. Create new or open one of your existing project
2	Add "Cloud Translator API" to your project	1. Open **APIs and Services > Dashboard** 2. Click **ENABLE APIS AND SERVICES** 3. Search for and click **Cloud Translation API** 4. Click **ENABLE** A console will ask you to enable billing. After you approve use of billing, Cloud Translator API is added to your project.
3	Create API key	1. Open **APIs and Services >**

		Credentials 2. Click **Create credentials > API key** API key is created and ready to use.

Microsoft

-

1	Sign into Azure	• Don't have an account? Sign-up for a Microsoft Azure account • Already have an account? Sign-in
2	Subscribe to Microsoft Translator	1. After you sign into Azure, navigate to **Cognitive Services** 2. Under **API Type** select **Text or Speech API** • You can only add one Translator API subscription at a time 3. In the Pricing Tier section, select the pricing tier that best fits your needs • Each subscription has a free tier. The free tier has the same features and functionalities as the paid plans and does not have an expiration date 4. Fill out the rest of the form, and select **Create** • All subscriptions go into effect immediately
3	Retrieve Authentication Key	1. Navigate to **All Resources** and click on your subscription to retrieve your authentication key • The Key value is used for authentication so keep

		the Key value confidential. You will need this when you develop your app.

Yandex

1	Sign into Yandex	Use the Yandex home page to sign-in or sign-up.
2	Create API key	Navigate to **API keys** and click **Create key**. In the popup, enter the description of your key and click **Create**.

IP Geolocation

> **Important**
> Collecting information about a customer's location and the way it is stored may be subject to regulations or restrictions within your country or countries you operate in. Please check with your national legislation to ensure you are not in violation. This feature can be turned off if needed.

What is Geolocation

Geolocation is the identification or estimation of the real-world geographic location of an object. IP geolocation is the process geolocation that is based on the client's IP address as the into a physical location.

When geolocation is enabled it allows Genesys Knowledge Center to store client IP address and its relevant geolocation information in the History index. Stored information is mostly useful in the reports allowing to understand regional differences in the knowledge usage by the agent and customer.

IP geolocation is inherently imprecise. Locations are often near the center of the population. Any location provided should not be used to identify a particular address or household.

The actual location of the IP address is likely within some radius area around the latitude and longitude coordinates.

Configuring IP Geolocation

The Administrator is able to configure the precision of the geolocation for the Knowledge Center cluster (cluster/reporting/geo) as:

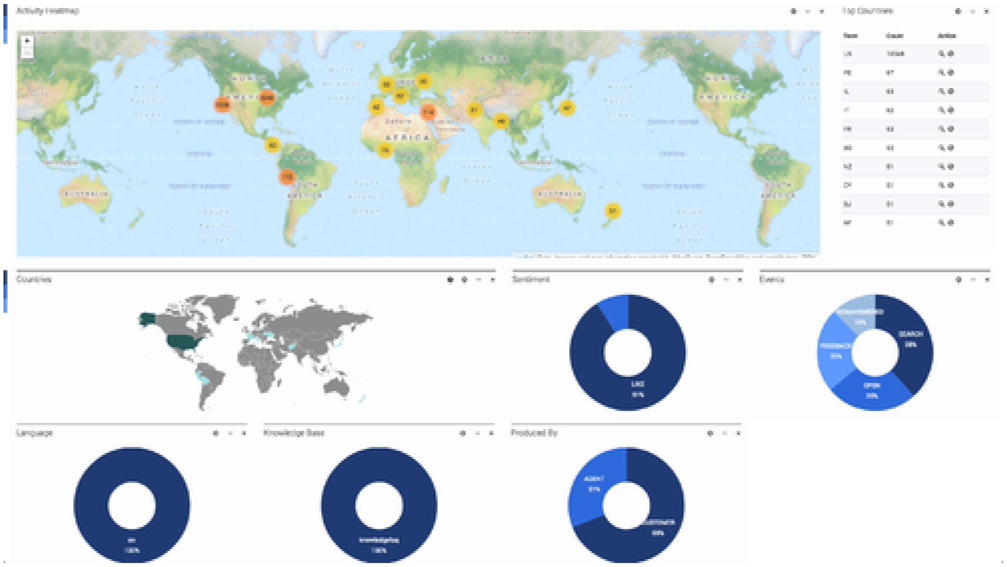
- off - disable the IP geolocation functionality: both IP and longitude and latitude are empty for historical records
- IP - only IP address is stored, Knowledge Center is not identifying geographic location of the customer
- country - IP and country name longitude and latitude of country are stored
- city (default) - IP, country name and and city longitude and latitude are stored

Described levels are defined in the Knowledge Center Cluster option geo that is located in section reporting.

Visualize the Geolocation Information

This stored data is used in the Kibana to visualize:

- a geo-map with requests heat indicators
- the top 10 countries



Activity Heatmap

How to Update the Geolocation Database

Geolocation functionality requires a special database to translate a client's IP address to the geographical location of the customer. When Genesys Knowledge Center Server is installed it provides the MaxMind GeoLite2 City database stored in **<installation directory>\linguatools\geoip folder**. The folder storing the database can be changed in the **gks.yml** file:

```
...
path.geoip : <IP folder>/GeoIP/GeoLiteCity.dat
...
```

To update the database you need to:

1. Visit MaxMind GeoLite2 database download page. Note: Knowledge Center is not supposed to work with other MaxMind products (for example, GeoLite or GeoIP, please use GeoLite2).
2. Download the most recent version of the City database.**Note**: Please download database in MaxMind DB binary format.
3. Unarchive the database.
4. Store the database in the folder configured in the `gks.yml` file
5. Restart Genesys Knowledge Center Server.

Important

- These steps needs to be executed for every Knowledge Center Server node in the cluster.
- You can store the geolocation database in shared network location to ensure that it is updated for all Knowledge Center Server nodes.

UTF8

You can configure your Knowledge Center Servers and Knowledge Center CMS to support UTF-8 in Configuration Server, which in turn supports multi-language categories.

Configuring a UTF-8 Connection to Configuration Server

Complete the following steps for your Knowledge Center Servers.

Prerequisites

- Your version of Configuration Server supports UTF-8. For details, see the compliant versions for mandatory components.

Start

1. Navigate to the installation directory for your Knowledge Center Server and open the **setenv.bat** file for Windows — or the **setenv.sh** file for Linux — with a text editor. For example: *Path to installation directory*/server/setenv.bat.
2. Find the following string: **:: set JAVA_OPTS=%JAVA_OPTS% -Dgenesys.cfgServerUseUtf8=true**.
3. Remove the two colons (**::**) at the start. This converts the string from a comment to a command to use UTF-8. Your string should now look like this: **set JAVA_OPTS=%JAVA_OPTS% -Dgenesys.cfgServerUseUtf8=true**
4. Save your changes.

End

Supported Languages

Genesys Knowledge Center supports a search for the right answer in any language. It executes a knowledge search involving different natural language processing techniques to come up with the best suggestions for the question asked. The level of the search processing functionality depends on the language. The table below lists the languages that have advanced search processing, along with the level of advanced processing support for each language.

Content Language	Product Version	Advanced Natural Language Processing Level
English	8.5.000+	▮▮▮▮
Danish	8.5.302+	▮▯▯▯
Finnish	8.5.302+	▮▯▯▯
	9.0.003+	▮▮▯▯
French	8.5.100+	▮▮▮▯
German	8.5.100+	▮▯▯▯
	8.5.304+	▮▮▮▯
Italian	8.5.100+	▮▮▮▯
Norwegian	8.5.302+	▮▮▯▯
Portuguese	8.5.100+	▮▮▮▯
Spanish	8.5.100+	▮▯▯▯
	8.5.304+	▮▮▯▯
Swedish	8.5.302+	▮▮▯▯
	8.5.304+	▮▮▮▯
Croatian	9.0.003+	▮▮▯▯
Romanian	9.0.003+	▮▮▯▯

For languages not listed in the table above, Genesys Knowledge Center provides a keyword-based search of the available knowledge articles.

Supported syntax for questions

Knowledge Center can handle both natural language queries (when you express your question in human language) as well as keyword-based queries.

Example queries:

```
Natural-language query: How to install Knowledge Center CMS?
Keyword query: install CMS
```

For languages that support natural-language techniques, you can use either query type. For languages that use a basic keyword search (those not listed in the table above), keyword queries provide favorable results compared to natural language queries. If necessary, decrease the “out-of-domain” limit to include results having lower confidence levels in the final result set.

How to configure the out-of-domain limit

The out-of-domain limit defines the minimum confidence level for a document to appear in the result set. It enables you to hide less relevant documents in search results. To change the out-of-domain limit, edit the option in the properties of your knowledge base.

- For instructions on how to configure the out-of-domain limit, see the Behavior Options section of the Managing Knowledge Bases topic, in the *Genesys Knowledge Center Help*.

The out-of-domain limits range from `0`, representing 0% confidence, to `1`, 100% confidence. The value 0.75 is considered a *magic value*. It corresponds to the exact match between the search term and the document, without proof of learning signals. Every learning signal (for example, positive relevancy feedback) improves it further.

The following table lists recommended out-of-domain limits:

Advanced Natural Language Processing Level	Out-of-domain value
None	0.20
▮▮▮▮	0.50
▮▮▮▯	0.46
▮▮▯▯	0.38
▮▯▯▯	0.35

For knowledge bases with multiple languages, you must set the out-of-domain limit to the lowest of the possible values. For example, if your knowledge base includes articles in both English and French, the recommended values 0.5 for English and 0.46 for French. The recommended value for the entire knowledge base is 0.46.

Screening Rules and Standard Responses

Overview

Knowledge Center allows users to:

- Create and edit Standard Responses—an item in the Standard Response Library, which stores pre-written responses for use as suggestions to agents, acknowledgments, and/or autoresponses.
- Create and edit Screening Rules in order to screen interactions for specific words or phrases, which you can then use to decide how to handle the interaction.

Important

This functionality is aimed to be used in the environment that uses Universal Contact Server 9.1 and later. Additional information can be found in the UCS 9.1 documentation at the following locations:

- Integration with Genesys Knowledge Center/Content Management System 9.0
- Deploying GKC Content Management Server

Important

If you are using Universal Contact Server 8.x it is recommended you disable Screening Rules and Standard Responses in Knowledge Center CMS.
Universal Contact Sever 8.x uses its own storage for Standard Response and Screening Rules, and eService Manager must be used to manage them. For more information, see eServices Manager Plug-in for GAX.

