

webMethods Internal Data Store Administrator's Guide

Innovation Release

Version 10.2

April 2018

This document applies to Software AG Product Suite Version 10.2 and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Copyright © 2018 Software AG, Darmstadt, Germany and/or Software AG USA Inc., Reston, VA, USA, and/or its subsidiaries and/or its affiliates and/or their licensors.

The name Software AG and all Software AG product names are either trademarks or registered trademarks of Software AG and/or Software AG USA Inc. and/or its subsidiaries and/or its affiliates and/or their licensors. Other company and product names mentioned herein may be trademarks of their respective owners.

Detailed information on trademarks and patents owned by Software AG and/or its subsidiaries is located at <http://softwareag.com/licenses>.

Use of this software is subject to adherence to Software AG's licensing conditions and terms. These terms are part of the product documentation, located at <http://softwareag.com/licenses> and/or in the root installation directory of the licensed product(s).

This software may include portions of third-party products. For third-party copyright notices, license terms, additional rights or restrictions, please refer to "License Texts, Copyright Notices and Disclaimers of Third Party Products". For certain specific third-party license restrictions, please refer to section E of the Legal Notices available under "License Terms and Conditions for Use of Software AG Products / Copyright and Trademark Notices of Software AG Products". These documents are part of the product documentation, located at <http://softwareag.com/licenses> and/or in the root installation directory of the licensed product(s).

Use, reproduction, transfer, publication or disclosure is prohibited except as specifically provided for in your License Agreement with Software AG.

Table of Contents

About this Guide.....	5
Document Conventions.....	5
Online Information.....	6
About webMethods Internal Data Store.....	7
Administering Internal Data Store.....	9
Starting, Stopping, and Restarting Internal Data Store.....	10
Starting Internal Data Store in Command Central.....	10
Stopping Internal Data Store in Command Central.....	10
Starting, Stopping, and Restarting Internal Data Store on Windows.....	10
Starting, Stopping, and Restarting Internal Data Store on Unix.....	11
Changing the Internal Data Store HTTP Port.....	11
Changing the Internal Data Store TCP Port.....	12
Configuring an Internal Data Store Cluster.....	12
Configuring Custom Internal Data Store Properties.....	13
Securing Communication with Internal Data Store.....	14
The Internal Data Store Keystores.....	14
Configuring the Internal Data Store HTTP Keystore.....	15
Configuring the Internal Data Store TCP Keystore.....	15
Configuring the Internal Data Store sgadmin Keystore.....	16
Configuring the Internal Data Store Truststore.....	17
Using the Command Line to Manage Internal Data Store.....	19
Commands that Internal Data Store Supports.....	20
Configuration Types that Internal Data Store Supports.....	21
Run-Time Monitoring Statuses for Internal Data Store.....	21
Lifecycle Actions for Internal Data Store.....	22

About this Guide

This guide provides information about how to administer webMethods Internal Data Store, which is a Software AG packaging of Elasticsearch 5.6.

Document Conventions

Convention	Description
Bold	Identifies elements on a screen.
Narrowfont	Identifies storage locations for services on webMethods Integration Server, using the convention <i>folder.subfolder:service</i> .
UPPERCASE	Identifies keyboard keys. Keys you must press simultaneously are joined with a plus sign (+).
<i>Italic</i>	Identifies variables for which you must supply values specific to your own situation or environment. Identifies new terms the first time they occur in the text.
Monospace font	Identifies text you must type or messages displayed by the system.
{ }	Indicates a set of choices from which you must choose one. Type only the information inside the curly braces. Do not type the { } symbols.
	Separates two mutually exclusive choices in a syntax line. Type one of these choices. Do not type the symbol.
[]	Indicates one or more options. Type only the information inside the square brackets. Do not type the [] symbols.
...	Indicates that you can type multiple options of the same type. Type only the information. Do not type the ellipsis (...).

Online Information

Software AG Documentation Website

You can find documentation on the Software AG Documentation website at "<http://documentation.softwareag.com>". The site requires Empower credentials. If you do not have Empower credentials, you must use the TECHcommunity website.

Software AG Empower Product Support Website

You can find product information on the Software AG Empower Product Support website at "<https://empower.softwareag.com>".

