Genesys Knowledge Center Deployment Guide

Knowledge Center 8.5.0

2/23/2015

Table of Contents

Deployment Guide

Important

Genesys Knowledge Center is now available as a restricted offering. You must contact your Genesys representative to see if Genesys Knowledge Center is suitable for your environment and business needs. The documentation here anticipates a larger rollout of Genesys Knowledge Center in late 2015.

New in this Release

This is the first release of Genesys Knowledge Server. Here are the latest and greatest features:

- **Indexing and Federated Search**
  - Index knowledge from a variety of data sources and expose them via a single search interface
  - Search for knowledge using simple natural language–like sentences
  - Search content quickly with an auto-complete feature that provides suggestions as you type your search phrase
  - Collects user feedback in order to promote or demote a given knowledge article's relevance for future searches
- **Agent Empowerment**
  - Exposes knowledge seamlessly via a plugin to Workspace Desktop Edition, the app where agents spend most of their time interacting with customers
  - Gives agents customer search history so that they know what the customers have searched, reviewed, and ignored online before they escalated to human-assisted service
  - Allows agents to search knowledge bases for any content that may not have been exposed to public websites and filter the results based on context and metadata to find the right answer quickly
  - Transfer the resulting knowledge to the interaction response with a single click
  - Leverage your agent’s subject matter expertise and allow them to contribute content to the knowledge base—administrators can review the content before publishing it for customer consumption
- **APIs and Integrations**
  - Genesys Knowledge Center comes with a rich set of APIs for:
    - Session Management
    - Knowledge Base Operations
    - FAQ Retrieval
    - Feedback Management
    - Reporting
  - Proactively offer Chat or Callback or Call Us (phone number) with the help of Genesys Proactive Engagement, when there is negative feedback or no answer was found
  - Easily customizable widgets that can be exposed to the external website and intranet sites are available out-of-the-box
- **Content Management**

    - Configure knowledge base structure, custom tags, visibility, and other properties
    - Create content with or without rich media attachments
    - Predefined approval workflow allows administrators to approve content before publishing
- **Administration, Deployment, and Management**
    - Role-based access for Agents, Administrators, Content Managers and Reporting Users
    - Simple and easy-to-use user interfaces for configuration
- **Supported Platforms**
    - GKC Server and GKC CMS support the following operating systems:
        - Linux 6 64-bit
        - Linux 7 64-bit
        - Windows Server 2008 x64 (64-bit)
        - Windows Server 2012 x64 (64-bit)
    - The GKC plugin for Genesys Administrator supports the following operating systems:
        - Linux 5 64-bit
        - Linux 6 64-bit
        - Windows Server 2008 x64 (64-bit)
        - Windows Server 2012 x64 (64-bit)
    - The GKC plugin for Pulse supports the following operating systems:
        - Linux 5 64-bit
        - Linux 6 64-bit
        - Windows Server 2008 64-bit
        - Windows Server 2008 x64 (64-bit)
        - Windows Server 2012 x64 (64-bit)
    - The GKC plugin for Workspace Desktop Edition supports the following operating systems:
        - Windows Vista x86 (32-bit)
        - Windows 7 x86 (32-bit)
        - Windows 8 x86 (32-bit)
        - Windows Server 2008 x86 (32-bit)
        - Windows Server 2012 x86 (32-bit)
        - Windows Vista x64 (64-bit)
        - Windows 7 x64 (64-bit)
        - Windows 8 x64 (64-bit)
        - Windows Server 2008 x64 (64-bit)
        - Windows Server 2012 x64 (64-bit)
    - Java 7
    - Supported Browsers
        - Firefox

- Chrome
- Internet Explorer
- Safari

The GKC Components

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

- **GKC Server**—Combines indexing and natural language–based search capabilities to provide effective knowledge article retrieval from one or more knowledge bases.
- **GKC 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.
- **GKC Plugin for Administrator**—Enables system administrators to use Genesys Administrator to configure their knowledge clusters.
- **GKC Plugin for Pulse**—Allows contact center managers to view Genesys Knowledge Center reporting at near real-time from the Pulse user interface.
- **GKC 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.
- **GKC Data Import Tool**—Use this tool to import XML-based QNA data into a GKC index.
- **GKC REST API**—Can be used for both client and management functions.
- **Genesys Web Engagement Integration**—GKC can be used with GWE to provide proactive engagement capabilities.

GKC Server

The Genesys Knowledge Center Server combines indexing and search capabilities that allow for effective FAQ retrieval over one or more knowledge bases. It is web-based, and can run under the Jetty HTTP Server.

At its core GKC Server consists of two key parts:

- The Elasticsearch search and analytics engine
- Several Elasticsearch plugins

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 GKC Server

- GKC Server exposes a REST API that can be used for both client and management functions.
- GKC Server is a cluster application, meaning that several nodes or servers can be grouped within a single cluster.
- GKC Server requires two application objects in Genesys Administrator:
  - One to describe the server itself (type = *Genesys Generic Server*)
  - Another for storing high-level options and knowledge base configurations, and for integrating the GKC 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.
- GKC Server uses Genesys Roles to restrict access, and to authorize and authenticate users.
- The GKC installation package includes a launcher that can launch both Jetty and all of the applications deployed on JEtty as a standalone Genesys application. To accomplish this goal, the launcher communicates with the Genesys Config Server to fetch the required options.

GKC CMS

The GKC 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 GKC Server

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

Plugin for Administrator

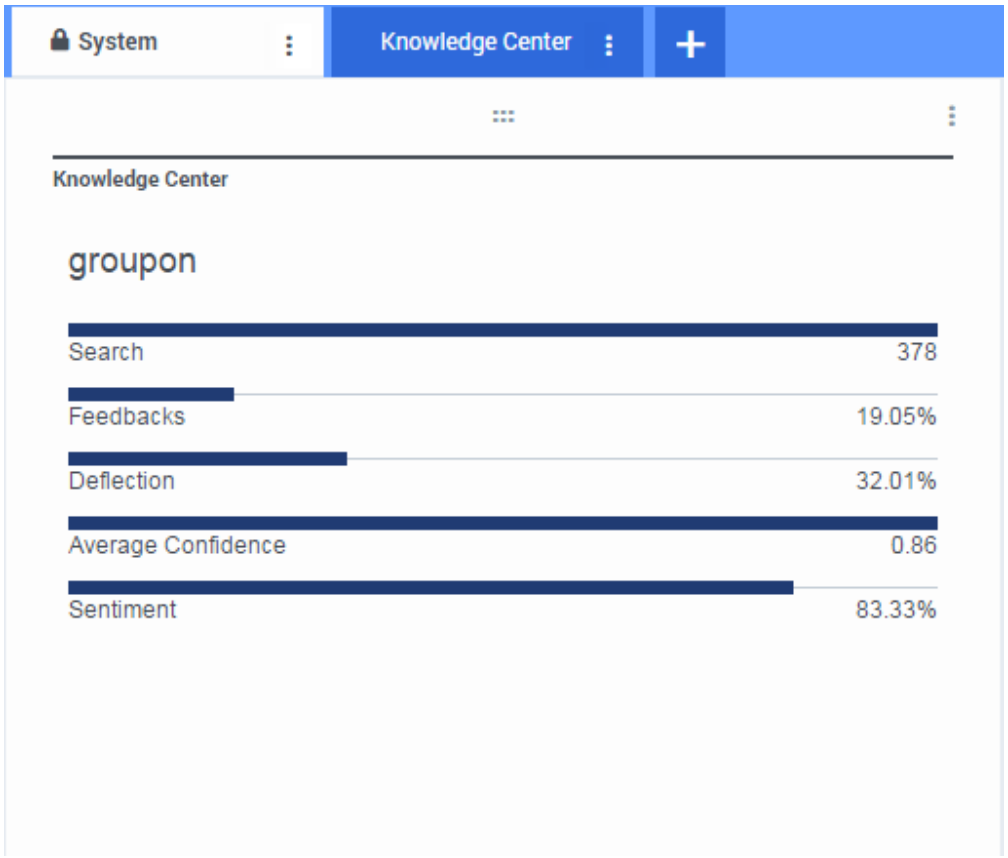
This plugin lets you manage the structure of the knowledge bases that are controlled by the GKC Server Cluster application object in Genesys Administrator.

After you install this plugin, you will have access to a separate page in Administrator that displays a user interface for creating new knowledge bases and for editing the descriptions, options, languages, and custom fields in existing knowledge bases.

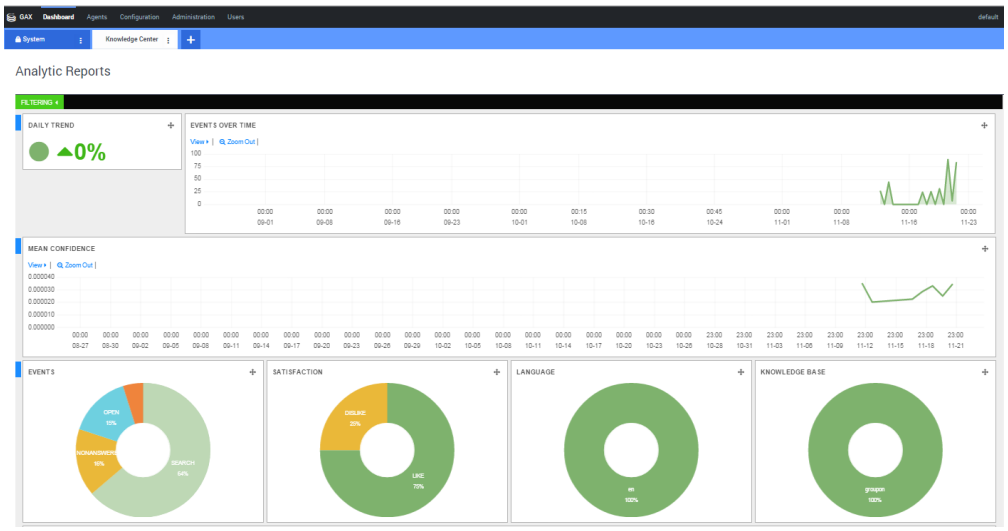
Plugin for Pulse

The GKC Plugin for Pulse displays GKC Server statistics, such as KPIs, user activity, trending topics, like and dislike trends, types of activities, and more.

Here is a sample display of key performance indicators:



This image shows a sample dashboard containing analytic reports:

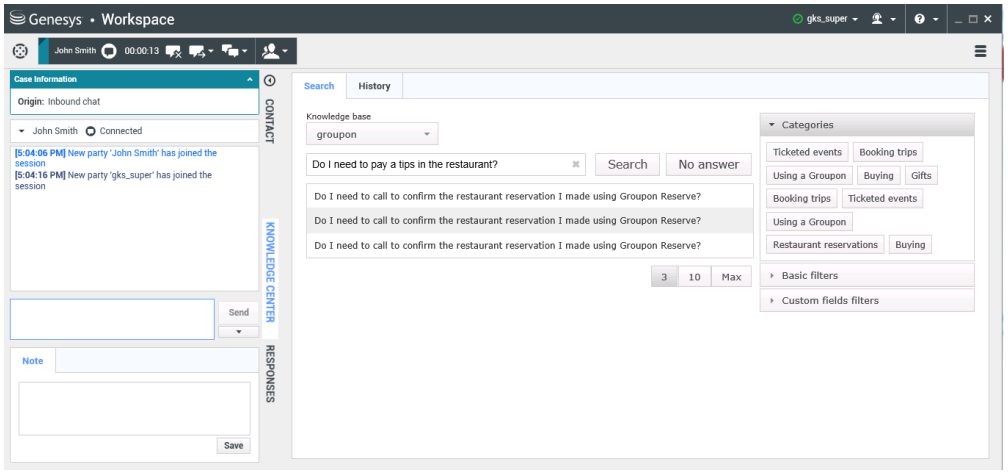


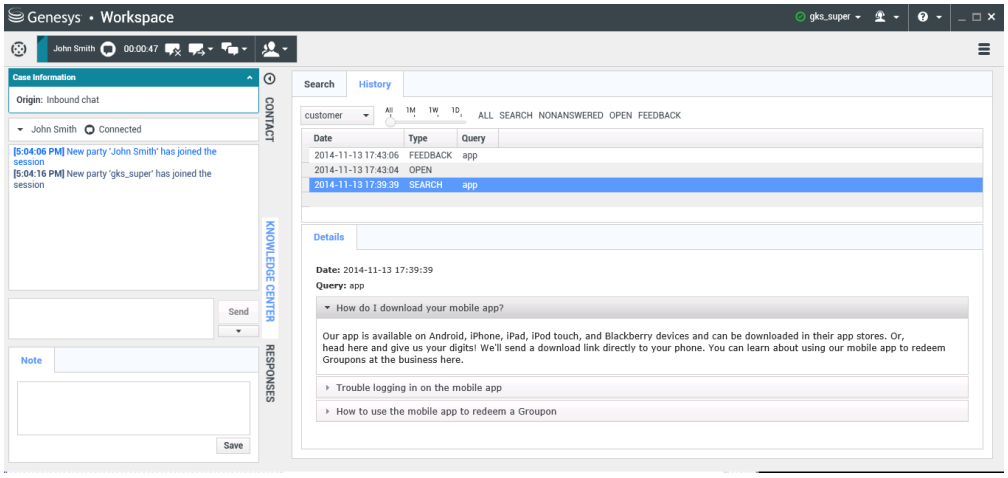
Plugin for WDE

Your agents can use the GKC Plugin for Workspace Desktop Edition (WDE) to access GKC 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, GKC 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 QNA search and customer history, respectively.