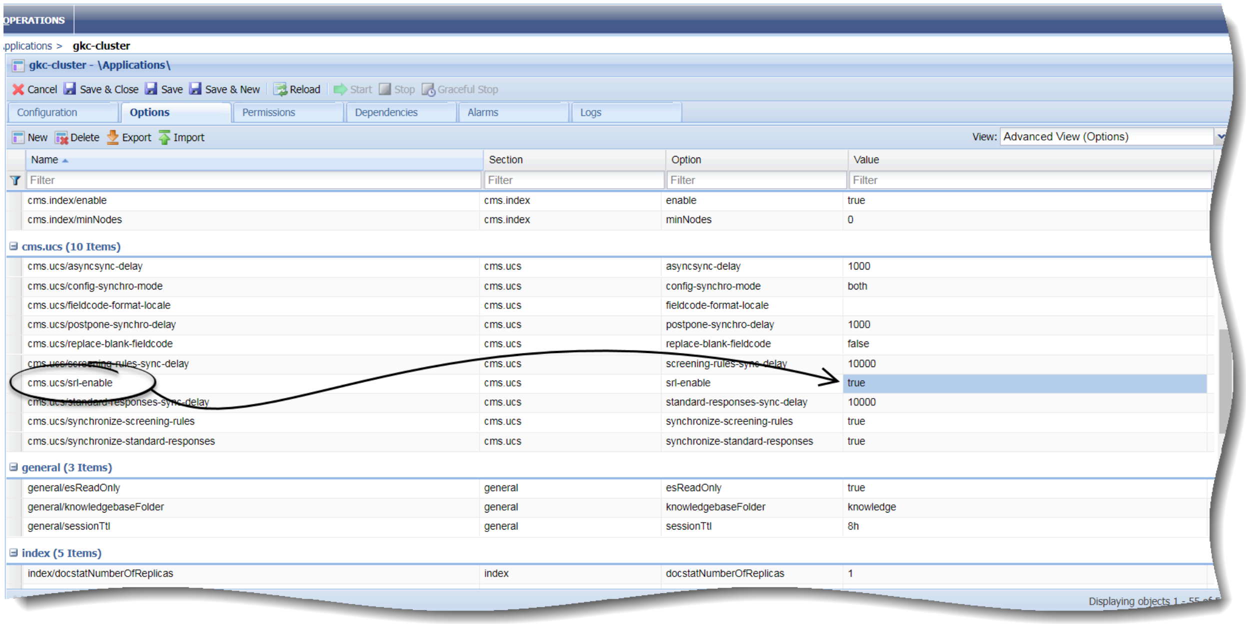
This following describes how to enable and disable Screening Rules and Standard Responses in Knowledge Center CMS.

Enabling Standard Reponse

By default, the Standard Response functionality is disabled so we must first enable it either through Genesys Administrator or Genesys Administrator Extension (GAX).

How to enable Standard Response through Genesys Administrator

1. Log in to Genesys Administrator through GAX.
2. Click the **Provisioning** tab.
3. From the **Environment** folder, select **Applications**.
4. Double-click **gkc-cluster**.
5. Select the **Options** tab.
6. Navigate to **cms.ucs > cms.ucs\srl-enable**.
7. Set the **Value** to `true`



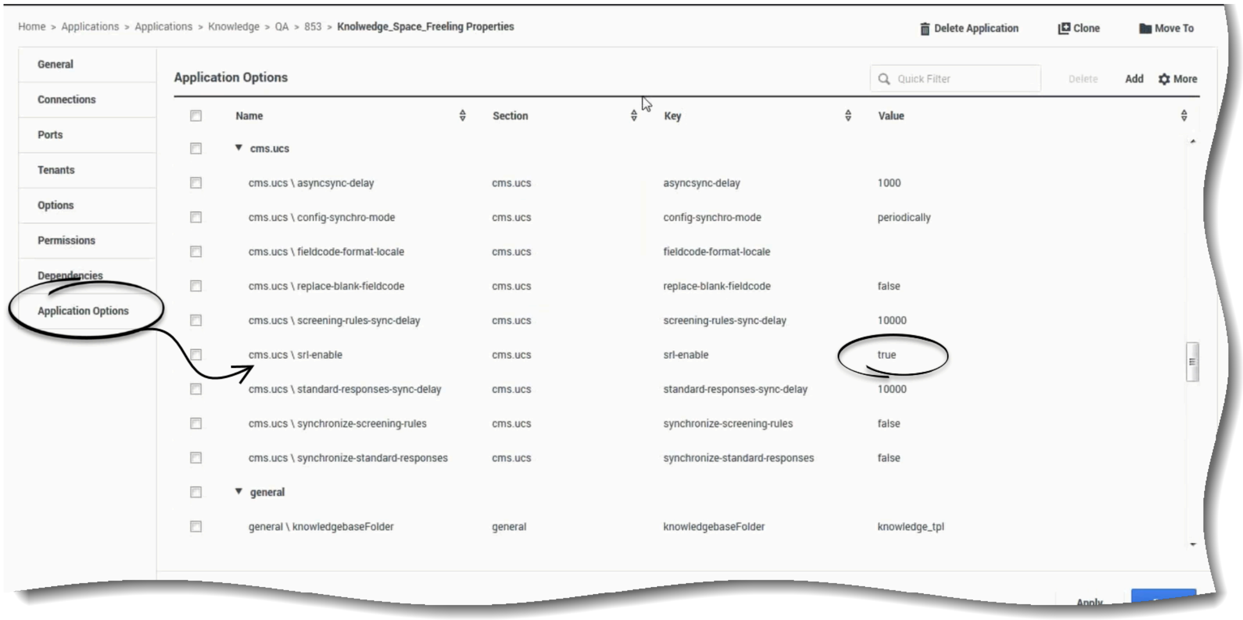
View: Advanced View (Options)

Name	Section	Option	Value
Filter	Filter	Filter	Filter
cms.index/enable	cms.index	enable	true
cms.index/minNodes	cms.index	minNodes	0
cms.ucs (10 Items)			
cms.ucs/asyncsync-delay	cms.ucs	asyncsync-delay	1000
cms.ucs/config-synchro-mode	cms.ucs	config-synchro-mode	both
cms.ucs/fieldcode-format-locale	cms.ucs	fieldcode-format-locale	
cms.ucs/postpone-synchro-delay	cms.ucs	postpone-synchro-delay	1000
cms.ucs/replace-blank-fieldcode	cms.ucs	replace-blank-fieldcode	false
cms.ucs/screening-rules-sync-delay	cms.ucs	screening-rules-sync-delay	10000
cms.ucs/srl-enable	cms.ucs	srl-enable	true
cms.ucs/standard-responses-sync-delay	cms.ucs	standard-responses-sync-delay	10000
cms.ucs/synchronize-screening-rules	cms.ucs	synchronize-screening-rules	true
cms.ucs/synchronize-standard-responses	cms.ucs	synchronize-standard-responses	true
general (3 Items)			
general/esReadOnly	general	esReadOnly	true
general/knowledgebaseFolder	general	knowledgebaseFolder	knowledge
general/sessionTtl	general	sessionTtl	8h
index (5 Items)			
index/docstatNumberOfReplicas	index	docstatNumberOfReplicas	1

8. Click **Save & Close** to apply your changes.

How to enable Standard Response through GAX

1. Log in to GAX.
2. Go to **Configuration > Environment > Applications**.
3. Navigate to the **Knowledge > QA > 853 > Knowldge_Space_Freeling Properties** folder.
4. Click **Application Options** from the left-hand menu.
5. Navigate to the **cms.ucs** section and click **cms.ucs\srl-enable**.
6. Set the **Value** to `true`.
7. Click **OK**, and **Save** to apply your changes.



Application Options

□	Name	Section	Key	Value
□	▼ cms.ucs			
□	cms.ucs \ asyncsync-delay	cms.ucs	asyncsync-delay	1000
□	cms.ucs \ config-synchro-mode	cms.ucs	config-synchro-mode	periodically
□	cms.ucs \ fieldcode-format-locale	cms.ucs	fieldcode-format-locale	
□	cms.ucs \ replace-blank-fieldcode	cms.ucs	replace-blank-fieldcode	false
□	cms.ucs \ screening-rules-sync-delay	cms.ucs	screening-rules-sync-delay	10000
□	cms.ucs \ srl-enable	cms.ucs	srl-enable	true
□	cms.ucs \ standard-responses-sync-delay	cms.ucs	standard-responses-sync-delay	10000
□	cms.ucs \ synchronize-screening-rules	cms.ucs	synchronize-screening-rules	false
□	cms.ucs \ synchronize-standard-responses	cms.ucs	synchronize-standard-responses	false
□	▼ general			
□	general \ knowledgebaseFolder	general	knowledgebaseFolder	knowledge_tpl

Knowledge Center in Production

This chapter provides you with information on the Knowledge Center once in production within your environment. It covers following topics:

- Monitoring Knowledge Center
- Sample UI

Monitoring Knowledge Center

Knowledge Center provides access to metrics and other key performance indicators (KPIs).

It also gives you the ability to configure Message Server alarms when a KPI passes its threshold value.

> **Important**
> Monitoring Capability supported by both Knowledge Center Server and Knowledge Center CMS.

Knowledge Center Metrics

Starting with release 8.5.000.13, Knowledge Center integrates with the third-party Metrics Java library to keep track of several Knowledge Center metrics. The Metrics toolkit includes counters, timers, histograms, and gauges.

You will probably want to use Java Management Extensions (JMX) as your main way of reporting on these metrics. We show how to do that here. Or you may want to check out some of the other tools that are available.

You can also use REST—which is helpful for performance testing—or write your metrics to a log file or to the console.

