## 4.2 Installation

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.1 Software to be installed in advance</td>
<td>32</td>
</tr>
<tr>
<td>4.2.2 Start of the installation</td>
<td>32</td>
</tr>
<tr>
<td>4.2.3 License agreement</td>
<td>33</td>
</tr>
<tr>
<td>4.2.4 New installation or update</td>
<td>34</td>
</tr>
<tr>
<td>4.2.5 License file</td>
<td>34</td>
</tr>
<tr>
<td>4.2.6 Installation directory</td>
<td>36</td>
</tr>
<tr>
<td>4.2.7 Start menu item</td>
<td>36</td>
</tr>
<tr>
<td>4.2.8 Database server</td>
<td>37</td>
</tr>
<tr>
<td>4.2.9 Index proxy server</td>
<td>38</td>
</tr>
<tr>
<td>4.2.10 Web Logins</td>
<td>40</td>
</tr>
<tr>
<td>Spider</td>
<td>40</td>
</tr>
<tr>
<td>SpiderAdmin</td>
<td>42</td>
</tr>
<tr>
<td>4.2.11 Database names</td>
<td>44</td>
</tr>
<tr>
<td>4.2.12 Language and format settings</td>
<td>46</td>
</tr>
<tr>
<td>4.2.13 SMTP settings</td>
<td>47</td>
</tr>
<tr>
<td>4.2.14 Administration account</td>
<td>48</td>
</tr>
<tr>
<td>4.2.15 IIS configuration</td>
<td>49</td>
</tr>
<tr>
<td>4.2.16 Transfer directory</td>
<td>50</td>
</tr>
<tr>
<td>4.2.17 Installation</td>
<td>51</td>
</tr>
<tr>
<td>4.2.18 Activate the license</td>
<td>52</td>
</tr>
</tbody>
</table>

## 4.3 Advanced configuration

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1 Operation with domain account</td>
<td>54</td>
</tr>
<tr>
<td>Prepare SQL server</td>
<td>54</td>
</tr>
<tr>
<td>Grant IIS rights to the domain account</td>
<td>57</td>
</tr>
<tr>
<td>Adapt the identity of the application pools</td>
<td>61</td>
</tr>
<tr>
<td>Conversion of the access data</td>
<td>64</td>
</tr>
<tr>
<td>4.3.2 Subsequent setup of the index proxy</td>
<td>69</td>
</tr>
<tr>
<td>Configuration entries</td>
<td>69</td>
</tr>
<tr>
<td>IIS application connectionStrings.config</td>
<td>69</td>
</tr>
<tr>
<td>Settings in the registry</td>
<td>70</td>
</tr>
<tr>
<td>4.3.3 Conversion to SSL operation</td>
<td>71</td>
</tr>
<tr>
<td>Configure IIS default web site</td>
<td>71</td>
</tr>
<tr>
<td>Configuration entries</td>
<td>77</td>
</tr>
<tr>
<td>Restart the IIS</td>
<td>77</td>
</tr>
<tr>
<td>4.3.4 HTTP(S) Redirect</td>
<td>79</td>
</tr>
<tr>
<td>4.3.5 Setup of Active Directory login</td>
<td>83</td>
</tr>
<tr>
<td>Settings in Spider</td>
<td>83</td>
</tr>
<tr>
<td>IIS settings - Authentication</td>
<td>89</td>
</tr>
<tr>
<td>4.3.6 Info page - support.config</td>
<td>92</td>
</tr>
<tr>
<td>4.3.7 Available languages - culture.config</td>
<td>94</td>
</tr>
<tr>
<td>4.3.8 Settings in the Config table</td>
<td>95</td>
</tr>
<tr>
<td>4.3.9 Display of advanced error messages</td>
<td>95</td>
</tr>
<tr>
<td>4.3.10 Encryption of the configuration</td>
<td>99</td>
</tr>
<tr>
<td>4.3.11 Error handling system</td>
<td>103</td>
</tr>
</tbody>
</table>

## 4.4 Update

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.4.1 Start of the update</td>
<td>104</td>
</tr>
<tr>
<td>4.4.2 Update</td>
<td>105</td>
</tr>
<tr>
<td>4.4.3 Selection of the Instance</td>
<td>105</td>
</tr>
<tr>
<td>4.4.4 Database server</td>
<td>106</td>
</tr>
</tbody>
</table>
5 Spider Web API ................................................................. 113
  5.1 Technical information .................................................. 113
    5.1.1 REST API .......................................................... 113
    5.1.2 Version management ............................................. 113
    5.1.3 Tenant selection .................................................. 113
    5.1.4 Request ............................................................. 114
    5.1.5 Response ........................................................... 114
  5.2 Authentication ........................................................... 115
    5.2.1 Generation of tokens ............................................. 115
    5.2.2 Use of tokens ..................................................... 115
    5.2.3 Validity of tokens ............................................... 116
    5.2.4 Management of tokens ........................................... 116
  5.3 Admin section ............................................................ 116
    5.3.1 Mandator .......................................................... 116
    5.3.2 User ................................................................ 116
    5.3.3 Profile ................................................................. 117
  5.4 Entity section ............................................................... 117
    5.4.1 Entity access ....................................................... 117
    5.4.2 Entity history access .............................................. 117
    5.4.3 Entity document access ......................................... 117
    5.4.4 Entity reminder access ........................................... 117
    5.4.5 Entity relationship access ....................................... 118
  5.5 Search section ............................................................. 118
    5.5.1 Parameterization .................................................... 119
  5.6 Report section .............................................................. 120
    5.6.1 Parameterization .................................................... 121
  5.7 Meta section ............................................................... 122
    5.7.1 Mandator ............................................................ 122
    5.7.2 Admin ................................................................ 122
    5.7.3 Entity ................................................................. 123
    5.7.4 Search ................................................................. 123
    5.7.5 Report ................................................................. 124
  5.8 Version information ....................................................... 124
    5.8.1 Simple version information ..................................... 124
    5.8.2 Advanced version information .................................. 124
  5.9 Swagger .......................................................... 125
    5.9.1 OpenAPI Document ............................................... 125
    5.9.2 Swagger UI .......................................................... 125
  5.10 Web API documentation .................................................. 128
  5.11 Spider Web API Explorer ................................................ 132
    5.11.1 Expected users ..................................................... 132
    5.11.2 Authentication .................................................... 132
    5.11.3 Session parameters (tenant, language, version) .......... 133
    5.11.4 Communication with the Spider Web API .................. 133
      Response ................................................................. 133
      Response model ....................................................... 133
    5.11.5 Web API Explorer sections .................................... 135
      Search API ................................................................ 135
      Report API ................................................................ 136
      Entity API .................................................................. 141

6 Software Services (Catalogs and Recognition) ......................... 152
  6.1 System requirements ....................................................... 152
## 6.1 Application server

6.1.1 Application server .................................................................................................................. 152
6.1.2 Database server ......................................................................................................................... 153

### Required database

6.1.2.1 Required database ............................................................................................................... 153

### Required SQL user

6.1.2.2 Required SQL user .............................................................................................................. 153

### Overview of required rights

6.1.2.3 Overview of required rights ............................................................................................... 154

## 6.2 Installation

6.2.1 Start of the installation ............................................................................................................. 155
6.2.2 License agreement ...................................................................................................................... 156
6.2.3 License file ............................................................................................................................... 156
6.2.4 Installation directory ............................................................................................................... 158
6.2.5 Database server ....................................................................................................................... 159
6.2.6 Database & Data Receiver ...................................................................................................... 160
6.2.7 SQL login, service user ........................................................................................................... 161
6.2.8 Summary ................................................................................................................................. 162
6.2.9 Installation ............................................................................................................................... 163

## 6.3 Advanced configuration

6.3.1 Data Receiver ......................................................................................................................... 165

### SSL Secured Transmission

6.3.1.1 SSL Secured Transmission ............................................................................................... 165

## 6.4 Update

6.4.1 Start of the update .................................................................................................................... 169
6.4.2 License agreement .................................................................................................................... 170
6.4.3 License file .............................................................................................................................. 171
6.4.4 Installation directory ............................................................................................................... 173
6.4.5 Database server ...................................................................................................................... 173
6.4.6 Summary ................................................................................................................................. 175
6.4.7 Installation ............................................................................................................................... 176

## 7 Data center module (nova ratio appliance)

7.1 Sizing of the virtual machine ...................................................................................................... 178

## 8 Log files

8.1 Brainware.log ............................................................................................................................ 185
8.2 Smart-Inspect log files (*.sii) .................................................................................................... 185
1 General

In this chapter

1.1 Typographical conventions

This manual uses various formats to highlight certain terms and actions. Specific notes and tips are shown with a different background color, according to their importance.