To submit feature/enhancement requests, get information about product availability, and download products, go to "[Products](#)".

To get information about fixes and to read early warnings, technical papers, and knowledge base articles, go to the "[Knowledge Center](#)".

Software AG TECHcommunity

You can find documentation and other technical information on the Software AG TECHcommunity website at "<http://techcommunity.softwareag.com>". You can:

- Access product documentation, if you have TECHcommunity credentials. If you do not, you will need to register and specify "Documentation" as an area of interest.
- Access articles, code samples, demos, and tutorials.
- Use the online discussion forums, moderated by Software AG professionals, to ask questions, discuss best practices, and learn how other customers are using Software AG technology.
- Link to external websites that discuss open standards and web technology.

1 About webMethods Internal Data Store

webMethods Internal Data Store is a data store for use only with Software AG products, such as webMethods API Gateway and webMethods OneData.

You can have only one Internal Data Store instance per Software AG installation. You can configure Internal Data Store as a single node storage, or you can combine multiple nodes to form a cluster.

You must install the following products to monitor and configure Internal Data Store:

- Software AG Command Central
- Software AG Platform Manager

2 Administering Internal Data Store

■ Starting, Stopping, and Restarting Internal Data Store	10
■ Changing the Internal Data Store HTTP Port	11
■ Changing the Internal Data Store TCP Port	12
■ Configuring an Internal Data Store Cluster	12
■ Configuring Custom Internal Data Store Properties	13
■ Securing Communication with Internal Data Store	14

Starting, Stopping, and Restarting Internal Data Store

You can start, stop, and restart your Internal Data Store instance using the Command Central web user interface and command line interface. Additionally, you can use scripts on Unix and Windows, and the Windows Start menu on Windows to manage the runtime status of your Internal Data Store instance.

Starting Internal Data Store in Command Central

Use the following procedure to start Internal Data Store in the Command Central web user interface.

To start Internal Data Store

1. In Command Central, navigate to **Environments > Instances > All > Internal Data Store**.
2. Click the status icon for Internal Data Store.
3. From the **Lifecycle Actions** drop-down menu, select **Start**.

Stopping Internal Data Store in Command Central

Use the following procedure to stop Internal Data Store in the Command Central web user interface.

To stop Internal Data Store

1. In Command Central, navigate to **Environments > Instances > All > Internal Data Store**.
2. Click the status icon for Internal Data Store.
3. From the **Lifecycle Actions** drop-down menu, select **Stop**.

Starting, Stopping, and Restarting Internal Data Store on Windows

When you install Internal Data Store on a Windows operating system, you can start and stop your Internal Data Store instance using the Windows Start menu or using scripts.

To start or stop Internal Data Store using the Windows Start menu, go to **Start > All Programs > Software AG**, select **Start Servers** or **Stop Servers**, and then select **Start Internal Data Store 10.2** or **Stop Internal Data Store 10.2**, respectively.

To start, stop, or restart Internal Data Store using scripts, run:

- Start Internal Data Store - *Software AG_directory*\EventDataStore\bin\startup.bat.
- Stop Internal Data Store - *Software AG_directory*\EventDataStore\bin\shutdown.bat.
- Restart Internal Data Store - *Software AG_directory*\EventDataStore\bin\restart.bat.

Starting, Stopping, and Restarting Internal Data Store on Unix

You can start, stop, and restart Internal Data Store by running the following scripts on Unix:

- Start Internal Data Store - *Software AG_directory/EventDataStore/bin/startup.sh.*
- Stop Internal Data Store - *Software AG_directory/EventDataStore/bin/shutdown.sh.*
- Restart Internal Data Store - *Software AG_directory/EventDataStore/bin/restart.sh.*

Changing the Internal Data Store HTTP Port

The default HTTP port that clients use to make calls to Internal Data Store is 9240. Use the following procedure to change the HTTP port number.

To change the Internal Data Store HTTP port

1. In Command Central, navigate to **Environments > Instances > All > Internal Data Store > Configuration.**
2. Select **Ports** from the drop-down menu.
3. Click **http port** and specify values for the following fields:

Field	Description
Port Number	Required. The HTTP port number. The default value is 9240.