Data Import Tool

You can use the data import tool to import QNA data from an XML file into a GKC index . The data in your XML file must be stored in a specific format, as shown in the following simple example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<documents kbsId="gkc" lang="en">
    <document>
        <id>gkc_1</id>
        <question>What is Genesys Knowledge Center
Server?</question>
        <answer>Genesys Knowledge Center Server combines indexing
and search capabilities that
                allow for effective FAQ retrieval over one or more
knowledge bases.</answer>
        <categories>
            <category>
                <id>1</id>
                <name>Common article</name>
            </category>
        </categories>
    </document>
</documents>
```

GKC REST API

The Genesys Knowledge Center (GKC) REST API exposes three sets of functionality:

- The Knowledge API can be used by Knowledge Center Server clients who are interested in retrieving FAQ-related information from a knowledge base, including things like the structure of the knowledge base and its feedback data
- The Management API allows service components—such as content management systems, the GKC Administrator plugin, and data importers—to create, populate, and manage knowledge basess
- The Reporting API provides reporting engines—such as Easy Pulse or third-party products—with data on the various knowledge-related activities carried out by agents and customers

Genesys Web Engagement Integration

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

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

Prerequisites

Prerequisites

OS Requirements

Knowledge Center Server

- OS Red Hat Enterprise Linux AS 5 (Intel 32-bit)
- OS Red Hat Enterprise Linux AS 5-7 (Intel EM64T)
- OS Windows Server 2008 (Intel EM64T)
- OS Windows Server 2012

Knowledge CMS

- OS Red Hat Enterprise Linux AS 5 (Intel 32-bit)
- OS Red Hat Enterprise Linux AS 5-7 (Intel EM64T)
- OS Windows Server 2008 (Intel EM64T)
- OS Windows Server 2012 (Intel EM64T)

Genesys Knowledge Center Plugin for Workspace Desktop Edition

- OS Windows Vista (Intel 32-bit)
- OS Windows Server 2008 (Intel 32-bit, Intel EM64T)
- OS Windows 7 (Intel 32-bit, Intel EM64T)
- OS Windows Server 2012 (Intel EM64T)
- OS Windows 8 (Intel EM64T)

Genesys Knowledge Center Plugin for Administrator

- OS Red Hat Enterprise Linux AS 5 (Intel EM64T)
- OS Windows Server 2008 (Intel EM64T)
- OS Windows Server 2012 (Intel EM64T)

Genesys Knowledge Center Plugin for Pulse

- OS Red Hat Enterprise Linux AS 5 (Intel EM64T)
- OS Windows Server 2008 (Intel 32-bit, Intel EM64T)
- OS Windows Server 2012 (Intel EM64T)

Web Browsers

- Google Chrome 34+
- Mozilla Firefox 24+
- Microsoft Internet Explorer 10+
- Apple Safari 7+

Java Requirements

- Java 7 SE Bundle

Genesys Environment

- Genesys Framework 8.1–8.5
- Configuration Server (8.1.300.21 / 8.5.100.02)
- Genesys Administrator Extension 8.1–8.5
- Workspace Desktop Edition 8.5

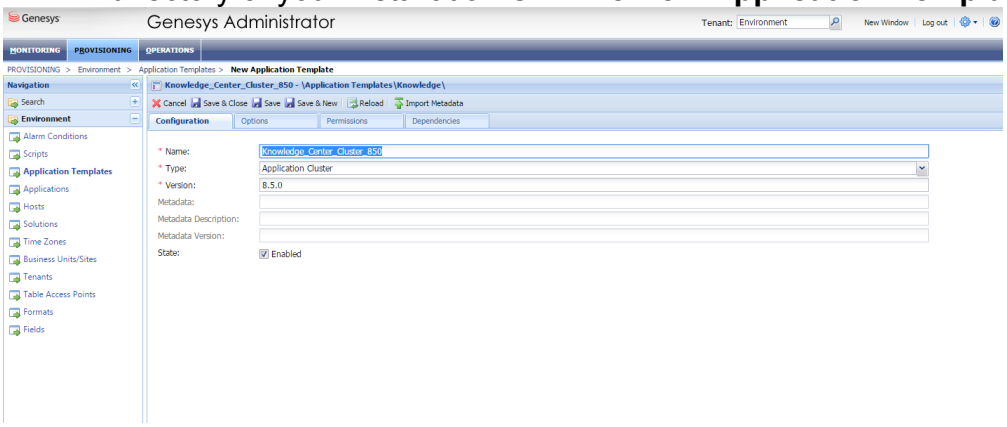
Installing the GKC Cluster Application

Carry out the following steps to install and configure the GKC Cluster Application:

1. Import the GKC Cluster Application Template
2. Create Cluster Applications
3. Configure the Cluster Application

Import the GKC 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_850.apd* file available in the templates directory of your installation CD. The **New Application Template** panel opens.

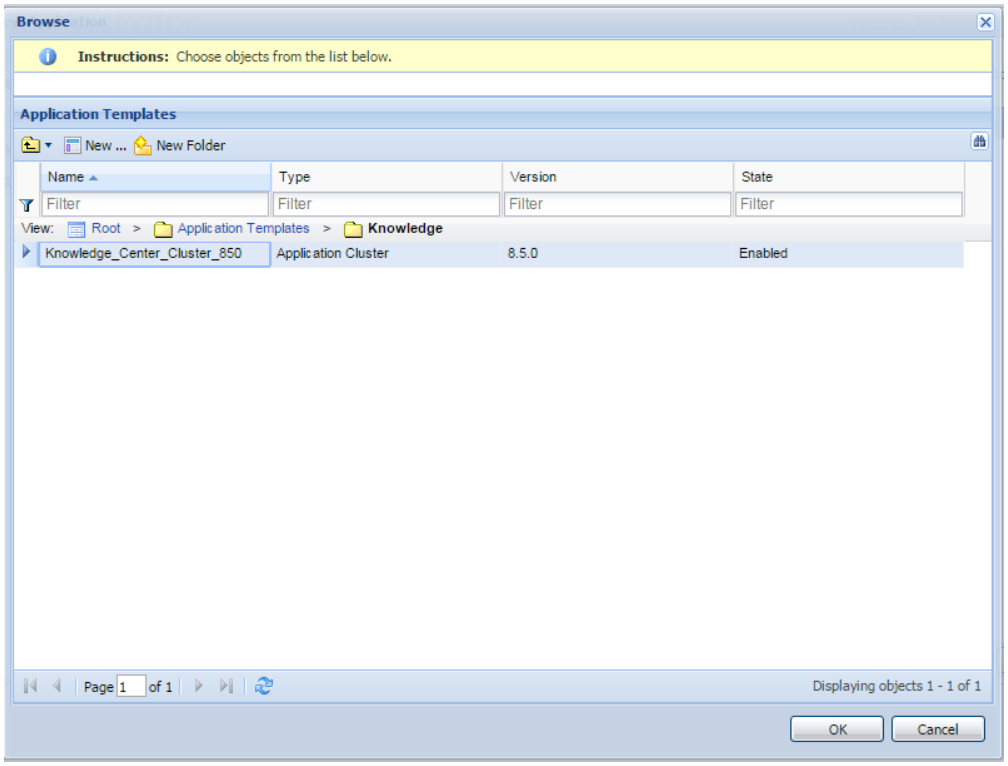


New Application Template Panel

5. Click **Save and Close**.

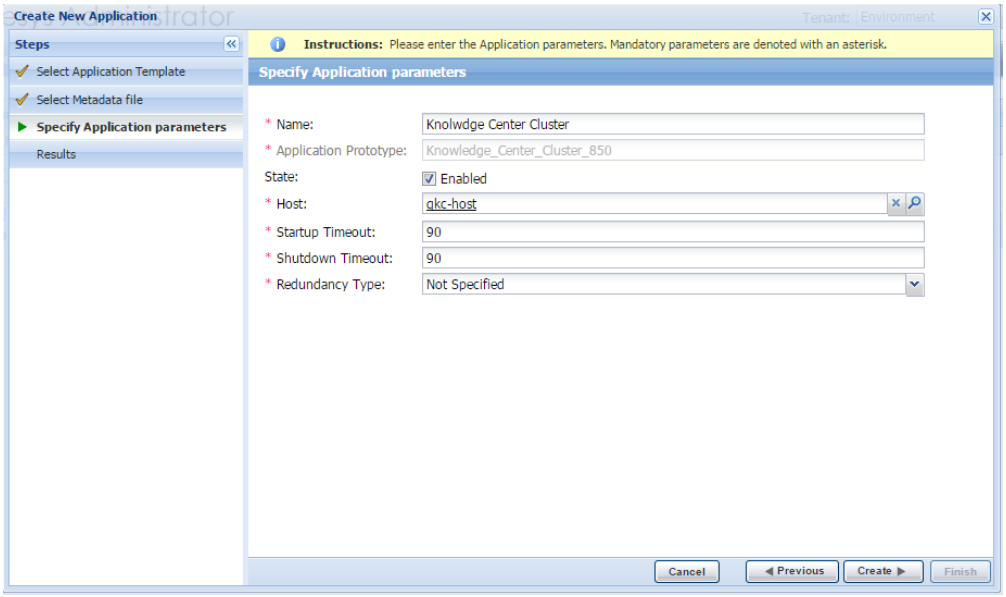
Create Cluster Applications

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**.



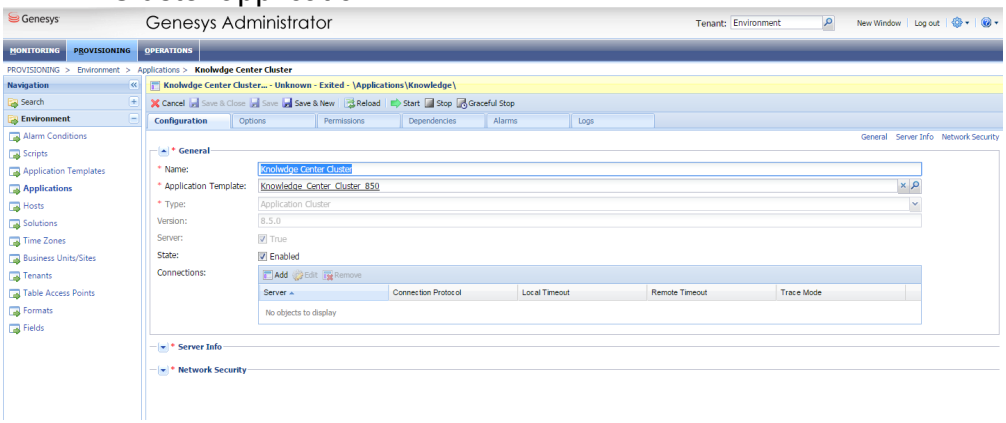
Selecting GKC Cluster Application Template

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_Cluster_850.xml* file. Click **Open**.
6. The metadata file is added to the **Select Metadata** file panel. Click **Next**.
7. In **Specify Application parameters**:
    1. Enter a name for your application. For instance, *Knowledge Center Cluster*.
    2. Enable the **State**.
    3. Select the **Host** on which the GKC Cluster load-balancer will reside.
    4. Click **Create**.



Specifying GKC Cluster Application Parameters

8. The **Results** panel opens.
9. Enable **Opens the Application details form after clicking 'Finish'** and click **Finish**. The GKC Cluster application form opens and you can start configuring the Cluster application.

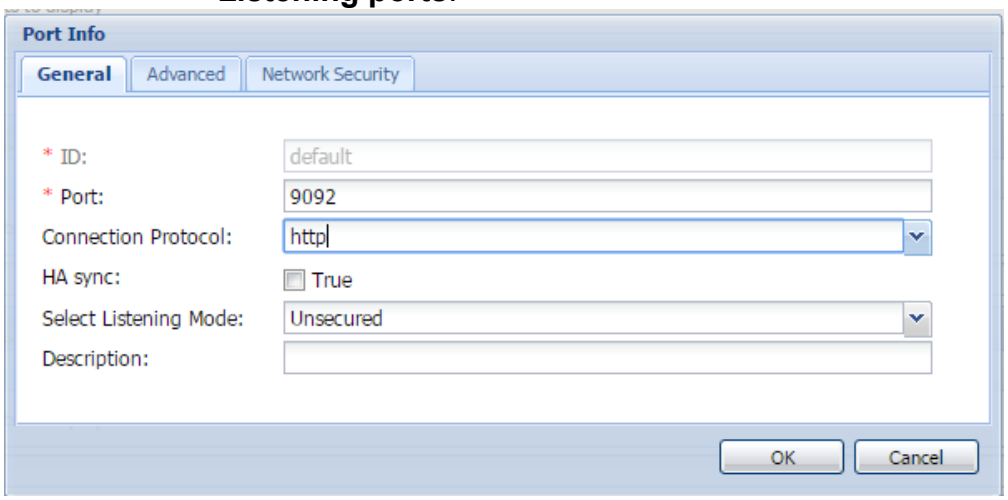


Configuring the GKC Cluster Application

Configure the Cluster Application

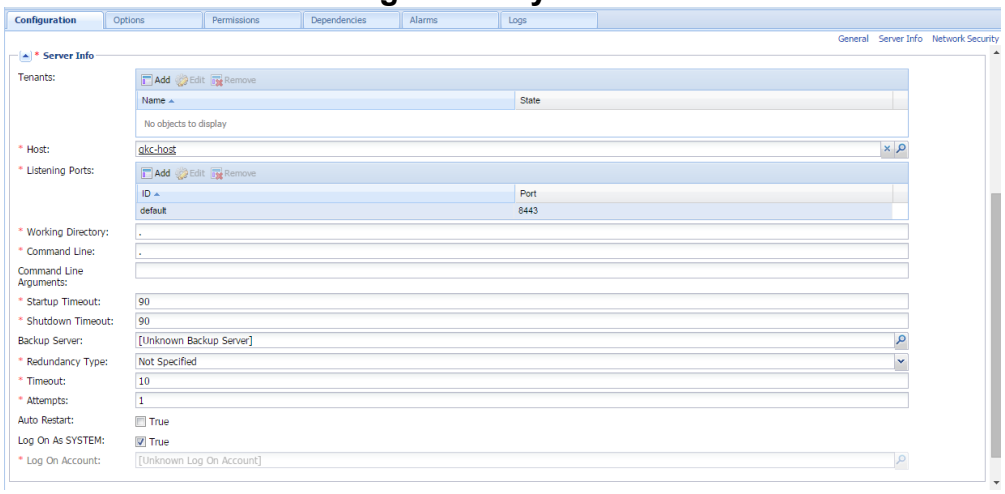
1. If your GKC Cluster application form is not open in Genesys Administrator, navigate to **Provisioning > Environment > Applications**. Select the application defined for the GKC Cluster and click **Edit...**.
2. Expand the **Server Info** pane.
3. If your **Host** is not defined, click the lookup icon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

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



GKC Cluster Port Information

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



GKC Cluster Server Information

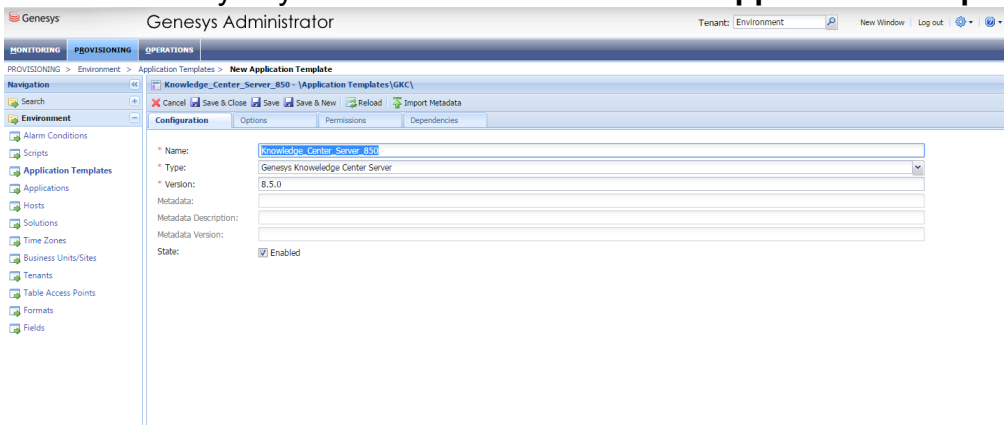
6. Click **Save**.
7. The **Confirmation** dialog for changing the application's port opens. Click **Yes**.

Installing GKC Server

Import the GKC 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_850.apd* file available in the *templates* directory of your installation CD. The **New Application Template** panel opens.



The GKC Server Application Template

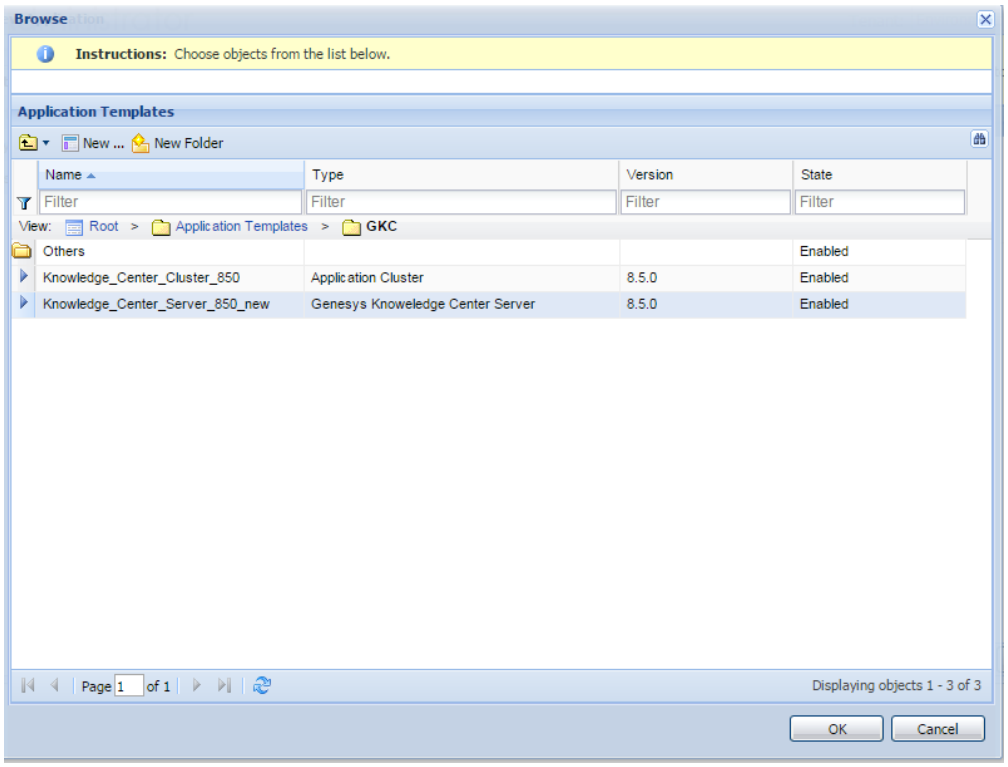
5. Click **Save and Close**.

End

Create Server applications

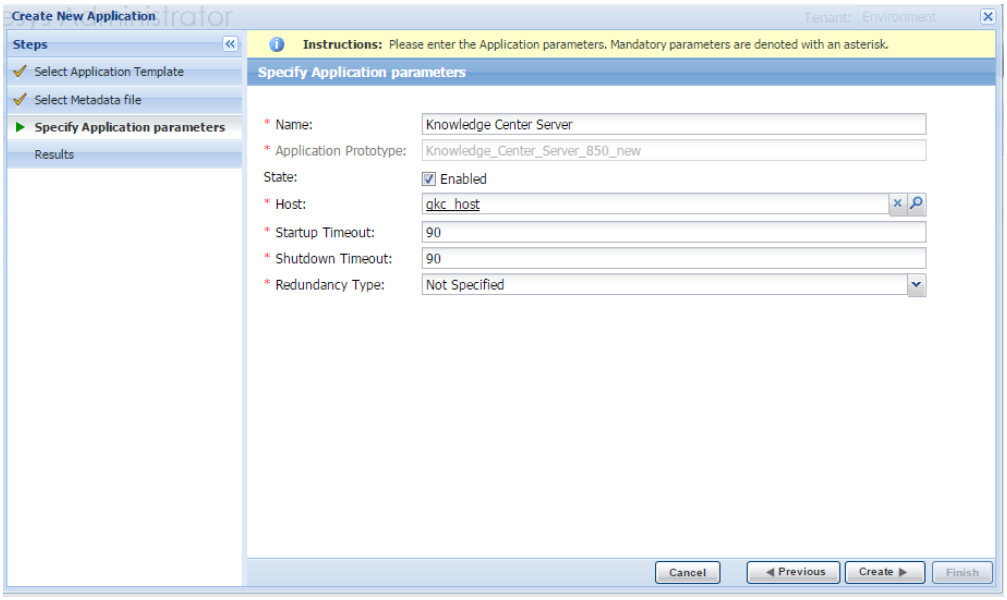
Start

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**.



Selecting the GKC Server Template

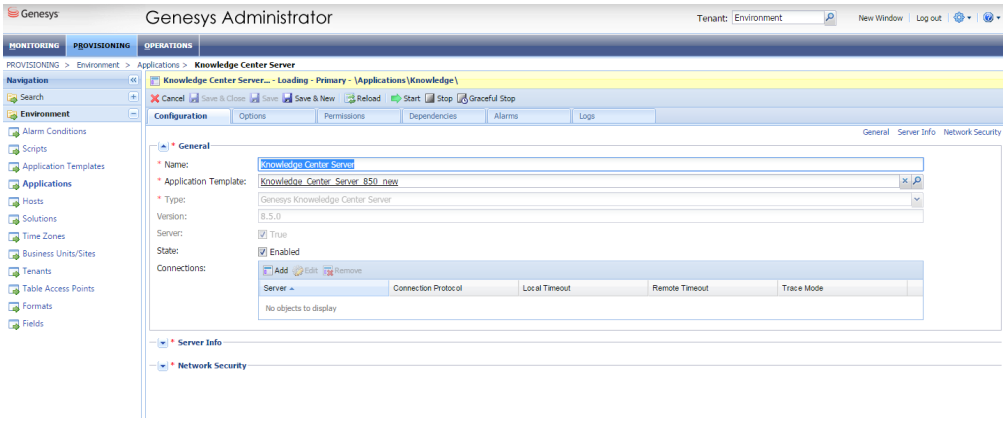
4. The template is added to the **Select Application Template** panel. Click **Next**.
5. In the **Select Metadata** file panel, click **Browse** and select the *Knowledge_Center_Server_850.xml* file. Click **Open**.
6. The metadata file is added to the **Select Metadata** file panel. Click **Next**.
7. In **Specify Application parameters**:
    1. Enter a name for your application. For instance, *Knowledge Center Server'* .
    2. Enable the **State**.
    3. Select the Host on which the GKC Server will reside.
    4. Click Create.



Creating the GKC Server Application

5. The **Results** panel opens.
6. Enable **Opens the Application details** form after clicking **Finish** and click **Finish**.

The Knowledge Center Server application form opens and you can start configuring the GKC Server application.



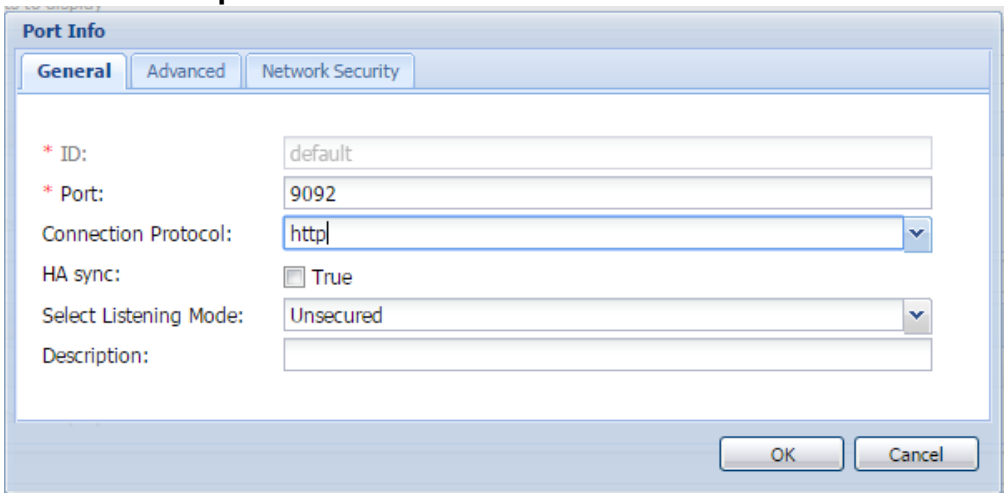
GKC Server Application Details

End

Configuring the GKC Server Application

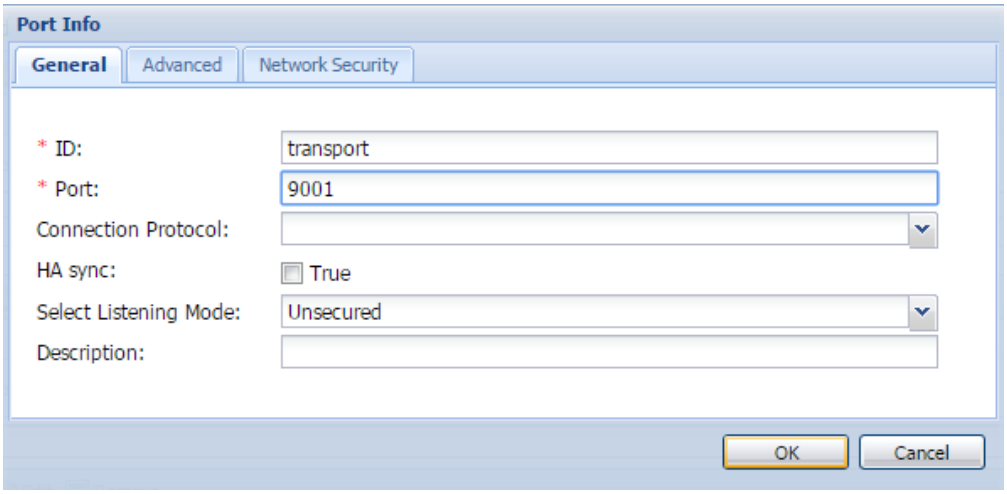
Start

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 GKC Server and click **Edit...**.
2. In the **Connections** section of the **Configuration** tab, click **Add**. The **Browse for applications** panel opens. Select the GKC Cluster application, then click **OK**.
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.
