

Altair Knowledge Hub

Linux Single Server

Installation Guide

Version 2.3



Altair Engineering, Inc. makes no representation or warranties with respect to the contents of this manual or the associated software and especially disclaims any implied warranties of merchantability or fitness for any particular purpose. Further, Altair Engineering, Inc. reserves the right to revise this publication and make changes from time to time to its contents without obligation to notify anyone of such revisions or changes.

Altair Knowledge Hub Single Server software is offered and is to be used in accordance with a SOFTWARE LICENSE AND MAINTENANCE AGREEMENT. This agreement stipulates that this software be used only in the computer system designated in that agreement. The agreement further stipulates that the customer shall not copy or alter, or permit others to copy or alter, the software or related materials in whole or in part, in any media for any purpose, except to make an archive (back-up) copy or to make a copy as an essential step in the use of the software with the customer's computer.

Altair Engineering, Inc. hereby grants the buyer the right to reprint this documentation for internal uses only. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, for any other purposes, without the prior written permission of Altair Engineering, Inc.

Altair Knowledge Hub Single Server v2.3 Installation Guide

Copyright © 2019 by Altair Engineering, Inc.

All rights reserved. Printed in the U.S.A.

Unpublished - Rights reserved under the copyright law of the United States.

Altair Knowledge Hub Single Server is a trademark of Altair Engineering, Inc. Other products mentioned herein may be trademarks or registered trademarks of their respective owners in the United States or other countries.

For U.S. Government End Users, the software is a "Commercial Item(s)," as that term is defined at 48 C.F.R. Section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. Section 12.212 or 48 C.F.R. Section 227.7202, as applicable. Consistent with 48 C.F.R. Section 12.212 or 48 C.F.R. Sections 227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the Altair Software License and Maintenance Agreement.

SALES INFORMATION

US: + 1.800.445.3311

International: + 1.978.441.2200

Sales Email

US: sales@datawatch.com

Europe: sales_euro@datawatch.com

Asia Pacific: sales_apac@datawatch.com

SUPPORT CONTACT INFORMATION

Customer Portal:

<https://support.datawatch.com>

Email: support@datawatch.com

US: +1 800.988.4739

International: +1 978.275.8350

Table of Contents

Altair Knowledge Hub Single Server Installation	1
Pre-Installation Steps	1
Pre-Installation Configuration	2
Installation.....	3
Post-Installation Steps.....	4
Checking the Installation Status	4
Installing JDBC Drivers	5
Logging	5
Configuring the Logging Module.....	6
Configuring the Logging Driver	6
Installing the Logging Module.....	7
Deleting the Logging module.....	7
Web Application Logs	7
Elasticsearch Log Import and Export	8
Updating Knowledge Hub.....	9
Updating the Knowledge Hub Application	9
Updating the Licensing Type of the Application	9
Deleting the Knowledge Single Server Application	9
Backing Up and Restoring the Application	11
Knowledge Hub Single Server Properties.....	13
Core-API.Properties.....	13
Data-Engine-API.Properties.....	15
Social-API.Properties.....	18
Setting Up LDAP/SSO Authentication	19
Volume Configuration	27
Utils Configuration	28
Memory Configuration	29
Troubleshooting.....	30
Aggregating Status information	30
Cleaning the server application.....	30

Altair Knowledge Hub Single Server Installation

This installation guide describes how to install and deploy the Altair Knowledge Hub (formerly Datawatch Monarch Swarm) Linux Single Server application.

Note that prior to installing the application, the following must be ensured:

- ❑ Swap needs to be turned off and the swap partition commented out of `/etc/fstab`
- ❑ The user you are installing with needs to be in the `admin/sudo` group
- ❑ The machine should have a static IP and an entry in `/etc/hosts`
- ❑ All `.sh` files must have execute permissions. To update permissions, use the command:

```
chmod +x setup-volumes.sh
```

Note also that an internet connection is required to install the application. Red Hat Enterprise Linux is not officially supported in the current version of Knowledge Hub because it does not support the community edition docker engine.

We strongly advise that all procedures to install Knowledge Hub Linux Single Server be completed by a knowledgeable system administrator.

Pre-Installation Steps

1. Download the installer from the link provided to you by Altair. This installer will come in a zipped file.
2. Unzip the folder and place its contents in a temp folder that you can easily access.

The following subfolders should be included in the zipped folder.

- `\admin`
 - `\bin`
 - `\knowledgehub`
 - `\logging`
3. If you intend to apply file licensing, ensure that you have a license file. The license file should be provided to you by Altair. License server information may be obtained from your system administrator.

If you intend to apply Hyper Works Units licensing, ensure that you have the correct license server port and license server port.

4. Download the necessary libraries from the link provided to you by Altair and then copy them to `\bin\utils\libs`.

Pre-Installation Configuration

The following configurations must be implemented prior to installing Knowledge Hub.

1. Edit `./knowledgehub/user-config/env.properties`. Knowledge Hub has two preset configurations: 4x16 (4-core CPU, 16 Gb memory) or 8x32 (8-core CPU, 32 Gb memory). For actual deployments, Knowledge Hub Single Server requires a minimum configuration of 8x32, so this configuration must be specified. For testing purposes, the configuration 4x16 may be sufficient.

```
SERVER_ENV=8x32
```

2. Specify the licensing type.

- If you are using **File Licensing**, place the license file `license.lic` in `./knowledgehub/user-config/` folder.
- If you are using HWU Licensing, set the following property in the `./knowledgehub/user-config/core-api.properties` file.

```
APPLICATION_LICENSE_REMOTE_HOST=<license server  
port>@<license server host>
```

(e.g., **APPLICATION_LICENSE_REMOTE_HOST=6200@10.65.245.20**)

Note that only one licensing system can be used at any one time.

3. Copy the Nginx certificates `tls.key` and `tls.crt` to the `./knowledgehub/user-config/` and `logging/user-config` folders. While your digital certificate and key may have different file names, we suggest renaming to `tls.cert` and `tls.key` to ensure smooth installation.
4. **(Optional)** Configure the necessary Knowledge Hub Single Server settings in the following files:
 - `core-api.properties` - Core configuration file
 - `data-engine-api.properties` - Data engine configuration file
 - `social-api.properties` - Social and machine learning configuration file
 - `tableau-writer-api.properties` - Tableau writer configuration file
 - `krb5.conf` - Kerberos configuration (for SSO)

For example, you can set the property `APPLICATION_SERVER_INTERNET_ADDRESS`, which is used to establish OAuth2 connections, such as Google Analytics, in `core-api.properties` and `data-engine-api.properties`.