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold font</strong></td>
<td>Elements in the software or in the operating system, such as menu items, buttons or elements of a selection list.</td>
</tr>
<tr>
<td><em>Italic font</em></td>
<td>Emphases (important details) and links to other chapters or documents.</td>
</tr>
</tbody>
</table>
| Triangle symbol "\cell{triangle}

Instruction step |
| Angle bracket ">" | Command menu sequences, e.g. `File > Open`                                    |
| **System font** | Directories, code and script samples.                                         |
| CAPITAL LETTERS | Key names, e.g. `SHIFT`, `CTRL`, or `ALT`.                                    |
| **KEY+KEY**    | Key combinations, i.e. the user has to hold one key and press another simultaneously, e.g. `CTRL+P` or `ALT+F4`. |

**Note**

Used for notes or tips which facilitate the work or for additional information which enhances understanding for the product.

**Important**

Information which should be observed by the user, because otherwise problems or additional work may be caused in operation.

**Attention**

Information which should be observed by the user in order to prevent malfunctions of the system (crashes, data loss, system failure).

1.2 Help

Please visit our Website for additional information and support. Here you can find all documents, a Knowledgebase as well as a support form if you have questions for our specialists.

1.2.1 Support

The support page features a link to the KnowledgeBase, the support form and information about our customer service.

- Open www.brainwaregroup.com in your browser and click on Support and KnowledgeBase on the right side.
- Start your search in the KnowledgeBase where you can find a list of the most common support cases.

If nothing matches your search criteria, you may use the support form for advanced information. Please provide a detailed description of your problem so that our specialists can help you as quick as possible.

- Click on Support Form.
Please fill in at least the fields marked with an asterisk (*) and click **Send Question**. You will receive a confirmation that your question has been received in the system.

The support page contains the telephone numbers necessary for telephone contacts.

### 1.2.2 Documentation

(German) A separate download area is available on our web site for the currently available documentation. This area contains all manuals in PDF and CHM format in German and English language. At present, some of the technical manuals are only available in English.

- Open [http://www.brainwaregroup.com](http://www.brainwaregroup.com) in your browser and click on **Downloads + Licenses** on the right side.
- Click on **Login**, enter your **User name** and **Password** and then click on **Register**.
- Please select **Documentation** as download type, then select the desired product and click on **Search**.
  - An overview of all available documents will be displayed.
- Click on the desired format and language to download the PDF/CHM file in the desired form.

You will find the Acrobat Reader on our support page or directly under [www.adobe.com](http://www.adobe.com).

### 1.2.3 Training information

brainwaregroup is taking all efforts to ensure that our products and solutions will be used and operated in an appropriate, qualified and proper way. Therefore, we are offering various training courses. You can find all information about training types and dates under the Training [https://www.brainwaregroup.com/de/support/trainings/](https://www.brainwaregroup.com/de/support/trainings/).
2 Introduction

In this chapter

Chronological order for new installations ............................................................................. 9

This document describes:

• System Requirements
• Installation
• Update
• Configuration of the products
  • Spider
  • Recognition

2.1 Chronological order for new installations

For a new installation, you have to observe the following installation order:

➢ Enterprise Services Infrastructure (ESI)
➢ Spider
➢ Software catalog
➢ Recognition

To read and transfer data from inventory systems, the Spider Data Collector (SDC) should be used.

Notes for the installation and setup are described in a separate document (Spider Data Collector - UserManual).
3 GDPR requirements in Spider

In this chapter

Personal data ................................................................................................................................................. 10
Personal data fields related to selected Spider data objects ............................................................................. 11
Principles relating to processing of personal data (Article 5 GDPR) ................................................................ 14
Lawfulness of processing (Article 6 GDPR) .................................................................................................. 17
Data protection by design and by default (Article 25 GDPR) ......................................................................... 17
Conditions for consent (Article 7 GDPR) ..................................................................................................... 18
Information obligation (Article 13 and 14 GDPR) ........................................................................................ 19
Records of processing activities (Article 30 GDPR) ..................................................................................... 19

3.1 Personal data

The European General Data Protection Regulation, Article 4, No. 1 GDPR provides the following definition:

"personal data means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

With regard to the Spider products, this means that a variety of modules, processes, and reports are affected by the establishment of a GDPR conformity. However, data to which the GDPR does not apply or which is subject to other legal foundations is not subject to any changes. This, for example, includes data of juristic persons.

3.1.1 Which data categories are processed in Spider products?

Within the spider products, the following data categories are processed by default:

- personal information (e.g. name, surname),
- contact information (e.g. email addresses, phone numbers),
- domain information (e.g. domain login, active directory identities, user logged in last, main user or IP addresses)
- and partial company service information (e.g. date of joining/leaving the company or personnel numbers).

The actually available data fields for personal data must be checked and documented on the customer side in case of individual adjustments. This is true in particular for possible additional data categories.

3.1.2 Special categories of personal data (Article 9, Section 1 GDPR)

In addition to the abovementioned data, the GDPR (Article 9, Section 1) specifies special categories of personal data which must not be processed on principle.

By default, Spider products do not contain any such special data categories.

Individual customer expansions must be checked!

In case of customer-specific adjustments there is a possibility that personal data belonging to special categories has been incorporated into Spider products. This may e.g. be the case in case of additional fields or the integration of third-party systems with personal data belonging to special categories. In this case, a customer-specific evaluation, documentation, and definition of necessary measures is required e.g. when processing personal data of minors or ad-
ditional information such as date of birth or religion. This applies in particular to customers who use our products to collect, store or process specific genetic, biometric, or other health-related data or features.

3.1.3 Processing of personal data (Article 4, No. 2 GDPR)

With regard to risk and compliance checks, it may be required to provide information on the processing of personal data in Spider products. When asked whether a corresponding processing takes place, this must be affirmed. The definition in Article 4, No. 2 GDPR clearly states:

"Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

In Spider products, personal data belonging to defined data categories are being processed. Without processing of such data, Spider products would be non-functional or their functions would be significantly limited.

3.2 Personal data fields related to selected Spider data objects

The following chapters show the specific fields of the data objects in which personal data is being stored. Since the Spider data model can be individually supplemented via parameter definition, this will only cover the standard version which cannot be changed in case of full update editions only. In case of flex editions, inspection and documentation must always be carried out in a customer-specific manner.

3.2.1 Personal data related to employees

Employee master data is usually imported into Spider from third-party systems. The system most frequently used for this purpose is Microsoft Active Directory.

The following data categories are stored in the employee data object:

- personal information (e.g. name, surname)
- contact information (e.g. email address, phone number)
- domain information (e.g. domain login, active directory identities, main user)
- partial company service information (e.g. date of joining/leaving the company)

The following fields are used for an employee. The scope has been reduced to the extend absolutely necessary. The main purpose here is to display the name of an employee as well as their identification in case of an import or the identification and the connection with the technical inventory of systems by means of domain identifiers. Since data from Microsoft Active Directory is being linked frequently and the interface as well as the data integration are included in the standard version of the product, the field names of Microsoft Active Directory are indicated as well. The columns to be exported can be set via the Active Directory Connector. By default, only the following fields are enabled:

- LastName (Active Directory: GivenName)
- Firstname (Active Directory: Surname)
- DomainLogin (Active Directory: SAMAccountName)
- Fullname
- EmailAddress (Active Directory: EmailAddress)
- EmploymentTypeID – categorization such as internal/external
- UserPrincipalName (Active Directory: UserPrincipalName)
- swrADUserObjectID – internal ID in recognition DB
- ExternalReference – identification in a third-party system
The following fields are no longer part of the standard configuration and will be removed when updating full update editions to Spider 6.4. The fields remain in the data table. Any permissions as well as visibility have been removed. In case of a customer-specific use which justifies the processing of such data, the fields can be enabled in the flex edition:

- Title
- StaffNo (Active Directory: StaffNo)
- PhoneNo (Active Directory: PhoneNo)
- MobilePhoneNo (Active Directory: MobilePhoneNo)
- DateOfEntry
- DateOfEmission
- FaxNo
- PrivatePhoneNo
- Department
- Location
- Country
- CountryCode
- State
- StreetAddress
- PostalCode

An index-based search is mapped via OneSearch. Employee data is indexed. OneSearch is available for all Spider users – it is not possible to restrict permissions to fields or data sets. Thus, only the following fields will be indexed for search and display via OneSearch in the future:

- LastName (Active Directory: GivenName)
- Firstname (Active Directory: Surname)
- DomainLogin (Active Directory: SAMAccountName)

Furthermore, the following field will be indexed. This is done for cross-module integration.