    1. Enter the **Port**. For instance, *9092*. This should be the port number for the GKC Server instance.
    2. Click **OK**. The port with the default identifier appears in the list of **Listening ports**.



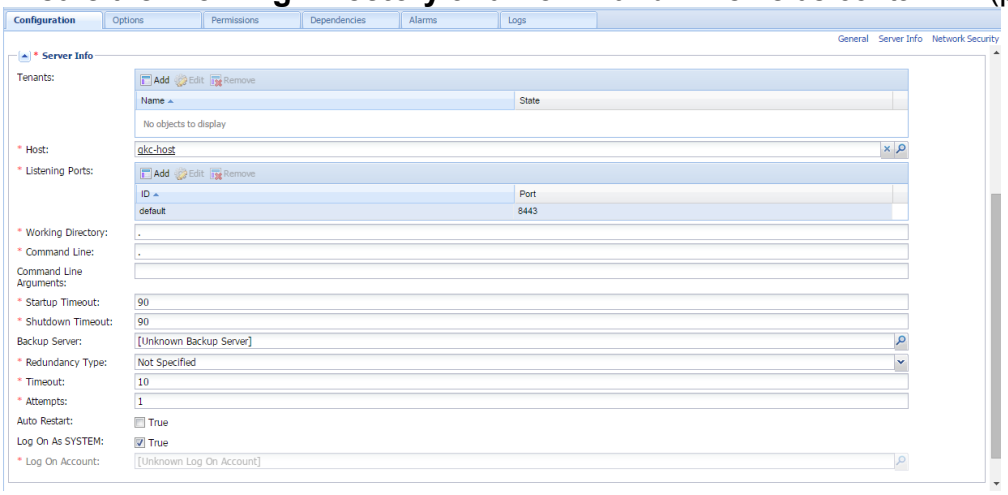
GKC Server Port Information

6. Optionally, you can explicitly add a Transport port for ElasticSearch engine. If you do not define a transport port, port 9300 will be used. To specify the stop port, click the **Add** button. The **Port Info** dialog opens.
    1. Enter *transport* for the ID field.
    2. Enter the **Port**. For instance, *9001*
    3. Click **OK**.



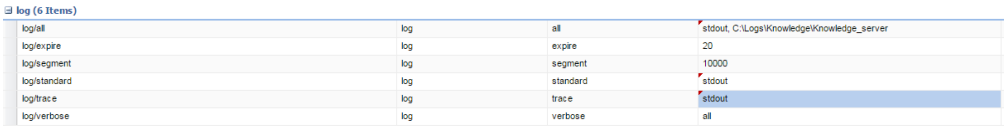
GKC Server Transport Port Information

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



GKC Server Application Information

5. Click **Save**.
6. The Confirmation dialog for changing the application's port opens. Click **Yes**.
7. (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.



GKC Server Application Logging Options

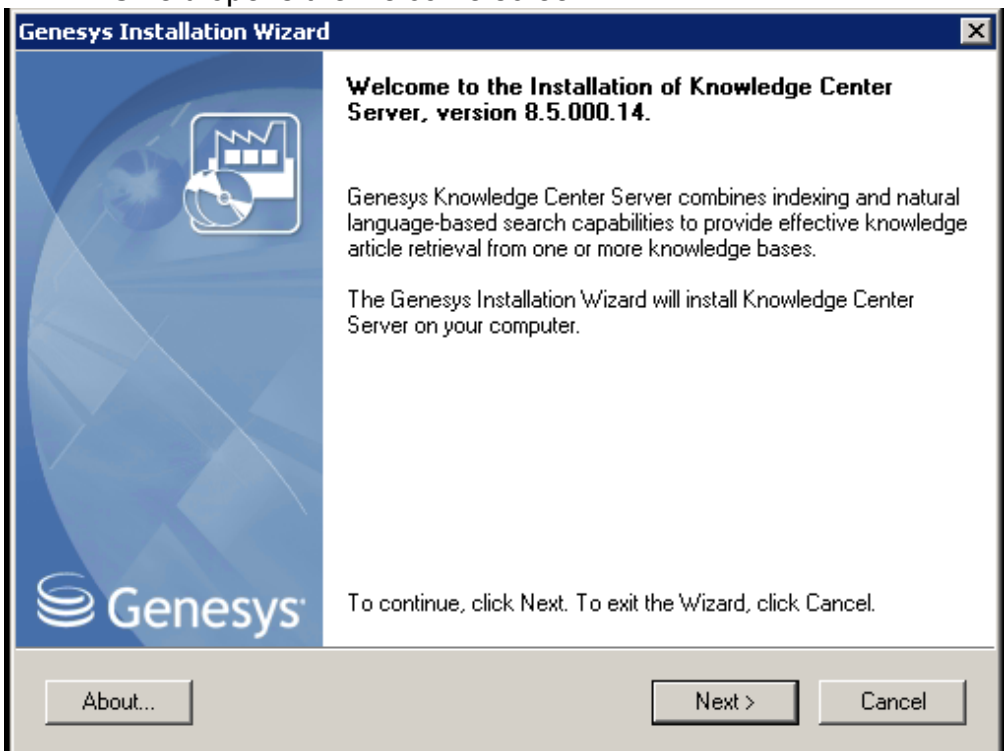
End

Installing GKC Server

Windows Installation Procedure

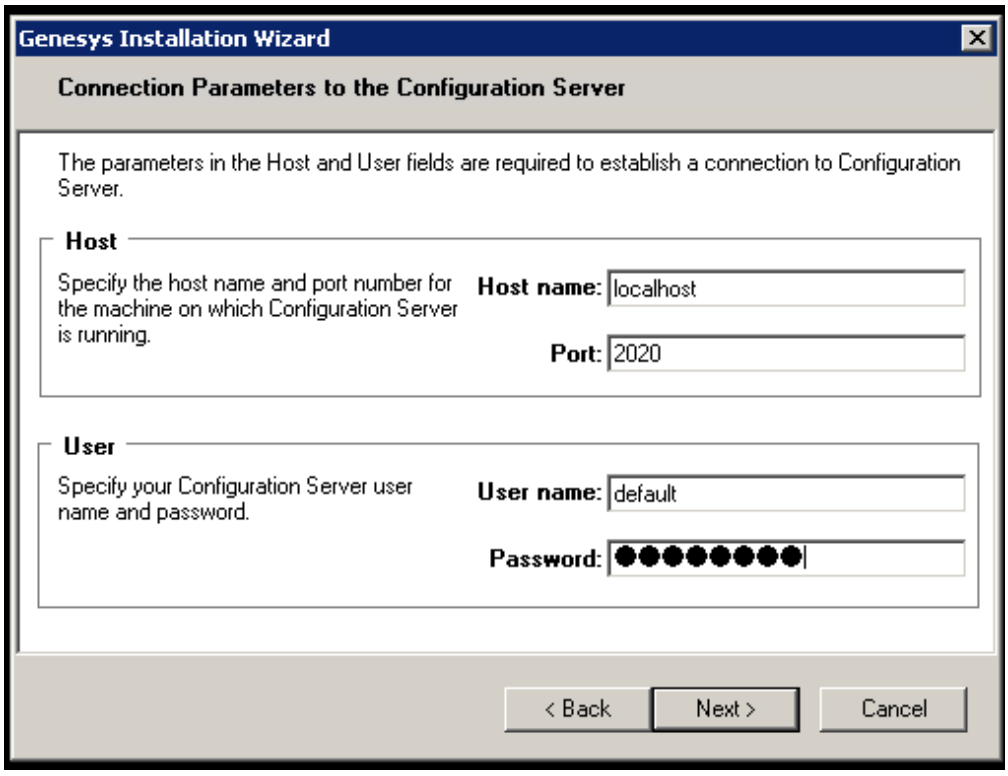
Start

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



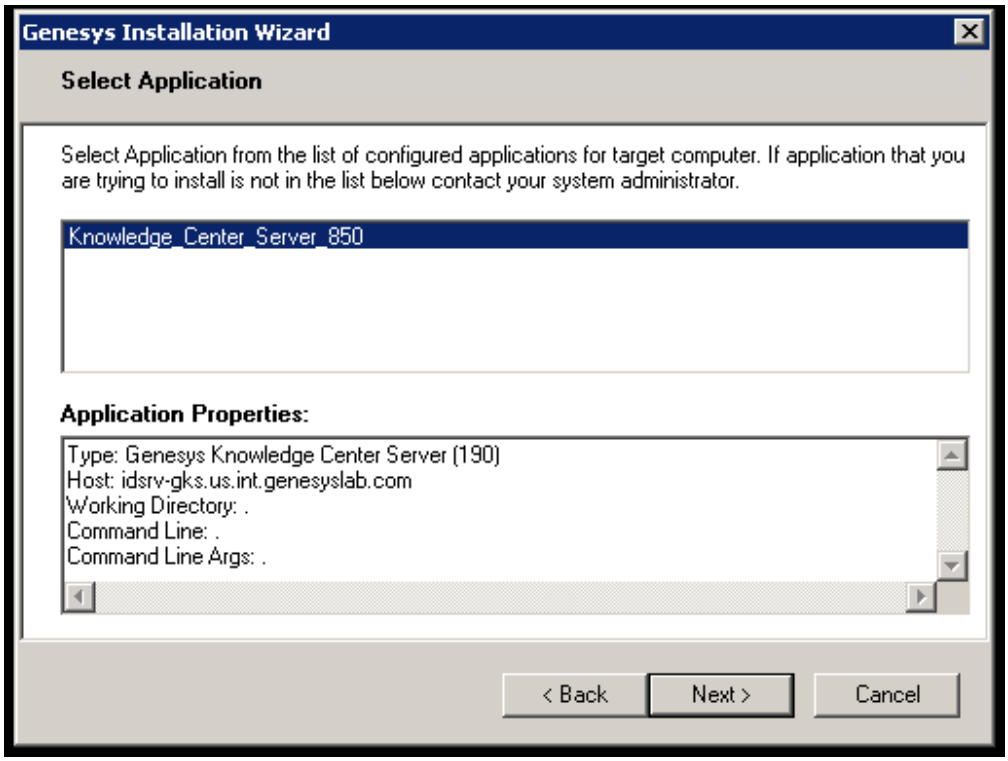
GKC Server Installation Window

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



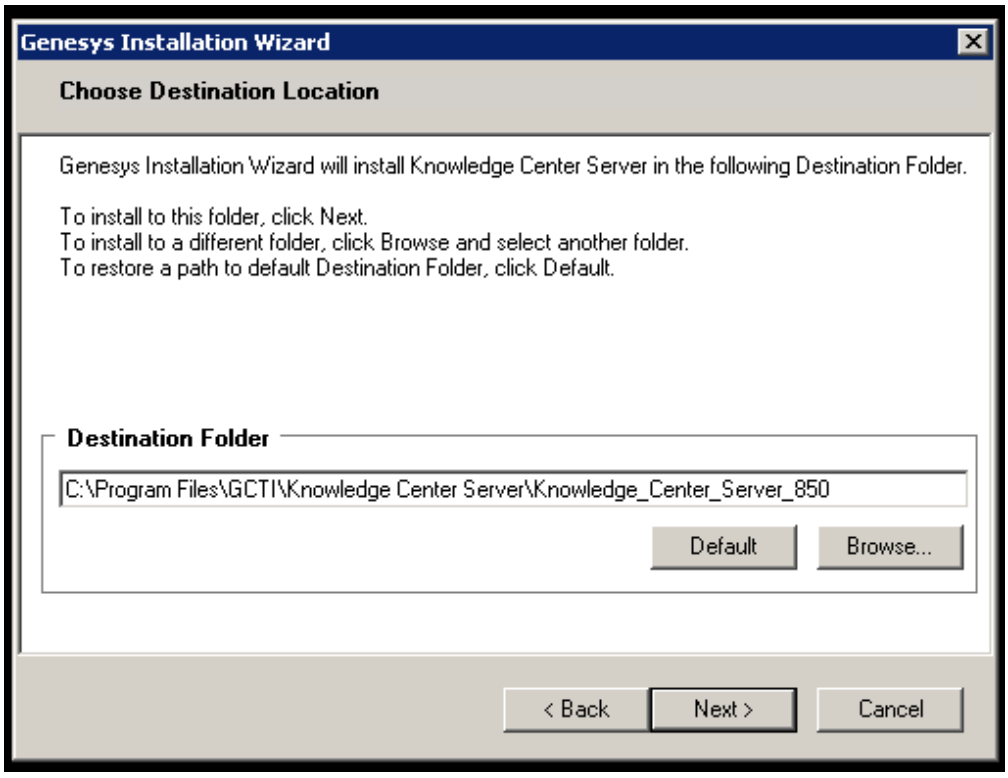
GKC Server Connection Parameters

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.



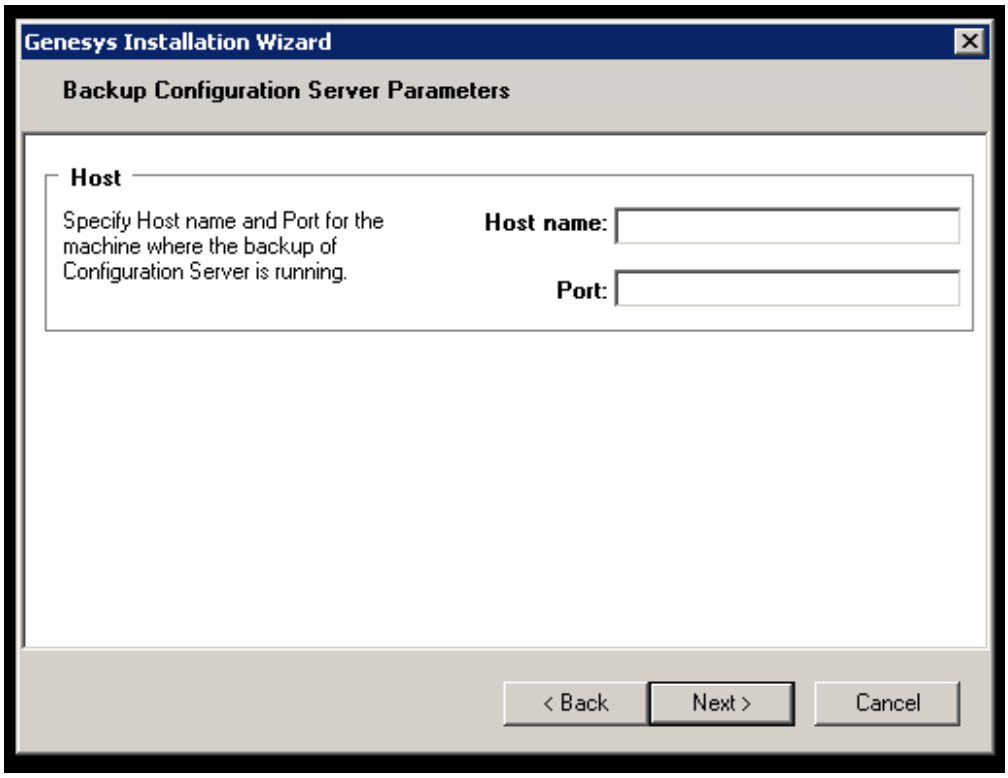
Selecting the GKC Server Application

6. Select the GKC 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.
7. Click **Next**. The **Choose Destination Location** screen appears.



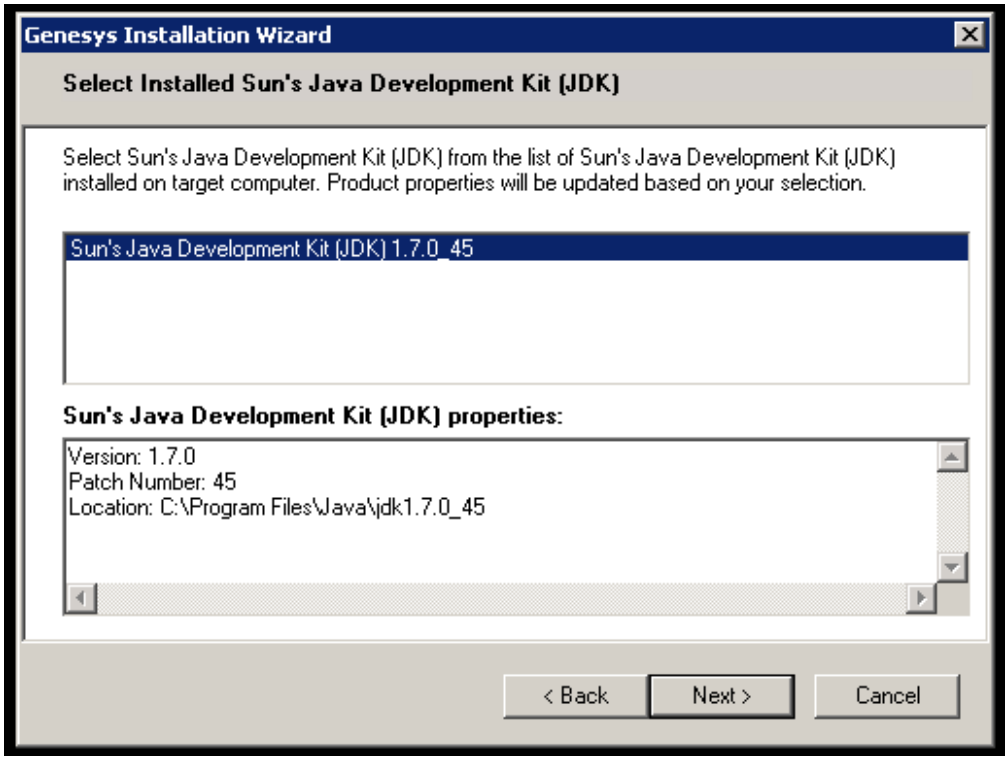
Choosing the GKC Server Installation Destination

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.



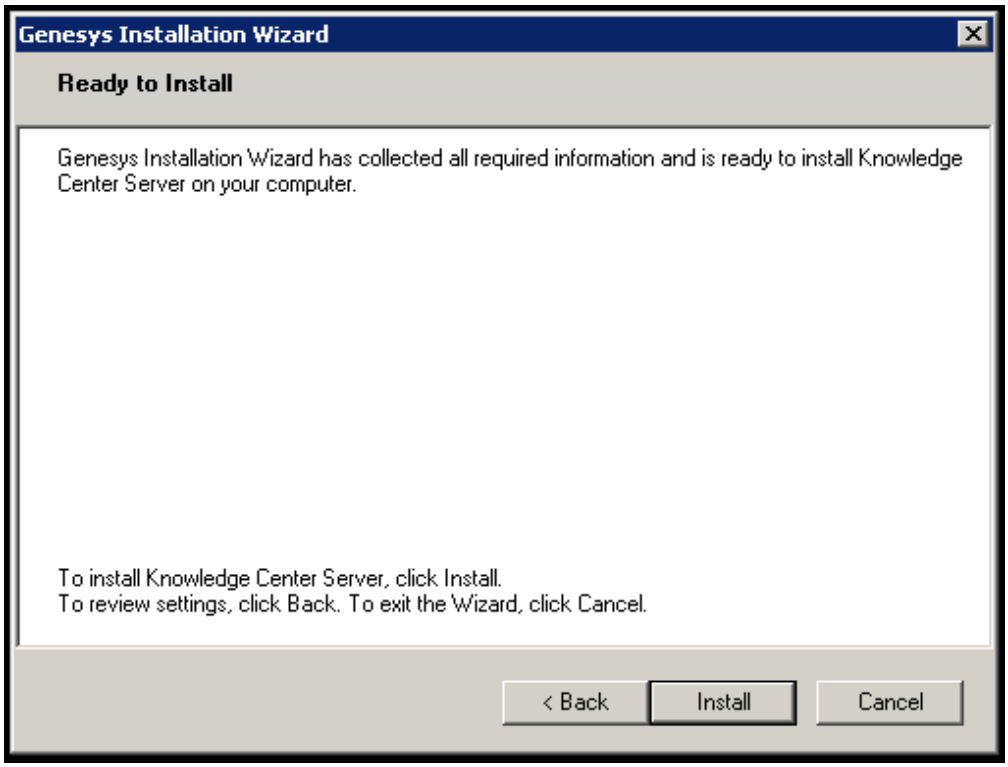
GKC Backup Config Server Parameters

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.



Selecting the GKC Server Java Version

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



GKC Server is Ready to Install

13. Click **Install**. The Genesys Installation Wizard indicates it is performing the requested operation for Backend Server. 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.

Important

The Windows service will not be automatically configured during installation. To configure the Windows service, start *server.bat* with the following parameters: **server.bat install**. To run the server as service, comment out the (REM) APP_TYPE property in *senenv.bat* before installing the service.

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:
    1. **Hostname**—For instance, *demosrv.genesyslab.com*
    2. **Listening port**—For instance, *2020*
    3. **User name**—For instance, *demo*
    4. **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

Understanding the GKC Server Configuration Files

GKC Server includes an embedded Jetty server and Lingua Tools in its installation folder. Product installation pre-configures all of the links between these resources, but there are cases in which they need to be changed. This section describes how to work with the configuration files stored in the GKC Server.

Jetty Configuration

1. Create a *work* directory inside the *./server* folder in the installation directory as a place to store temporary Jetty files.
2. Create a *data* directory inside the *./server* folder in the installation directory to store the ElasticSearch data files.
3. After you complete these steps, GKC Server will be available as a web service on the following URLs:
    - http://host:jetty.port/gks-server—GKC Server
    - http://host:jetty.port/gks-sample-ui—Sample UI sandbox

ElasticSearch Engine Configuration

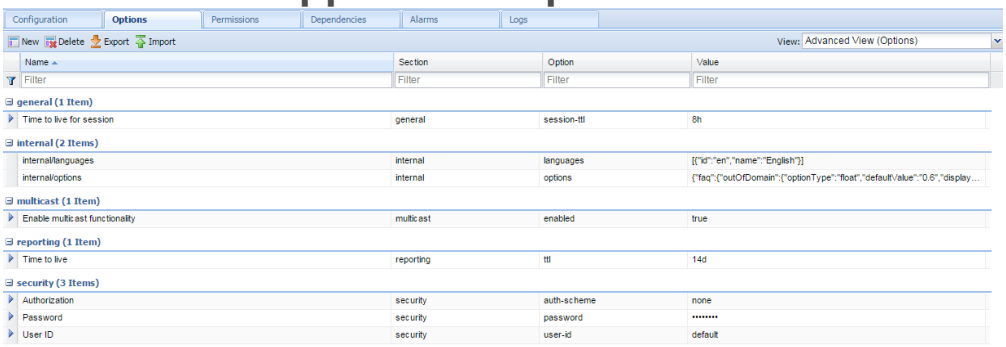
1. Go to the *./server* folder and open the *gks.yml* configuration file.
2. Configure the following settings:
    1. index.number_of_shards: #—Number of ElasticSearch shards
    2. path.data : [PATH]—Path to the folder that contains index data for this node (default: */gks/data*)
    3. path.similarwords.en: [PATH]—Path to dictionary compendium
    4. path.freeling : [PATH]—Path to Freeling data folder

Language Resources Configuration

- Dictionary compendium
    - You can set the path to */linguatools/disco/enwiki-20130403-sim-lemma-mwl-lc* inside the installation directory to *path.similarwords.en* in *gks.yml*
- Freeling tokenizer:
    - In Windows
        - The path to */linguatools/freeling/data/* can be changed in the *gks.yml* file: *path.freeling*.
        - The following path will be added to the Windows PATH variable during installation: *Path to installation directory*/linguatools/freeling/bin.
    - In Linux
        - The path to */linguatools/freeling/data/* can be changed in the *gks.yml* file: *path.freeling*.
        - *setenv.sh* exports the following environment variables:
            - FREELINGSHARE—Path to *Path to installation directory*/linguatools/freeling
            - LD_LIBRARY_PATH—Path to *Path to installation directory*/linguatools/freeling/bin

Configuration Options

GKC Cluster Application Options



GKC Cluster Application Configuration Options

[general] section

session-ttl Default Value: 8h
Valid Values: number + unit, e.g. 1d or 3m. Supported units: d (days), m (minutes), h (hours), or w(weeks)
Changes Take Effect: After restart.
Specify time that server will store session information while no activities are taking place.

[multicast] section

enabled Default Value: true
Valid Values: true, false
Changes Take Effect: After restart.
Specify whether enabled node should use multicast or unicast to discover other servers within the same cluster.

[reporting] section

ttl Default Value: 14d
Valid Values: number + unit, e.g. 1d or 3m. Supported units: d (days), m (minutes), h (hours), or w(weeks)
Changes Take Effect: After restart.
Specify time that records will be stored in the history.

[security] section

auth-scheme Default Value: none
Valid Values: none, basic
Changes Take Effect: After restart.
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.

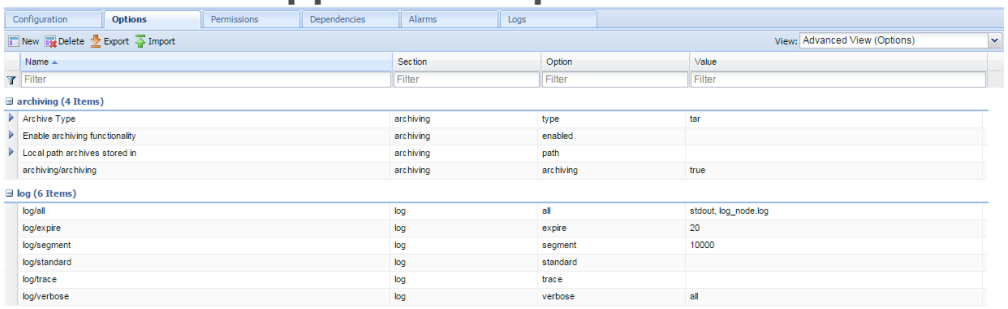
user-id Default Value: none
Valid Values: string
Changes Take Effect: After restart.
The user identifier (login) used in authentication for the REST API

password Default Value: none
Valid Values: string
Changes Take Effect: After restart.
The user password used in authentication for the REST API.

[internal] section

> **Important**
>
> GKC Server uses this section to store internal initialization parameters. Do not attempt to change these options.

GKC Server Application Options



GKC Server Application Configuration Options

[archiving] section

enabled
Default Value: true
Valid Values: true, false
Changes Take Effect: After restart.
Specifies whether a node will allow to execute archiving using its API. Enabling archiving on the node does not affect other nodes of the cluster. Archiving is resource consuming functionality - use it wisely.

type
Default Value: tar
Valid Values: tar, zip, cpio
Changes Take Effect: After restart.
Defines format of resulted archive will be stored in.

path