Knowledge Center Alarms

Knowledge Center lets you use tools from the Genesys Management Layer for monitoring and controlling your applications. These tools can be an important factor in improving performance—especially alarms, which let you set performance thresholds for these key metrics:

- Garbage collection latency
- Heap memory usage

Alarm Configuration

Alarm name	Alarm description	Alarm Condition object					Related configuration option
Threshold type	**Selection mode**	**Application type**	**Detect Event ID**	**Cancel Event ID**			
Heap Memory Usage	Defines the heap memory usage threshold value. This is the ratio of used heap memory to maximum heap memory.	predefined	Select by Application Type	Knowledge Center Backend Server	100001	100002	HeapMemoryUsage.threshold
GC Latency	Defines the garbage collection latency threshold value, in milliseconds, in relation to the last time the garbage was collected within the configured time interval.				10005	10006	GcLatency.threshold

Viewing Metrics with JMX

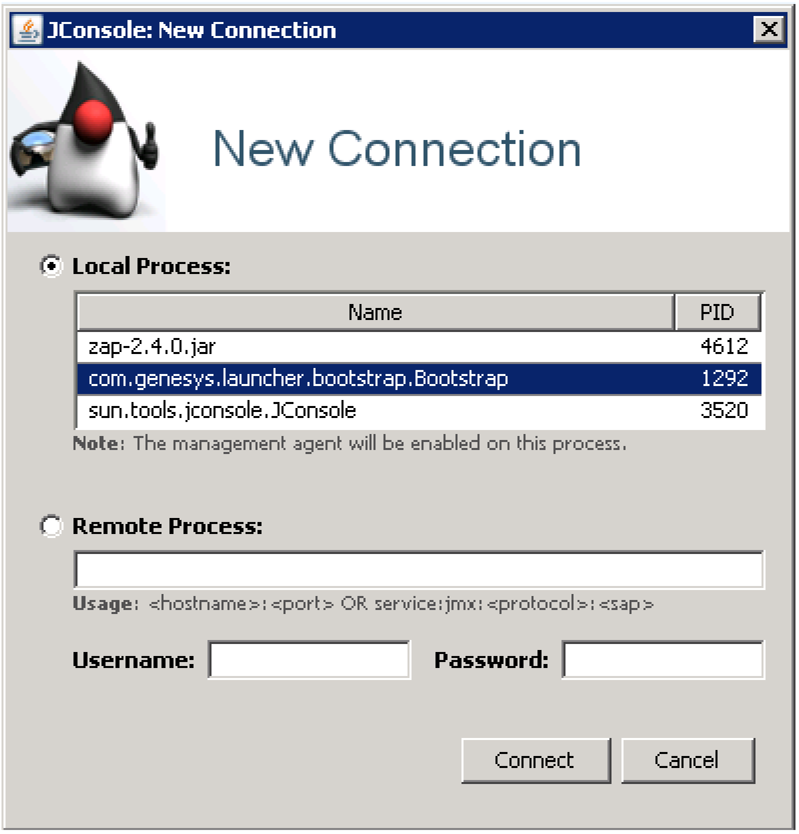
You can use JConsole to view metrics provided by your Knowledge Center Server. To do this, you can start Knowledge Center Server as a:

- Local java process
- Server on a remote host
- Windows service

Once you have connected, you can view your metrics in a JConsole JMX panel.

You may also want to look into some of the other tools that are available for viewing your Knowledge Center metrics.

Connect to Knowledge Center started as a **local java process**.



● **Local Process:**

Name	PID
zap-2.4.0.jar	4612
com.genesys.launcher.bootstrap.Bootstrap	1292
sun.tools.jconsole.JConsole	3520

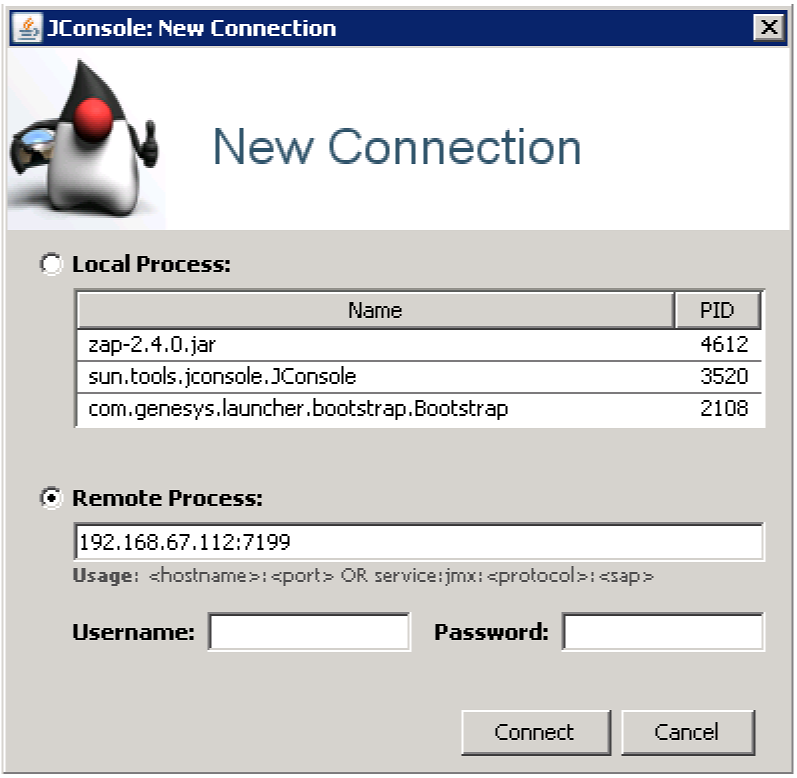
Note: The management agent will be enabled on this process.

Usage: <hostname>:<port> OR service:jmx:<protocol>:<sap>

1. Run **jconsole.exe** from the ***jdk*/bin** directory.
2. In the **New Connection** dialog, specify the Knowledge Center launcher java process.

   If the Knowledge Center Server was started via a BAT file in the same host where the JMX console is opened, this launcher process is the **com.genesys.launcher.bootstrap.Bootstrap** process from the **Local Process** list.

Connect to Knowledge Center Server started on a **remote host**.



○ Local Process:

Name	PID
zap-2.4.0.jar	4612
sun.tools.jconsole.JConsole	3520
com.genesys.launcher.bootstrap.Bootstrap	2108

● Remote Process: 192.168.67.112:7199

Usage: <hostname>:<port> OR service:jmx:<protocol>:<sap>

If the Knowledge Center Server was started remotely as a server, follow these steps:

1. Run **jconsole.exe** from the ***jdk*/bin** directory.
2. Open **setenv.bat** and uncomment all of the lines under the line that begins:

   ```
   :: Uncomment for enabling JMX
   ```

3. Save your changes.
4. Restart the Knowledge Center Server application.
5. Specify *host*:*JMX port* in the **Remote Process** section, as shown in the screenshot on the left.

Connect to Knowledge Center started as a **Windows service**.

If Knowledge Center Server is started as a Windows service, you should first stop the service, reinstall it, and restart it, as shown in these steps:

1. Stop the service.
2. Open **setenv.bat** and find the service name in the line that says `SVC_NAME=`.

3. Run this command to remove the service:

   ```
   server.bat -service <service name> remove
   ```

4. Open **setenv.bat** and uncomment all of the lines under this one:

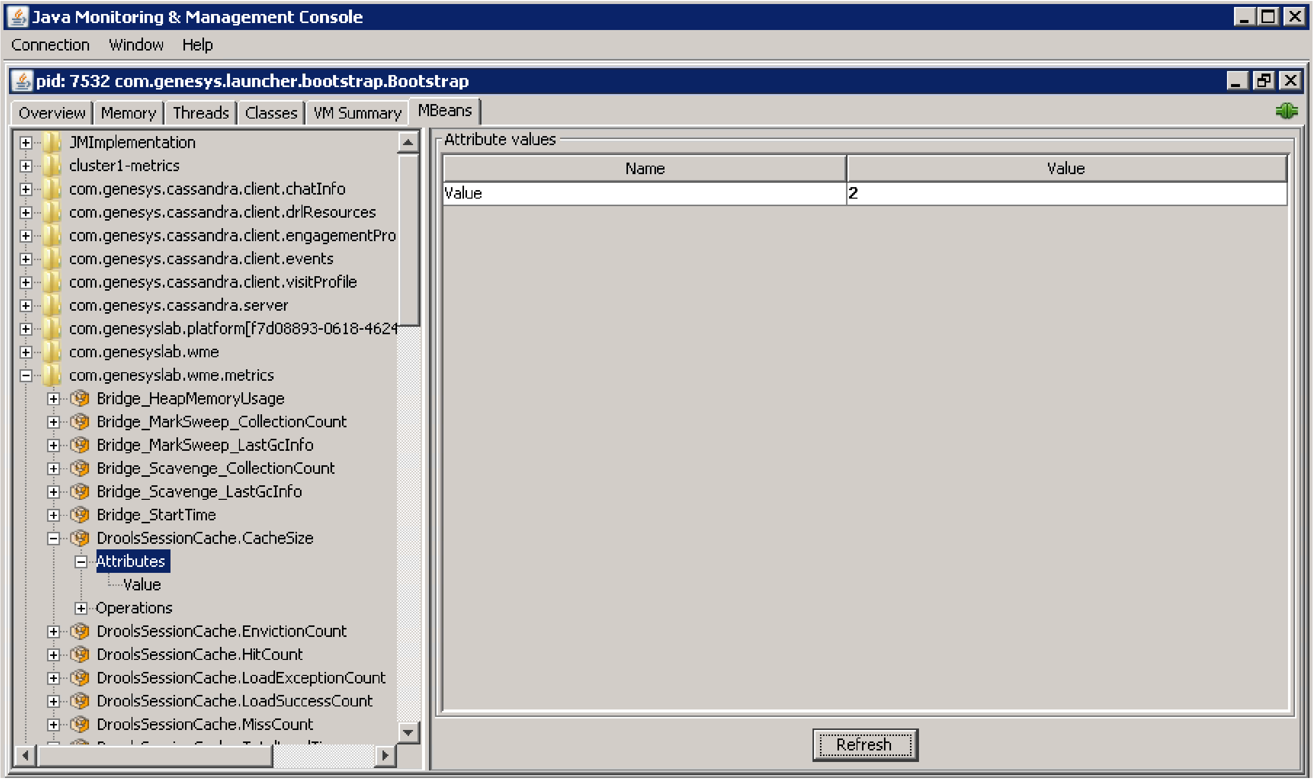
   ```
    :: Uncomment for enabling JMX Remote. Memorize JMX port.
   ```