NOTE: If you are deploying Knowledge Hub Single Server Edition for the first time, **DO NOT MODIFY** following properties:

- `APPLICATION_SECURITY_CIPHER_KEYPAIR_PRIVATEKEY`,
`APPLICATION_SECURITY_CIPHER_KEYPAIR_PUBLICKEY` – In `core-api.properties` and `data-engine-api.properties`
- `APPLICATION_SECURITY_AUTHENTICATION_XAUTH_SECRET` – In `core-api.properties`, `data-engine-api.properties`, `social-api.properties`, and `tableau-writer-api.properties`

These properties will be updated in the config files during execution of the `linux-4-setup-single-server.sh` script.

5. **(Optional)** To configure custom volume locations, run the script `./setup-volumes.sh` in `./bin/Utils`. Set `ROOT_FOLDER` in the script file (by default, `ROOT_FOLDER=/tmp`) and update `LIBS`, `FILE_LIBRARY`, `META_DB_DATA`, `SOCIAL_DB_DATA`, and `DATA_ENGINE_DB_DATA` if needed. The root folder stores the Knowledge Hub Data.

This step should be done before executing `./linux-4-setup-single-server.sh`.

6. Open the following ports:
 - **80, 443** – Knowledge Hub Single Server application (8080: http; 8443: https)
 - **9000** - Docker Swarm administration console, Portainer
 - **5601** - Logging application, Kibana UI

Installation

Unless otherwise indicated, the following scripts must be run from the `./bin/` directory to install Knowledge Hub:

1. Run `./linux-0-install-docker.sh` to install Docker.
2. After running these scripts, log out and then log back into the server to re-evaluate your group membership and use Docker properly.
3. Run `./linux-1-configure-docker.sh` to setup Docker Swarm.
4. Run `./linux-2-setup-admin.sh` to install the Docker Swarm admin tool [Portainer](#).
5. Run `./linux-3-setup-logging.sh` to install the logging manager, ELK Stack.
6. Run `setup-volumes.sh` from the `/utils` folder.

7. Run `./linux-4-setup-single-server.sh` to install the Knowledge Hub Single Server application
8. Upload the libraries to the server using the steps outlined [here](#).

Post-Installation Steps

CHECKING THE INSTALLATION STATUS

- ❑ To check the status of installation, run `docker stack ps <knowledgehub single server stack name>` (e.g., `docker stack ps knowledgehub`) from the `/bin` folder. This command displays all of the Knowledge Hub containers installed and their status.
- ❑ To check whether services are running correctly, run `docker stack services <knowledgehub single server stack name>` (e.g., `docker stack services knowledgehub`) from the `/bin` folder.
- ❑ Wait several minutes (e.g., 10 minutes) before launching the Knowledge Hub application in your browser. After the last script is executed, a number of other scripts are still being executed in the background. A "Bad Gateway 502" error may be returned if you access the URL for the application before these background scripts are completed.

Once installation is complete, the following URLs may be opened in your browser:

- ❑ **`https://<server url>`** – Knowledge Hub Single server application
- ❑ **`https://<server url>:5601`** – Logging application, Kibana UI
- ❑ **`http://<server url>:9000`** – Docker Swarm admin

Note: When running the Portainer application for the first time, set username/password and on next screen choose ``Local`` and ``Connect``.

INSTALLING JDBC DRIVERS

To create connections to third-party applications such as Google BigQuery, SQL Server, and Amazon Redshift, the appropriate drivers must be obtained and uploaded to the `/libs` folder.

Steps:

1. Download the Altair Knowledge Hub Linux (JDBC) drivers from the link provided to you by Altair. The drivers will come in a zipped file.
2. Unzip the file and place its contents in `./bin/utils/libs`.
3. Run the script `./bin/utils/linux-config.sh` and then choose option 3.
4. Restart the Knowledge Hub services by running the script `./bin/utils/linux-config.sh` and then choose option 9.

Users seeking to create custom connections using other drivers (i.e., those not currently included in the set of drivers provided by Altair) in Knowledge Hub should follow the steps above to do so. Note that the JDBC versions of these drivers must be used.

Logging

ELK Stack is used to aggregate and visualize logs.

- ❑ [Kibana](#) is a tool for visualizing log data
- ❑ [ElasticSearch](#) is a search and analytics data engine
- ❑ [Fluentd](#) is a data collector for unified logging layers

To use Kibana, you must define the Knowledge Hub index pattern `fluentd-*`, which is available by default. This configuration is described in the documentation [Defining Your Index Patterns](#). After configuring the Knowledge Hub pattern, you can work with Knowledge Hub Single Server logs on the [Discover page](#).

By default, all logs (time and source) from the whole cluster (from all namespaces) from the last 15 minutes are displayed. You can [filter logs by date or any available field](#) to view them more conveniently and add other log information if you wish. You can view detailed information for all logs in [Document data view](#).

CONFIGURING THE LOGGING MODULE

The following steps must be accomplished to configure the logging module.

- ❑ Edit basic authentication credentials in `./logging/user-config/nginx_htpasswd` (default value is `logs@logs`)
- ❑ Copy the Nginx certificates `tls.key` and `tls.crt` to `./logging/user-config/`
- ❑ Review/edit the curator job configuration in `./logging/user-config/curator_action.yml`
- ❑ To change scheduling for curator actions, update the cron expression in `CURATOR_CRON` in the `./logging/docker-compose.yml` curator service environment (e.g., `CURATOR_CRON: "*/5 * * * *" - job is run every 5th minute)`

Note that:

- ❑ Default credentials (username/password) can be changed by application administrators in the config file.
- ❑ The default dashboard is by Metricbeats.
- ❑ Metrics for the System, File system, Docker Swarm, and PostgreSQL databases are available.

CONFIGURING THE LOGGING DRIVER

Knowledge Hub Single Server support two log drivers: `fluentd` and `json-file`. By default, `fluentd` is used. To switch to **json-file**:

- ❑ Set the property `LOGGING_DRIVER=json-file` in `./knowledgehub/docker.properties`
- ❑ Set `LOGGING_LOGSTASH_STDOUT=false` in
 - `./knowledgehub/user-config/core-api.properties`
 - `./knowledgehub/user-config/data-engine-api.properties`
 - `./knowledgehub/user-config/social-api.properties`
 - `./knowledgehub/user-config/tableau-writer-api.properties`

Additional Information

[Configure Logging Drivers | Docker Documentation](#)

INSTALLING THE LOGGING MODULE

Execute the following in a terminal from `./bin/` directory to install the logging manager, ELK Stack:

```
./linux-3-setup-logging.sh
```

The logging module can be accessed through **https://<server url>:5601**

DELETING THE LOGGING MODULE

To delete the logging module, run:

```
docker stack rm logs
```

To delete logging data, run:

```
docker volume rm logs_esdata
```

WEB APPLICATION LOGS

You can view logs from any component of Knowledge Hub Single Server. To do so, add the `LOGGING_LOGSTASH_STDOUT` property to the config file of this component and then, in Kibana, filter logs according to the required component's name.