Default Value: none
Valid Values: string
Changes Take Effect: After restart.
Path to the stored archive. The archive will be stored as <path>/history_<requested_date_range>.<archive>

[security] section

trusted-ca-type
Default Value: MSCAPI
Valid Values: MSCAPI – MSCAPI certificate storage is used for TLS certificate verification.
PEM – PEM certificate storage is used for TLS certificate verification. In this case, the trusted-ca option should also be specified and should contain the path to the PEM file.
JKS – JKS certificate storage is used for TLS certificate verification. In this case, the trusted-ca option should also be specified and should contain the path to the JKS file. You should also set the trusted-ca-pwd option to the password for the JKS file.
Changes Take Effect: After restart.
Specifies the type of trusted certificate authority. No TLS is applied for connections between this server and other Genesys servers if this option is absent.

trusted-ca
Default Value: none
Valid Values: Path to the trusted store file (valid for PEM and JKS types, depending on value of the trusted-ca-type option).
Changes Take Effect: After start or restart.
Specifies the path to the trusted store file (valid for PEM and JKS types, depending on value of the trusted-ca-type option).

trusted-ca-pwd
Default Value: none
Valid Values: Password for the trusted store file (valid for JKS type only).
Changes Take Effect: After start or restart.
Specifies the password for the trusted store file (valid for JKS type only).

[log] section

all
Default Value: stdout
Valid Values (log output types):

stdout	Log events are sent to the Standard output (stdout).
stderr	Log events are sent to the Standard error output (stderr).
network	Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
memory	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
[filename]	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: After start or restart.
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

standard
Default Value: stdout
Valid Values:

stdout	Log events are sent to the Standard output (stdout).
stderr	Log events are sent to the Standard error output (stderr).
network	Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database.
memory	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.

[filename]	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: Immediately
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

trace
Default Value: stdout
Valid Values:

stdout	Log events are sent to the Standard output (stdout).
stderr	Log events are sent to the Standard error output (stderr).
network	Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database.
memory	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
[filename]	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: Immediately
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

verbose
Default Value: standard
Valid Values:

all	All log events (that is, log events of the Standard, Trace, Interaction, and Debug levels) are generated.
debug	The same as all.
trace	Log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels) are generated, but log events of the Debug level are not generated.

interaction	Log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels) are generated, but log events of the Trace and Debug levels are not generated.
standard	Log events of the Standard level are generated, but log events of the Interaction, Trace, and Debug levels are not generated.
none	No output is produced.

Changes Take Effect: Immediately
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.

segment
Default Value: 1000
Valid Values:

false	No segmentation is allowed.
<number> KB or <number>	Sets the maximum segment size, in kilobytes. The minimum segment size is 100 KB.
<number> MB	Sets the maximum segment size, in megabytes.
<number> hr	Sets the number of hours for the segment to stay open. The minimum number is 1 hour.

Changes Take Effect: After restart.
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.

expire
Default Value: 3
Valid Values:

false	No expiration; all generated segments are stored.
<number> file or <number>	Sets the maximum number of log files to store. Specify a number from 1—1000.
<number> day	Sets the maximum number of days before log files are deleted. Specify a number from 1—100.

Changes Take Effect: After restart.
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.

Important

If an option's value is not set within the range of valid values, it will automatically be reset to 10.

affectedLoggers
Default Value: None
Valid Values: The names of loggers, separated by a semicolon (;), specified in the LOG4J2.xml. For example:
com.genesyslab.webme.commons;PROTOCOL;org.apache.cassandra
Changes Take Effect: Immediately
Verbosity settings are explicitly applied for the following loggers:

- Loggers that are not declared explicitly in the *log4j2.xml* configuration file.
- Loggers that are specified explicitly in the *log4j2.xml* and are specified in the value for this affectedLoggers option.

For other loggers specified in *log4j2.xml*, but not mentioned in the value for this option, the verbosity level is not re-applied.

Here is a use case for when you might need to set this option:

- Cassandra needs to write error messages to a log file, and at the same time, Genesys components also need to write debug messages to the log file.

To resolve this use case, you would:

1. Specify the following logger in *log4j2.xml*: *<logger name="org.apache.cassandra" level="error" additivity="false">*
2. **Do not** include *org.apache.cassandra* in the value for the **affectedLoggers** option.
3. The default *log4j2.xml* file contains the following logger: *<logger name= "com.genesyslab.platform" level="info" additivity="false">*
4. Include *com.genesyslab.platform* in the value for the **affectedLoggers** option.
5. Set the **verbose** option to *debug*.

In the sample above, the value of **affectedLoggers** should be *com.genesyslab.platform*. Error (but not debug or info) messages from Cassandra will be available in logs, and debug messages from *com.genesyslab.platform* will be available in logs.

time_format
Default Value: time
Valid Values:

time	The time string is formatted according to the 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
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

time_convert
Default Value: local
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
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.

Provide GKC Access to Agents

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

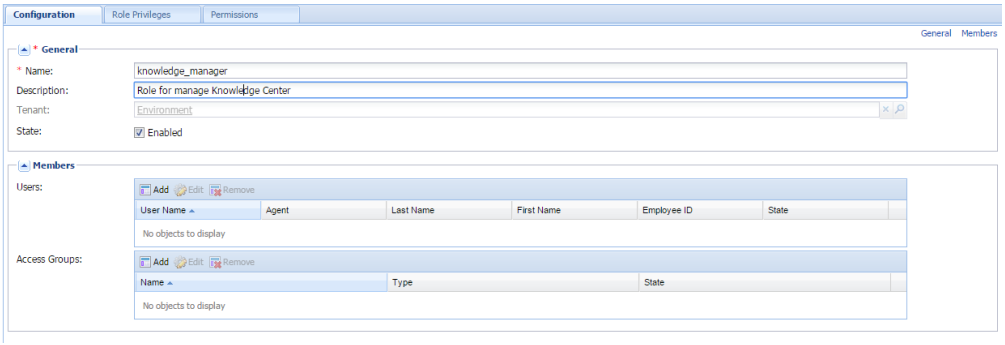
- **Knowledge.ADMINISTER**—Configure knowledge bases in the GKC Cluster application
- **Knowledge.AUTHOR**—Create, populate, and manage knowledge bases

- **Knowledge.REPORTING**—Extract data on the activities carried out by agents and customers while using the knowledge service

To configure the appropriate privileges for an Agent:

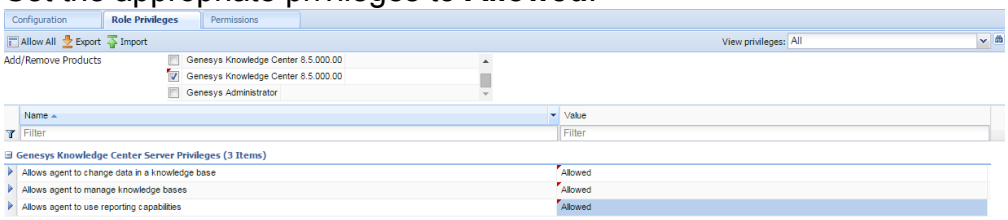
Start

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.



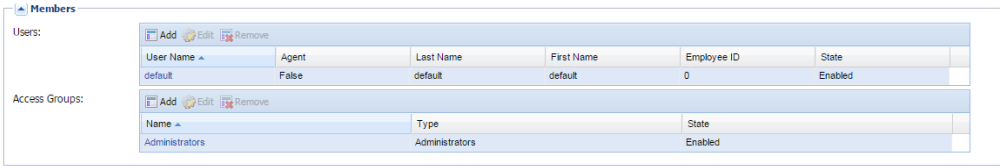
GKC Server Access Roles

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