5. Save your changes.
6. Run this command to install the service:

   ```
   server.bat -service <service name> install
   ```

7. Start the service.
8. Specify *host*:*JMX port* in the **Remote Process** section, as shown in the above screenshot.

Open the JMX panel to view the metrics.



```
JMImplementation
cluster1-metrics
com.genesys.cassandra.client.chatInfo
com.genesys.cassandra.client.drlResources
com.genesys.cassandra.client.engagementPro
com.genesys.cassandra.client.events
com.genesys.cassandra.client.visitProfile
com.genesys.cassandra.server
com.genesyslab.platform[f7d08893-0618-4624
com.genesyslab.wme
com.genesyslab.wme.metrics
    Bridge_HeapMemoryUsage
    Bridge_MarkSweep_CollectionCount
    Bridge_MarkSweep_LastGcInfo
    Bridge_Scavenge_CollectionCount
    Bridge_Scavenge_LastGcInfo
    Bridge_StartTime
    DroolsSessionCache.CacheSize
        Attributes
            Value
        Operations
    DroolsSessionCache.EnvictionCount
    DroolsSessionCache.HitCount
    DroolsSessionCache.LoadExceptionCount
    DroolsSessionCache.LoadSuccessCount
    DroolsSessionCache.MissCount
```

Name	Value
Value	2

1. Click **Connect** in the **New Connection** dialog. The JMX panel opens.
2. Open the **MBeans** tab and expand **com.genesyslab.wme.metrics**. All of the Knowledge Center metrics are there.
3. To refresh the metrics, click **Refresh**.

Other Tools

We have just explained how to use the JConsole tool bundled with Oracle Java (TM) to view your metrics, but there are several other tools you can use to do this:

- The EJTools JMX Browser
- Panoptes
- jManage
- MC4J
- Zabbix

Sample UI

Overview

Knowledge Center comes with a Sample UI, hosted on a sample website, which provides basic access to your installation of Knowledge Center and your configured knowledge base content. You can use it to test and demonstrate what Knowledge Center can do or as an example of how to integrate Knowledge Center access into your existing website.

The Sample UI is based on independent and easily configurable components. Its website was created using Bootstrap and works on all web browsers that support Bootstrap. See the Bootstrap documentation for details.

After you install your Knowledge Center Servers and configure the Knowledge Center Cluster, you can access the Sample UI sandbox via the following URLs:

- If you have configured a load-balancer for your cluster: *http://host_load_balacer:port_load_balancer/gks-sample-ui*
- If you use a Knowledge Center Cluster with a single node: *http://gkc_server_host:gkc_server_port/gks-sample-ui*

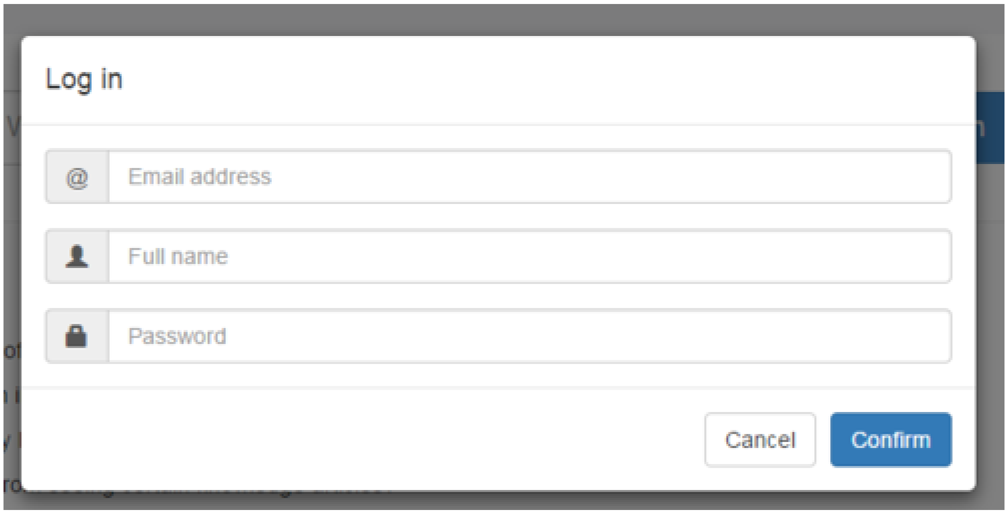
The Sample UI is pre-configured to show all Active and Public knowledge bases configured in Knowledge Center Server in language en (English).

Authorizing

You can use the Sample UI to:

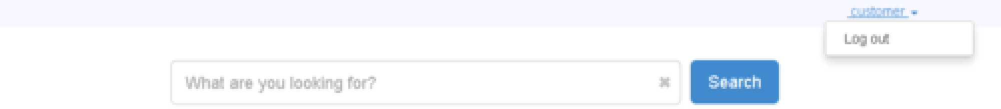
- Browse the site, either as an anonymous user or by authorizing yourself as a customer.
  To authorize, click the **Log in** link, enter your credentials, and click **Confirm**

> ### Important
> This is not a real site authorization, as Knowledge Center server will only use an email as a *customerId* to identify sessions in History records.



Sample UI Login

- To log out, click the link with your customer name and select "Logout"



Sample UI Logout

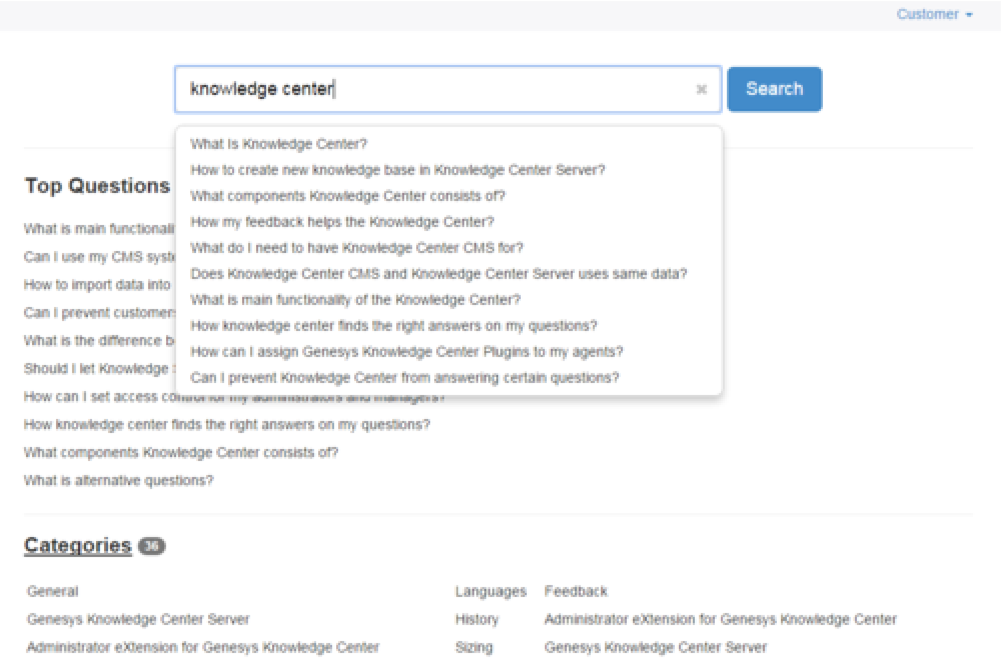
Searching

Search for any QNA document using the search bar.

Conduct a search

Start

1. Enter a question in the search bar and **Search** or press **Enter**.



Customer ▾

knowledge center

Search

What Is Knowledge Center?
How to create new knowledge base in Knowledge Center Server?
What components Knowledge Center consists of?
How my feedback helps the Knowledge Center?
What do I need to have Knowledge Center CMS for?
Does Knowledge Center CMS and Knowledge Center Server uses same data?
What is main functionality of the Knowledge Center?
How knowledge center finds the right answers on my questions?
How can I assign Genesys Knowledge Center Plugins to my agents?
Can I prevent Knowledge Center from answering certain questions?

Top Questions

What is main functionali
Can I use my CMS syst
How to import data into
Can I prevent customer
What is the difference b
Should I let Knowledge
How can I set access control for my administrators and managers?
How knowledge center finds the right answers on my questions?
What components Knowledge Center consists of?
What is alternative questions?

Categories 36

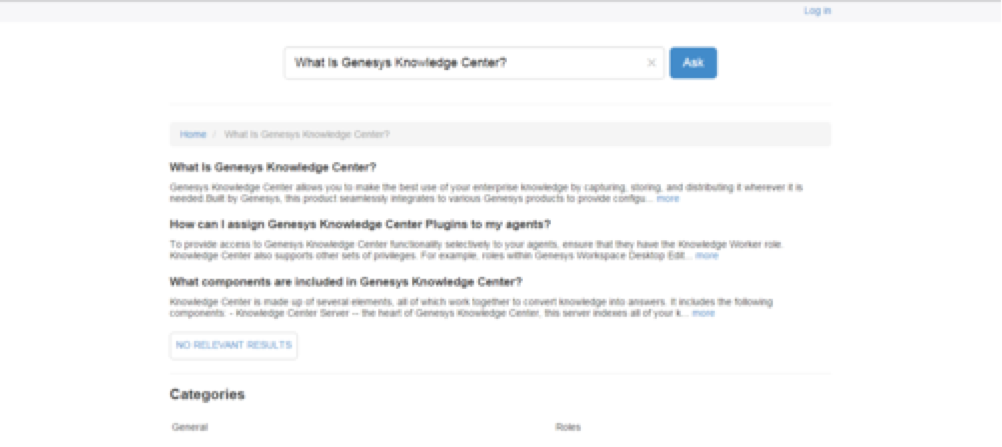
General
Genesys Knowledge Center Server
Administrator eXtension for Genesys Knowledge Center

Languages
History
Sizing

Feedback
Administrator eXtension for Genesys Knowledge Center
Genesys Knowledge Center Server

Sample UI Search

2. Review search results. You can use the **No relevant result** button to let Knowledge Center know that your search was unsuccessful. At the bottom of the page, there is a list of categories to which your search result documents belong.



Log in

What Is Genesys Knowledge Center?

Ask

Home / What Is Genesys Knowledge Center?