Kibana also supports the import of pre-defined objects, such as Dashboards, Searches, and Visualization. These objects can be imported as JSON files. To make them part of your Kibana dashboard, perform the following steps:

1. Open the Kibana URL.
2. Click the **Management** tab at the left-hand portion of the screen.
3. Click the **Saved Objects** link.
4. Click the **Import** button.
5. In the opened window, select the JSON file of your object and then click **Open**.
6. Click the **Yes, overwrite all objects** button in the popup that displays.

Additional Information

[Kibana User Guide](#).

Elasticsearch Log Import and Export

Knowledge Hub Single Server supports the export and import of logs stored in Elasticsearch:

To export logs, run the following script from `./bin/utils/`:

```
./elastic-export.sh
```

This command supports the following arguments:

- ❑ `--from <date>` - date to start export from in ISO format. Default yesterday. Example 2019-01-01
- ❑ `--to <date>` - date to export to in ISO format. Default today's end of day. Example 2019-12-31
- ❑ `--elastic <elastic_url>` - Elasticsearch URL (default, `http://127.0.0.1:9200`)
- ❑ `--dir <output directory>` - Directory to save exported file. Default to export sub directory

The resulting file will be named: `elastic-export-<datetime>.json.gz`

To import logs, run the following script from `./bin/utils/`:

```
./elastic-import.sh --file <file name>
```

The command supports the following arguments:

- ❑ `--file <input_file>` - File to use as input for import. Should be in plain `.gz` format. Required
- ❑ `--esprefix <esprefix>` - Name to use as index prefix for imported file
- ❑ `--elastic <elastic_url>` - Elasticsearch URL (default, `http://127.0.0.1:9200`)

Updating Knowledge Hub

UPDATING THE KNOWLEDGE HUB APPLICATION

The following steps are used to update an existing Knowledge Hub Single Server application to a newer version.

Steps:

1. Download and unzip a new Single Server Knowledge Hub archive.
2. Merge the license file (if any), certificate files (tls.crt, tls.key, knhub.key), and updated properties from the config files (core-api.properties, data-engine-api.properties, social-api.properties, tableau-writer-api.properties, krb5.conf, secrets.properties) to the new installer.
3. Run ./linux-4-setup-single-server.sh from the /bin directory.

UPDATING THE LICENSING TYPE OF THE APPLICATION

You can switch to HWU licensing from a file license when updating an existing Knowledge Hub application. To do so, open the `knowledgehub/user-config/core-api.properties` file and then set the property `APPLICATION_LICENSE_REMOTE_HOST` to '`<license server port>@<license server host>`' (e.g., `APPLICATION_LICENSE_REMOTE_HOST=6200@10.65.245.20`) and then run the command `linux-4-setup-single-server.sh` from the `bin/` directory.

Note that only one licensing system can be implemented at any one time.

DELETING THE KNOWLEDGE SINGLE SERVER APPLICATION

- To delete the Knowledge Hub Single Server application, run:

```
docker stack rm <knowledgehub single server stack name>
```

- ❑ To delete the Docker Swarm server, run:

```
docker swarm leave --force
```

Note: If you cannot download Docker images, run `docker logout` and `./linux-1-configure-docker.sh`.

Backing Up and Restoring the Application

Knowledge Hub Single Server supports the backup and restoration of the following components.

- ❑ social-db – the Cassandra databases
- ❑ meta-db – the PostgreSQL databases
- ❑ file-system – the file-libraries and libs docker volumes

- ❑ To backup Knowledge Hub Single Server, run the following command from `./bin/utils/`.

```
./linux-backup.sh
```

The components will be backed up in `./bin/utils/backup/<date_time>` (e.g.: `./bin/utils/backup/2019-03-06_07-48-51`).

After successful backup, you can find the following files in the backup folder: `dataengineapi_db.gz`, `newserver_db.gz`, `fs-file_library.tar`, `fs-libs.tar`, `newserver_keyspace.tar.gz`, and `datawatch_keyspace.tar.gz`

- ❑ To restore Knowledge Hub, run the following command from `./bin/utils/`:

```
# stop services
./linux-config.sh # option 8
# restore backup
./linux-restore.sh <date_time>
# start services
./linux-config.sh # option 7
```

where `<date_time>` - backup folder name from `./bin/utils/backup/` (e.g., `./linux-restore.sh 2019-03-06_07-48-51`)

Note: Cassandra backups do not allow restoration on empty volumes when migration is not preformed.

The following workflow is recommended:

1. Delete existing installation
2. Delete volumes
3. Perform new Installation
4. Restore backup

Knowledge Hub Single Server

Properties

Use the following config files to configure various Knowledge Hub Single Server properties:

- ❑ `core-api.properties`
- ❑ `data-engine-api.properties`
- ❑ `social-api.properties`
- ❑ `tableau-writer-api.properties`

Note: Key properties should be in upper case and use '_' instead of '.' and '-' (e.g., `spring.data.cassandra.enabled` should be `SPRING_DATA_CASSANDRA_ENABLED`; `application.server.internet-address` should be `APPLICATION_SERVER_INTERNET_ADDRESS`).

CORE-API.PROPERTIES

The file `core-api.properties` specifies settings for the Knowledge Hub service.

The following table describes, in detail, the parameters that may be added to/modified in this configuration file.

PARAMETER	DESCRIPTION
SPRING	
<code>SPRING_DATA_CASSANDRA_ENABLED</code>	Accepts the values true or false Enables (when true) or disables (when false) exports to the Library and exports of pinned data
<code>SPRING_DATASOURCE_URL</code> <code>SPRING_DATASOURCE_URL_JDBC</code> <code>SPRING_DATASOURCE_URL_USERNAME</code> <code>SPRING_DATASOURCE_URL_PASSWORD</code>	Describes the connection to the Postgres database for the Knowledge Hub service
<code>SPRING_HTTP_MULTIPART_MAXFILESIZE</code> <code>SPRING_HTTP_MULTIPART_MAXREQUESTSIZE</code>	Describes the maximum size of files that may be uploaded to the application (e.g., 2000MB)
SERVER	
<code>SERVER_PORT</code>	Port on which the application is running
<code>SERVER_PORT_SSL_ENABLED</code> <code>SERVER_PORT_SSL_KEY_STORE</code>	true if HTTPS is enabled