Setting GKC Server Access Privileges

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



GKC Server Members Section

9. Save and Close.

End

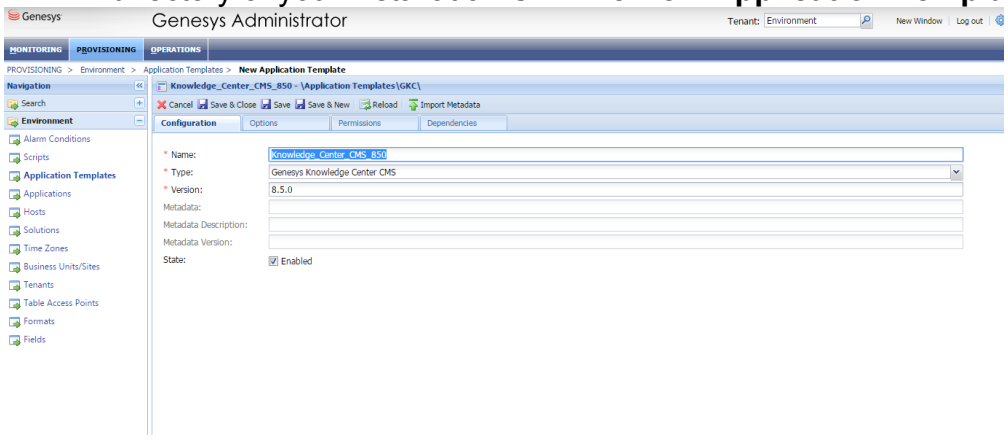
Installing the GKC CMS

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_850.apd* file available in the templates directory of your installation CD. The **New Application Template** panel opens.



The GKC CMS Application Template

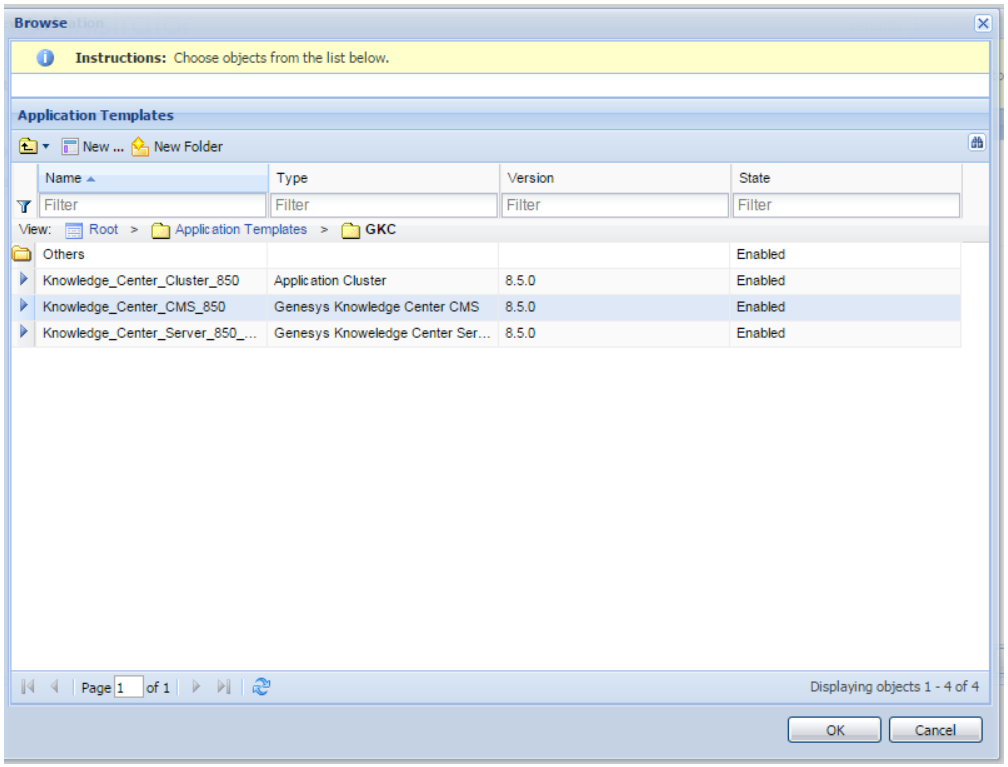
5. Click **Save and Close**.

End

Create CMS Applications

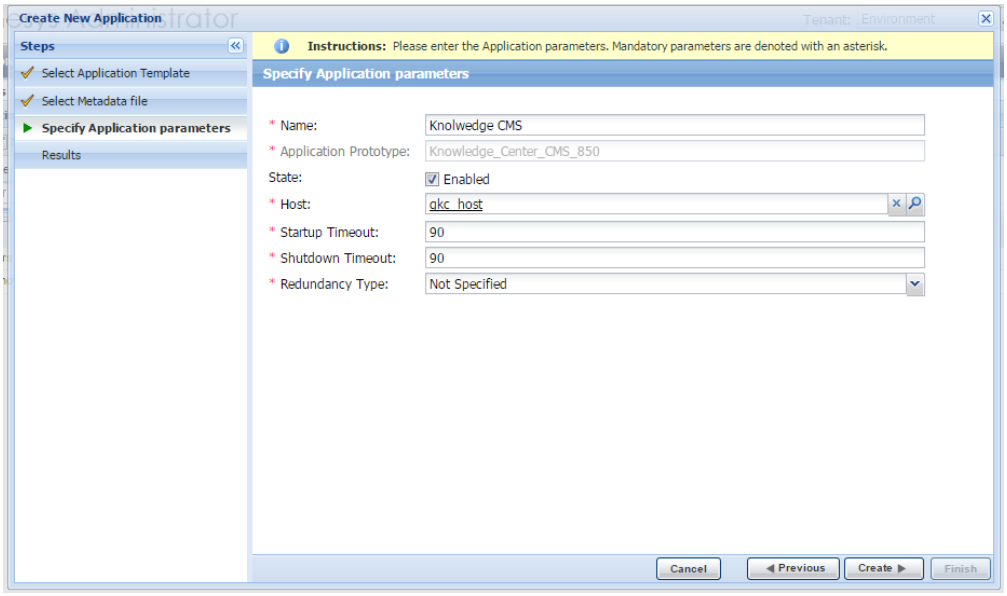
Start

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 Server application template that you imported earlier. Click **OK**.



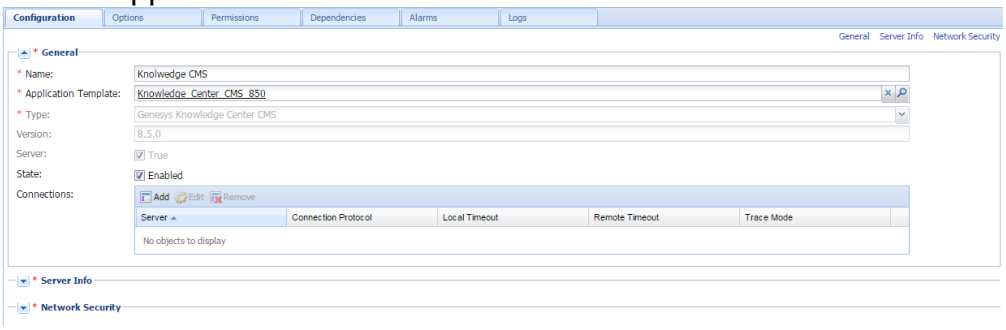
Selecting the GKC CMS Template

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_850.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**:
    1. Enter a name for your application. For instance, *Knowledge Center CMS*.
    2. Enable the **State**.
    3. Select the Host on which the CMS load-balancer will reside.
    4. Click **Create**.



Creating the GKC CMS Application

8. The **Results** panel opens.
9. Enable **Opens the Application details form after clicking 'Finish'** and click **Finish**. The GKC Cluster application form opens and you can start configuring the Cluster application.



Configuring the GKC CMS Cluster

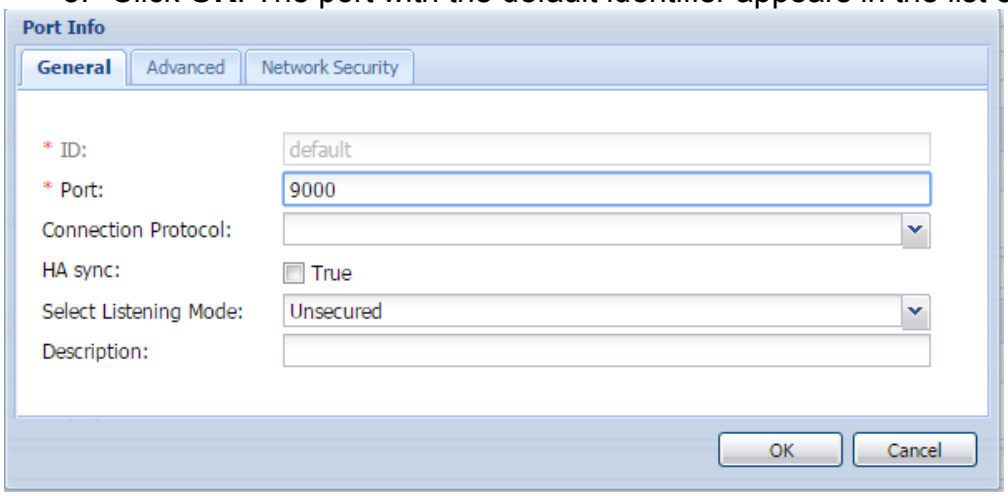
End

Configure the CMS Application

Start

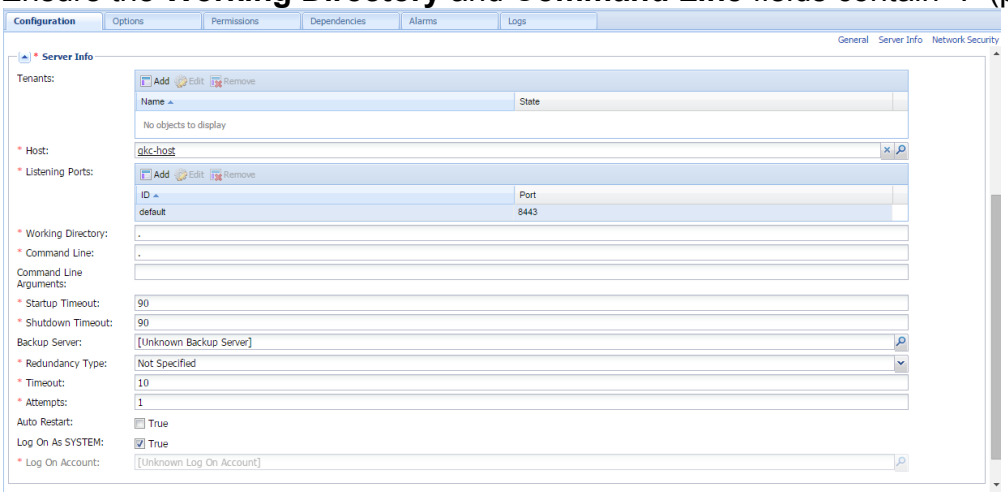
1. If your Knowledge Center CMS application form is not open in Genesys Administrator, navigate to **Provisioning > Environment > Applications**. Select the application defined for the GKC CMS and click **Edit...**.

2. In the **Connections** section of the **Configuration** tab, click **Add**. The **Browse for applications** panel opens.
3. Select the GKC 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.
7. Enter the Port. For instance, *9000*.
8. Click **OK**. The port with the default identifier appears in the list of **Listening ports**.



GKC CMS Port Information

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



GKC CMS Cluster Information

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

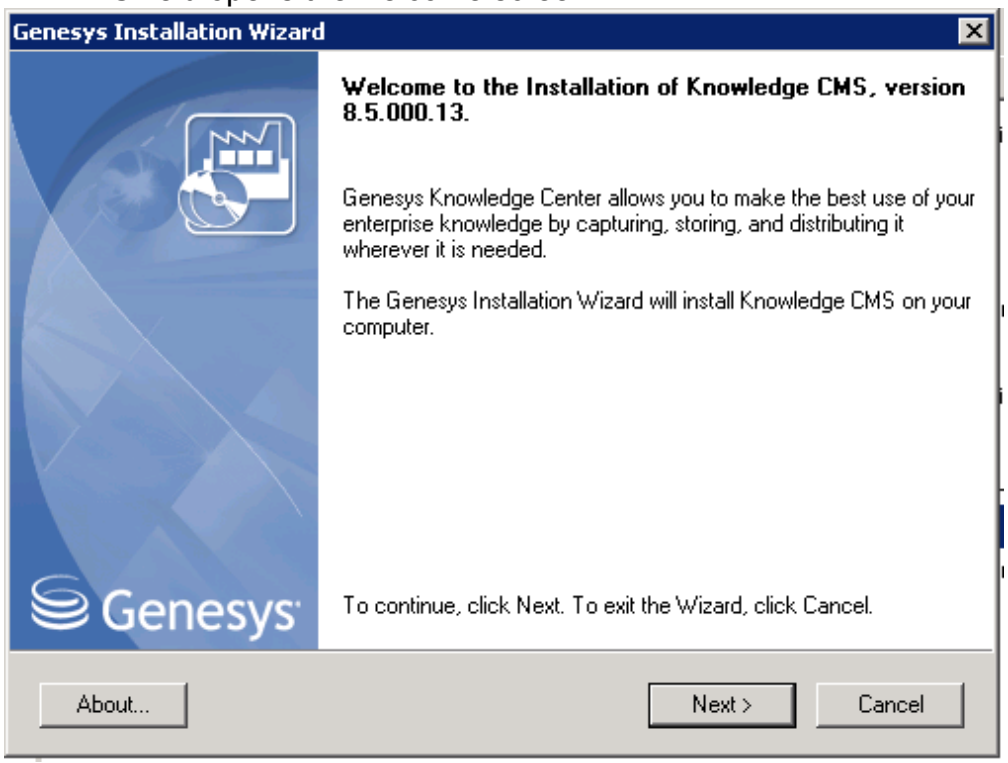
End

Installing the CMS

Windows Installation Procedure

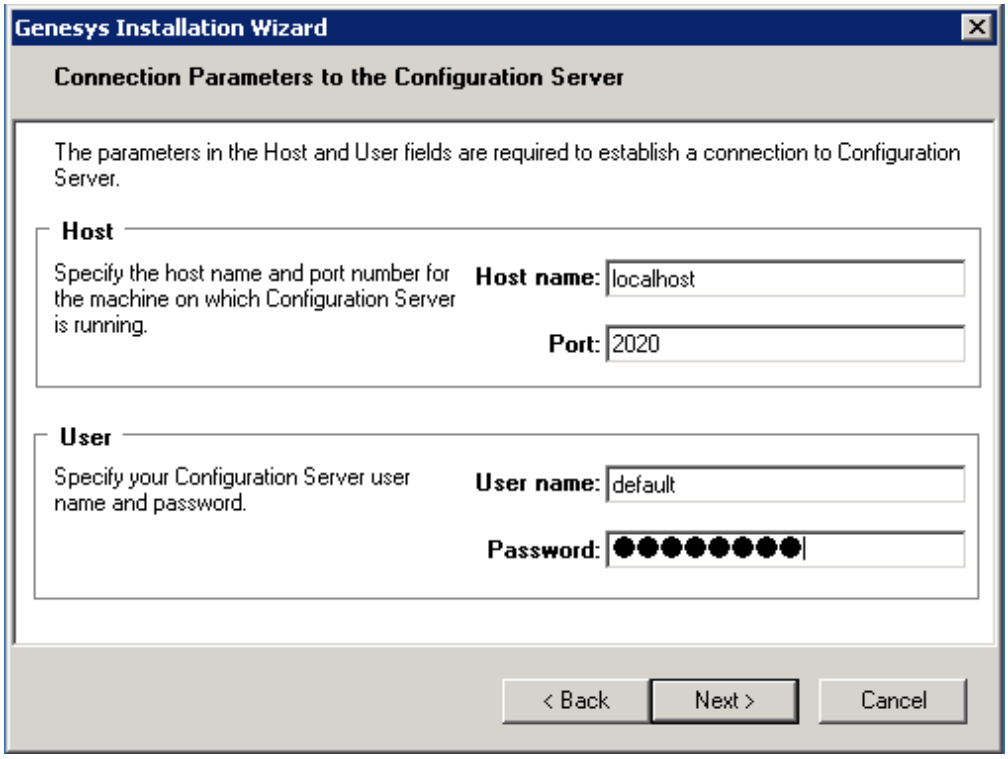
Start

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



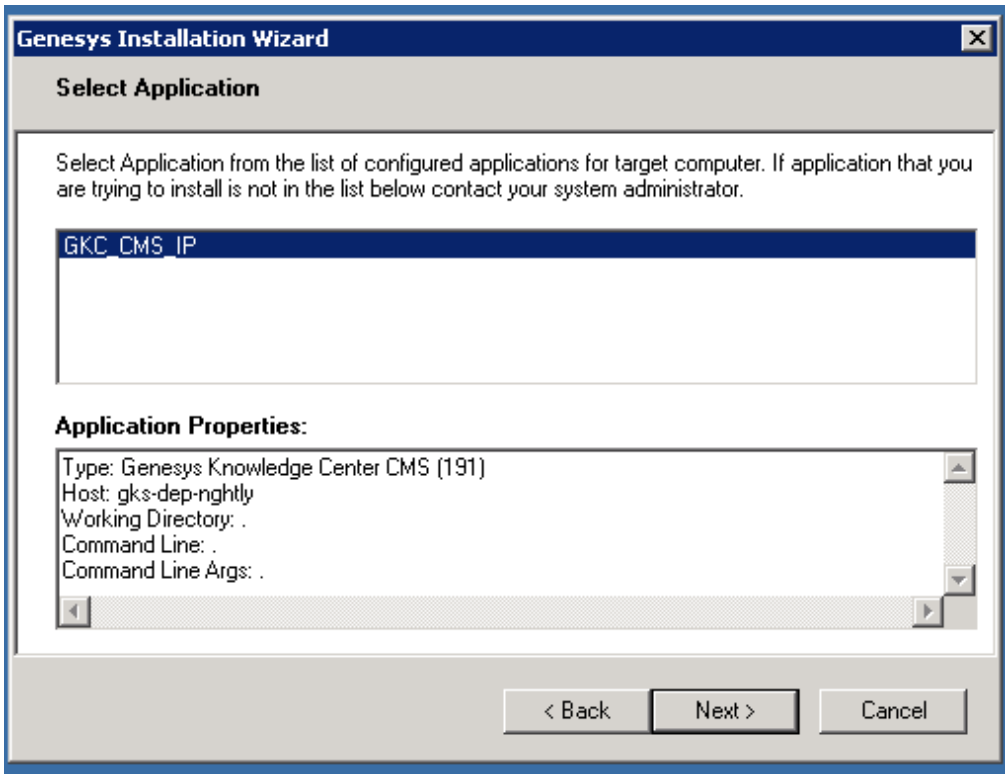
GKC CMS installation Window

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



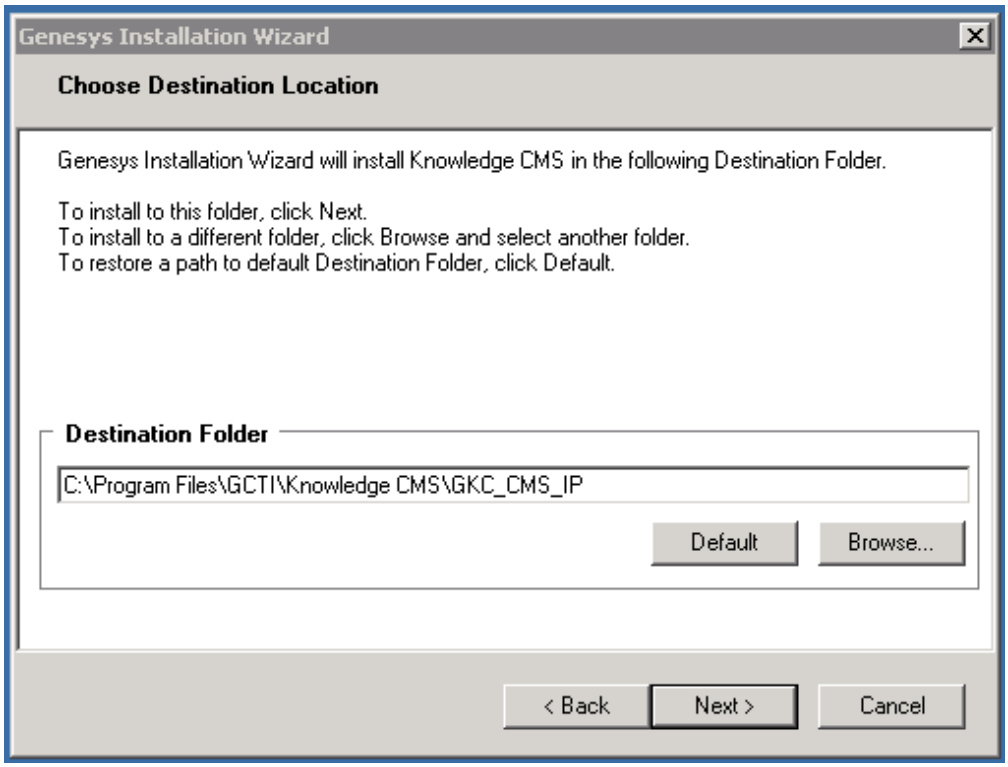
GKC CMS Connection Parameters

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 GKC 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.



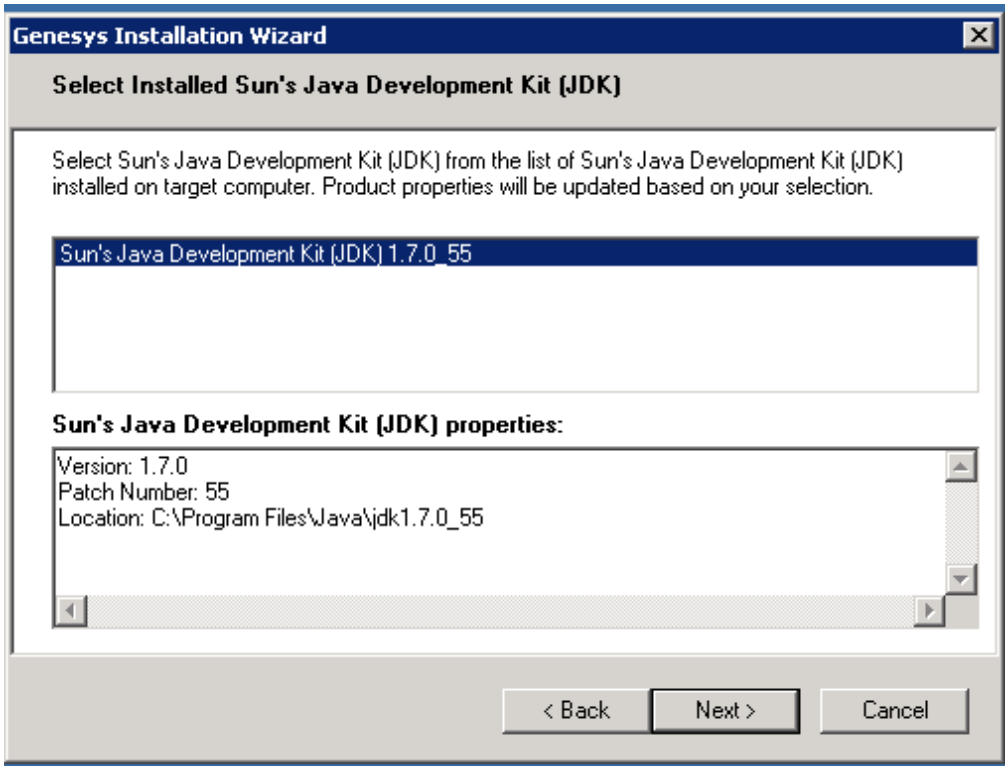
Selecting the GKC CMS Application

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



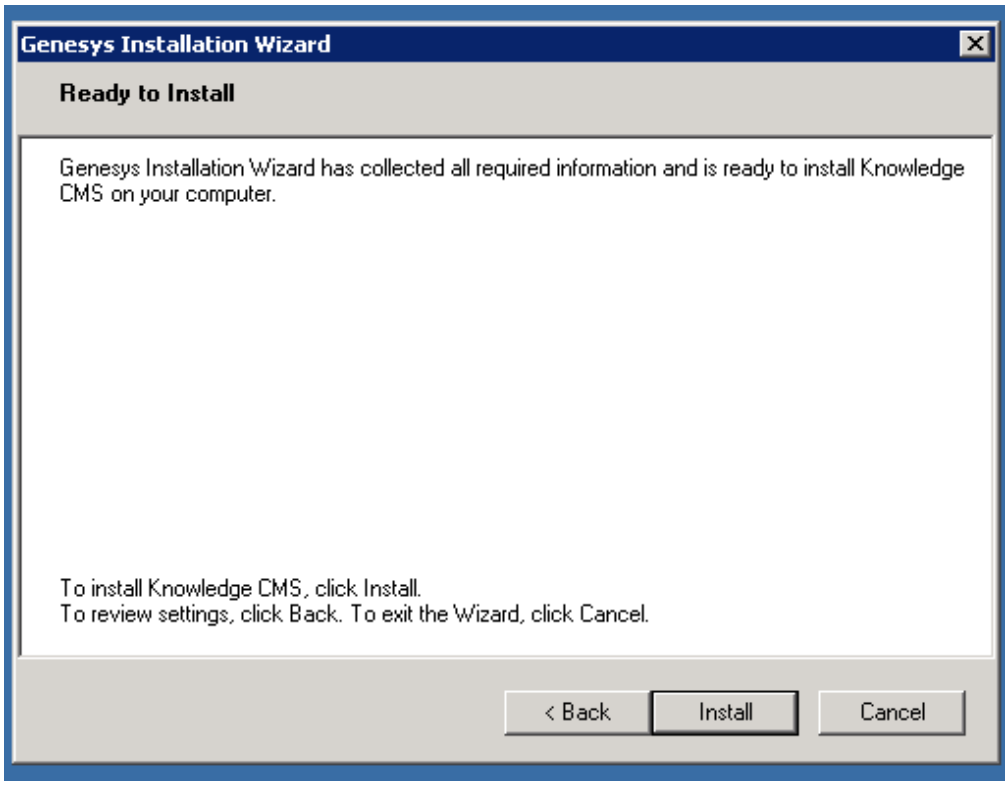
Choosing the GKC CMS Installation Destination

9. Click **Next**. Choose the appropriate version of the Java JDK.



Selecting the GKC CMS Java Version

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



GKC CMS 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.

Important

The Windows service will not be automatically configured during installation of the CMS. To configure the Windows service, start *server.bat* with the following parameters: **server.bat install**. To run the server as service, comment out the (REM) APP_TYPE property in *senenv.bat* before installing the service.

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:
    1. **Hostname**—For instance, *demosrv.genesyslab.com*
    2. **Listening port**—For instance, *2020*
    3. **User name**—For instance, *demo*
    4. **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 GKC CMS applications is displayed.
6. Enter the key for the GKC 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, version 8.5.x has completed successfully.*

End

Configuring the CMS

The GKC Server includes an embedded Jetty server. After installation, you can carry out your initial configuration by creating a *work* directory for temporary Jetty files inside the *./server* folder.

Configure Required CMS Access Options

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

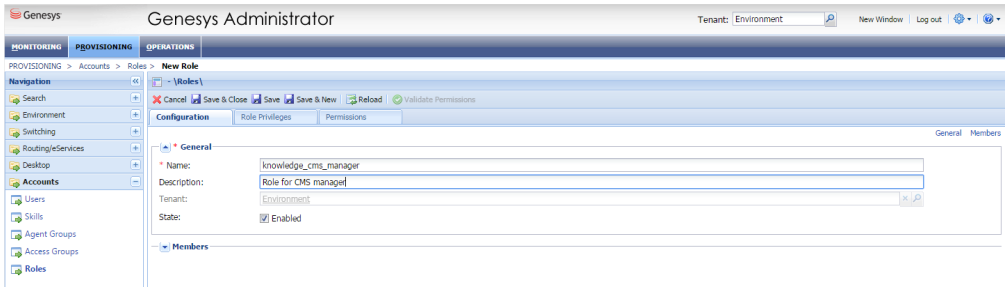
- **Knowledge.CMS.Document.Author**—create, edit, or delete documents
- **Knowledge.CMS.Category.Author**—create, edit, or delete categories
- **Knowledge.CMS.Approver**—approve documents and categories, and export data
- **Knowledge.CMS.Administrator**—create, edit, or delete knowledge bases

> **Important**
>
> Only agents who have both **Knowledge.CMS.Document.Author** and **Knowledge.CMS.Category.Author** privileges can successfully import data from XML files.

To configure the appropriate privileges for an agent:

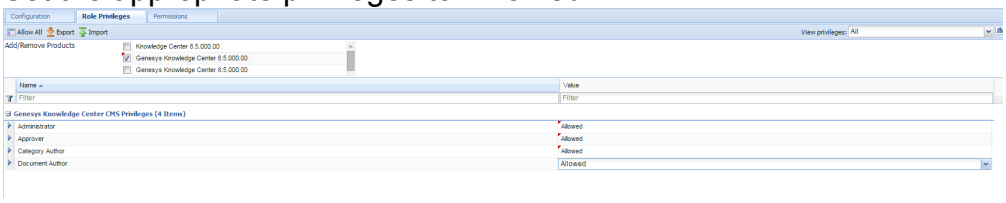
Start

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.



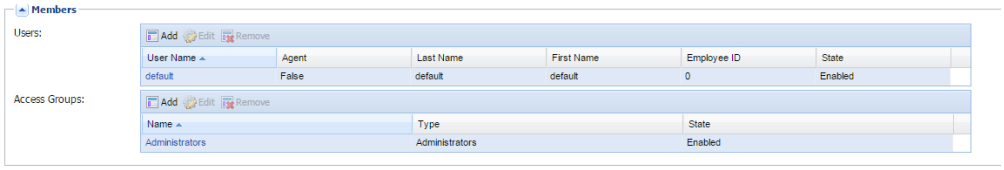
GKC CMS Access Roles

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**.



Setting GKC CMS Access Privileges

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



GKC CMS Members Section

9. Save and Close.

End

Installing and Using the Administrator Plugin

Installing the GKC Plugin for Administrator

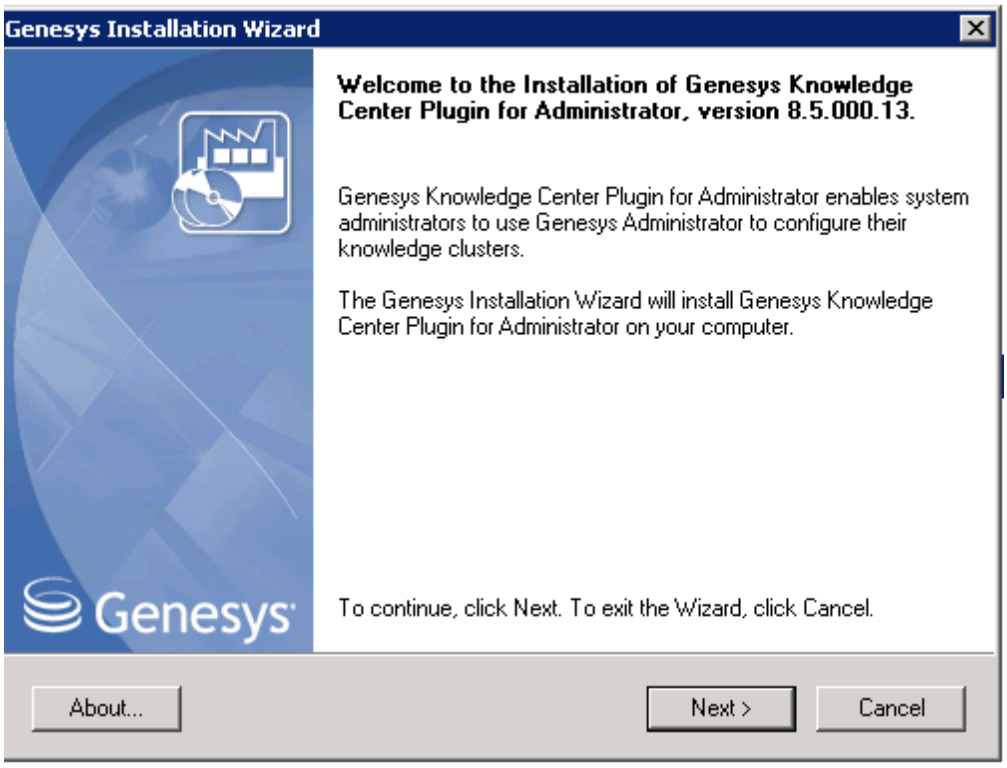
Prerequisites

- Genesys Administrator must have been installed, but should be stopped before installing the plugin
- If the Administrator Plugin was previously installed on the current host, manually remove the previous version from the */plug-ins* folder in the Genesys Administrator installation directory

Windows Installation Procedure

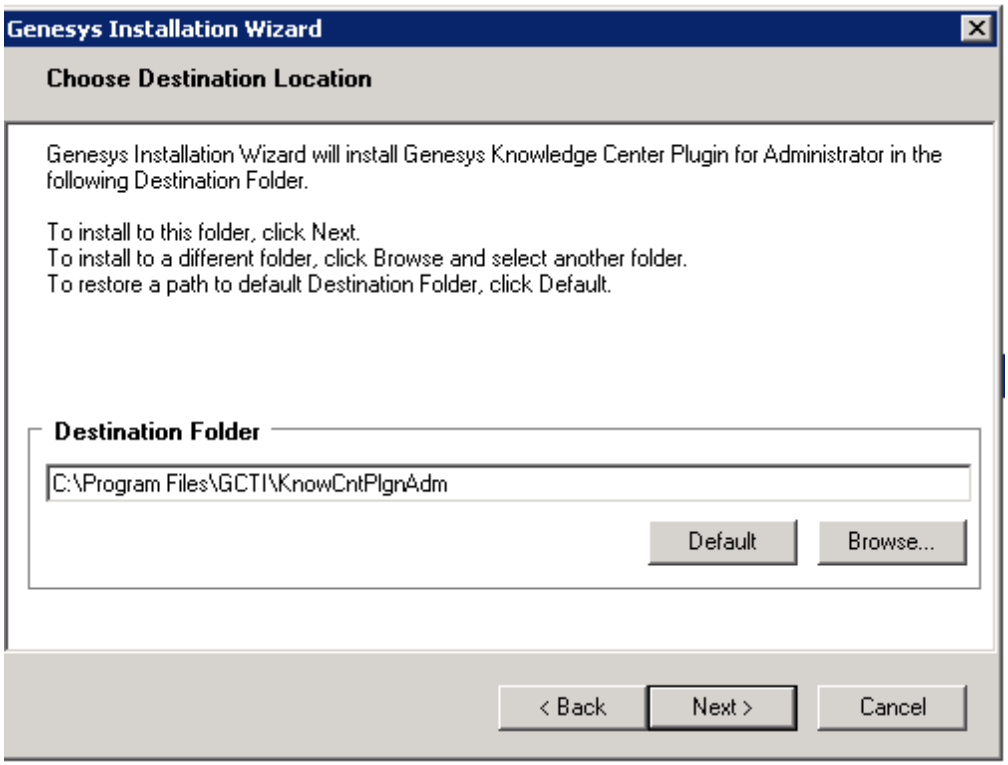
Start

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



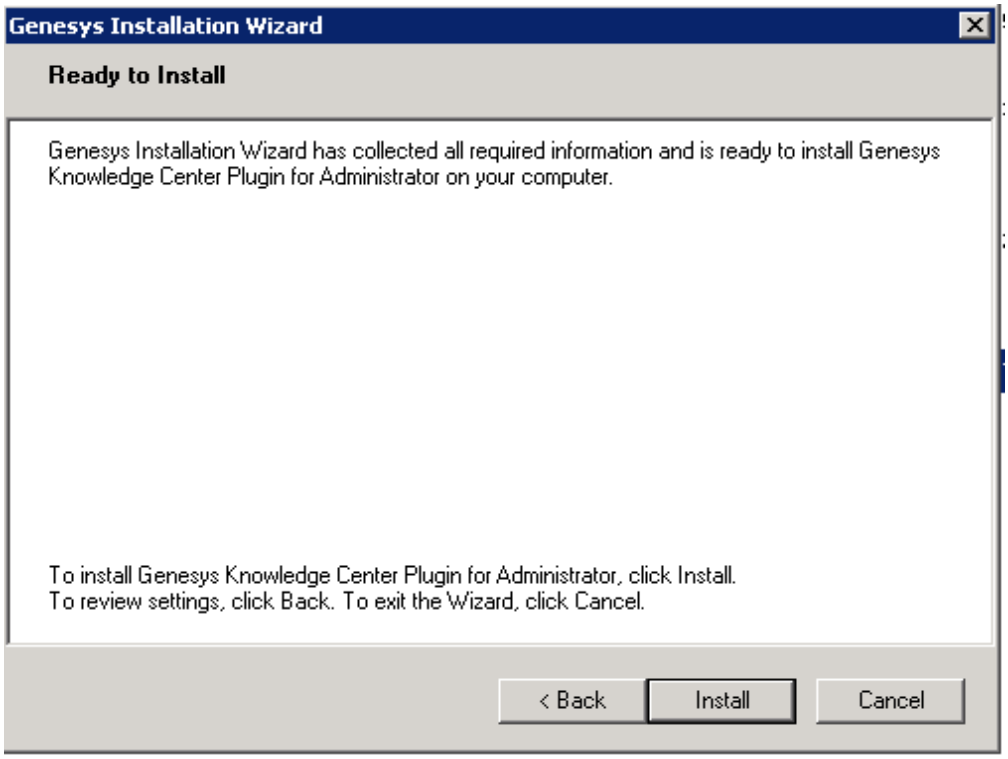
GKC Administrator Plugin Install Shield Window

2. Click **Next**. The **Choose Destination Location** screen appears.



GKC Administrator Plugin Destination Window

3. Under **Destination Folder**, keep the default value or browse to the desired installation location. Click **Next**.
4. Click **Install**. The Genesys Installation Wizard indicates it is performing the requested operation for the Backend Server. When it has finished, the **Installation Complete** screen appears.



GKC Administrator Plugin Installation Complete

5. Click **Finish** to complete your installation.
6. Inspect the directory tree of your system to make sure that the files have been installed in the location that you intended.
7. *gax-plugin-knowledge.jar* should be added as a Genesys Administrator plugin.
8. Restart Genesys Administrator.

End

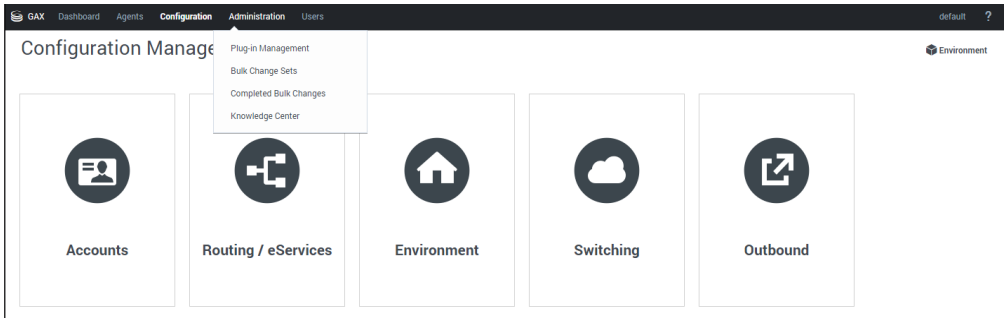
Linux Installation Procedure

Start

1. Open a terminal in the Genesys Knowledge Center Plugin for Administrator IP, and run the *install.sh* file. The Genesys Installation starts.
2. Enter full path to the GAX installation directory.
3. Enter full path to your installation directory for the plugin and confirm it.
4. If the installation is successful, the console displays the following message: Installation of Genesys Knowledge Center Plugin for Administrator, version 8.5.x has completed successfully.