What Is Genesys Knowledge Center?

Genesys Knowledge Center allows you to make the best use of your enterprise knowledge by capturing, storing, and distributing it wherever it is needed Built by Genesys, this product seamlessly integrates to various Genesys products to provide configu... more

How can I assign Genesys Knowledge Center Plugins to my agents?

To provide access to Genesys Knowledge Center functionality selectively to your agents, ensure that they have the Knowledge Worker role. Knowledge Center also supports other sets of privileges. For example, roles within Genesys Workspace Desktop Edit... more

What components are included in Genesys Knowledge Center?

Knowledge Center is made up of several elements, all of which work together to convert knowledge into answers. It includes the following components: - Knowledge Center Server -- the heart of Genesys Knowledge Center, this server indexes all of your k... more

NO RELEVANT RESULTS

Categories

General

Roles

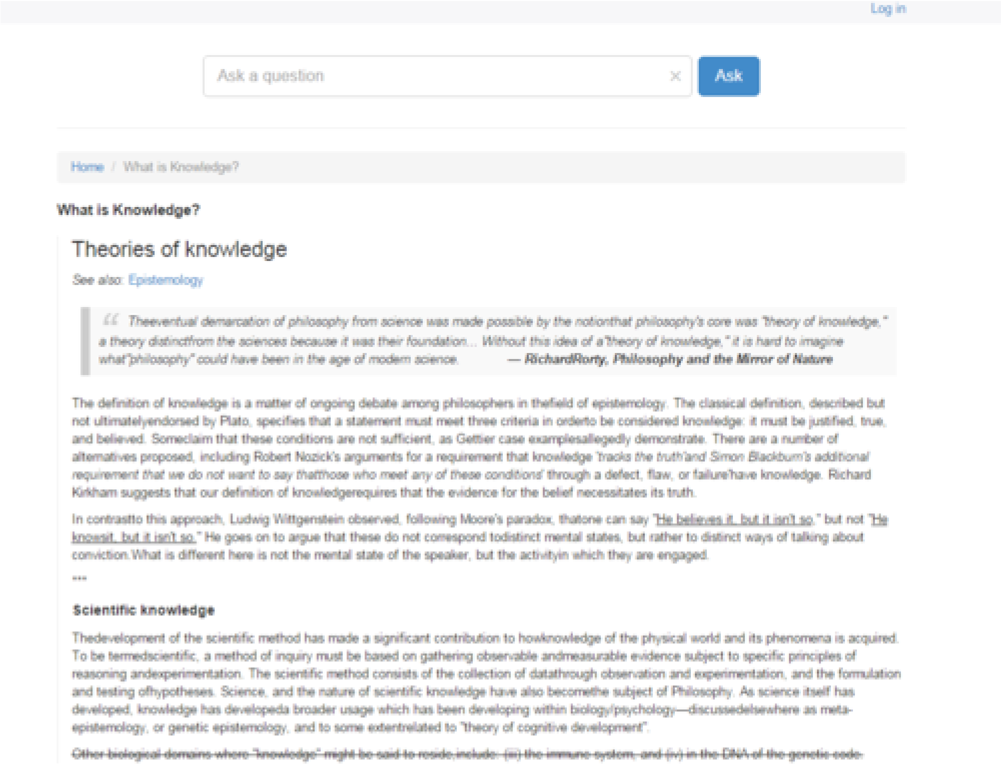
Sample UI Search Results

End

Open and Review a Document

Important

Documents can be in plain text or rich text



What is Knowledge?

Theories of knowledge

See also: Epistemology

> *“Theeventual demarcation of philosophy from science was made possible by the notionthat philosophy's core was "theory of knowledge," a theory distinctfrom the sciences because it was their foundation... Without this idea of a"theory of knowledge," it is hard to imagine what"philosophy" could have been in the age of modern science.* — ***RichardRorty, Philosophy and the Mirror of Nature***

The definition of knowledge is a matter of ongoing debate among philosophers in thefield of epistemology. The classical definition, described but not ultimatelyendorsed by Plato, specifies that a statement must meet three criteria in orderto be considered knowledge: it must be justified, true, and believed. Someclaim that these conditions are not sufficient, as Gettier case examplesallegedly demonstrate. There are a number of alternatives proposed, including Robert Nozick's arguments for a requirement that knowledge *'tracks the truth'and Simon Blackburn's additional requirement that we do not want to say thatthose who meet any of these conditions'* through a defect, flaw, or failure'have knowledge. Richard Kirkham suggests that our definition of knowledgerequires that the evidence for the belief necessitates its truth.

In contrastto this approach, Ludwig Wittgenstein observed, following Moore's paradox, thatone can say "He believes it, but it isn't so," but not "He knowsit, but it isn't so." He goes on to argue that these do not correspond todistinct mental states, but rather to distinct ways of talking about conviction.What is different here is not the mental state of the speaker, but the activityin which they are engaged.

...

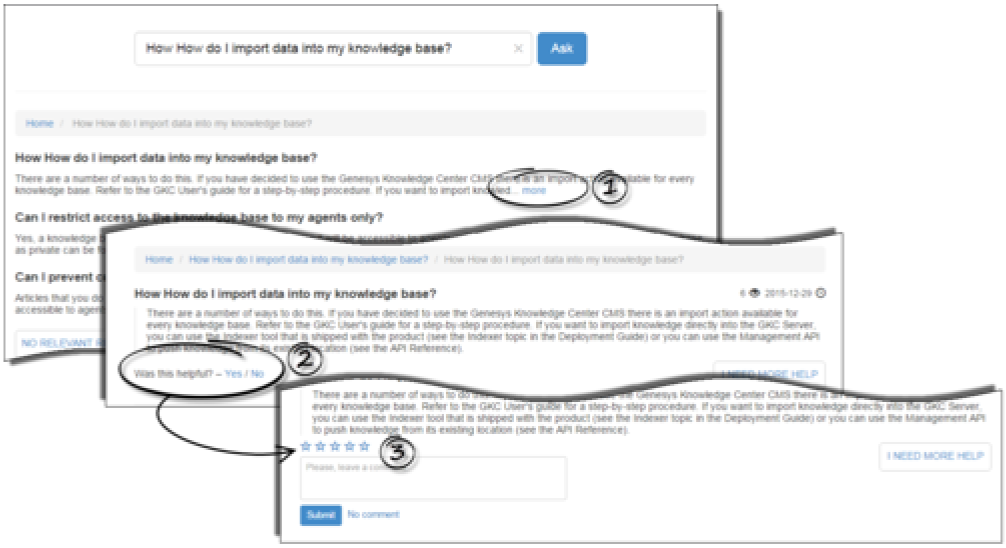
Scientific knowledge

Thedevelopment of the scientific method has made a significant contribution to howknowledge of the physical world and its phenomena is acquired. To be termedscientific, a method of inquiry must be based on gathering observable andmeasurable evidence subject to specific principles of reasoning andexperimentation. The scientific method consists of the collection of datathrough observation and experimentation, and the formulation and testing ofhypotheses. Science, and the nature of scientific knowledge have also becomethe subject of Philosophy. As science itself has developed, knowledge has developeda broader usage which has been developing within biology/psychology—discussedelsewhere as meta-epistemology, or genetic epistemology, and to some extentrelated to "theory of cognitive development".

~~Other biological domains where "knowledge" might be said to reside,include: (iii) the immune system, and (iv) in the DNA of the genetic code.~~

Example of Rich Text

- To expand the document, click the **more** link.
- Send feedback about the relevance of a search, using the **Yes/No** link to Like or Dislike the quality of the search. If you like or dislike an answer, you are asked to provide a star-rating and a comment (optional) to improve the Knowledge article.


How How do I import data into my knowledge base?
×
Ask
Home / How How do I import data into my knowledge base?
1
NO RELEVANT
Home / How How do I import data into my knowledge base? / How How do I import data into my knowledge base?
6
2015-12-29
2
Was this helpful? – Yes / No
I NEED MORE HELP
3
☆ ☆ ☆ ☆ ☆
Please, leave a com
Submit
No comment
I NEED MORE HELP

How How do I import data into my knowledge base?

There are a number of ways to do this. If you have decided to use the Genesys Knowledge Center CMS there is an import ... able for every knowledge base. Refer to the GKC User's guide for a step-by-step procedure. If you want to import knowled... more

Can I restrict access to the knowledge base to my agents only?

Yes, a knowledge ... as private can be ...

Can I prevent ...

Articles that you d... accessible to agen...

How How do I import data into my knowledge base?

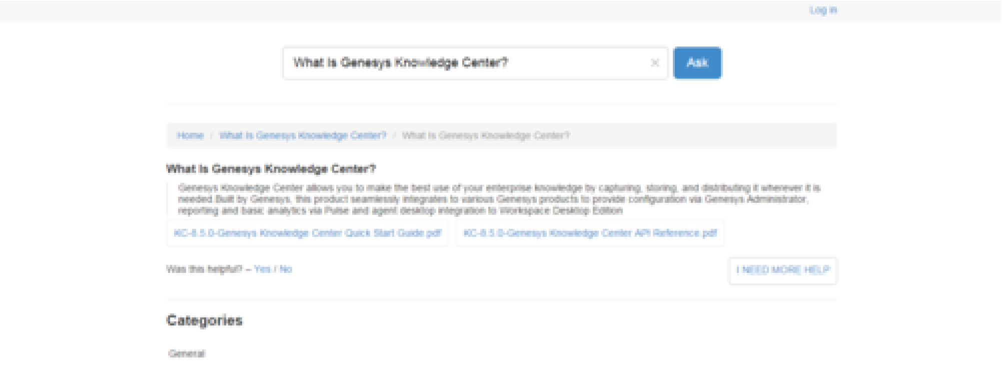
There are a number of ways to do this. If you have decided to use the Genesys Knowledge Center CMS there is an import action available for every knowledge base. Refer to the GKC User's guide for a step-by-step procedure. If you want to import knowledge directly into the GKC Server, you can use the Indexer tool that is shipped with the product (see the Indexer topic in the Deployment Guide) or you can use the Management API to push knowledge from its existing location (see the API Reference).

Negative Feedback Comment Field

- Click the **I need more help** button to send a request for proactive help from Genesys Web Engagement.