- EmailAddress (Active Directory: EmailAddress)

### 3.2.2 Personal data related to assets

Asset data processed in Spider is usually imported from and kept up to date based on inventory systems. Certain fields may directly contain personal data (e.g. LastLoggedOnUser). Other fields may contain technical identifiers which may be used to obtain information on the natural person.

The following data categories are stored in the asset data object:

- domain information (e.g. LastLoggedOnUser, host name, IP addresses, UUID)

The following fields are technical identifiers or identification fields which are required for processing and identification. These are essential and cannot be disabled.

- Hostname
- AssetNo
- UUID
- URN
- ID
The following fields contain personal domain information from user accounts.

- LastLoggedOnUser
- PrimaryUser (detected main user)

LastLoggedOnUser may be used to obtain information on a Microsoft Active user account which is linked to a natural person. This is resolved in Spider. These fields are required for several reasons. Important in particular are the requirements for mapping of user-based license metrics and the necessity for determination of main users on a device. These are essential and cannot be disabled in Spider. However, if no LastLoggedOnUser data is provided by a supplying system, user-based license mapping cannot be carried out.

The following fields contain additional technical information which does not have any specific use in the standard version. These fields are no longer part of the standard configuration and will be removed when updating full update editions to Spider 6.4. The fields remain in the data table. Any permissions as well as visibility have been removed. In case of a customer-specific use which justifies the processing of such data, the fields can be enabled in the flex edition:

- IPAddressV4
- IPAddressV6
- MacAddress 1-4

An index-based search is mapped via OneSearch. Asset data is indexed. OneSearch is available for all Spider users – it is not possible to restrict permissions to fields or data sets. The following fields are indexed for search and display via OneSearch:

- Hostname
- AssetNo
- UUID

### 3.2.3 Personal data related to Spider users

A Spider user account is required in order to access data in Spider. The user accounts can be granted rights to functions and data in Spider by means of a permission concept.

The following data categories are stored in the employee data object:

- personal information (e.g. name)
- contact information (e.g. email address)
- domain information (e.g. login)

The following data fields are provided for the user object and required for identification, display, and use in Spider.

- Login
- RealName

Furthermore, it is recommended to register an email address. The email address is absolutely necessary for using the 'password forgotten' function for Spider-internal user accounts.

- EmailAddress

It is possible to either create Spider-internal user accounts or link a Microsoft Active Directory via which user accounts which belong to AD groups intended for this purpose are transferred automatically. When using user accounts from Microsoft Active Directory, the SAMAccountName is used as LoginName. In case of Spider-internal user accounts, it is recommended to use automatically generated login identifiers in order to make it more difficult to obtain information on a natural person (pseudonym).
In Spider, the login is recorded in the following situations/locations:

- The login is stored for each data object which has been created or changed by a user.
- The login is stored in the change histories of any changes which have been initiated by the user.

Furthermore, an employee master data set can be linked to a Spider user account. In case of an Active Directory account, the master data set can be linked automatically.

### 3.2.4 Personal data related to contact persons

In contract management, so-called contact persons can be manually registered in relation to contractors. These contact persons are natural persons. The data processing of such data is subject to the requirements of the GDPR. Such data must only be stored with consent of the data subject or on a contractual basis. Compliance with the requirements must be ensured on the customer side or in the accompanying processes. If this cannot be ensured, this area should be disabled entirely.

The following data categories are stored in relation to a contact person:

- personal information (e.g. name, surname)
- contact information (e.g. email address, phone number)
- organization information (e.g. function)

The intended use is to facilitate contact with the responsible contact partner of a contractor.

Since any desired fields, which may contain personal data, can be added via the Spider meta data model, this document will only cover those fields which are included in the standard version. In case of full update systems, where the entire configuration is updated and no additional fields can be added, the version corresponds to the standard scope. For all other systems, the specific parameterization must be documented in a customer-specific manner.

The following fields are provided in case of the standard configuration:

- LastName
- FirstName
- Title
- Phone
- Fax
- Email
- MobilePhoneNo

An index-based search is mapped via OneSearch. Data of contact persons is not indexed.

### 3.3 Principles relating to processing of personal data (Article 5 GDPR)

The Spider products are used for different business processes. Compliance with the requirements of the GDPR depends on multiple factors. The following, frequently occurring factors shall be mentioned as examples:

- Type and characteristic of the accompanying or underlying business processes
- Scope of the customer-specific expansions or characteristics in the use of the Spider products
- Extent of the inclusion of personal data from external systems and the design of the interfaces
An evaluation which only relates to the product standard is insufficient. A general statement on the compliance with the different GDPR requirements of the Spider product in a customer environment must always be checked in a customer-specific manner due to the options for flexible adjustment. The assessments in this document refer to the basic standard functions of the Spider products.

The spider products will technically support the different GDPR requirements in accordance with Article 5. In addition to mere compliance with the requirements, we are also aiming for simplification as well as additional advantages which are achieved with the implementation of our products. Any requirements and improvements identified based on experiences made with our customers will be taken into account and implemented in future product versions.

### 3.3.1 Adequacy and relevance of personal data as well as limitation of their processing to the extend absolutely necessary (Article 5, No. 1, lit. c GDPR)

In the products, only such personal data which is required for the underlying business processes and functions shall be processed.

In case of customer-specific adjustments or extensions of the Spider products and when linking Spider products with third-party systems (e.g. Microsoft Active Directory) which provide personal data, these principles must be checked and it must be ensured that these are observed individually.

The standard configuration has been reworked with regard to the limitation to the extend absolutely necessary. For the employee data object in particular, several fields have been removed from the standard version.

### 3.3.2 Adequate storage of personal data as well as their possible anonymization (Article 5, No. 1, lit. e GDPR)

Erasure functions are provided for managed personal data which do not depend on supplying systems and which are no longer considered necessary for the underlying business process (e.g. an employee leaving the company). Functions for anonymization, for example, for statistical purposes are not provided. Thus, the data must be physically erased. The erasure of the data must be ensured in a customer-specific manner.

### 3.3.3 Rights of the data subject

**Right of access by the data subject (Article 15 GDPR)**

Data subjects have a general right to obtain confirmation as to whether their personal data is being processed. The right to obtain information can be complied with on principle using the current product versions.

**Information page for employees**

The personal data of data subjects (e.g. employment data) can be viewed and printed out via the information page. For this purpose, a new page (EmployeeEditGDPRInfo) for which access rights can be granted individually has been added with Spider 6.4. This page shows all fields of the employee object as well as any assets of the employee.

**External contact persons**

Registered data of a contract person can be viewed via the details form. It must be ensured that the user who compiles the fields for an information request has the access rights for all fields which contain personal data.

**Information page for Spider users**

Spider users are able to view their own personal data via the user settings.
**Rectification or erasure of personal data (Article 5, No. 1, lit. d GDPR)**

In Spider, personal data can be managed, changed, and also erased on principle.

For data which is provided by supplying systems, changes can usually not be carried out in Spider since such data is overwritten on a regular basis. A change of such data must be carried out in the respective source systems.

In case of Spider products, the erasure of personal data which is provided by external systems cannot be solved in a uniform manner. One reason for this are possible legal storage periods. Automatic erasure of data must always be determined and set by the customer.

The right to rectification and the right to erasure are covered separately in the following sections.

**Right to rectification (Article 16 GDPR)**

In Spider products, options for rectification of personal data are provided on principle. These may be reserved to permission groups defined via the permission concept.

When personal data is provided via third-party systems, the permissions must be defined in the third-party system.

Changes to personal data will only apply from their date of entry or application. Thus, change histories will not be affected.

**Right to erasure (Article 17 GDPR)**

In Spider products, options for erasure of personal data are provided on principle. These may be reserved to permission groups defined via the permission concept.

The erasure is carried out in two steps: When erasing a data object, the data object is erased from the data table and moved to a recycle bin. The recycle bin is also available in the databases in the form of a table. While the data set is no longer present in the data tables, it is still physically stored in the database. The cleansing of the recycle bin – physical erasure from the database – is carried out by the product. The storage time in days can be set.