5. *gax-plugin-knowledge.jar* should be added as a Genesys Administrator plugin.
6. Restart Genesys Administrator.

End

A **Knowledge Center** item should appear under the Administration menu.



Knowledge Center in Administrator Menu

> **Important**
>
> Users must have Knowledge.ADMINISTER privileges in order to use the Administrator plugin.

Managing Knowledge Bases

In order to use GKC Server you need to create at least one knowledge base in the GKC Cluster application, using the GKC Plugin for Administrator. This section describes the structure and specific options you need in order to create an index for this knowledge base in GKC Server.

Selecting the GKC Cluster Application

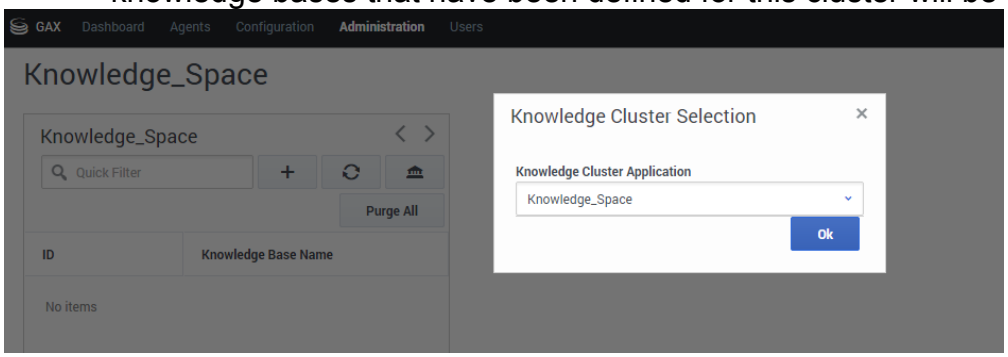
Prerequisites

- The Administrator user must have **Knowledge.ADMINISTER** privileges

Start

1. Log in to Genesys Administrator and navigate to the **Administration > Knowledge Center** menu item.

2. Using the  button, open the menu for **Select Knowledge Cluster**. Select the appropriate cluster from the drop-down and click the **Ok** button. A list of the knowledge bases that have been defined for this cluster will be displayed.



Selecting a Knowledge Cluster

End

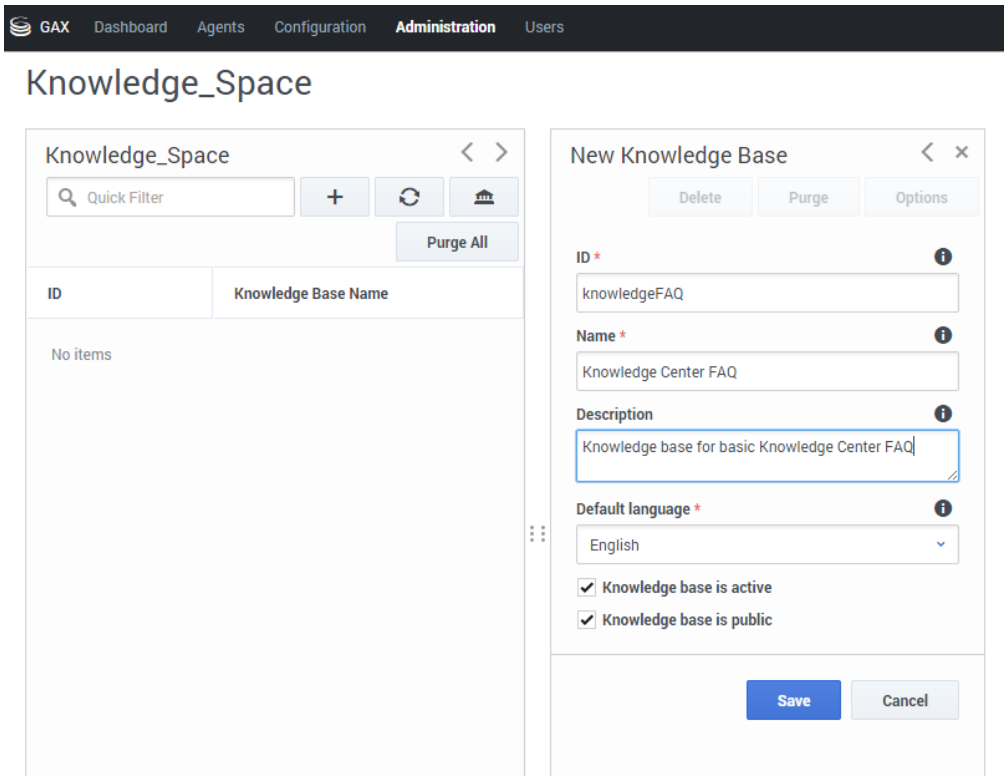
Creating a Knowledge Base

Prerequisites

- The Administrator user must have **Knowledge.ADMINISTER** privileges
- You must create and select a GKC Cluster application

Start

1. Click the **+** button. A panel with the main knowledge base parameters will be displayed. Fill in the following fields:
    - **ID**—The ID should only contain numbers, lower-case Latin letters, and underscores, with a maximum length of 50 characters. The limitation to lower-case letters is because ElasticSearch is case-insensitive and will therefore render all names as lower-case.
    - **Name**—Maximum length is characters
    - **Description**—optional
    - Select the default knowledge base language.
    - Make the knowledge base public or private. (If the knowledge base is made public, it will be visible to all users, whether or not they are authorized.)
    - Make the knowledge base active or inactive. (If the knowledge base is made inactive, the knowledge base will be hidden from active users.)



Creating a Knowledge Base

2. Click **Save**. The knowledge base will be created.

End

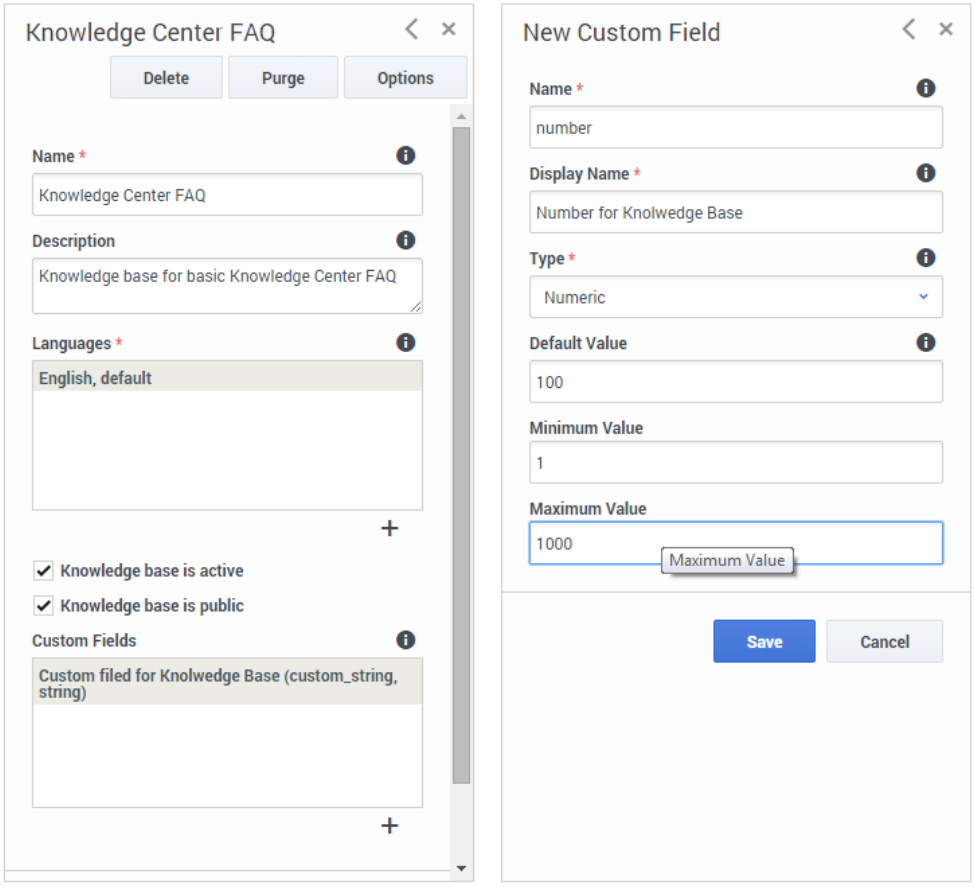
Creating Custom Fields

Prerequisites

- The Administrator user must have **Knowledge.ADMINISTER** privileges
- You must create and select a GKC Cluster application
- You must create and select a knowledge base definition

Start

1. Click the **+** sign under the **Custom Fields** section. The **New Custom Field** panel will be displayed.



Creating a Custom Field

2. To define a custom field, fill in the following information:
    - **Name**—Should consist only of numbers, Latin letters and underscores, with a maximum length of 50 characters.
    - **Display name**
    - Select the type of field
    - For **String** fields define:
        - Default value (optional)
        - If the field can be left empty, set the check box to **Allow empty**
    - For **Numeric** fields define:
        - Default value (optional)
        - Minimum value (optional)
        - Maximum value (optional)
    - For **DateTime** fields define:
        - Default value (optional)
        - Format (optional)

5. Click **Save** to save your changes.

End

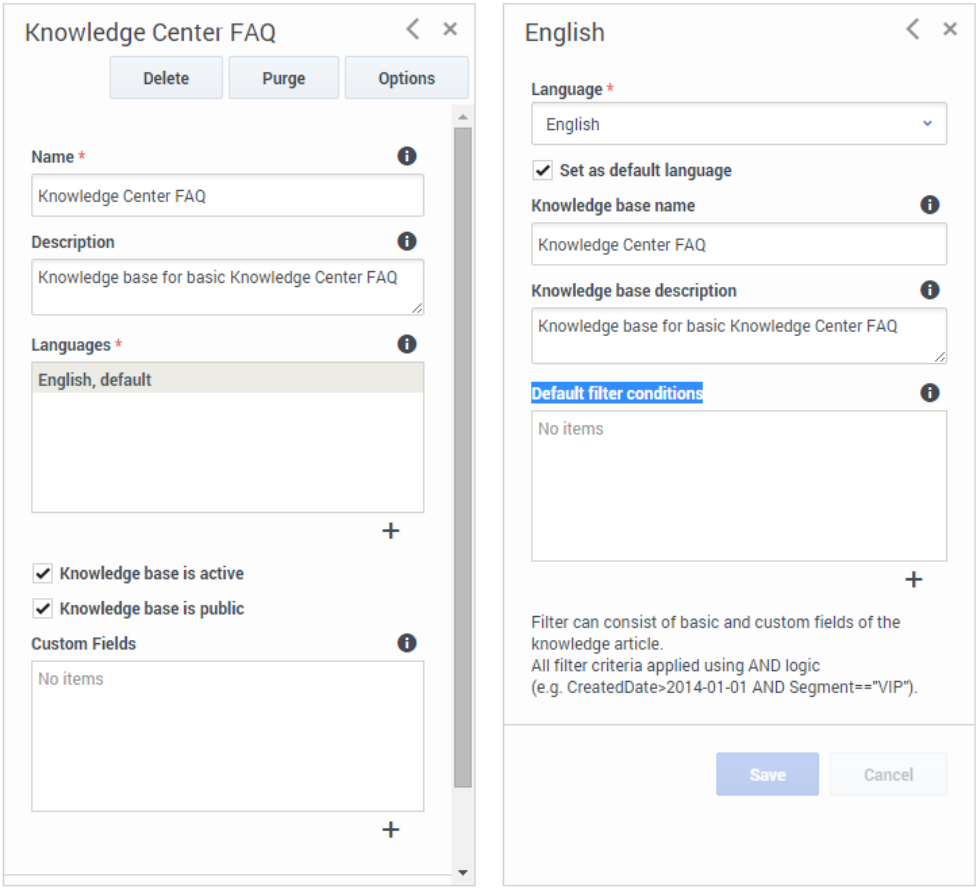
Adding Language-specific Information

Prerequisites

- The Administrator user must have **Knowledge.ADMINISTER** privileges
- You must create and select a GKC Cluster application
- You must create and select a knowledge base definition

Start

1. Click the **English, default** row in the **Languages** section. A panel with language-specific settings will be displayed.

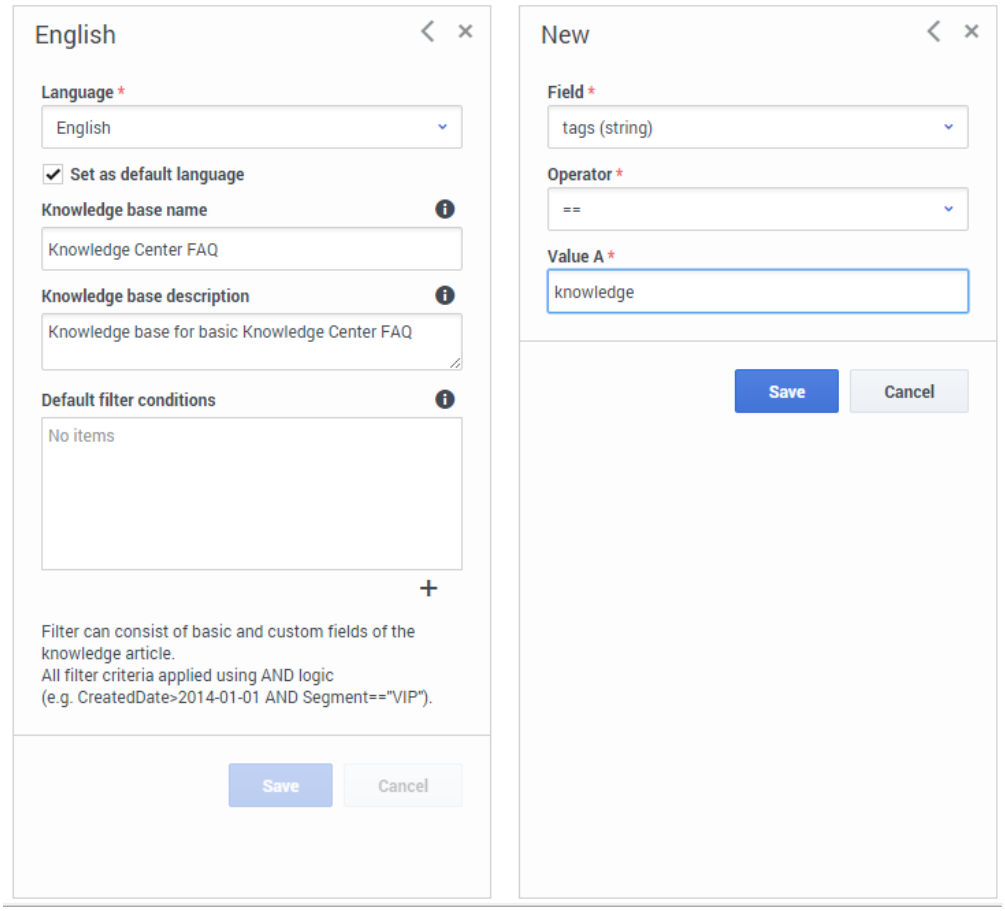


Adding Language-Specific Information

2. You can define the following parameters in this section:
    - A localized knowledge base name
    - A localized knowledge base description
    - Whether or not the selected language is the default
    - Default filter conditions
5. To create a default filter condition click on the **+** under the **Default filter conditions** section and fill in the appropriate mandatory fields:
    - Select the appropriate field (custom or basic)
    - Select a filter operator
    - Fill in the values for the filter criteria

Important

All filter criteria are applied using AND logic. For example, **CreatedDate>2014-01-01** AND **Segment=="VIP"**.



Default Filter

4. Click the **Save** button

End

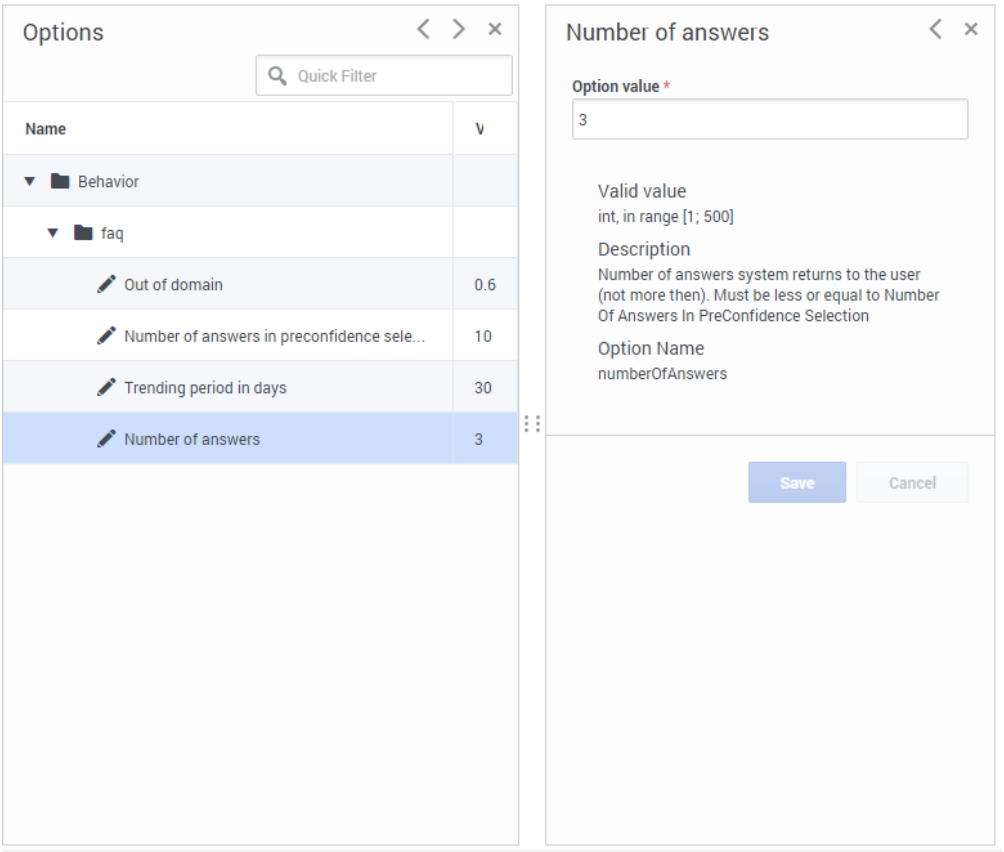
Editing Knowledge Base Options

Prerequisites

- The Administrator user must have **Knowledge.ADMINISTER** privileges
- You must create and select a GKC Cluster application
- You must create and select a knowledge base definition

Start

1. To edit the options for a particular knowledge base, click the **Options** button and then click the appropriate option to edit its value. The options are initialized with their default values.



Editing Knowledge Base Options

2. Enter the new option value and click the **Save** button.

End

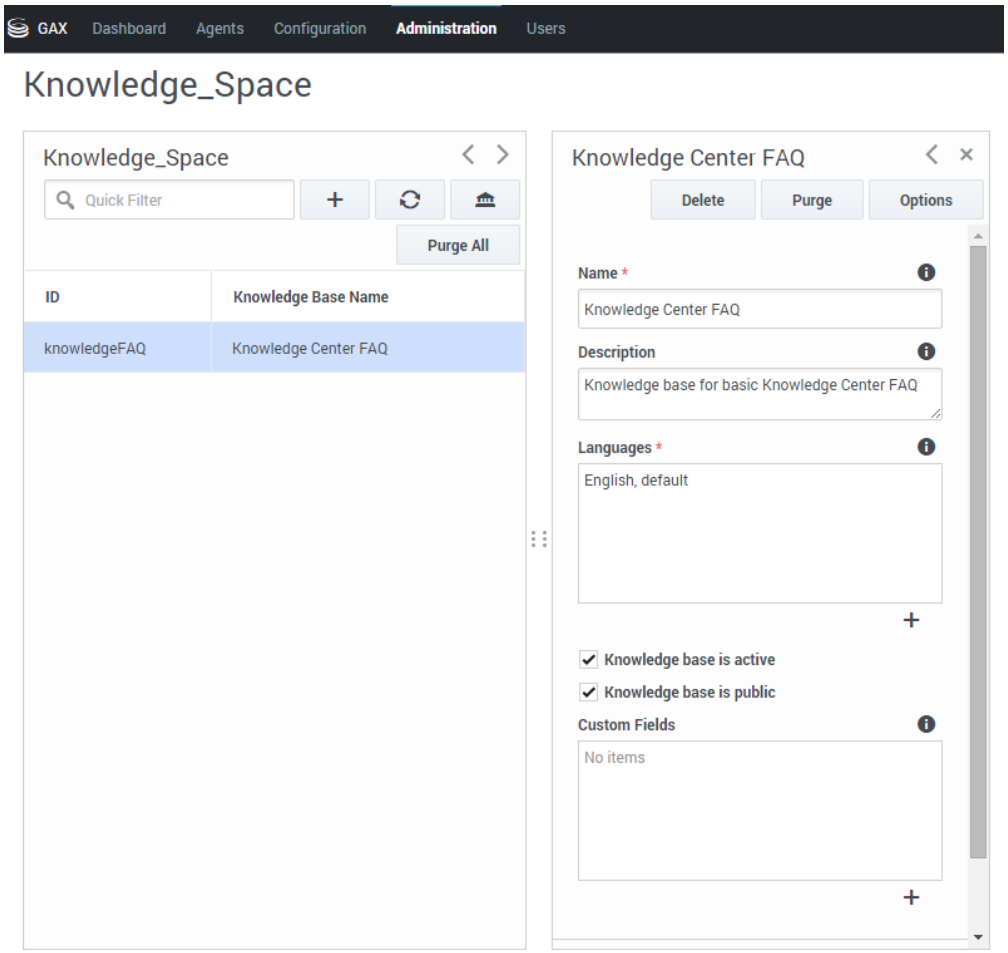
Editing a Knowledge Base Definition

Prerequisites

- The Administrator user must have **Knowledge.ADMINISTER** privileges
- You must create and select a GKC Cluster application

Start

1. Select a knowledge base from the list.



Editing Knowledge Base Definition

2. Edit the knowledge base definition and click the **Save** button.

End

Deleting a Knowledge Base Definition

Prerequisites

- The Administrator user must have **Knowledge.ADMINISTER** privileges
- You must create and select a GKC Cluster application
- You must have created a knowledge base definition

Start

1. Select a knowledge base from the list.
2. Press the **Delete** button and confirm the action.

End

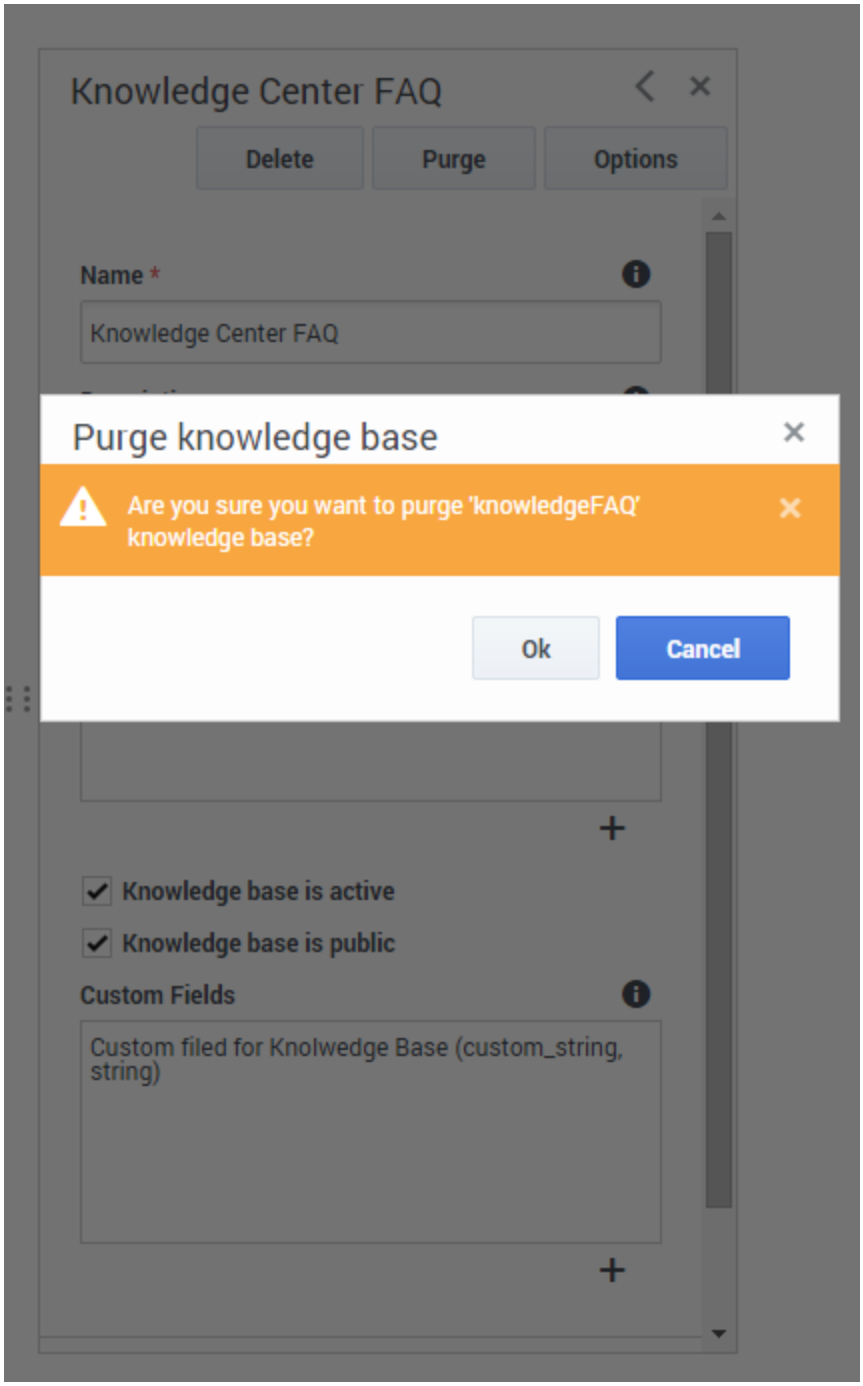
Purging Knowledge Bases

Prerequisites

- The Administrator user must have **Knowledge.ADMINISTER** privileges
- You must create and select a GKC Cluster application

Start

1. To purge a particular knowledge base, select it from the list, press the **Purge** button, and confirm the action.



Purging a Knowledge Base

2. To purge all knowledge bases, use the **Purge All** button.

End

Installing the Pulse Plugin

The Genesys Knowledge Center Plugin for Pulse provides access to GKC Server statistics such as KPI, user activity, trending topics, like and dislike trends, and activity types.

Install Genesys Knowledge Center Plugin for Pulse

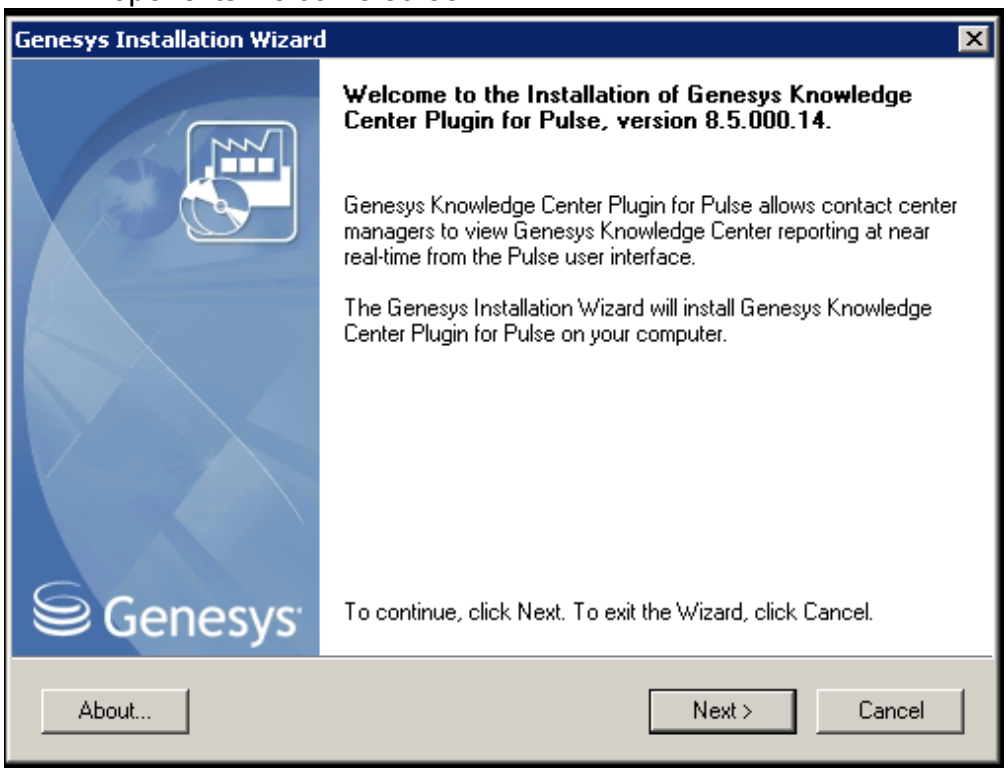
Prerequisites

- Genesys Knowledge Center Server must be installed on the host

Windows Installation Procedure

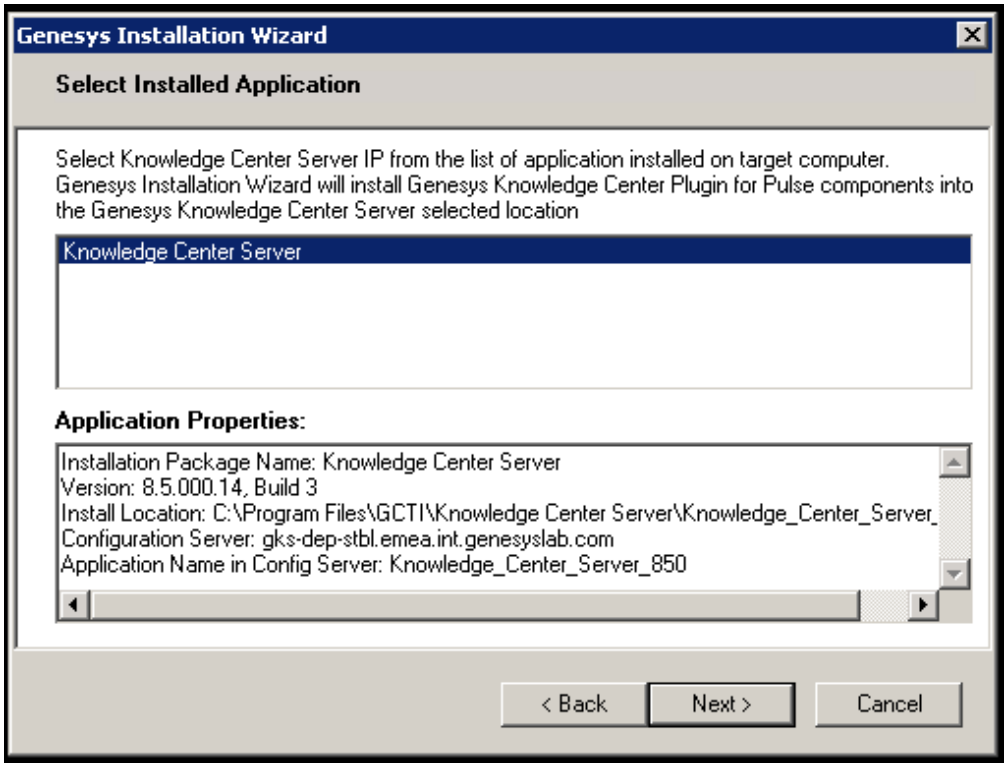
Start

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



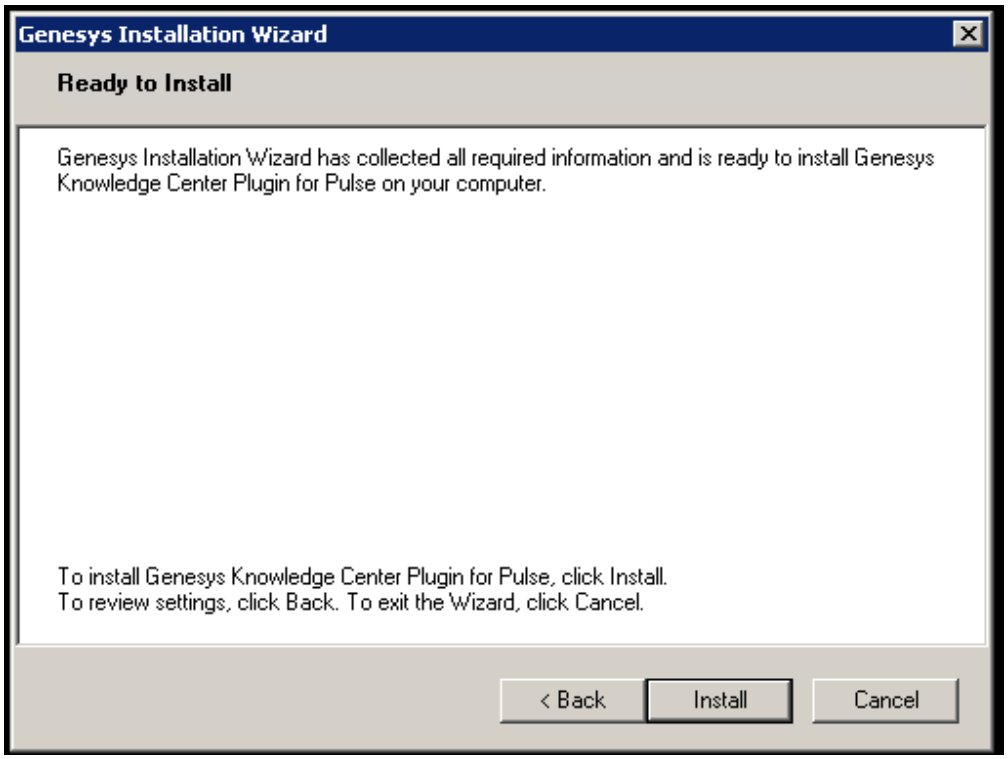
Pulse Plugin Install Shield Window

2. Click **Next**. The **Select Installed Application** screen appears.



Select Installed Application

3. Select the Knowledge Center Server 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.