PARAMETER	DESCRIPTION
SERVER_PORT_SSL_KEY_STORE_PASSWORD SERVER_PORT_SSL_KEY_PASSWORD	Describe parameters for the SSL certificate
SERVER_TOMCAT_ACCESSLOG_ENABLED SERVER_TOMCAT_ACCESSLOG_DIRECTORY SERVER_TOMCAT_ACCESSLOG_ACCEPT_COUNT SERVER_TOMCAT_ACCESSLOG_BUFFERED SERVER_TOMCAT_ACCESSLOG_PATTERN SERVER_TOMCAT_ACCESSLOG_PREFIX SERVER_TOMCAT_ACCESSLOG_RENAME_ON_ROTATE SERVER_TOMCAT_ACCESSLOG_REQUEST_ATTRIBUTES_ENABLED SERVER_TOMCAT_ACCESSLOG_ROTATE SERVER_TOMCAT_ACCESSLOG_SUFFIX	<p>These items describe settings for Tomcat logs:</p> <ul style="list-style-type: none"> • buffered - Buffer output so that it is flushed periodically • pattern - Format pattern for access logs • prefix - Log filename prefix • rename-on-rotate - Defer inclusion of the date stamp in the filename until rotate time • request-attributes-enabled - Set request attributes for IP address, hostname, protocol, and port used for the request • rotate - enable access log rotation • suffix - Log filename suffix
APPLICATION	
APPLICATION_SERVER_INTERNET_ADDRESS	Describes the redirect URL for login to Salesforce, Google Analytics, Google Adwords (should be identical to the URL specified for ClientId and ClientSecret for these connections), etc.
APPLICATION_HTTP_CACHE_TIMETOLIVEINDAYS	Describes the amount of time in days that may elapse before a data source's cache times out
APPLICATION_DATA_ENGINE_STORE_DESIGN_MODE_LIMIT	Describes the row limit to be used for data sources in Design Mode; the default value is 10K
APPLICATION_DATA_ENGINE_SUGGESTION_PREPARE_CRON	<p>Describes settings for jobs that calculate suggestions based on data type and content</p> <p>e.g., 0 */30 * ? * * - jobs are run every 30 min</p>
APPLICATION_DATA_ENGINE_API_URL	URL for internal communication between Knowledge Hub and Knowledge Hub Data Engine services (http://<machine name>:8081)
APPLICATION_DSL_SOURCE_CLEANER_CRON APPLICATION_DSL_SOURCE_EXPIRATION_IN_HOURS APPLICATION_DSL_TEMPORARY_ITEM_CLEANER_CRON APPLICATION_DSL_TEMPORARY_ITEM_EXPIRATION_IN_HOURS	Describes settings for jobs that delete temporary objects
APPLICATION_DSL_PROCESS_RUN_CLEANER_CRON	Settings related to the job run cleaner

PARAMETER	DESCRIPTION
APPLICATION_DSL_PROCESS_RUN_CLEANER_EXPIRATION_TIME	
APPLICATION_LICENSE_PROVIDER	Type of license provider; can be "local" , "remote" , or "hwu"
APPLICATION_LICENSE_LOCAL_FILEPATH	Path to license.lic file
APPLICATION_LICENSE_REMOTE_URL	URL to the remote server
APPLICATION_LICENSE_HWU_HOST	Altair License Server address. Should be written as "<port>@<host>". Note that the URL to the Altair License Server should be set as an environment variable.
APPLICATION_LICENSE_HWU_CHECKER_CRON	Schedule to execute remote license pool check (e.g., 00/5 * * * *)
APPLICATION_LICENSE_HWU_GROUP	Name of group on Altair License Server (e.g., <code>\${COMPUTERNAME}</code>). Note that this property should also be set as an environment variable.
APPLICATION_LICENSE_HWU_LOG_ENABLED	Enable (true) or disable (false) hwu logging
APPLICATION_LICENSE_HWU_LOG_LEVEL	Level of hwu logging (e.g., info)
APPLICATION_LICENSE_HWU_LOG_FACILITY	Type of output (e.g., stderr)
APPLICATION_SCHEDULES_MONITORING_INTERVAL_INMINUTES	Number of minutes that must elapse before the next monitoring operation should be executed in a monitoring schedule
APPLICATION_SECURITY_AUTHENTICATION_FAILED_ATTEMPT_MIN_DELAY_SEC	Delay after the first failed login attempt e.g., 8
APPLICATION_SECURITY_AUTHENTICATION_FAILED_ATTEMPT_MAX_DELAY_SEC	Maximum delay time after a failed login attempt e.g. 600

DATA-ENGINE-API.PROPERTIES

The file `data-engine-api.properties` specifies settings for the Knowledge Hub Data Service Engine service.

The following table describes, in detail, the parameters that may be added to this configuration file.

PARAMETER	DESCRIPTION
SPRING	
SPRING_DATA_CASSANDRA_ENABLED	Accepts the values true or false Enables (when true) or disables (when false) exports to the Library and exports of pinned data

SPRING_DATASOURCE_URL_JDBC SPRING_DATASOURCE_URL_USERNAME SPRING_DATASOURCE_URL_PASSWORD	Describes the connection to the Postgres database for the Knowledge Hub service
LOGGING	
LOGGING_FILE	full path to Data Engine service log file
LOGBACK	
LOGBACK_LOGLEVEL	Logging level of the Data Engine service log file
SERVER	
SERVER_PORT	8081 – port on which the Data Engine is running
SERVER_PORT_SSL_ENABLED SERVER_PORT_SSL_KEY_STORE SERVER_PORT_SSL_KEY_STORE_PASSWORD SERVER_PORT_SSL_KEY_PASSWORD	true if HTTPS is used. Describes parameters for the SSL certificate.
APPLICATION	
APPLICATION_DATA_ENGINE_SUGGESTION_RANK_THRESHOLD	Describes settings for suggestions based on data type and content; shows minimum rank for retrieving and sorting suggestions
APPLICATION_DATA_ENGINE_STORE_STATISTICS_AWAIT_TIMEOUT	Time to wait before statistics requests time out e.g., 60s
APPLICATION_DATA_ENGINE_STORE_DESIGN_MODE_LIMIT	Describes the row limit to be used for data sources in Design Mode; the default value is 10K
APPLICATION_DATA_ENGINE_STORE_GLOBALROWLIMIT	Row limit applied when the Design Mode limit is disabled e.g., 5000
APPLICATION_DATA_ENGINE_STORE_COLUMN_LIMIT	100 - column limit after Pivot and Transpose.
APPLICATION_DATA_ENGINE_STORE_DISTINCT_VALUE_LIMIT	250 - number of displayed distinct values limit
APPLICATION_DATA_ENGINE_STORE_LIMIT_DATA_NODES	Enables or disables limit to count of rows in all data nodes e.g., true (enabled); false (disabled)
APPLICATION_DATA_ENGINE_STORE_EXPORT_DATA_AWAIT_TIMEOUT_IN_SEC	3600 - export timeout
APPLICATION_IO_WRITER_COGNOS_HTTP_CLIENT_TIMEOUT	600 - timeout for connection to IBM Cognos Analytics
APPLICATION_SERVER_INTERNET_ADDRESS	Redirect URL for logins to Salesforce, Microsoft Sharepoint, Google Analytics, Google BigQuery, Google Adwords, Google Drive (redirect url should be specified for ClientId and ClientSecret for Google connections).
APPLICATION_IO_READER_PREVIEW_LIMIT	1000 – row limit for previewing data sources