When the recycle bin is cleansed, any change histories will be cleansed as well. Data sets with personal data are only considered physically deleted after the recycle bin has been cleansed.

Backup strategies and storage times for the backups must be taken into account in a customer-specific manner.

**Peculiarity of personal data from linked third-party systems**

When personal data is provided by third-party systems, the erasure must be carried out in the third-party system. In case of Spider products, the erasure of personal data which is provided by external systems cannot be solved in a uniform manner and can thus not be included in the standard product. For erasure of personal data, factors such as legal storage periods must be taken into account. Thus, erasure must be realized based on the linked third-party systems and the business process type.

**Right to restriction of processing (Article 18 GDPR)**

Since the legitimacy of processing in accordance with Article 6, No. 1 lit. f GDPR, among others, is assumed and, thus, legitimate reasons may outweigh the right to restriction, no dedicated technical measures need to be taken.

**Notification obligation (Article 19 GDPR)**

The notification obligation in case of any change of personal data must be taken into account in the accompanying processing processes (e.g. account management) on the customer side. This is a clear recommendation. It would probably be irritating for the affected persons (employees) in an organization and ultimately cause disproportional ef-
fort for the organization if any system would automatically inform the persons affected on changes regarding the pe-
sonal data, in particular in case of indirect use of these data from a source system.

If automatic notification by the Spider system is desired, this must be realized by means of a customer-specific expan-
sion and a corresponding setup. The product-integrated Alert&Reporting system, which dynamically sends daily emails
based on prepared database views, can be used for this purpose. This way, the email recipients may be set dynamically
depending on the data set. As a data basis for the evaluation of changes, the Spider change histories may be used.

### Right to data portability (Article 20 GDPR)
A data portability of personal data is not relevant since Spider products are used for internal company processes and
systems only. If any data shall be transmitted, the data can be accessed via a REST API.

### Right to object (Article 21 GDPR)
Since the legitimacy of processing in accordance with Article 6, No. 1 lit. f GDPR, among others, is assumed and, thus,
legitimate reasons may outweigh the right to object, no technical measures are taken.

### Suitable methods for demonstrating compliance with the requirements in accountabil-
ity cases (Article 5, No. 2 GDPR)
Changes to personal data can be viewed via the change histories for which separate permissions may be given.

### 3.4 Lawfulness of processing (Article 6 GDPR)
The lawfulness of the processing of personal data in Spider products is given by the legal foundations provided in the
following articles:

**Article 6, No. 1, lit. c GDPR**
"Processing is necessary for compliance with a legal obligation to which the controller is subject."

**Article 6, No. 1, lit. f GDPR**
"Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except
where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which re-
quire protection of personal data, in particular where the data subject is a child."

In this case, both passages implicitly mainly refer to the obligations from the German Civil Code (BGB), the German
Commercial Code (HGB), the Law Against Unfair Competition, and the German Copyright Act (UrhG).

### 3.5 Data protection by design and by default (Article 25 GDPR)
Spider products and infrastructure products used (e.g. Microsoft SQL Server) include different technical functions for
supporting technical and organizational measures. The specific technical and organizational measures must be deter-
mined in a customer-specific manner.

#### 3.5.1 Confidentiality (Art. 32, Section 1, lit. b GDPR)
- **Access control**: e.g. no unauthorized access to the data processing systems
  (to be ensured by the customer)
- **Access control**: no unauthorized system use by means of passwords
  (to be ensured by the customer)
- The data is processed in Microsoft SQL Server databases.
• Certain data is also stored in the index (ESI).

• **Access control**: no unauthorized reading, copying, changing, or removal within the system
  - Access for writing/changing of data is controlled via a role-based Spider permission concept.
  - Thus, direct access of users to the SQL server should be prevented by all means since it is not protected by Spider permission checks.

• **Separation control**: separate processing of data which has been obtained for different purposes; e.g. multitenancy
  - In case of multitenancy systems, a tenant ID is registered for each data set. Segregation of tenants is carried out when accessing the data via the Spider business logic. Users can only access data from a current session for which they have access.
  - Within a tenant, objects and their data can be assigned to business units. Users can only access the data of objects from business units for which they have permission.

### 3.5.2 Integrity (Art. 32, Section 1, lit. b GDPR)

• **Transfer control**: No unauthorized reading, copying, changing, or removal during electronic transfer or transmission; e.g. encryption, connection encryption (HTTPS) (to be ensured by the customer)
  - We strongly recommended using https for accessing the Spider Web User Interface (Web UI) and the Web API.
  - When sending data exports from the Spider system, the customer must ensure transfer control by means of suitable, technical, organizational measures.

### 3.5.3 Availability and resilience (Art. 32, Section 1, lit. b GDPR)

• **Availability control**: Protection against random or purposeful destruction or loss; e.g. backup strategy, uninterruptible power supply (UPS), virus protection, firewall, reporting channels, and emergency plans (to be implemented by the customer)

### 3.6 Conditions for consent (Article 7 GDPR)

If personal data of the data subject is collected directly via software, technical means for giving consent as well as for recording and explaining this action must be provided. Also, the data subject must be able to withdraw their consent under the described conditions.

#### 3.6.1 Self-service functions

Self-service functions by means of which a user (data subject in the sense of the GDPR) directly registers their personal data must comply with the conditions for consent. In the standard Spider product, there is no direct registration of data by the data subject. Most of personal data is taken from external systems and processed in Spider. If self-service functions are possible due to customer-specific extensions, appropriate measures for fulfilling the requirements must be taken by the customer.

When processing employment data (e.g. Microsoft Active Directory), consent may be mapped via the accompanying processing processes or upstream information processes on the customer side.
3.6.2 Consent for personal data from external systems or for collection of additional data

When personal data from third-party systems (e.g. Microsoft Active Directory) is provided, consent must be obtained from the responsible authority.

For additional personal data which is entered into and processed in Spider, consent by the data subject is required. This must be ensured in the accompanying processing processes on the customer side.

3.7 Information obligation (Article 13 and 14 GDPR)

When personal data is collected directly or indirectly, the controller is obliged to inform the data subject about this action.

In case of the current product versions, the active information obligation can only be complied with by means of customer-specific settings and extensions. Email-based information procedures are often used to inform the data subjects. On principle, it is questionable whether it makes sense to actively notify the data subjects using Spider since the products are usually used for dedicated subtasks and indirectly use personal data relevant to the task from external systems.

3.7.1 Processing of employment data

For the quite common processing of employment data (e.g. from Microsoft Active Directory), we recommend ensuring compliance with the information obligation in the accompanying processing processes or the upstream information processes on the customer side.

3.7.2 Direct notification of the data subject

Should a direct notification of the data subject from the Spider system still be necessary, the specific information processes must be mapped in a customer-specific manner.

3.8 Records of processing activities (Article 30 GDPR)

In order to comply with the documentation obligations in accordance with Article 30 GDPR, it is necessary to, among other things, maintain a record of all processing tasks which use personal data. The record must be made available to the supervisory authority upon request (Article 30, Section 4 GDPR and Suitable Recital 82). Companies which are subject to German regulatory supervision must maintain the processing record in German (§23, Section 1 and 2 of the German Administrative Procedure Act (VwVfG)). An exception in accordance with Article 30, Section 5 GDPR is to be excluded even if the quantitative factor of less than 250 employees is given. This is a result of the required IT protocols which are essential for the proper functioning of the Spider products.

The processing record must be created in a customer-specific manner.
4 Spider

In this chapter
System requirements ................................................................. 20
Installation .............................................................................. 32
Advanced configuration ......................................................... 54
Update ..................................................................................... 104

4.1 System requirements

4.1.1 Application server

Operating system

<table>
<thead>
<tr>
<th>Operating system:</th>
<th>Windows Server 2016 Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported versions:</td>
<td>2019</td>
</tr>
<tr>
<td></td>
<td>2016</td>
</tr>
<tr>
<td></td>
<td>2012 / 2012 R2</td>
</tr>
</tbody>
</table>

Supported editions:

- Standard
- Datacenter

Microsoft .NET Framework

Microsoft .NET Framework Version 4.7.2

Microsoft Internet Information Server (IIS)

- Internet Information Service (IIS) Manager
- Installed role service "IIS Management Scripts and Tools"
### 4.1.2 Database - Microsoft SQL Server

<table>
<thead>
<tr>
<th>Recommended versions:</th>
<th>Microsoft SQL Server 2016 Standard (64 bit) or Microsoft SQL Server 2017 Standard (64 bit)</th>
</tr>
</thead>
</table>
| Supported versions:   | • 2019  
• 2017  
• 2016  
• 2014  
• 2012 |
| Supported editions:   | • **Standard** - for Spider environments with one mandator  
• **Enterprise** - for large multi-mandator-environments  
• **Express** ** - for very small environments; some restrictions will apply |
| Required settings:    | The TCP/IP protocol and Named Pipes must be activated for the SQL server in the SQL Server Configuration Manager.  
During installation the SQL server has to be run with Mixed Mode Authentication (SQL And Windows Authentication). After the first installation and changing database access to domain authentication, the SQL server can be changed to Windows Authentication only. |

**Note:**  
*The function Always On is not supported  
**The full text search requires an Express edition with Advanced Services.