Use SSL	Optional. Enable Secure Sockets Layer (SSL) to secure communication with Internal Data Store.
----------------	-----------------------------------------------------------------------------------------------

- Note:**
- When you enable SSL for the HTTP port, you automatically enable SSL for the TCP port as well.
 - Internal Data Store uses the Search Guard SSL plugin for Elasticsearch. For more information about the Search Guard plugin, see the Search Guard documentation.

4. Optionally, click **Test** to verify your configuration.
5. Save your changes.
6. Restart the Internal Data Store instance.

Changing the Internal Data Store TCP Port

Java clients use the TCP port to make calls to Internal Data Store. In addition, the nodes in an Internal Data Store cluster use the TCP port to communicate with one another. The default TCP port is 9340.

Important: If you change the default TCP port, you must change the respective TCP port value in the **Clustering** configuration.

To change the Internal Data Store TCP port

1. In Command Central, navigate to **Environments > Instances > All > Internal Data Store > Configuration**.
2. Select **Ports** from the drop-down menu.
3. Click **tcp port** and specify values for the following fields:

Field	Description
Port Number	Required. The TCP port number. The default value is 9340.
Use SSL	Optional. Enable Secure Sockets Layer (SSL) for the TCP port. <div data-bbox="581 1178 1360 1476" style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Note:</p> <ul style="list-style-type: none"> ■ When you enable SSL for the TCP port, you automatically enable SSL for the HTTP port as well. ■ Internal Data Store uses the Search Guard SSL plugin for Elasticsearch. For more information about the Search Guard plugin, see the Search Guard documentation. </div>

4. Optionally, click **Test** to verify your configuration.
5. Save your changes.
6. Restart the Internal Data Store instance.


Configuring an Internal Data Store Cluster

You can run an Internal Data Store instance as a single node, or you can configure multiple Internal Data Store instances to run as a cluster to provide high availability and

redundancy. You must specify at least one host and port pair for your configuration in Command Central. Internal Data Store comes with a default host and port pair.

To configure an Internal Data Store cluster

1. In Command Central, for each Internal Data Store instance that is part of the cluster, navigate to **Environments > Instances > All > Internal Data Store > Configuration**.
2. Select **Clustering** from the drop-down menu, and then click **Edit**.
3. Specify values for the following fields:

Field	Description
Cluster Name	Required. The name of the cluster. All instances must have the same cluster name.
Cluster Discovery Nodes	<p>Required. Click , and then do the following to add host and port information for each Internal Data Store instance that is part of the cluster:</p> <ol style="list-style-type: none"> a. In the Host column, specify the host information for an Internal Data Store instance. The default host is <code>localhost</code>. b. In the Port column, specify the port for an Internal Data Store instance. The default port is <code>9340</code>.

4. Optionally, click **Test** to verify that your configuration is valid.
5. Save your changes.
6. Select **Properties** from the drop-down menu, and then click **Edit**.
7. Specify a value for `discovery.zen.minimum_master_nodes`. The number of master eligible nodes must be either 3 or greater than half of the nodes you have in a cluster. For example, in a cluster with three nodes, you specify `discovery.zen.minimum_master_nodes : 2`.
8. Click **Apply** to save your changes.
9. Restart the Internal Data Store instance.

Configuring Custom Internal Data Store Properties

You can specify custom properties for your Internal Data Store configuration.

To specify custom properties for Internal Data Store

1. In Command Central, navigate to **Environments > Instances > All > Internal Data Store > Configuration**.

2. Select **Properties** from the drop-down menu and click **Edit**.
3. In the **Content** field, specify custom parameters. Use YAML syntax and the *property_name : value* format.
4. Restart the Internal Data Store instance.

Securing Communication with Internal Data Store

When you install Internal Data Store it comes with a pre-configured SSL certificate, and default *keystore* and *truststore* files. The keystore and truststore function as repositories for the storage of keys and certificates necessary for SSL authentication, encryption/decryption, and digital signing/verification services. You can find the default truststore and keystore files in the following locations:

- *Software AG_directory/EventDataStore/plugins/search-guard-2/sgconfig/demouser-keystore.jks*
- *Software AG_directory/EventDataStore/plugins/search-guard-2/sgconfig/truststore.jks*

Internal Data Store is enabled for SSL through the Elasticsearch Search Guard plugin. You do not need to interact with the Search Guard plugin configuration to use SSL with Internal Data Store. However, if you want to customize your Search Guard configuration, you can use the `sgadmin` command line tool.