JDBC	
APPLICATION_IO_READER_JDBC_FETCH_SIZE	Describes the number of rows to fetch for a query to a database using JDBC drivers, e.g., 200
APPLICATION_IO_READER_JDBC_TIMEOUT_IN_SEC	Describes the time in seconds that may elapse before connections to JDBC drivers time out e.g., 60
APPLICATION_IO_READER_JDBC_DRIVER_*	Configuration settings for JDBC drivers
APPLICATION_IO_READER_JDBC_DRIVER_DEFAULT_LOGINTIMEOUT	Describes the time in seconds that may elapse before connections to JDBC drivers time out after login e.g., 60
APPLICATION_IO_READER_JDBC_DRIVER_DEFAULT_SOCKETTIMEOUT	Describes the time in seconds that may elapse before a socket timeout occurs when using connections to JDBC drivers e.g., 60
APPLICATION_IO_READER_JDBC_DRIVER_CDATA_JDBC_ALL_TIMEOUT	Describes the time in seconds that may elapse before all connections to JDBC drivers time out e.g., 60
APPLICATION_IO_READER_JDBC_DRIVER_COM_MYSQL_JDBC_DRIVER_USECURSORFETCH APPLICATION_IO_READER_JDBC_DRIVER_COM_MYSQL_JDBC_DRIVER_LOGINTIMEOUT APPLICATION_IO_READER_JDBC_DRIVER_COM_MYSQL_JDBC_DRIVER_SOCKETTIMEOUT	Settings for MySQL JDBC driver
APPLICATION_IO_READER_JDBC_DRIVER_ORACLE_JDBC_ORACLEDRIVER_ORACLE_NET_CONNECT_TIMEOUT APPLICATION_IO_READER_JDBC_DRIVER_ORACLE_JDBC_ORACLEDRIVER_ORACLE_JDBC_READTIMEOUT	Settings for Oracle JDBC driver
APPLICATION_IO_READER_JDBC_DRIVER_COM_FACEBOOK_PRESTO_JDBC_PRESTODRIVER_SSL APPLICATION_IO_READER_JDBC_DRIVER_COM_FACEBOOK_PRESTO_JDBC_PRESTODRIVER_PASSWORD	Settings for Presto JDBC driver
APPLICATION_IO_READER_JDBC_DRIVER_ORG_APACHE_HIVE_JDBC_HIVEDRIVER_JAVA_SECURITY_KRB5_CONF APPLICATION_IO_READER_JDBC_DRIVER_ORG_APACHE_HIVE_JDBC_HIVEDRIVER_JAVA_SECURITY_AUTH_LOGIN_CONFIG	Settings for Apache Hive JDBC driver
APPLICATION_SECURITY_AUTHENTICATION_XAUTH_SECRET	security token, should be equal to all other security tokens in all other application config files

APPLICATION_CORE_API_URL	address for internal communication with the Knowledge Hub service
READER	
READER_PREVIEW_LIMIT	1000 - row limit for preview data sources.
REPORT	
REPORT_TEXT_VIEW_MAX_CACHE_IN_MB	This option sets the limit in megabytes for storing the converted reports.
REPORT_TEXT_VIEW_MAX_CACHE_COUNT	This option sets the limit in counts for storing the converted reports.
REPORT_TEXT_VIEW_NUMBER_OF_PAGES	If the page number of THE report exceeds this setting, then conversion option converts from PDF reports to TXT report

SOCIAL-API.PROPERTIES

The file `social-api.properties` specifies settings for the Knowledge Hub Social and Machine Learning service.

The following table describes, in detail, the parameters that may be added to the configuration file.

PARAMETER	DESCRIPTION
SERVER	
SERVER_JWT_SECRET	A security token that should be identical to all other security token indicated in all other application config files (e.g., <code>application.security.authentication.xauth.secret</code> in other config files)
SERVER_PORT_SSL_ENABLED SERVER_PORT_SSL_KEYSTORE_PASSWORD SERVER_PORT_SSL_KEYSTORE_PATH	true if HTTPS is used. Describes parameters for the SSL certificate.
SPARK	
SPARK_APP_NAME SPARK_APP_SCHEDULE SPARK_APP_SCHEDULING_ENABLED	Spark application name Cron for Spark job for calculating suggestions (e.g., <code>0 0/20 * 1/1 * ? *</code>) False if only a single run is applied
SPARK_DRIVER_MEMORY	Allocated memory size for Spark service
DATABASE	
DATABASE_CASSANDRA_CONNECTION_ATTEMPTS_AMOUNT	Number of attempts to connect to the Cassandra database
DATABASE_CASSANDRA_CONNECTION_WAIT_TIME_SECONDS	Number of second for each attempt to connect to the Cassandra database
LOGGING	
LOGGING_LOGLEVEL LOGGING_LOGFILEPATH	Logging level

PARAMETER	DESCRIPTION
	Full path to the ML and Spark services log file (e.g., C:\Windows\Temp\MonarchSwarm\Logs\ml-app.log)
NEXT_CHANGE	
NEXT_CHANGE_MIN_CHANGES	Minimum number of actions in sequence to generate suggestions

Setting Up LDAP/SSO Authentication

Execute the following steps to enable LDAP/SSO authentication.