For the editions Spider SAM, ITM or Enterprise, 8 databases are required:  
• Core  
• Core_TempDB  
• Asset  
• Licence  
• Contract  
• Recognition  
• SessionDB  
• Integration (optional)

For Spider Contract, 5 databases are required:  
• Core  
• Core_TempDB  
• Contract  
• SessionDB  
• Integration (optional)

**Pay attention to the following:**  
• The names can be chosen individually. The name may not start with a number.  
• All Spider databases have to have the same collation. It has to be a case-insensitive collation (CI-Collation), e.g. SQL_Latin1_General_CP1_CI_AS.  
• The databases must be completely empty.
• The rule for the Spider Core temporary database has to be observed, it is the core database name with an attached suffix of "_TempDB", e.g. SpiderCore_TempDB.

• The rule for the Spider Core SessionState database has to be observed, it is the core database name with an attached suffix of "_SessionState", e.g. SpiderCore_SessionState.

4.1.3 Indexing - OneSearch

With the OneSearch function, the brainwaregroup Enterprise Services Infrastructure (ESI) is introduced as an additional component which will be more and more integrated in future versions.

The indexing infrastructure can be installed on a Spider Application server or on a separate server.

• approx. 750 MB installation files (incl. embedded Java)
• >= 3GB HDD space for index files, depending on the data volume
• 1 to 1.5 GB RAM

Further information is to be found in the document "Brainwaregroup ESI Release Notes".

4.1.4 Hardware requirements

Regarding the hardware requirements for the application and database server, we would like to recommend an individual server sizing for medium to large system sizes.

The following general orientation values will apply for production instances. Smaller configurations can be used for test instances.

**Processor**

**Recommendation:** Quad Core Processor system with 2 GHz or higher

Small system: 1+ Quad Core processor(s)

Medium system: 2+ Quad Core processors

Large system: 4+ Quad Core processors

**RAM**

Small system: 4 - 8 GB RAM

Medium system: 8 - 32 GB RAM

Large system: 32 GB RAM min.

**Hard disk capacity**

Application directory: 300 MB

Database: Database and transaction memory are depending on the managed data, documents and change histories.

Backup memory: Depending on the backup strategy and based on the data volume of databases and transactions, a factor of 1-2 memory capacity must be reserved for back-ups.

Small system: 5 - 20 GB

Medium system: 10 - 50 GB
Large system: > 50 GB
4.1.5 Clients / Browser

Supported browsers

Internet Explorer
- Version 11
- Version 10
- *Older versions and compatibility levels are not supported.*

Edge

Firefox
- ab Version 38 (ESR)

Chrome
- ab Version 46

Note: Active Scripting (IE) or Java Script (Firefox) must be activated.

Recommended software

Microsoft Excel
- Viewing and editing of Excel files

PDF Viewer
- PDF Viewer, e.g. Acrobat Reader

4.1.6 Implementation system

The implementation system is a workplace system which can be used to run the Spider implementation.

The following software is required:
- Microsoft SQL Server Management Studio
- Microsoft Office (Word, Excel)
- PDF Viewer, e.g. Acrobat Reader
- Spider Administration Tool

The following access options must be enabled:
- Remote access to the application server
- Access to the Spider databases
4.1.7 Permission requirements

For the installation, configuration and realization of the application as well as the relevant interfaces, the following access rights and settings are required:

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
<td>SQL account for installations</td>
<td>Installation user. DBO- permissions only for the Spider databases.</td>
</tr>
<tr>
<td>Account</td>
<td>SQL accounts &quot;Spider&quot; and &quot;SpiderAdmin&quot;</td>
<td>Standard account for Spider. Receive the rights to the Spider databases during the setup.</td>
</tr>
<tr>
<td>Account</td>
<td>Domain Login account for the application server</td>
<td>Account with administrator rights on application server</td>
</tr>
<tr>
<td>Account</td>
<td>Interfaces for domain users</td>
<td>Permanent service account without password change / expiry policy for the continuous interfaces.</td>
</tr>
<tr>
<td>Network policy</td>
<td>Communication between application and database server</td>
<td>The two servers must be able to communicate if they are running on two different server platforms. SQL Standard Port 1433</td>
</tr>
<tr>
<td>FW policy</td>
<td>Configuration of firewall</td>
<td>Checking of the firewall configuration to make sure that the defined accesses to the external systems (incl. interfaces for the InventoryScanner) are enabled.</td>
</tr>
</tbody>
</table>

Please refer to the table below for the required rights for execution of the setup:

<table>
<thead>
<tr>
<th>Task</th>
<th>Rights to</th>
<th>Right(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating logins</td>
<td>Server</td>
<td>ALTER ANY LOGIN</td>
</tr>
<tr>
<td>Creating databases</td>
<td>Server</td>
<td>CREATE DATABASE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CREATE ANY DATABASE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ALTER ANY DATABASE</td>
</tr>
<tr>
<td>Creating extended properties</td>
<td>Database</td>
<td>ALTER</td>
</tr>
<tr>
<td>Setting up the SessionState database</td>
<td>Database</td>
<td>msdb -&gt; EXECUTE</td>
</tr>
</tbody>
</table>

**Required SQL users**

If the SQL installation user does not have the permission to create new logins on the database server, these logins must be created beforehand. 2 SQL users are required for the setup. The login data are requested during the installation. The setup will then grant the permissions to the Spider databases.

1. **Spider Login**

The Spider login is required as application login for Spider. The web application and the services are using this login for accessing the databases.

2. **Spider Admin login**

This user is intended for usage with the Admin tool.
4.1.8 Hardware-Scaling

Please find below the description of the system sizes and four different scenarios. These recommendations are based on experience values from numerous customer environments. For large systems, we would like to recommend an individual server sizing.

### System sizing

<table>
<thead>
<tr>
<th>Size</th>
<th>Product</th>
<th>Figures</th>
<th>Scenario(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>Asset</td>
<td>&lt; 5,000 Systems</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Contract</td>
<td>&lt; 2,500 Contracts</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td>Asset</td>
<td>5,000 – 20,000 Systems</td>
<td>1 or 2</td>
</tr>
<tr>
<td></td>
<td>Contract</td>
<td>2,500 – 10,000 Contracts</td>
<td></td>
</tr>
<tr>
<td>Large</td>
<td>Asset</td>
<td>&gt; 20,000 Systems</td>
<td>2, 3, or 4</td>
</tr>
<tr>
<td></td>
<td>Contract</td>
<td>&gt; 10,000 Contracts</td>
<td></td>
</tr>
</tbody>
</table>
Scenario 1: Database and application server in one system

- Database and application server reside on one system
- 64-bit system for application server and database
- Possible scaling of processors / cores and RAM
- Software Load Balancing (SLB): Requests are distributed to deployed processes
- For a virtual machine a good I / O performance for the database must be ensured
Scenario 2: Database and application servers on separate systems

- Database and application servers are located on separate systems.
- 64-bit systems for application server and database.
- Possible scaling via processors/cores and RAM per system.
- Software Load Balancing (SLB): Requests are distributed among the provided processes.
- For a virtual system, the database must have a good I/O performance.
Scenario 3: Databases are installed in an SQL cluster

- Based on the 2nd scenario
- The databases are installed in an SQL server cluster.
- Possible scaling via processors/cores and RAM per system.
- Software Load Balancing (SLB): Requests are distributed among the provided processes.
Scenario 4: Using a web farm

- Based on the 2nd and 3rd scenario
- A web farm is operated from multiple web nodes and one management node. The initial Spider web installation, License Service and Spider Services are located on the management node.
- Possible scaling of processors / cores and RAM per system
- A combination of Network Load Balancing of the web farm and Software Load Balancing of each web server on the web farm
- Software Load Balancing (SLB): Requests are distributed to deployed processes
4.2  Installation

4.2.1  Software to be installed in advance

If the Index Proxy functionality (part of ESI) is to be used with the Spider system, it must be installed in advance.