> ## Important
> This feature has been created only for use in conjunction with Genesys Web Engagement. No real message will be sent without integrating your Knowledge Center installation with GWE.

- Click attachment names to open any attachments in the document. Attachments will open in a new window.


Log in
What Is Genesys Knowledge Center?
×
Ask
Home / What Is Genesys Knowledge Center? / What Is Genesys Knowledge Center?
KC-8.5.0-Genesys Knowledge Center Quick Start Guide.pdf
KC-8.5.0-Genesys Knowledge Center API Reference.pdf
Was this helpful? – Yes / No
I NEED MORE HELP
Categories
General

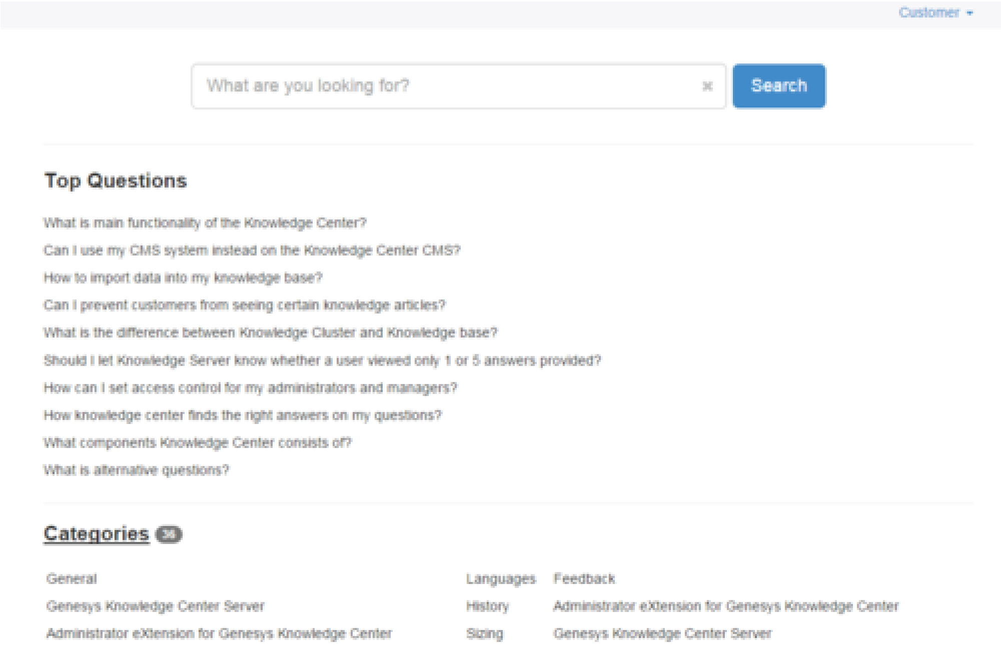
What Is Genesys Knowledge Center?

Genesys Knowledge Center allows you to make the best use of your enterprise knowledge by capturing, storing, and distributing it wherever it is needed. Built by Genesys, this product seamlessly integrates to various Genesys products to provide configuration via Genesys Administrator, reporting and basic analytics via Pulse and agent desktop integration to Workspace Desktop Edition

Opening Attachments

Browsing

To browse Categories click the "Categories" link from main page.



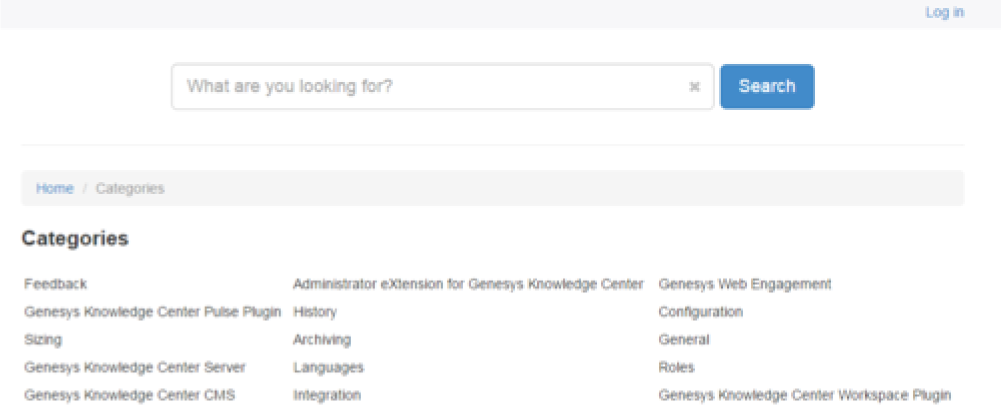
Top Questions

What is main functionality of the Knowledge Center?
Can I use my CMS system instead on the Knowledge Center CMS?
How to import data into my knowledge base?
Can I prevent customers from seeing certain knowledge articles?
What is the difference between Knowledge Cluster and Knowledge base?
Should I let Knowledge Server know whether a user viewed only 1 or 5 answers provided?
How can I set access control for my administrators and managers?
How knowledge center finds the right answers on my questions?
What components Knowledge Center consists of?
What is alternative questions?

Categories

General
Genesys Knowledge Center Server
Administrator eXtension for Genesys Knowledge Center
Languages
History
Sizing
Feedback
Administrator eXtension for Genesys Knowledge Center
Genesys Knowledge Center Server

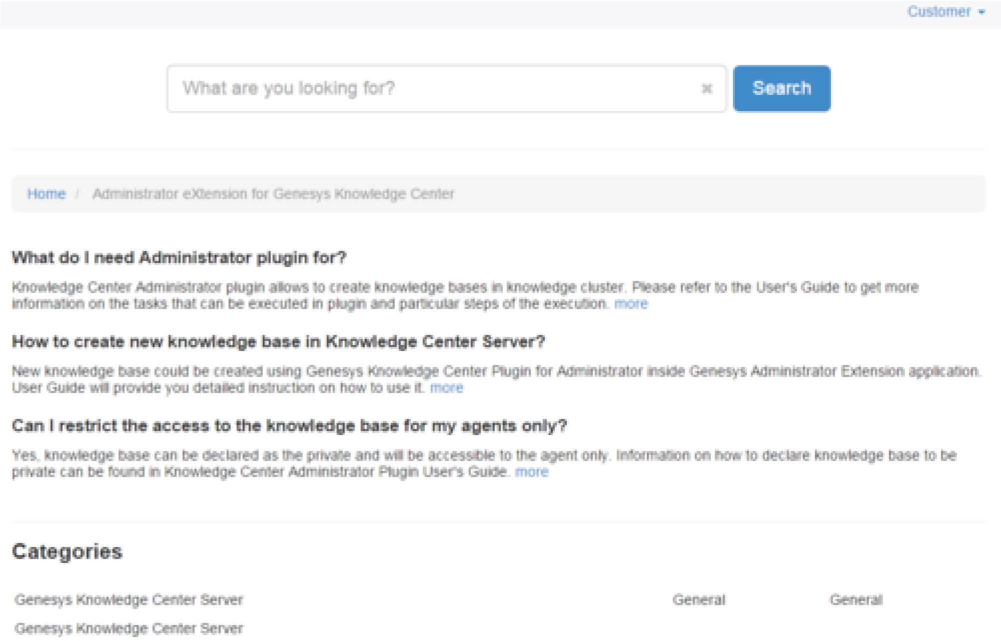
Sample UI Main Questions



Categories

Feedback
Genesys Knowledge Center Pulse Plugin
Sizing
Genesys Knowledge Center Server
Genesys Knowledge Center CMS
Administrator eXtension for Genesys Knowledge Center
History
Archiving
Languages
Integration
Genesys Web Engagement
Configuration
General
Roles
Genesys Knowledge Center Workspace Plugin

Sample UI Categories


Customer
What are you looking for?
Search
Home / Administrator eXtension for Genesys Knowledge Center

What do I need Administrator plugin for?

Knowledge Center Administrator plugin allows to create knowledge bases in knowledge cluster. Please refer to the User's Guide to get more information on the tasks that can be executed in plugin and particular steps of the execution. more

How to create new knowledge base in Knowledge Center Server?

New knowledge base could be created using Genesys Knowledge Center Plugin for Administrator inside Genesys Administrator Extension application. User Guide will provide you detailed instruction on how to use it. more

Can I restrict the access to the knowledge base for my agents only?

Yes, knowledge base can be declared as the private and will be accessible to the agent only. Information on how to declare knowledge base to be private can be found in Knowledge Center Administrator Plugin User's Guide. more

Categories

Genesys Knowledge Center Server	General	General
Genesys Knowledge Center Server		

Sample UI Document Categories

Importing Data into the Knowledge Center Server

Indexer Tool

If you are not going to use a CMS you can use the indexer to import data for use with Genesys Knowledge Center. The indexer is installed during the installation of Knowledge Center Server. It is located inside your Knowledge Center Server installation folder in the **\server\tools\indexer** subdirectory.