Steps:

1. Install Knowledge Hub with default parameters.
2. Edit the Kerberos configuration file `./knowledgehub/user-config/krb5.conf`.

```
[libdefaults]
default_realm = <DOMAIN>
default_keytab_name = /keytab/linuxsso.keytab
forwardable=true
dns_lookup_realm = true
rdns = false
dns_lookup_kdc = true

[realms]
<DOMAIN> = {
    kdc = <name of domain controller>.<domain>:88
    admin_server = <name of domain controller>.<domain>:88
}

[domain_realm]
<domain> = <DOMAIN>
.<domain> = <DOMAIN>

[appdefaults]
kinit = {
    renewable = true
    forwardable= true
}
```

For example, if the full computer name of the domain controller is **WIN-LDAPSERVER** and the domain name is **altair.com**:

```
[libdefaults]
default_realm = ALTAIR.COM
default_keytab_name = /keytab/linuxsso.keytab
forwardable=true
dns_lookup_realm = true
rdns = false
dns_lookup_kdc = true

[realms]
ALTAIR.COM = {
  kdc = WIN-LDAPSERVER.altair.com:88
  admin_server = WIN-LDAPSERVER.altair.com:88
}

[domain_realm]
altair.com = ALTAIR.COM
.altair.com = ALTAIR.COM

[appdefaults]
kinit = {
  renewable = true
  forwardable= true
}
```

3. Add JAVA-OPTS to the core-api.configuration.

```
JAVA_OPTS=-Djava.security.krb5.conf=/sso/krb5.conf -
Dsun.security.krb5.debug=true
-
```

4. Generate a **linuxsso.keytab** and replace this keytab in `./knowledgehub/user-config/linuxsso.keytab`.

Additional Information

[ktpass | Microsoft Docs All you need to know about Keytab files.](#)

For example, if the full computer name of the Knowledge Hub server is **WIN-SWARMSEVER** and the domain name is **altair.com**, run the following script in Powershell:

```
setspn -A HTTP/WIN-SWARMSEVER.altair.com knhubsingle

ktpass /out c:\temp\linuxsso.keytab /mapuser knhubsingle@ALTAIR.COM /princ
HTTP/WIN-SWARMSEVER@ALTAIR.COM /pass Password# /ptype KRB5_NT_PRINCIPAL
/crypto All
```

5. Check the principal in the keytab file in linux: `klint -k -t linuxsso.keytab`.

The result should contain a valid principal and the same principal should be in `core-api.properties`.

6. Configure `./knowledgehub/user-config/core-api.properties` as follows.

For SSO Authentication

```
JAVA_OPTS=-Djava.security.krb5.conf=/sso/krb5.conf -
Dsun.security.krb5.debug=true
APPLICATION_SECURITY_AUTHENTICATION_PROVIDER=ldap <available values:
basic, ldap, oauth2>
APPLICATION_SECURITY_AUTHENTICATION_USERS_PROVISIONED=false
APPLICATION_SECURITY_AUTHENTICATION_DEFAULT_PASSWORD=<default password
for users created through LDAP and added multiple users>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SSO_ENABLED=true
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SSO_SERVICE_PRINCIPAL=HTTP<full
computer name of Knowledge Hub server>/@<DOMAIN NAME>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SSO_KEY_TAB_LOCATION=<path of
keytab file>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SSO_REQUEST_REGEX=^/api/.+/ldap_
sso
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_LOGIN=us
erPrincipalName
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_FIRST_NA
ME=givenname
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_LAST_NAM
E=sn
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_COMMON_N
AME=cn
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_EMAIL=ma
il
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_PHONE_NU
MBER=telephonenumber
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_GROUPS=m
emberOf
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_CUSTOM_ATTRIBUTES='["displ
ayName", "distinguishedName", "name", "objectCategory", "objectClass", "primar
yGroupID", "sAMAccountName", "sAMAccountType", "servicePrincipalName"]'
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ACTIVE_DIRECTORY=true
APPLICATION_SECURITY_AUTHENTICATION_LDAP_DOMAIN=<DOMAIN>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SERVER=ldap://<full computer
name of LDAP server>.<domain name>/
APPLICATION_SECURITY_AUTHENTICATION_LDAP_MANAGE_DN=<LDAP admin user>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_MANAGE_PASSWORD=<password of
admin user>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_BASE=DC=<domain component
1>,DC=<domain component 2>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_FILTER=(|
(userPrincipalName={0}) (sAMAccountName={0}))
APPLICATION_SECURITY_AUTHENTICATION_LDAP_USER_ROLES=3
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ADMIN_USERS=<admin user1>,
<admin user2>
```

For example, if the full computer name of the Knowledge Hub server is **WIN-SWARMSEVER**, the LDAP server is **WIN-LDAPSERVER**, and the domain name is **altair.com**:

```
JAVA_OPTS=-Djava.security.krb5.conf=/sso/krb5.conf -
Dsun.security.krb5.debug=true
APPLICATION_SECURITY_AUTHENTICATION_PROVIDER=ldap
APPLICATION_SECURITY_AUTHENTICATION_USERS_PROVISIONED=false
APPLICATION_SECURITY_AUTHENTICATION_DEFAULT_PASSWORD=Passw0rd#
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SSO_ENABLED=true
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SSO_SERVICE_PRINCIPAL=HTTP/WIN-SWARMSEVER.altair.com/@ALTAIR.COM
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SSO_KEY_TAB_LOCATION=/keytab/linuxsso.keytab
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SSO_REQUEST_REGEX=^/api/.+/ldap_sso
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_LOGIN=us
erPrincipalName
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_FIRST_NA
ME=givenname
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_LAST_NAM
E=sn
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_COMMON_N
AME=cn
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_EMAIL=ma
il
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_PHONE_NU
MBER=telephonenumber
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_GROUPS=m
emberOf
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_CUSTOM_ATTRIBUTES='["displ
ayName", "distinguishedName", "name", "objectCategory", "objectClass", "primar
yGroupID", "sAMAccountName", "sAMAccountType", "servicePrincipalName"]'
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ACTIVE_DIRECTORY=true
APPLICATION_SECURITY_AUTHENTICATION_LDAP_DOMAIN=ALTAIR.COM
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SERVER=ldap://WIN-LDAPSERVER.altair.com/
APPLICATION_SECURITY_AUTHENTICATION_LDAP_MANAGE_DN=swarmadmin@altair.com
APPLICATION_SECURITY_AUTHENTICATION_LDAP_MANAGE_PASSWORD=#Passw0rd#
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_BASE=DC=altair,DC=com
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_FILTER=( |
(userPrincipalName={0}) (sAMAccountName={0}))
APPLICATION_SECURITY_AUTHENTICATION_LDAP_GROUPMAPPING=true
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ROLEMAPPING=true
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ROLES_MAP_1=Accounting, Finance
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ROLES_MAP_2=BusDev, Sales
APPLICATION_SECURITY_AUTHENTICATION_LDAP_USER_ROLES=3
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ADMIN_USERS=mbarnes@altair.com,
tjones@altair.com
```