To modify the Search Guard configuration of an SSL-enabled Internal Data Store, you must authenticate the `sgadmin` tool with a `.jks`-based keystore and truststore. Run one of the following scripts to access the `sgadmin` tool:

- For Linux - *Software AG_directory/EventDataStore/repo/search-guard-2/tools/sgadmin.sh*.
- For Windows - *Software AG_directory\EventDataStore\repo\search-guard-2\tools\sgadmin.bat*.

For more information about modifying your Search Guard configuration, see the Search Guard documentation.

If you use Internal Data Store in a production environment, you must replace the Internal Data Store default certificates, keystore and truststore files with custom files. For more information about creating keystores and truststores, importing keys and certificates into keystores and truststores, and other operations with these files, see the documentation for your certificate management tool.

The Internal Data Store Keystores

By default, Internal Data Store has the following pre-configured keystores:

- **HTTP Keystore** - A keystore for HTTP clients.
- **TCP Keystore** - A keystore for TCP clients.

- **sgadmin Keystore** - A keystore that authenticates the sgadmin tool.

You cannot add or remove the pre-configured keystores. However, you can use custom keystore files instead. For more information about creating keystores, see the documentation of your certificate management tool.

Configuring the Internal Data Store HTTP Keystore

Use the following procedure to modify the keystore for the HTTP port of the Search Guard plugin.

To modify the keystore for the HTTP port of the Search Guard plugin

1. In Command Central, navigate to **Environments > Instances > All > Internal Data Store > Configuration**.
2. Select **Keystores** from the drop-down menu.
3. In the **Alias** column, click **HTTP_KEYSTORE** and then click **Edit**.
4. Specify values for the following fields:

Field	Description
Description	Optional. Specify a description for the keystore for the HTTP port of the Search Guard plugin.
Location	Required. Specify the absolute filepath to the Java keystore file as follows: <i>folder/sub_folder/filename</i> . The default value is: <code>../plugins/search-guard-5/sgconfig/node-0-keystore.jks</code>
Password	Optional. Specify the password for the keystore.

5. Optionally, click **Test** to verify that your configuration is valid.
6. Save your changes.
7. Restart the Internal Data Store instance.

Configuring the Internal Data Store TCP Keystore

Use the following procedure to modify the keystore for the TCP port of the Search Guard plugin.

To modify the keystore for the TCP port of the Search Guard plugin

1. In Command Central, navigate to **Environments > Instances > All > Internal Data Store > Configuration**.
2. Select **Keystores** from the drop-down menu.

- In the **Alias** column, click **TCP_KEYSTORE** and then click **Edit**.
- Specify values for the following fields:

Field	Description
Description	Optional. Specify a description for the keystore for the TCP port of the Search Guard plugin.
Location	Required. Specify the absolute filepath to the Java keystore file as follows: <i>folder/sub_folder/filename</i> . The default value is: <code>../plugins/search-guard-5/sgconfig/node-0-keystore.jks</code>
Password	Optional. Specify the password for the keystore.

- Optionally, click **Test** to verify that your configuration is valid.
- Save your changes.
- Restart the Internal Data Store instance.

Configuring the Internal Data Store sgadmin Keystore

The sgadmin tool authenticates itself against the SSL-enabled Internal Data Store with a keystore.

To modify the keystore for the sgadmin tool

- In Command Central, navigate to **Environments > Instances > All > Internal Data Store > Configuration**.
- Select **Keystores** from the drop-down menu.
- In the **Alias** column, click **SGADMIN_KEYSTORE** and then click **Edit**.
- Specify values for the following fields:

Field	Description
Description	Optional. Specify a description for the keystore for the sgadmin tool.
Location	Required. Specify the absolute filepath to the Java keystore file as follows: <i>folder/sub_folder/filename</i> . The default value is: <code>../plugins/search-guard-5/sgconfig/sgadmin-keystore.jks</code>

Field	Description
Password	Optional. Specify the password for the keystore.