4.2.2  Start of the installation

Start the installation by executing Spider 6.x Setup.exe.

At first, you are asked to select the language for the installation assistant. To do this, click on the desired language in the selection box and confirm your input with "OK".
After that, the installation assistant for Spider will open. This assistant will guide you through the setup installation in the selected language. Click on "Next" to start the installation.

### 4.2.3 License agreement

In the next step, you are asked to read and accept the license agreement before starting the installation. The setup can only be continued after accepting the license agreement.
4.2.4 **New installation or update**

If an instance of Spider is already installed, you will be prompted to decide for one type of installation.

![New installation or update dialog](image)

4.2.5 **License file**

Select the matching license file to continue the setup. The setup cannot be continued without the license file.

![License file dialog](image)
Click on "..." Button:

Select the license and then click "Open".

The selected license will be loaded and its details are shown.

---

**Note**

If a license is found in the same directory which has been used to start the setup, it will be loaded automatically into the dialog (if valid).
4.2.6 **Installation directory**

In the following step, you can select a target directory for the installation. You may change the proposed default path.

![Installation directory setup](image)

**4.2.7 Start menu item**

Here, you can determine the folder used by Spider for the start menu.

![Start menu item setup](image)
4.2.8  Database server

In the following step, the installation assistant will ask you to specify the name and the instance of a Microsoft SQL Server, on which the Spider databases are to be installed.

The user, with which the connection is established, can either be the logged-in (Windows) user or an SQL user.

To be able to use an SQL user, you must tick the check box **Use SQL user for database connection** and fill in the fields **User name** and **Password** with the desired data.
Note  The users have to be set up beforehand on the database server with the corresponding rights. Depending on the rights of the user, the subsequent dialogs will show different options.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL server name</td>
<td>Name of the SQL server, including instance name and port if required e.g. SQLSERVER\SQLINSTANZ,1234</td>
</tr>
<tr>
<td>Using SQL users for database connection</td>
<td>Select whether to use the logged-in domain user or an SQL user.</td>
</tr>
<tr>
<td>User name</td>
<td>Name of SQL user.</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the SQL user.</td>
</tr>
</tbody>
</table>

### 4.2.9 Index proxy server

Next, you can select whether the index proxy shall be configured during the setup.

The Index Proxy Server is part of the Enterprise Services Infrastructure (ESI).
By ticking the check box, the dialog will be activated and the required data can be entered.

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the index proxy</td>
<td>Activation of the dialog and query of the details</td>
</tr>
<tr>
<td>Name of the index proxy portal server</td>
<td>Name (FQDN) of the server, on which the index proxy is installed,</td>
</tr>
<tr>
<td>Port of the index proxy portal servers</td>
<td>Port (default: 7080) on which the index proxy reacts to requests</td>
</tr>
<tr>
<td>User name of the token service account</td>
<td>The client ID of the user which shall be used for the connection to the index proxy; the client ID has been created during the installation of the index proxy. Observe capital and small letters for the client ID!</td>
</tr>
<tr>
<td>Password of the token service account</td>
<td>Password belonging to the client ID.</td>
</tr>
</tbody>
</table>

After entering all data and selecting the **Next >** button, the connection to the index proxy will be checked. If an error should occur, the following message will be displayed.

- **Abort** - Cancel check and change values
- **Retry** - Try again with current values
- **Ignore** - Continue setup without check
### 4.2.10 Web Logins

#### Spider

The Spider Web login is a database user, which is required by the product components for accessing the databases. It is used by Spider Web and the Spider services.

For the Web Login, you can either create new users or use existing users if the SQL installation user possesses the rights to create a new login on the database server.

**Use an existing user**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use an existing user</td>
<td>Select the radio button to enter the data of an existing user</td>
</tr>
<tr>
<td>User name</td>
<td>The drop-down can be used to select the users found on the SQL server.</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the selected user</td>
</tr>
</tbody>
</table>

![Spider Web Login](image)
Create new user

Field | Description
--- | ---
Create new user | Select the radio button to let the setup create a new user.
User name | Desired user name
Password | Password for the user to be created.

Note
The option to create a user will only be provided if the corresponding rights have been granted. The users have to be set up beforehand on the database server with the corresponding rights.

Please select a password which corresponds to the complexity guidelines of your domain and/or your SQL server.
SpiderAdmin

The Spider admin login is used to access the Admin tool for administrating the database on the business layer.

As long as the SQL installation user possesses the rights for creating a new login on the database server, a new user may be created here. Otherwise, an existing user can be used.

Use an existing user

![Spider Admin Login](image)

Use an existing user

Select the radio button to enter the data of an existing user

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use an existing user</td>
<td>Select the radio button to enter the data of an existing user</td>
</tr>
<tr>
<td>User name</td>
<td>The drop-down can be used to select the users found on the SQL server.</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the selected user</td>
</tr>
</tbody>
</table>
Create new user

Field | Description
--- | ---
Create new user | Select the radio button to let the setup create a new user.
User name | Desired user name
Password | Password for the user to be created.

Note
If is only possible to create a user if the corresponding rights have been granted, i.e. users must be setup in advance on the database server with the appropriate rights.

Please select a password which corresponds to the complexity guidelines of your domain and/or your SQL server.
4.2.11 Database names

The databases can be either created in advance or by the setup.

**Note** The new databases are created using the default settings of the SQL server. If you need specific settings, the database must be provided in advance on the SQL server.

Select database created in advance

![Database selection screenshot]

Select the databases detected on the SQL server from the corresponding drop-down for each product.

**Note** The Integration database is only available for specific license types.

The following databases are required for the installation:

- Core
- Core_TempDB
- Core_SessionState
- Asset
- License
- Contract
- (Integration)

**Attention** The database names may be chosen freely; if the databases are created in advance, you have to observe that the TempDB and the SessionState databases must be created according to the template:

- `<Name of the core database>_TempDB`
- `<Name of the Core database>_SessionState`
Let databases be created by the setup.

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core, Asset, Contract, License, Integration</td>
<td>Name of the databases which are available for selection.</td>
</tr>
<tr>
<td>Prefix</td>
<td>Prefix which is put in front of all(!) database names.</td>
</tr>
<tr>
<td>Suffix</td>
<td>Suffix which is put at the back of all(!) database names.</td>
</tr>
</tbody>
</table>

The names of the product databases are pre-defined as

- Core
- Asset
- Contract
- License
- Integration

Changes can be made via adaptation of the prefix or suffix.

**Attention** Theoretically, also a mix of newly created and existing databases may be possible. However, we do not recommend to use a mixed creation of databases.
4.2.12 Language and format settings

The language selected for Settings determines the basic language with which the Settings are installed. These settings cannot be changed later on.

The default culture for Spider, however, may also be changed later on.
4.2.13 SMTP settings

The SMTP server is used to send the different e-mail reminders from Spider. You will need a user for access to the SMTP server.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP server</td>
<td>FQDN of the SMTP server</td>
</tr>
<tr>
<td>SMTP user</td>
<td>User ID used to authenticate oneself for the SMTP server</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the above mentioned user</td>
</tr>
<tr>
<td>Sender</td>
<td>Sending address used to send the e-mails of Spider.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>If selected, the communication with the SMTP server is tried with SSL (if supported by the SMTP server)</td>
</tr>
</tbody>
</table>

**Note** These data will be entered in each product and used by the Spider services to send e-mails. A later setup or change of the SMTP settings has to be made in each product.
4.2.14 Administration account

The Administrator account is the account for managing Spider. This account obtains administrative rights in parts of Spider and is available after installation for the access of the <Spider> Web.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>Login of the user with which a login to Spider-Web is possible.</td>
</tr>
<tr>
<td>User name</td>
<td>Name of the user</td>
</tr>
<tr>
<td>Password</td>
<td>Password used for creating the login.</td>
</tr>
</tbody>
</table>
4.2.15 IIS configuration

You can determine the IIS application name for the Spider Web, the default is "Spider". The Spider Web will then be available under http://server name/Spider.