For LDAP Authentication

```
JAVA_OPTS=-Djava.security.krb5.conf=/sso/krb5.conf -
Dsun.security.krb5.debug=true
APPLICATION_SECURITY_AUTHENTICATION_PROVIDER=ldap <available values:
basic, ldap, oauth2>
APPLICATION_SECURITY_AUTHENTICATION_USERS_PROVISIONED=false
APPLICATION_SECURITY_AUTHENTICATION_DEFAULT_PASSWORD=<default password
for users created through LDAP and added multiple users>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_LOGIN=us
erPrincipalName
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_FIRST_NA
ME=givenname
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_LAST_NAM
E=sn
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_COMMON_N
AME=cn
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_EMAIL=ma
il
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_PHONE_NU
MBER=telephonenumber
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_GROUPS=m
emberOf
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_CUSTOM_ATTRIBUTES='["displ
ayName", "distinguishedName", "name", "objectCategory", "objectClass", "primar
yGroupID", "sAMAccountName", "sAMAccountType", "servicePrincipalName"]'
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ACTIVE_DIRECTORY=true
APPLICATION_SECURITY_AUTHENTICATION_LDAP_DOMAIN=<DOMAIN>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SERVER=ldap://<full computer
name of LDAP server>.<domain name>/
APPLICATION_SECURITY_AUTHENTICATION_LDAP_MANAGE_DN=<LDAP admin user>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_MANAGE_PASSWORD=<password of
admin user>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_BASE=DC=<domain component
1>,DC=<domain component 2>
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_FILTER=(|
(userPrincipalName={0}) (sAMAccountName={0}))
APPLICATION_SECURITY_AUTHENTICATION_LDAP_USER_ROLES=3
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ADMIN_USERS=<admin user1>,
<admin user2>
```

For example, if the full computer name of the Knowledge Hub server is **WIN-SWARMSEVER**, the LDAP server is **WIN-LDAPSERVER**, and the domain name is **altair.com**:

```

JAVA_OPTS=-Djava.security.krb5.conf=/sso/krb5.conf -
Dsun.security.krb5.debug=true
APPLICATION_SECURITY_AUTHENTICATION_PROVIDER=ldap
APPLICATION_SECURITY_AUTHENTICATION_USERS_PROVISIONED=false
APPLICATION_SECURITY_AUTHENTICATION_DEFAULT_PASSWORD=Passw0rd#
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_LOGIN=userPrincipalName
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_FIRST_NAME=givenname
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_LAST_NAME=sn
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_COMMON_NAME=cn
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_EMAIL=mail
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_PHONE_NUMBER=telephonenumber
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_GROUPS=memberOf
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_CUSTOM_ATTRIBUTES='["displayName", "distinguishedName", "name", "objectCategory", "objectClass", "primaryGroupID", "sAMAccountName", "sAMAccountType", "servicePrincipalName"]'
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ACTIVE_DIRECTORY=true
APPLICATION_SECURITY_AUTHENTICATION_LDAP_DOMAIN=ALTAIR.COM
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SERVER=ldap://WIN-LDAPSERVER.altair.com/
APPLICATION_SECURITY_AUTHENTICATION_LDAP_MANAGE_DN=swarmadmin@altair.com
APPLICATION_SECURITY_AUTHENTICATION_LDAP_MANAGE_PASSWORD=#Passw0rd#
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_BASE=DC=altair,DC=com
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_FILTER=(|(userPrincipalName={0})(sAMAccountName={0}))
APPLICATION_SECURITY_AUTHENTICATION_LDAP_GROUPMAPPING=true
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ROLEMAPPING=true
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ROLES_MAP_1=Accounting, Finance
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ROLES_MAP_2=BusDev, Sales
APPLICATION_SECURITY_AUTHENTICATION_LDAP_USER_ROLES=3
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ADMIN_USERS=mbarnes@altair.com, tjones@altair.com

```

Each of the properties added to the core-api configuration file is described as follows:

PROPERTY	DESCRIPTION
APPLICATION	
APPLICATION_SECURITY_AUTHENTICATION_PROVIDER	Use ldap for LDAP/SSO; may also be basic for basic or oauth2 for OAuth2 authentication
APPLICATION_SECURITY_AUTHENTICATION_USERS_PROVISIONED	Enables (true) or disables (false) explicit provisioning. If explicit provisioning is disabled, the system creates Knowledge Hub users automatically. When set to true, users must be created manually

PROPERTY	DESCRIPTION
APPLICATION_SECURITY_AUTHENTICATION_DEFAULT_PASSWORD	The default password for new users created through LDAP and added multiple users
APPLICATION_SECURITY_AUTHENTICATION_SSO_ENABLED	true to enable SSO; false if using LDAP authentication
APPLICATION_SECURITY_AUTHENTICATION_SSO_SERVICE_PRINCIPAL	Full computer name of the Knowledge Hub server in the form HTTP/<COMPUTER NAME>.<domain>/@<DOMAIN> (e.g., HTTP/WIN-SWARMSEVER.altair.com@ALTAIR.COM)
APPLICATION_SECURITY_AUTHENTICATION_SSO_KEY_TAB_LOCATION	Path to keytab file (e.g., /keytab/linuxsso.keytab)
APPLICATION_SECURITY_AUTHENTICATION_SSO_REQUEST_REGEX	^/api/.+ /ldap_sso - Setting for SSO
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_ATTRIBUTE_MAPPING_ LOGIN: USERPRINCIPALNAME FIRST_NAME: GIVENNAME LAST_NAME: SN COMMON_NAME: CN EMAIL: MAIL PHONE_NUMBER: TELEPHONENUMBER GROUPS: MEMBEROF	Attributes used to add users by LDAP query
APPLICATION_SECURITY_AUTHENTICATION_LDAP_QUERY_CUSTOM_ATTRIBUTES DISPLAYNAME DISTINGUISHEDNAME NAME OBJECTCATEGORY OBJECTCLASS PRIMARYGROUPID SAMACCOUNTNAME SAMACCOUNTTYPE SERVICEPRINCIPALNAME	
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ACTIVE_DIRECTORY	true when AD is used
APPLICATION_SECURITY_AUTHENTICATION_LDAP_DOMAIN	Domain name