4. Click **Next**. The **Ready to Install** screen appears.



Ready to Install screen

5. Click **Install**. The Genesys Installation Wizard indicates it is performing the requested operation for Backend Server. When it has finished, the **Installation Complete** screen appears.
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.
    - *GKSserverfolder\server\webapps\gkc-dashboard.war*
    - *GKSserverfolder\server\webapps\gkc-kpi.war*

End

Linux Installation Procedure

Start

1. Open a terminal in the directory for the Genesys Knowledge Center Plugin for Pulse IP.
2. Run the install.sh file. The Genesys installation starts.
3. Enter the full path to your plugin installation directory and confirm that it is correctly specified.

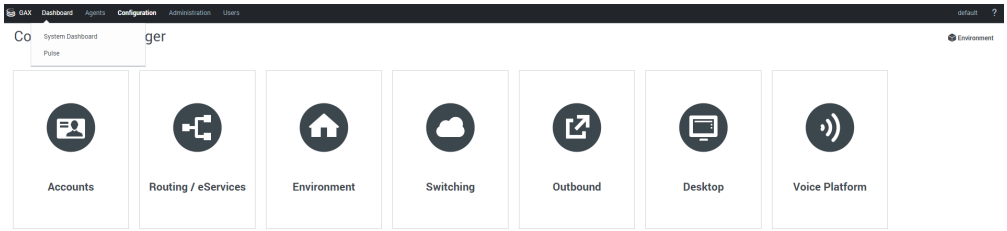
4. If the installation is successful, the console displays the following message: *Installation of Genesys Knowledge Center Plugin for Administrator, version 8.5.x has completed successfully.*
5. Inspect your system directory tree to make sure that the files have been installed in the location that you intended, as shown here:
    - *\webapps\gkc-dashboard.war*
    - *\webapps\gkc-kpi.war*

End

Configure Genesys Knowledge Center Plugin for Pulse

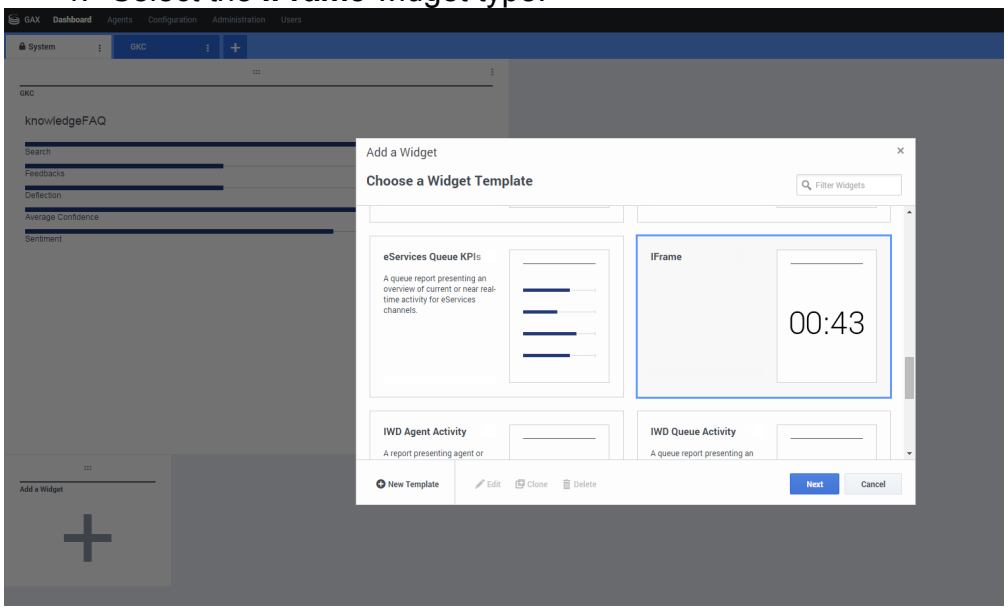
Start

1. Log into Genesys Administrator.
2. Go to **Dashboard > Pulse**.



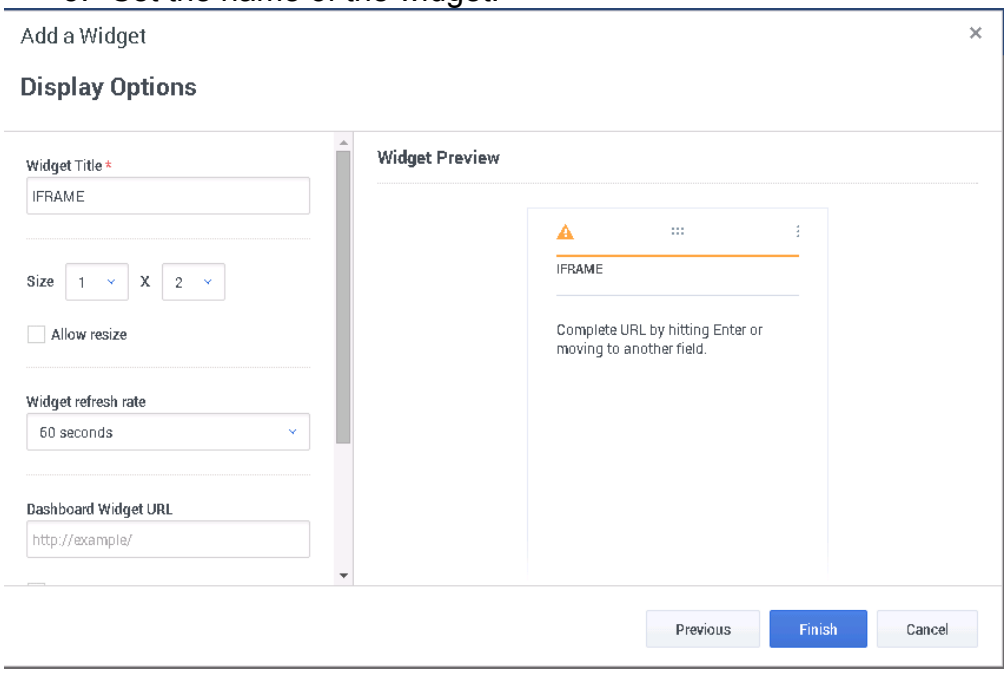
Selecting the Pulse Dashboard options in Genesys Administrator

3. Click **Add a Widget**.
4. Select the **IFrame** widget type.



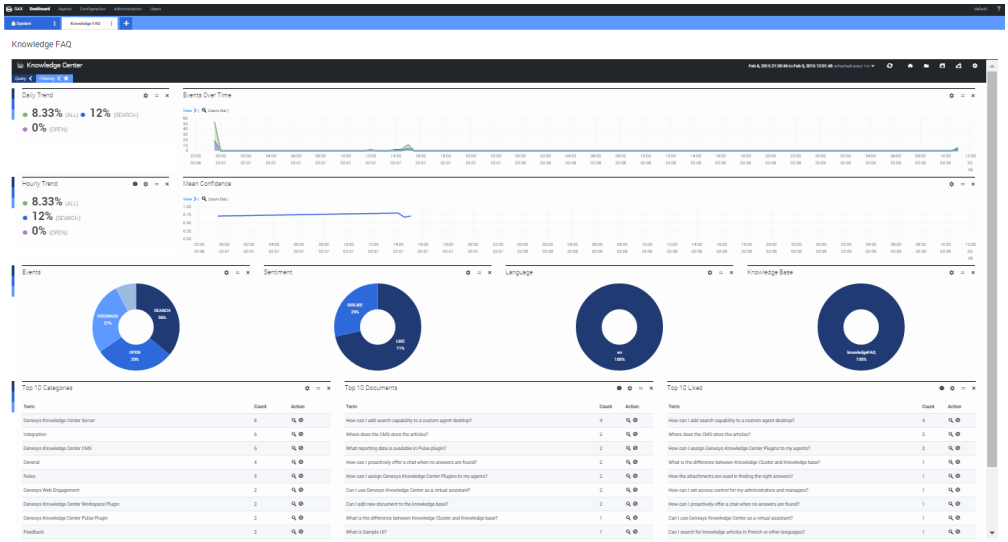
Adding a Pulse iFrame widget

5. Set the name of the widget.



Setting the Pulse widget options

6. Set the widget URL to: http://*host of GKC node with installed plugin*:*port of GKC node*/gkc-kpi/#/kb/*knowledge base name*/lang/en
7. Set the Maximized widget URL to: http://*host of GKC node with installed plugin*:*port of GKC node*/gkc-dashboard/#/dashboard/file/default.json
8. Click **Finish**.



Pulse Dashboard Widget

You have successfully added a widget for accessing GKC statistics.

End

GKC Pulse Plugin Configuration Options

You can customize the KPI widget by adding the bolded parameters to the URL:

http://*host of GKC node with installed plugin*:*port of GKC node*/gkc-kpi/#/kb/**knowledge base name**/lang/**en**?timeframe=**select timeframe**

- /kb/**knowledge base name**—Set the appropriate knowledge base name
- /lang/**en**—Choose Knowledge Base's Language representation
- timeframe=**select timeframe**—Select KPI's timeframe, for example *now-1M*

Installing the Workspace Desktop Edition Plugin

Installing the Plugin for Workspace Desktop Edition

Agents can use the GKC 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, GKC 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 following procedures:

1. Installing the Plugin for Workspace Desktop Edition
2. Configuring the WDE Application to work with the WDE Plugin
3. Providing Knowledge Center Access to Agents

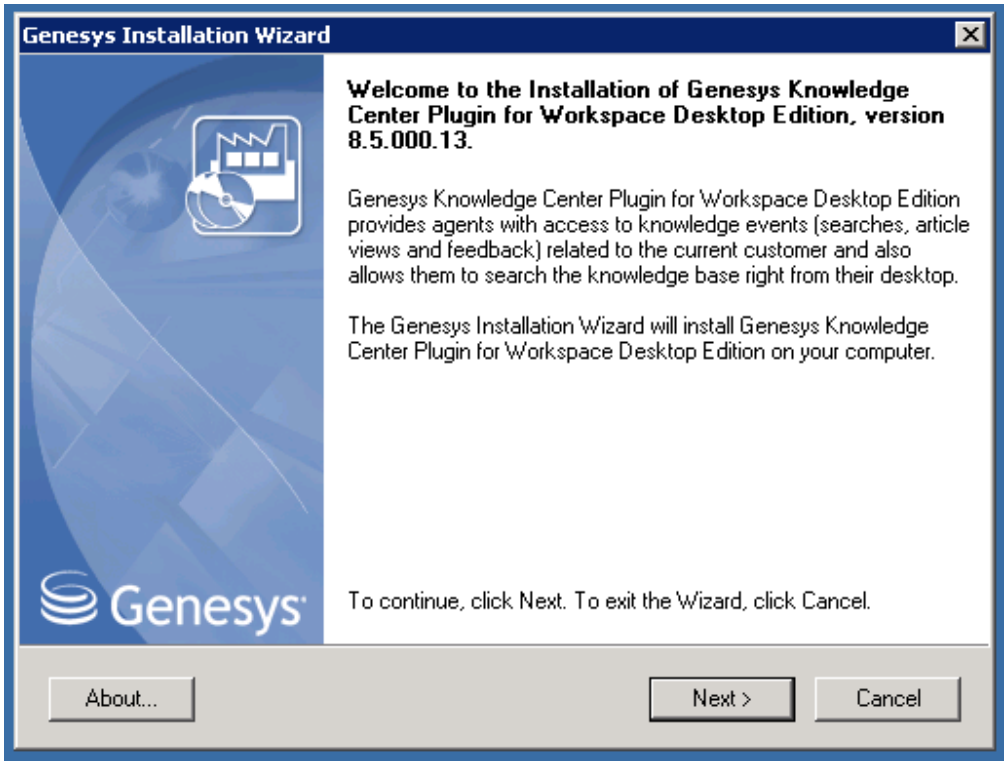
Installing the Plugin for Workspace Desktop Edition

Prerequisites

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

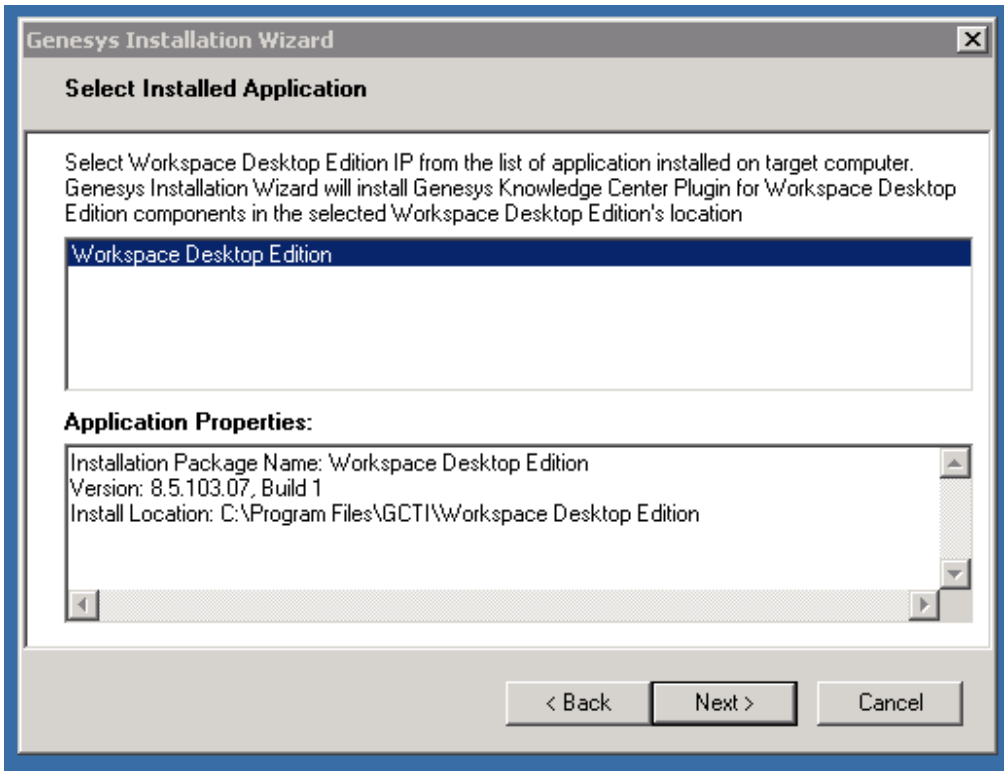
Start

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



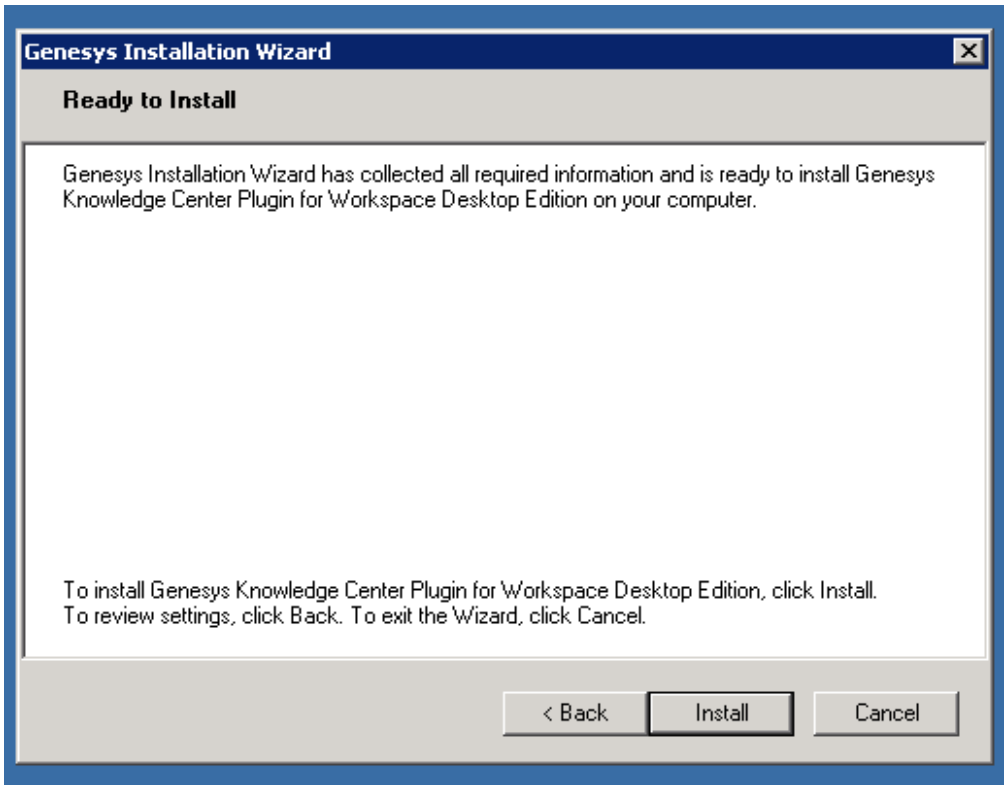
GKC WDE Plugin—Install Shield Screen

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.



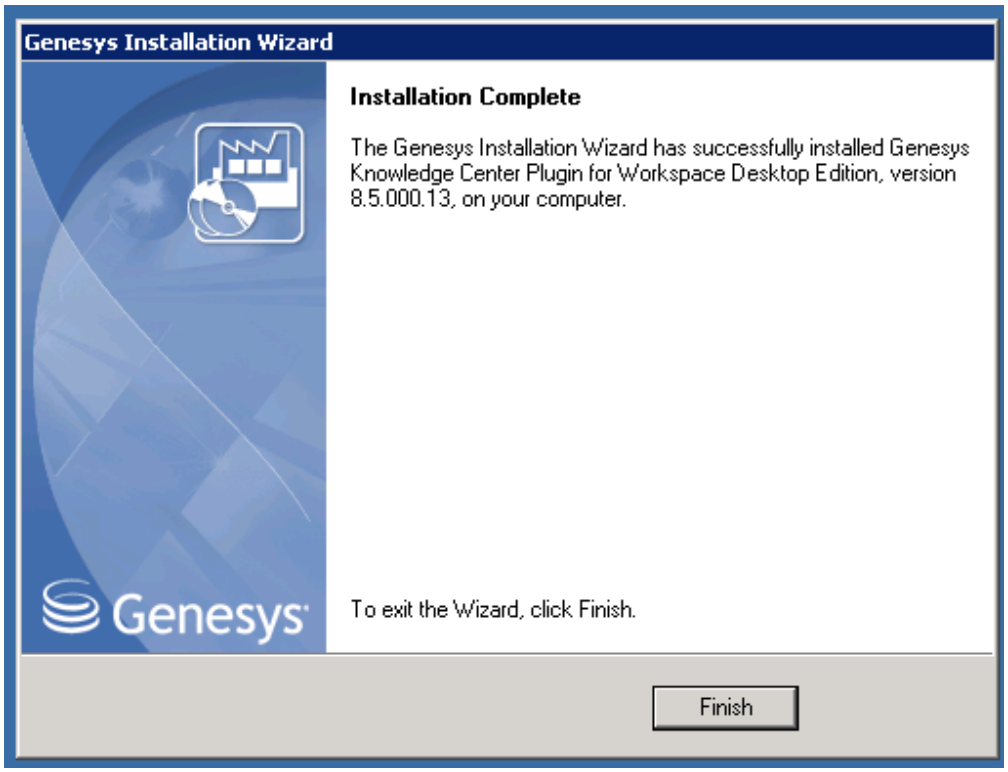
Select Installed Workspace Desktop Edition Application

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



GKC 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.



GKC WDE Plugin—Installation Complete

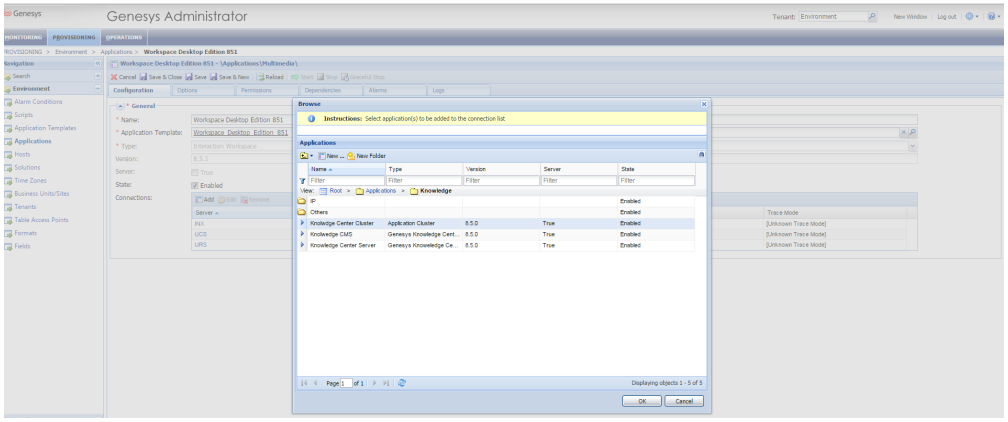
6. Click **Finish** to complete your installation.
7. Inspect the directory tree of your system to make sure that the following files have been installed in the location that you intended:
    - *GWEInstallationFolder\Genesyslab.Desktop.Modules.Knowledge.dll*
    - *GWEInstallationFolder\Genesyslab.Desktop.Modules.Knowledge.module-config*
    - *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

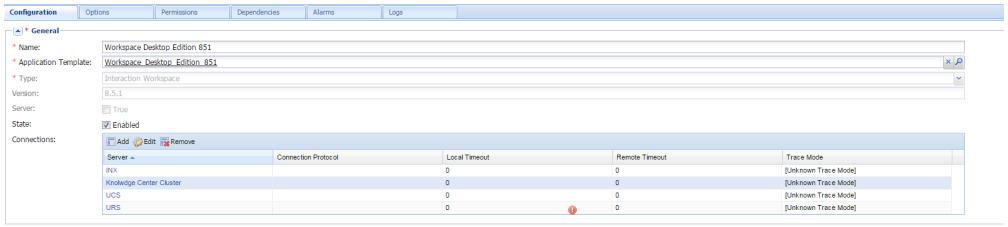
Configuring the WDE Application to work with the WDE Plugin

Add the GKC 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**.



GKC WDE Plugin—Browse for applications 1



GKC WDE Plugin—Browse for applications 2

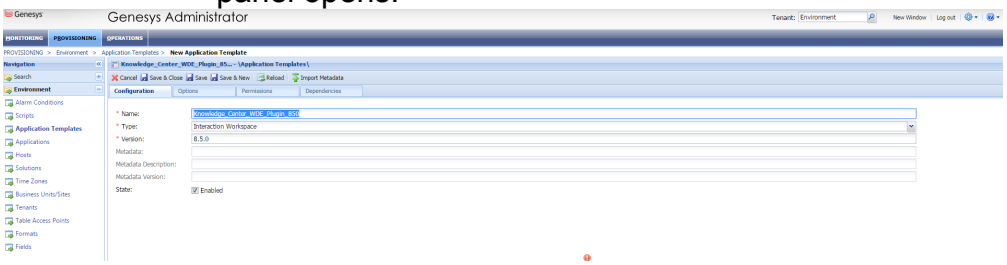
Add GKC Options to Your WDE Application

To use the GKC 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:

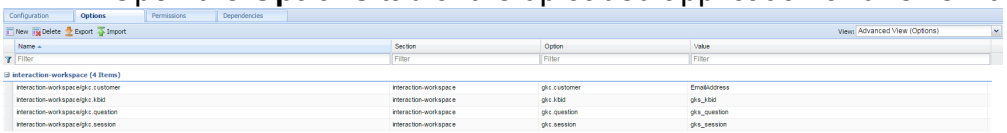
1. Open Genesys Administrator and navigate to **Provisioning > Environment > Application Templates**.
2. In the **Tasks** panel, click **Upload Template**.
3. In the *Click 'Add' and choose application template (APD) file to import* window, click **Add**.
4. Choose the application template (APD) file from the import window and click **Add**.
5. Browse to the *Knowledge_Center_WDE_Plugin_850.apd* file available in the templates directory of your installation CD. The **New Application Template** panel opens.



GKC WDE Plugin—New Application Template panel

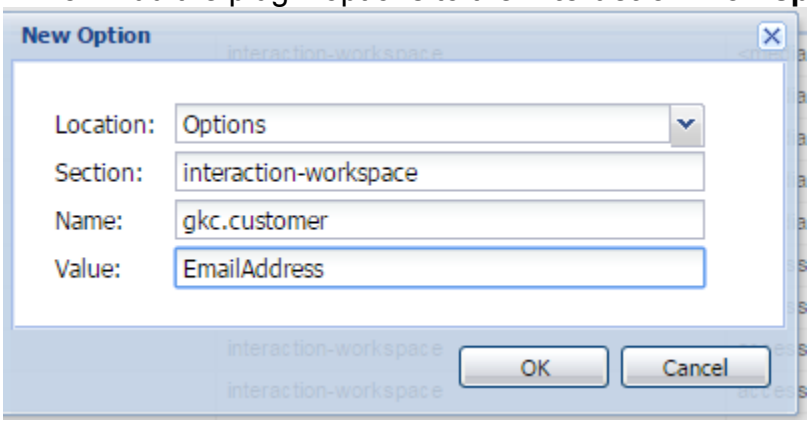
6. Click **Save and Close**

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



GKC 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.



GKC WDE Plugin—Add plugin options

End

The GKC Plugin for WDE uses the following additional options:

- **gkc.question**—This key points to the customer's question for the pre-populated search and is stored in the interaction's user data
- **gkc.kbid**—This key points to the knowledge base ID for the pre-populated search and is stored in the interaction's user data
- **gkc.customer**—This key points to the *customerId* in the interaction's user data (the default value for this key is the customer's email address)
- **gkc.session**—This key stores the session ID in the interaction's user data

Providing Knowledge Center Access to Agents

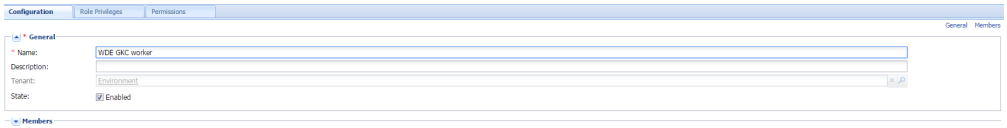
Genesys Knowledge Center supports the following privilege in order to restrict Agent access:

- **Knowledge.WORKER**—Enables access to the Genesys Knowledge Center tab in WDE

To configure the appropriate role for an agent:

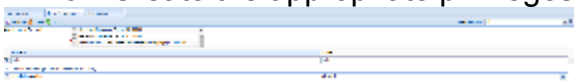
Start

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_850.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.



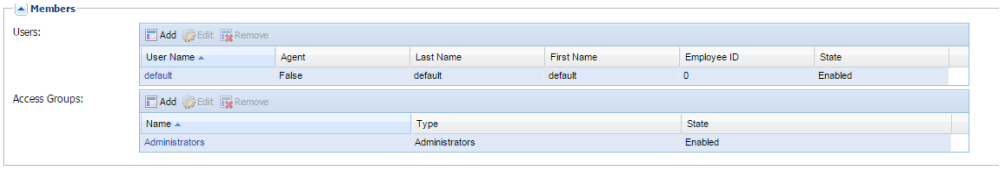
GKC WDE Plugin—Set Role Names

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



GKC WDE Plugin—Create Privileges

14. Go back to the **Configuration** tab.
15. Add the appropriate Agent or Agent Group to the **Members** section by clicking the **Add** button.



GKC WDE Plugin—Members Section

16. Save and Close.

End

Importing Data Into the Knowledge Base

You can use the Import Tool to add sample QNA data to your knowledge base. This tool is located in the *./server/tools* directory in the GKC installation folder. It comes with the following resources:

- **knowledgeFAQ.xml**—List of basic QNA data, provided with the GKC Server indexing tool
- **gks-indexer-tool.jar**—Java-based indexing tool
- **importFAQ.bat**—Simple data import script

Data Import Syntax

Use the following syntax to import data:

```
- java -jar gks-indexer-tool.jar
--host <GKC server node URL>
--file <path to XML data or folder that contains it>
--user <authorized user>
--authorization "username:password"
```

The authorization parameter is only required if you have enabled the security option for GKC Cluster.

Sample Import Script

Here is an example of what your import script might look like:

```
java -jar <Path to GKC Server>\GKC_Server\server\tools\
gks-indexer-tool.jar
--host "http://sample.com:9001/gks-server"
--file "<Path to GKC
Server>\GKC_Server\server\tools\knowledgeFAQ.xml"
--user "gkc_admin"
```

If it works, this script will import sample QNA data into the knowledge base.

Sample QNA Data

Here is an example of the data stored in the XML file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<documents kbsId="knowledgeFAQ" lang="en">
    <document>
        <question>What Is Knowledge Center?</question>
        <answer>The Genesys Knowledge Center ultimate goal is to
convert
your knowledge into the answers on the question your clients or
agents have.
It delivers set of the component for administration, authoring and
using the
knowledge. The heart of the system is the Knowledge Center Server
that
aimed to find the best answer on the question you have
asked.</answer>
        <categories>
            <category>
                <name>General</name>
            </category>
        </categories>
    </document>
</documents>
```

Sizing

> **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 following estimates may give you some basic ideas on how to size your deployment.

Hardware Sizing Information

Genesys Knowledge Center Server

	Minimal	Recommended
CPU	Multicore (8+)	
RAM	8GB	16GB
Disk Space	100GB or more, depending on the number of knowledge bases and the depth of the history	

Genesys Knowledge Center CMS

	Minimal	Recommended
CPU	Multicore (8+)	
RAM	8GB	16GB
Disk Space	10GB or more, depending on the number of knowledge bases	

Recommended Software Configuration

- **OS version**—Linux 6 x64 or higher, Windows Server 2008R2 x64 or higher
- **Java version**—Java version 1.7 or higher, 64-Bit Server VM

Java Options	Initial heap size (Xms)	Maximum heap size (Xmx)
Genesys Knowledge Center Server (without archiving)	4096m	4096m
Genesys Knowledge Center Server (with archiving)	4096m	8192m
Genesys Knowledge Center CMS	1024m	1024m