All other settings result from the selected application name and cannot be altered. In this step, you can only set the encryption of the configuration files.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IIS application name</td>
<td>Name given to the IIS application in the course of the installation.</td>
</tr>
<tr>
<td>Encrypt configuration files.</td>
<td>By selecting the check box, the details, which are stored for the connection between &lt;Spider&gt; Web and database, will be encrypted.</td>
</tr>
</tbody>
</table>

**Note** Details for encryption and decryption of the IIS configuration can be found in chapter *Encryption of the configuration* (on page 99).
4.2.16  Transfer directory

In the last step of the installation, you will be asked to specify a directory for the file transfer. The transfer directory provides the working path for imports and exports of various services of Spider. Then click on "Install" to start the installation.
4.2.17 Installation

The installation assistant will now install Spider. This can take some time. Please wait, until the installation is completed.

The successful completion of the installation will be shown in the progress dialog.
The setup has been completed successfully and can now be closed.

After completion of the installation, a log file will be written. For details to the log files, please refer to chapter Log files (on page 185).

4.2.18 Activate the license

The installation of Spider requires a valid license. In order to be able to use Spider after the installation, this license must be activated. The license is activated via the license console (via Start menu -> Spider -> License Console).

Use the context menu to create a file for the license activation request. Select the item Save Activation Information File, save the created file and send it to brainwaregroup.
brainwaregroup creates an activation file, which is imported via the item **Import Activation Information File** of the context menu.

Spider is now ready to use. The first login on a client can be made with the user data used in the setup.
4.3 Advanced configuration

In this chapter, advanced configurations for Spider are described.

4.3.1 Operation with domain account

Alternatively to the operation with SQL users, Spider can also be operated with a domain user.

Please find following steps below for a more detailed explanation

- Preparation of the SQL server
- Permission of the IIS
- Adaption of the IIS application pool
- Conversion of the service accounts
- Conversion of the connection strings

Precondition:

- A domain account with user rights in the domain

Prepare SQL server

The desired user account must obtain the usage rights in SQL server.

- Start Microsoft SQL Server Management Studio and connect to the desired database [\Instance].
- Right click on Security > Logins > New Login
Enter the **Login name**:

![Login window with options]

- **Windows authentication**
- **SQL Server authentication**
  - **Password**:
  - **Confirm password**:
  - **Specify old password**
  - **Old password**:
  - **Enforce password policy**
  - **Enforce password expiration**
  - **User must change password at next login**
- **Mapped to certificate**
- **Mapped to asymmetric key**
- **Map to Credential**
  - **Mapped Credentials**
  - **Credential**
  - **Provider**

- **Default database**:
- **Default language**:

[OK] [Cancel]
Navigate to menu item **User Mapping**

![User Mapping screenshot]

Entering the **Roles memberships** for the Spider databases by setting the tick on **Map** and selecting the membership in the lower part of the dialog.

<table>
<thead>
<tr>
<th>Database</th>
<th>Database role membership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>public, sr_user</td>
</tr>
<tr>
<td>Contract</td>
<td>public, sr_user</td>
</tr>
<tr>
<td>Core</td>
<td>public, sr_user</td>
</tr>
<tr>
<td>Core_SessionState</td>
<td>public</td>
</tr>
<tr>
<td>Core_TempDB</td>
<td>public, sr_user</td>
</tr>
<tr>
<td>Integration</td>
<td>public, sr_user</td>
</tr>
<tr>
<td>License</td>
<td>public, sr_user</td>
</tr>
</tbody>
</table>

**Note** The Integration database is not included in all installations or can have another name.
Navigate to the menu item **Status** and check whether the connecting right has been granted and the login has been activate.

- Exit the dialog with **OK**.

**Grant IIS rights to the domain account**

- Start the **Management Control Panel** of the computer
- **Computer Management (local) > System Tool > Local Users and Groups > Groups**
Double click on the group IIS_IUSRS
- **Add...** Click on button

  ![Windows Server Management Console - IIS_IUSRS Properties](image)

  - **Select Users, Computers, Service Accounts, or Groups**
    - **Select this object type:** Users, Service Accounts, or Groups
    - **Enter the object names to select (examples):** `svc-TechAccount` (svc-TechAccount@domain)

- Enter the domain user name and then exit the dialog with **Check Names > OK**
➢ Exit the dialog with **OK** and close the **Computer Management**
Adapt the identity of the application pools

- Start the **Internet Information Services (IIS) Manager**
- **Start Page > Application Pools**
- Select the application pool
- Right click on the application pool and select **Advanced Settings...** from the context menu (the name of the application pool has been defined during the installation under **IIS configuration** (on page 49))
Select under **Process Model > Identity** the ... button.

Select the radio button under **Custom Account** and click on the **Set...** button.
Enter the user name and password of the domain user and click on OK.

Exit all dialogs with OK.
Repeat all previous steps with the application pool with suffix IndexAppPool.

To finish the process, restart the IIS with command iisreset.
Conversion of the access data

In order to use the domain user also for the connection, the different components must be informed about this.

Adapt service accounts

The Spider services must be adapted for the use with the domain user.

- Start the Management Control Panel of the computer

- Select Spider Service and open it with a double click
Go to the Log On ribbon, select This account and adapt the data of the domain user.

OK and exit the dialog.
Note  In some cases, dialogs may be displayed which inform about the fact that the user has been granted the Log-on-as-a-service right resp. that the service has to be restarted, before the change becomes active.

Repeat the procedure for all Spider services belonging to this instance(CoreServer_xx).

- Asset
- Contract
- Core
- License
- Integration (not always installed)

Attention  The services do not have to be started now, but only after the Connection Strings have been adapted.
Adapt the connection strings

The file ConnectionStrings.config is used for the access of application and services. This file must be adapted for each different component.

Storage locations of the connection strings

<table>
<thead>
<tr>
<th>Component</th>
<th>Storage location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spider Web</td>
<td>C:\Program Files\Spider\CoreServer_XX\Web_Settings\connectionStrings.config</td>
</tr>
<tr>
<td>SessionState</td>
<td>C:\Program Files\Spider\CoreServer_XX\Web_Settings\SessionState.config</td>
</tr>
<tr>
<td>IndexProxyApi</td>
<td>C:\Program Files\Spider\CoreServer_XX\IndexProxy_Settings\connectionStrings.config</td>
</tr>
<tr>
<td>Services</td>
<td>C:\Program Files\Spider\CoreServer_00\Services&lt;ServiceName&gt;\Spider.&lt;ServiceName&gt;.Service.Exe.config</td>
</tr>
</tbody>
</table>

The entries uid=... and pwd=... must be replaced by Integrated Security=True.

Spider Web and IndexProxyApi connectionStrings.config

```
<?xml version="1.0" encoding="utf-8"?>
<connectionStrings>
  <add name="CoreConnectionString" connectionString="server=.;
  database=SpiderCore;
    uid=Spider;
    pwd=abcde;
    application name=Spider;
    persist security info=True;
    packet size=4096"
    providerName="System.Data.SqlClient" />
</connectionStrings>
```

```
<?xml version="1.0" encoding="utf-8"?>
<connectionStrings>
  <add name="CoreConnectionString" connectionString="server=.
  database=SpiderCore;
    Integrated Security=True;
    application name=Spider;
    persist security info=True;
    packet size=4096"
    providerName="System.Data.SqlClient" />
</connectionStrings>
```

Session State Database

```
<?xml version="1.0" encoding="utf-8"?>
<SessionState mode="SQLServer" sqlConnectionString="Data Source=.
  Database=SpiderCore_SessionState;
  User Id=Spider;"/>
```
Attention

It could happen that the content of certain .config files is encrypted. The decryption process is described in chapter Encryption of the access data (see "" on page 99).
4.3.2 Subsequent setup of the index proxy

The subsequent setup of the index proxy installation can be carried out via a regular update. There, you will be prompted in each update to set up the Index Proxy (see "" on page 38) as long as this has not been done, yet.

If this is not working, execute the following steps:

**Configuration entries**

**Entries in the [dbo].[config] table in the Core database**

**Area:** Application.Indexing

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>True</td>
</tr>
<tr>
<td>IndexProxyEndpoint</td>
<td>http://&lt;ESIServer&gt;:&lt;Port&gt;/indexproxy/api/2/</td>
</tr>
<tr>
<td></td>
<td>e.g. <a href="http://sername.domain:7080/indexproxy/api/2/">http://sername.domain:7080/indexproxy/api/2/</a></td>
</tr>
<tr>
<td>PortalClientId</td>
<td>User name given in the ESI setup</td>
</tr>
<tr>
<td>PortalClientSecret</td>
<td>Password for user name given above</td>
</tr>
<tr>
<td>PortalEndpoint</td>
<td>http://&lt;ESIServer&gt;:&lt;Port&gt;/portal/api/2/</td>
</tr>
<tr>
<td></td>
<td>e.g. <a href="http://sername.domain:7080/portal/api/2/">http://sername.domain:7080/portal/api/2/</a></td>
</tr>
</tbody>
</table>

**IIS application connectionStrings.config**

The IIS application will be installed parallel to the instance of Spider (Path: ..\CoreServer_XX\IndexProxy\_Settings). In order to establish a connection between application and database, a so-called connectionStrings.config file must be created in the subfolder _Settings.