PROPERTY	DESCRIPTION
APPLICATION_SECURITY_AUTHENTICATION_LDAP_DOMAIN_USERS	Allow LDAP authentication for any of two forests in one domain. The default value for this setting is false . To authenticate users from just one domain via LDAP, set this property to true and then set the correct domain in the property APPLICATION_SECURITY_AUTHENTICATION_LDAP_DOMAIN
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SERVER	Full computer name of LDAP server
APPLICATION_SECURITY_AUTHENTICATION_LDAP_MANAGE_DN APPLICATION_SECURITY_AUTHENTICATION_LDAP_MANAGE_PASSWORD	User name and password to use to connect to LDAP server when SSO_ENABLED = false and LDAP_ACTIVE_DIRECTORY = false If SSO_ENABLED = true and LDAP_ACTIVE_DIRECTORY = true , these properties may be omitted from the config file. These credentials are also used to add multiple users to Knowledge Hub using LDAP query
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_BASE	Domain name components (e.g., DC= altair ,DC= com if domain is altair.com)
APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_FILTER	Filter used to search for LDAP users
APPLICATION_SECURITY_AUTHENTICATION_LDAP_USER_ROLES	User role(s) for SSO users
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ADMIN_USERS	List of users automatically created with the Super Administrator role in Knowledge Hub (if USERS_PROVISIONED = false). When this list is provided, there is no need to login as an administrator and create the first LDAP user.
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ROLEMAPPING	true to enable role-mapping in Knowledge Hub; false to disable
APPLICATION_SECURITY_AUTHENTICATION_LDAP_GROUPMAPPING	true to enable group-mapping in Knowledge Hub; false to disable
APPLICATION_SECURITY_AUTHENTICATION_LDAP_ROLESMAP	Mapping of Knowledge Hub roles to LDAP groups

Notes:

- The property [APPLICATION_SECURITY_AUTHENTICATION_LDAP_SEARCH_FILTER](#) uses the format "username@domain".
- If a user does not specify the domain in the login form, the value in [APPLICATION_SECURITY_AUTHENTICATION_LDAP_DOMAIN](#) will be used as the domain.
- LDAP search attributes should have values in "username@domain" format.

- If the property `USERS_PROVISIONED` is set to `TRUE`, and the user is not included in the `ADMIN_USERS` list, an error (i.e., “Users %user_login% does not exist”) is returned when the user logs into the application via SSO. In this case, the user must be manually added through the User Management page (via LDAP) of Knowledge Hub.
- If the property `USERS_PROVISIONED` is set to `FALSE`, and the user exists in Active Directory, a new user is created upon login to Knowledge Hub via SSO. This user’s profile will include a login, last name, and first name, and s/he will have the role(s) specified in `USER_ROLES`.
- If the user exists in Active Directory, and the new user is included in the `ADMIN_USERS` list, the user can log into Knowledge Hub via SSO and this user will have the role Super Administrator regardless if the property `USERS_PROVISIONED` is set to `TRUE` or `FALSE`.

To enable role/group mapping, set the following properties:

- `APPLICATION_SECURITY_AUTHENTICATION_LDAP_ROLEMAPPING` – **true** to enable role mapping; **false** otherwise
- `APPLICATION_SECURITY_AUTHENTICATION_LDAP_GROUPMAPPING` – **true** to enable group mapping; **false** otherwise
- `APPLICATION_SECURITY_AUTHENTICATION_LDAP_ROLESMAP %role_id1%`: “%GroupName1, GroupName2%” – Mapping of first Knowledge Hub role to LDAP groups
- `APPLICATION_SECURITY_AUTHENTICATION_LDAP_ROLESMAP %role_id2%`: “%GroupName1, GroupName2%” – Mapping of second Knowledge Hub role to LDAP groups

7. After configuration, restart all services and then launch Knowledge Hub.

Volume Configuration

To deploy Single Server Knowledge Hub to custom volume locations, the following steps are performed:

1. Open the `./bin/utils/setup-volumes.sh` file for and then set the `ROOT_FOLDER` property to a folder to which you have access (e.g., `ROOT_FOLDER=/home/<user>`). Note that by default, `ROOT_FOLDER=/tmp`.
2. (Optional) Update paths for the properties `LIBS`, `FILE_LIBRARY`, `META_DB_DATA`, `SOCIAL_DB_DATA`, and `DATA_ENGINE_DB_DATA` if needed.
3. Save changes to the `./bin/utils/setup-volumes.sh` file and then run `./setup-volumes.sh` from the `./bin/utils` directory. Doing so creates the required docker volumes.

4. Run `./linux-4-setup-single-server.sh` from the `./bin` directory. Knowledge Hub Single Server will be deployed to the pre-configured volumes.

Utils Configuration

To configure the Knowledge Hub Single Server application, run `./bin/utils/linux-config.sh` and then select:

- ❑ 1 - Libs-ls
Show libs from the shared `/libs` folder
- ❑ 2 - Libs-download
Download libraries on the local machine to the `./bin/utils/libs` from the shared `/libs` folder
- ❑ 3 - Libs-upload
Upload libraries from the local machine folder `./bin/utils/libs` to the shared `/libs` folder. After execution of this command, all services must be restarted to apply changes.
- ❑ 4 - Libs-remove
Removes libraries from the shared `/libs` folder. After execution of this command, all services must be restarted to apply changes.
- ❑ 5 - License-update
Before execution, copy a new version of `license.lic` to the folder `./knowledgehub/user-config/`.
- ❑ 6 - Certificate-update
Before execution, copy new versions of `tls.crt` and `tls.key` to the folder `./knowledgehub/user-config/`
- ❑ 7 - Start services
Start all API services in Docker Swarm.
- ❑ 8 - Stop services
Stop all API services in Docker Swarm.
- ❑ 9 - Restart services
Stop and start all API services in Docker Swarm.
- ❑ 10 - Exit
Exit the utils menu.

Memory Configuration

The Knowledge Hub Single Server application has two predefined CPU/memory configurations: 4x16 or 8x32.

To change configuration options, modify:

- ❑ 4x16 - `./knowledgehub/docker-compose.4x16.yml`
- ❑ 8x32 - `./knowledgehub/docker-compose.8x32.yml`

Knowledge Hub Single Server requires a minimum configuration of 8x32, so this configuration must be used. To change the default configuration, edit the properties of **SERVER_ENV** in `./knowledgehub/user-config/env.properties`.

- ❑ To configure resources for each service, modify the following parameters:

```
reservations:
  cpus: '0.25'
  memory: 100M
limits:
  cpus: '2.0'
  memory: 4100M
```

IMPORTANT: CPU and memory limits must be added to all services.

- ❑ To apply the new configuration, run `./linux-4-setup-single-server.sh`.

Troubleshooting

AGGREGATING STATUS INFORMATION

- ❑ [Export all logs](#). Navigate to `./bin/utils` and run:

```
./elastic-export.sh --from 2019-01-01
```

Archive all folders in `./bin/utils/export-*` with exported logs and attach to email/ticket for support.

CLEANING THE SERVER APPLICATION

- ❑ Delete the Knowledge Hub deployment by running `docker stack rm knowledgehub`
- ❑ Wait 2–3 minutes, delete the volume `docker volume prune`, and check `docker volume ls`. The following volumes should be deleted: `data-engine-db-data`, `meta-db-data`, `social-db-data`, `file_library`, and `libs`.
- ❑ To install Knowledge Hub Single Server, run `./linux-4-setup-single-server.sh`.