Command line:

```
java -jar indexer.jar  [parameters]
```

Parameters:

Short Parameter	Qualified Parameter	Mandatory	Example	Description
-u	--user	n/a	--user gkc_super	Name of internal user with authoring permissions
-a	--authorization	n/a	-a user:password	Username and password for basic authorization
-author	--author	n	--author gks_super	(introduced in 9.0.002.09) Common author identifier for all documents that are being published
-approver	--approver	n	--approver gks_super	(Introduced in 9.0.002.09) Common approver identifier for all documents that are being published
-f	--file	Y	--file c:\xml	Path to file or directory with files for importing
-h	--host	Y	--host http://gks/gks-server:8080	target knowledge server url
-o	--overwrite	n/a	-o	For replacing all existing

Short Parameter	Qualified Parameter	Mandatory	Example	Description
				documents with documents from importing file
-tenant	--tenantId	n/a	--tenantId 1	Target tenant identifier
-sbt	--subTenantId	n/a	--subTenantId default	Target subtenant identifier
-sk	--sslKeys	n/a	--sslKeys c:\keys\sslkey	Path to trust store
-sp	--sslPassword	n/a	--sslPassword topsecret	trust store password
-t	--transformer	n/a	--transformer c:\transformers\transformer.xsl	Path to XSL transformer

Knowledge File Structure

field	type	mandatory	format	description
knowledge	Object	Y	n/a	Container of documents and categories for indexing. **There are two mandatory attributes of a node of "knowledge":** • kbId - Knowledge base identifier • lang - language identifier • version - version identifier (current: "8.5.304")
knowledge.categories	Array	N	n/a	Knowledge base categories directory
knowledge.categories[].category	Object	Y	n/a	Knowledge category
knowledge.categories[].category.id	String	Y	n/a	Category identifier
knowledge.categories[].category.categoryParentId	String	N	n/a	Parent category

field	type	mandatory	format	description
				identifier. Omit for root categories.
knowledge.categories[].category.name	String	Y	n/a	Category name
knowledge.documents	Arrray	N	n/a	Documents for indexing. Omitting of this field means that indexer must not touch already indexed documents at all.
knowledge.documents[].id	String	N	n/a	Document identifier. Server may generate identifier automatically in case when documents[].id is omitted
knowledge.documents[].templateId	String	Y	n/a	Document template identifier
knowledge.documents[].author	String	No	n/a	(Introduced in 9.0.002.09) Document author
knowledge.documents[].approver	String	No	n/a	(Introduced in 9.0.002.09) Document approver
knowledge.documents[].validFrom	Date	N	YYYY-MM-DD	Document start date
knowledge.documents[].validTo	Date	N	YYYY-MM-DD	Document expiration date
knowledge.documents[].media	Array	N	n/a	List of media channels that this document is related to.
knowledge.documents[].media.media	String	N	n/a	Document media channel value
knowledge.documents[].tags	Array	N	n/a	List of tags related to this document
knowledge.documents[].tags.tag	String	Y	n/a	Document tag value
knowledge.documents[].url	String	N	n/a	Document external url
knowledge.documents[].title	String	Y	n/a	Document title
knowledge.documents[].title.id	String	Y	n/a	Document title name

field	type	mandatory	format	description
knowledge.documents[].title.value	String	Y	n/a	Document title value
knowledge.documents[].content	Array	Y	n/a	Document content
knowledge.documents[].content[].docField	Object	Y	n/a	Document content field
knowledge.documents[].content[].docField.id	String	Y	answer, description, body	Document content field name
knowledge.documents[].content[].docField.value	String	Y	n/a	Document additional content field value Important For importing Rich Text in HTML format via indexer use <![CDATA[and]] tags inside <value> field.
knowledge.documents[].additional	Array	N	n/a	Document additional content
knowledge.documents[].additional[].docField	String	Y	n/a	Document additional content field
knowledge.documents[].additional[].docField.id	String	Y	n/a	Document additional content field name
knowledge.documents[].additional[].docField.value	String	Y	n/a	Document additional content field value Important For importing Rich Text in HTML format via indexer use <![CDATA[and]] inside <value> field.
knowledge.documents[].alternatives	Array	N	n/a	Alternative names/ questions for the document
knowledge.documents[].alternatives[].alternative	String	N	n/a	Relevant text item
knowledge.documents[].attachments	Array	N	n/a	Document attachments
knowledge.documents[].attachments[].attachment	String	N	n/a	Document attachment URL
knowledge.documents[].categories	Array	N	n/a	Document category identifiers
knowledge.documents[].categories[].category	Object	N	n/a	Document

field	type	mandatory	format	description
				category object
knowledge.documents[].categories[].category.id	String	Y	n/a	Document category identifier
knowledge.documents[].customFields	Array	N	n/a	Document custom attributes
knowledge.documents[].customFields[].entry	Object	N	n/a	Document custom attribute item
knowledge.documents[].customFields[].entry.key	String	Y	n/a	Document custom attribute name
knowledge.documents[].customFields[].entry.value	VAR	N	n/a	Document custom attribute value

Example of content of indexing file (v2)

```
<?xml version="1.0" encoding="UTF-8">
<knowledge kbId="knowledgefaq" lang="en" version="8.5.304">

    <categories>
        <category>
            <id>c1</id>
            <name>category 1</name>
        </category>

        <category>
            <id>c2</id>
            <name>category 2</name>
            <categoryParentId>c1</parentId>
        </category>
    </categories>

    <documents>
        <document>
            <id>doc1</id>
            <templateId>basefaq</templateId>
            <validFrom>2017-02-20</validFrom>
            <validTo>2017-02-21</validTo>
            <media>
                <media>m1</media>
                <media>m2</media>
            </media>
            <tags>
                <tag>t1</tag>
                <tag>t2</tag>
            </tags>
            <url>doc1url</url>

            <title>
                <id>question</id>
                <value>document question</value>
            </title>
            <content>
                <docField>
                    <id>answer</id>
                    <value>answer body</value>
                </docField>
            </content>
            <alternatives>
                <alternative>document alt1</alternative>
                <alternative>document alt2</alternative>
            </alternatives>

            <attachments>
                <attachment>a1</attachment>
                <attachment>a2</attachment>
            </attachments>

            <categories>
                <category><id>c1</id></category>
                <category><id>c2</id></category>
            </categories>

            <customFields>
                <entry>
                    <key>strField</key>
                    <value>some string</value>
                </entry>
                <entry>
                    <key>numField</key>
                    <value>123</value>
                </entry>
            </customFields>
        </document>

        <document>
            <id>doc2</id>
            <templateId>basefaq</templateId>
            <validTo>2017-02-21</validTo>
            <media>
                <media>m1</media>
                <media>m2</media>
            </media>
            <tags>
                <tag>t1</tag>
                <tag>t2</tag>
            </tags>
            <url>doc2url</url>

            <title>
```

```
                <id>question</id>
                <value>document question</value>
            </title>
            <content>
                <docField>
                    <id>answer</id>
                    <value>faq answer</value>
                </docField>
            </content>
            <alternatives>
                <alternative>document alt1</alternative>
                <alternative>document alt2</alternative>
            </alternatives>

            <attachments>
                <attachment>a1</attachment>
                <attachment>a2</attachment>
            </attachments>

            <categories>
                <category><id>c1</id></category>
                <category><id>c2</id></category>
            </categories>

            <customFields>
                <entry>
                    <key>strField</key>
                    <value>some string</value>
                </entry>
                <entry>
                    <key>numField</key>
                    <value>123</value>
                </entry>
            </customFields>
        </document>

        <document>
            <id>doc3</id>
            <templateId>basearticle</templateId>
            <media>
                <media>m1</media>
            </media>
            <title>
                <id>title</id>
                <value>document title</value>
            </title>

            <content>
                <docField>
                    <id>description</id>
                    <value></value>
                </docField>
            </content>

            <additional>
                <docField>
                    <id>summary</id>
                    <value>document summary</value>
                </docField>
            </additional>

            <customFields>
                <entry>
                    <key>cf1</key>
                </entry>
            </customFields>
        </document>
    </documents>
</knowledge>
```

Importing Sample Data

In the `./server/tools` directory in the Knowledge Center installation folder, you can find a sample knowledge base along with the indexer tool:

- knowledgeFAQ.xml — Sample knowledge base describing some of the questions related to Knowledge Center
- indexer.jar—Java-based indexing tool
- importFAQ.bat—Simple data import script

> **Important**
>
> Users must have Knowledge.AUTHOR privileges in order to use the Administrator plugin.

To import a sample knowledge base you need to:

1. open import.bat file:
   - ensure that --host parameter is pointing on one of your Knowledge Center Servers or the load balancer in front of the cluster (recommended)
   - ensure that --user parameter is set to valid used with Knowledge.AUTHOR privileges (knowledge by default)
2. save changes if any
3. open knowledgeFAQ.xml:
   - ensure that kbId attribute is set to desired knowledge base you would like to import data to (knowledgeFAQ by default)
   - ensure that language is set to properly configured one and added to the knowledge base
4. save changes if any
5. run import.bat

Upgrade Genesys Knowledge Center Server

It is recommended that you upgrade your system to Genesys Knowledge Center Server 9.0.006.16. It is not recommended to select the Fresh or Maintenance options (if available). Also, to be on the safe side, it is highly recommended that you create and save a copy of your existing `launcher.ini` file when working with Windows or your existing `setenv.sh` file when working with Linux.

Although it is not recommended, if you do choose to select a Fresh (new) installation you must update the Windows `launcher.ini` file or the Linux `setenv.sh` file with the following content so that it points to the previous configuration server:

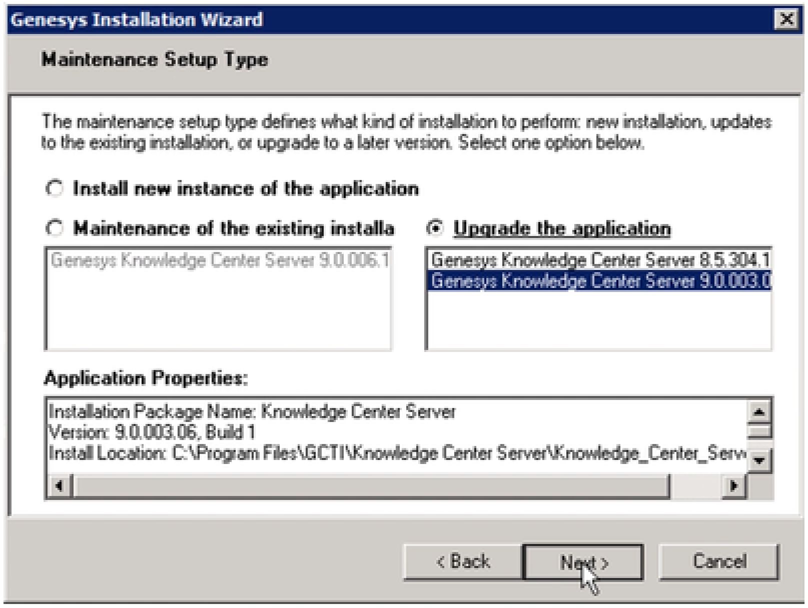
> **Important**
>
> The `launcher.ini` file and the `setenv.sh` file located in the root directory of the location in which the Genesys Knowledge Server is installed.

- Dwcc.appName=<previous_app_name>
- Dwcc.primaryConfServer=<previous configuration server path>

Upgrade Genesys Knowledge Center Server in a Windows environment
Upgrade Genesys Knowledge Center Server in a Linux environment

Upgrade Genesys Knowledge Center Server in a Windows environment

1. In your upgrade package, locate and double-click the setup.exe file. The **Maintenance Setup Type** screen appears.
2. In the **Maintenance Setup Type** window, select **Upgrade the application** and from the list provided select the component you want to upgrade to.