- Optionally, click **Test** to verify that your configuration is valid.
- Save your changes.
- Restart the Internal Data Store instance.

Configuring the Internal Data Store Truststore

By default, Internal Data Store has a single pre-configured truststore for both the TCP and the HTTP ports.

If you use Internal Data Store in a production environment, replace the Internal Data Store default truststore file with a custom file. For more information about creating truststore files, see the documentation of your certificate management tool.

To modify the default Internal Data Store truststore

- In Command Central, navigate to **Environments > Instances > All > Internal Data Store > Configuration**.
- Select **Truststores** from the drop-down menu and click **Edit**.
- Specify values for the following fields:

Field	Description
Description	Optional. Specify a description for the truststore for the Search Guard plugin.
Location	Required. Specify the absolute filepath to the truststore file as follows: <i>folder/sub_folder/filename</i> . The default value is: <code>../plugins/search-guard-5/sgconfig/truststore.jks</code>
Password	Optional. Specify the password for the truststore.

- Optionally, click **Test** to verify that your configuration is valid.
- Save your changes.
- Restart the Internal Data Store instance.

3 Using the Command Line to Manage Internal Data Store

- Commands that Internal Data Store Supports 20
- Configuration Types that Internal Data Store Supports 21
- Run-Time Monitoring Statuses for Internal Data Store 21
- Lifecycle Actions for Internal Data Store 22

Commands that Internal Data Store Supports

Internal Data Store supports the Platform Manager commands listed in the following table. The table lists where you can find information about each command.

Commands	For more information, see...
<code>sagcc get configuration data</code>	For general information about the command, see <i>Software AG Command Central Help</i> .
<code>sagcc update configuration data</code>	For general information about the command, see <i>Software AG Command Central Help</i> .
<code>sagcc get configuration instances</code>	For general information about the command, see <i>Software AG Command Central Help</i> .
<code>sagcc list configuration instances</code>	For general information about the command, see <i>Software AG Command Central Help</i> .
<code>sagcc get configuration types</code>	For general information about the command, see <i>Software AG Command Central Help</i> .
<code>sagcc list configuration types</code>	For general information about the command, see <i>Software AG Command Central Help</i> .
<code>sagcc exec configuration validation update</code>	For general information about the command, see <i>Software AG Command Central Help</i> .
<code>sagcc exec lifecycle</code>	For general information about the command, see <i>Software AG Command Central Help</i> .
<code>sagcc get monitoring</code>	For general information about the command, see <i>Software AG Command Central Help</i> .

Configuration Types that Internal Data Store Supports

The Internal Data Store run-time component supports the following configuration types:

Configuration Type	Use to configure...
COMMON-CLUSTER	<p>Settings for an Internal Data Store cluster. You can configure the name of the cluster and the host and port pairs of the server endpoints of the cluster.</p> <p>Note: The changes that you make to a cluster configuration take effect after you restart Internal Data Store.</p>
COMMON-KEYSTORES	Configuration instance for a keystore alias that identifies a keystore file.
COMMON-PORTS	Configuration instances for HTTP and TCP ports.
COMMON-TRUSTSTORES	Configuration instance for a truststore alias that identifies a truststore file.
CUSTOM-PROPERTIES	Additional properties for the configuration of an Internal Data Store server.

Run-Time Monitoring Statuses for Internal Data Store

The following table lists the run-time statuses that the Internal Data Store run-time component can return in response to the `sagcc get monitoring state` command, along with the meaning of each run-time status.

Run-time Status	Meaning
ONLINE	The Internal Data Store instance is running.
STOPPED	The Internal Data Store instance is stopped.

Lifecycle Actions for Internal Data Store

The following table lists the actions that Internal Data Store supports with the `sagcc exec lifecycle` command. You can also perform these actions in the Command Central web user interface.

Action	Description
<code>start</code>	Starts the Internal Data Store instance.
<code>stop</code>	Stops the Internal Data Store instance.
<code>restart</code>	Restarts the Internal Data Store instance.