Maintenance Setup Type

The maintenance setup type defines what kind of installation to perform: new installation, updates to the existing installation, or upgrade to a later version. Select one option below.

○ Install new instance of the application

○ Maintenance of the existing installa

Genesys Knowledge Center Server 9.0.006.1

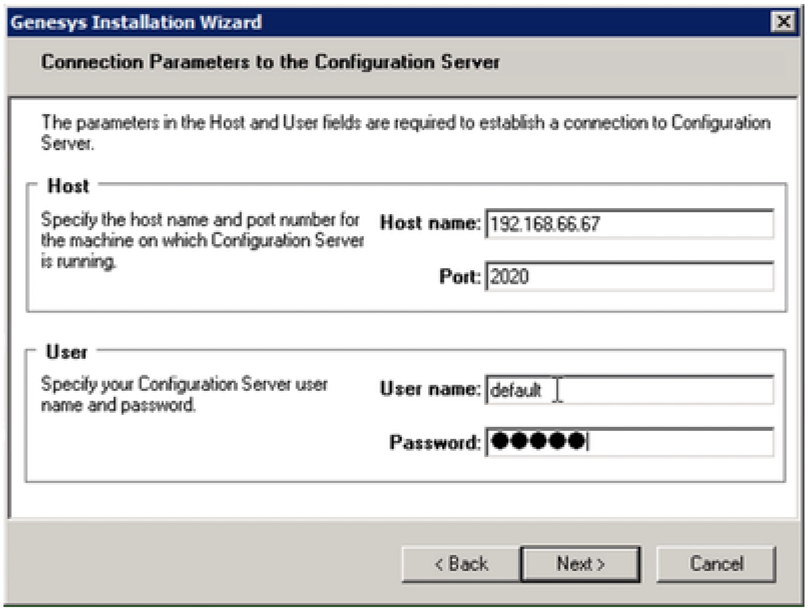
● Upgrade the application

Genesys Knowledge Center Server 8.5.304.1
Genesys Knowledge Center Server 9.0.003.0

Application Properties:

Installation Package Name: Knowledge Center Server
Version: 9.0.003.06, Build 1
Install Location: C:\Program Files\GCTI\Knowledge Center Server\Knowledge_Center_Serv

3. Click **Next**. The **Connection Parameters to the Configuration Server** screen appears.
4. In the **Host** and **User** fields enter your host name, port and configuration server credentials.



Connection Parameters to the Configuration Server

The parameters in the Host and User fields are required to establish a connection to Configuration Server.

Host

Specify the host name and port number for the machine on which Configuration Server is running.

Host name: 192.168.66.67

Port: 2020

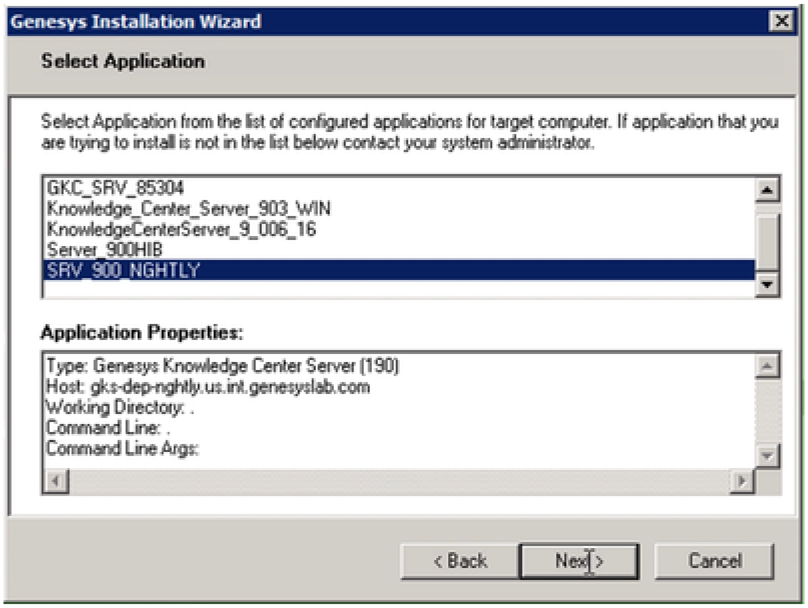
User

Specify your Configuration Server user name and password.

User name: default

Password: ●●●●●

5. Click **Next**. The **Select Application** screen appears.
6. In the list provided, select the Genesys Knowledge Center Server application. Select the Genesys Knowledge Center Server that is currently running.



Genesys Installation Wizard

Select Application

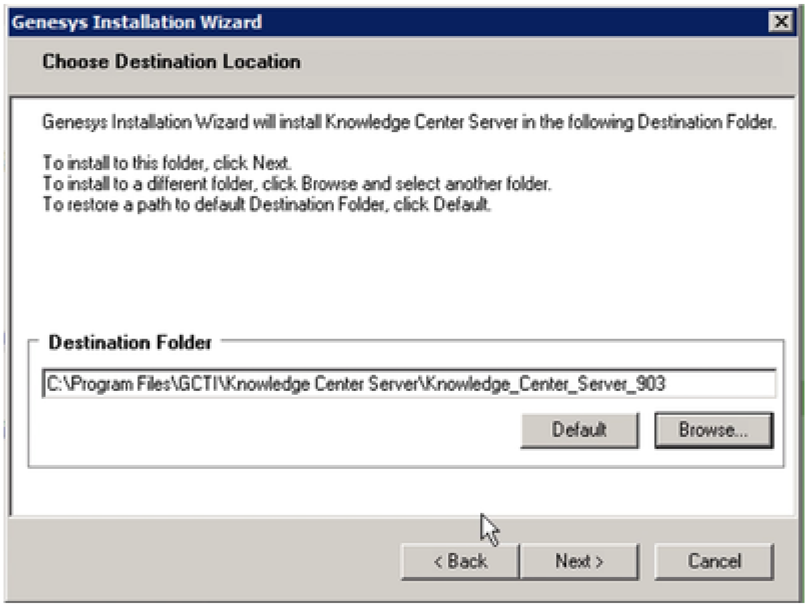
Select Application from the list of configured applications for target computer. If application that you are trying to install is not in the list below contact your system administrator.

GKC_SRV_85304
Knowledge_Center_Server_903_WIN
KnowledgeCenterServer_9_006_16
Server_900HIB
SRV_900_NGHTLY

Application Properties:

Type: Genesys Knowledge Center Server (190)
Host: gks-dep-nghtly.us.int.genesyslab.com
Working Directory: .
Command Line: .
Command Line Args:

7. Click **Next**. The **Choose Destination Location** screen appears.
8. In the **Destination Folder** enter the path to the location of your previous Genesys Knowledge Center Server.



Genesys Installation Wizard

Choose Destination Location

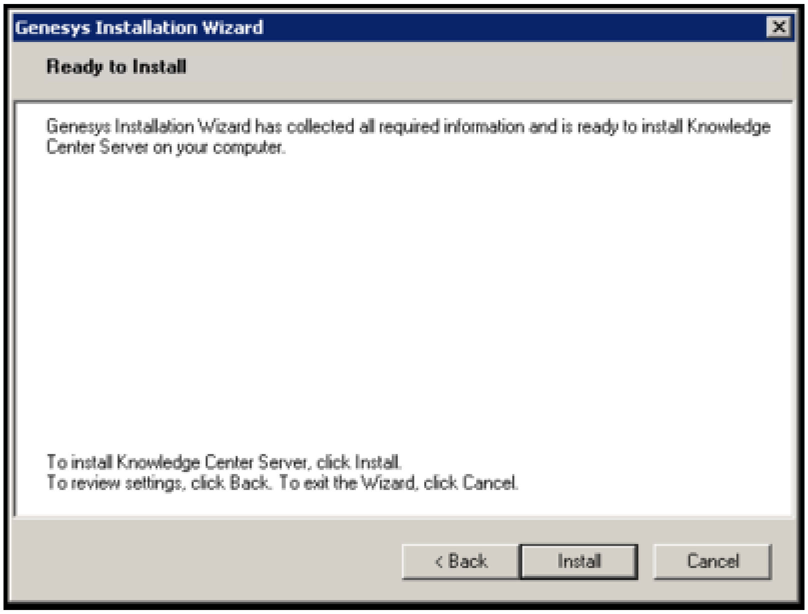
Genesys Installation Wizard will install Knowledge Center Server in the following Destination Folder.

To install to this folder, click Next.
To install to a different folder, click Browse and select another folder.
To restore a path to default Destination Folder, click Default.

Destination Folder

C:\Program Files\GCTI\Knowledge Center Server\Knowledge_Center_Server_903

9. Click **Next**. The **Ready to Install** screen appears.



Genesys Installation Wizard

Ready to Install

Genesys Installation Wizard has collected all required information and is ready to install Knowledge Center Server on your computer.

To install Knowledge Center Server, click Install.
To review settings, click Back. To exit the Wizard, click Cancel.

10. Click **Install**. The Genesys Installation Wizard indicates it is performing the requested operation. When through, the **Installation Complete** screen appears.
11. Click **Finish** to complete your installation.
12. Start the Genesys Knowledge Center Server.

Upgrade Genesys Knowledge Center Server in a Linux environment

Start

1. Open a terminal in the Genesys Knowledge Center Server CD/DVD or the Genesys Knowledge Center Server installation package and run the install.sh file. The Genesys installation starts.
2. Enter the hostname of the host on which you are going to install.
3. Enter the connection information required to log in to the Configuration Server:
   a. Hostname—For instance, demosrv.genesyslab.com
   b. Listening port—For instance, 2020
   c. User name—For instance, demo
   d. Password
4. If you have a backup Configuration Server, enter the Host name and Port.
5. If the connection settings are successful, a list of keys and Genesys Knowledge Center Server applications is displayed.
6. Enter the key for the Genesys Knowledge Center Server application that you created previously on Configuration Server.
7. Enter the full path to your installation directory and confirm that it is correct.

If the installation is successful, the console displays the following message: *Installation of Genesys*

Knowledge Center Server, version 8.5.x has completed successfully.

End