**Note** In case of a manual installation at a later time, the folder ".\Settings" must be created first.

The required values can be taken from the connectionStrings.config file of the Spider IIS application (Path: ..\CoreServer_XX\Web\_Settings).

**Login with integrated security**

```xml
<?xml version="1.0" encoding="utf-8"?>
<connectionStrings>
  <add name="CoreConnectionString"
    providerName="System.Data.SqlClient"
    connectionString="server=<SQL server>;
database=<Core database>;
    Integrated Security=True;
    application name=SpiderIndex;
persist security info=True;
packet size=4096"/>
</connectionStrings>
```
<connectionStrings>
  <add name="CoreConnectionString" providerName="System.Data.SqlClient"
       connectionString="server=<SQL server>;
database=<Core database>;
uid=<SQL User>;
pwd=<SQL User Password>
       Integrated Security=True;
application name=SpiderIndex;
persist security info=True;
packet size=4096" />
</connectionStrings>

**Login with SQL user**

```xml
<?xml version="1.0" encoding="utf-8"?>
<connectionStrings>
  <add name="CoreConnectionString"
       providerName="System.Data.SqlClient"
       connectionString="server=<SQL server>;
database=<Core database>;
uid=<SQL User>;
pwd=<SQL User Password>
       Integrated Security=True;
application name=SpiderIndex;
persist security info=True;
packet size=4096" />
</connectionStrings>
```

**Note**

If using SQL users, it might be desirable to locally encrypt the data. You can find the corresponding instructions in Encryption of the configuration (on page 99).

**Settings in the registry**

In order to prevent the setup form asking again for the details in the next update, some entries have to be made in the registry.

**Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\brainwaregroup\Spider\CoreServer_XX\IndexProxy

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>IndexProxyClientID</td>
<td>REG_SZ</td>
<td>&lt;User name for the connection with the ESI&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The password is not stored on purpose.</td>
</tr>
<tr>
<td>IndexProxyServerName</td>
<td>REG_SZ</td>
<td>FQDN of the ESI server</td>
</tr>
<tr>
<td>IndexProxyServerPort</td>
<td>REG_SZ</td>
<td>Port of the ESI server (standard: 7080)</td>
</tr>
<tr>
<td>UseIndexProxy</td>
<td>REG_SZ</td>
<td>1</td>
</tr>
</tbody>
</table>
4.3.3 Conversion to SSL operation

In order to protect the communication, accessing Spider via SSL can be enabled.

**Attention** The IIS application of the license service is not SSL-capable. Please find below information about how to configure this as an exception.

**Important** A prerequisite for the operation is a valid SSL certificate that is issued to the Spider application server

**Configure IIS default web site**

- Start the **Internet Information Services (IIS) Manager**
- **Select server > Server certificates**
Actions > Import

Select the certificate > Enter password > Select certificate store:  Web Hosting > OK

Default web site > Edit site > Bindings
This image shows the Internet Information Services (IIS) Manager interface. It displays the server and websites hierarchy. The selected site is `Default Web Site`. The `Site Bindings` window is open, showing bindings for `http` using port 80. The `IP Address` field is marked with an `*`.
Add... 

Add Site Binding

<table>
<thead>
<tr>
<th>Field</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>https</td>
</tr>
<tr>
<td>IP address:</td>
<td>All Unassigned, or if the server shall receive requests only from one IP address (from several configured addresses).</td>
</tr>
<tr>
<td>Host name:</td>
<td>Host name stored in the certificate</td>
</tr>
<tr>
<td>SSL certificate:</td>
<td>Select the corresponding certificate.</td>
</tr>
</tbody>
</table>

OK
Marking the **http** binding > **Edit**...

Enter localhost in "Host name:" to ensure that applications such as the license service or IndexProxyApi can continue to communicate with the local machine.
### Site Bindings

<table>
<thead>
<tr>
<th>Type</th>
<th>Host Name</th>
<th>Port</th>
<th>IP Address</th>
<th>Binding Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>https</td>
<td>server.domain.local</td>
<td>443</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>http</td>
<td>localhost</td>
<td>80</td>
<td>*</td>
<td></td>
</tr>
</tbody>
</table>

- **OK**

- **Close**
Now it is ensured that the server communicates externally via HTTPS, while HTTP is used for the local communication.

**Attention**
The communication with the license server via HTTP is a precondition for the setup to be able to update the system.

**Configuration entries**

Entries in the [dbo].[config] table in the Core database

**Area:** Application

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>http$://server.domain.local</td>
</tr>
</tbody>
</table>

server.domain.local must be replaced by the FQDN stated in the certificate.

**Restart the IIS**

To ensure that all changes are correctly accepted, the IIS must be restarted with the `iisreset` command.
Now, the communication with the Spider application via SSL is possible.
### 4.3.4 HTTP(S) Redirect

If the address of the IIS server is called up directly (Example https://server.domain.local), the IIS default web site will be displayed in general.

![Internet Information Services](https://example.com/image.png)

In order to ensure that the address of the IIS server will also show the Spider application, a redirection can be configured.

- Start the **Internet Information Services (IIS) Manager**
- **Default Web Site > IIS > HTTP Redirect**
- Enter the target web site (ensure correct HTTP/S) and click on **Apply**.
Note  Should the menu item HTTP Redirect be missing, the Roles feature may have to be installed:
Select server roles

Before You Begin
Installation Type
Server Selection

Select one or more roles to install on the selected server.

Roles
- Hyper-V
- MultiPoint Services
- Network Policy and Access Services
- Print and Document Services
- Remote Access
- Remote Desktop Services
- Volume Activation Services
- Web Server (IIS) (16 of 43 installed)
  - Default Document (Installed)
  - Directories (Installed)
  - HTTP Errors (Installed)
  - Static Content (Installed)
  - HTTP Redirection
- WebDAV Publishing
- Health and Diagnostics (1 of 6 installed)
- Performance (1 of 2 installed)
- Security (1 of 9 installed)

Description
HTTP Redirection provides support to redirect user requests to a specific destination. Use HTTP redirection whenever you want customers who might use one URL to actually end up at another URL. This is helpful in many situations, from simply renaming your Web site, to overcoming a domain name that is difficult to spell, or forcing clients to use a secure channel.
4.3.5 Setup of Active Directory login

In order to enable domain users to access the Spider system, the Active Directory may be used. The setup will require groups in the Active Directory, which are assigned to one or more Spider roles.

Settings in Spider

- Call of the Spider web site (as administrator)
- System > Active Directories > New

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login context</td>
<td>NetBios name of the domain</td>
</tr>
<tr>
<td>Prefix</td>
<td>Selected prefix for identification</td>
</tr>
<tr>
<td>Top level</td>
<td>LDAP entry of the top level of the domain to be connected.</td>
</tr>
<tr>
<td>User</td>
<td>AD user which is used to establish the connection to the AD.</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the above mentioned AD user</td>
</tr>
<tr>
<td>Menu</td>
<td>Default menu for this AD</td>
</tr>
<tr>
<td>Active</td>
<td>The Active Directory entry is active and can be used.</td>
</tr>
<tr>
<td>Only authentication</td>
<td>The AD will only be used for the authentication of the users; rights and roles are managed in Spider as usual.</td>
</tr>
</tbody>
</table>
- Test...

The connection to the active directory has been successfully established.

- Save

Data successfully saved!

- Ribbon Groups > Assign groups

- Enter domain user used for determination of the groups

- Search

Active directory groups
Highlight desired groups > Transfer

Active directory groups

7 results

- ADGroup
- CN=Users,CN=Built-in,DC=bwg,DC=corp
- CN=Domain Users,CN=Users,DC=bwg,DC=corp
- CN=ADGroup-Admin,CN=Users,DC=bwg,DC=corp
- CN=ADGroup-Reader,CN=Users,DC=bwg,DC=corp
- CN=ADGroup-User,CN=Users,DC=bwg,DC=corp

The selected groups have been ported.
Start

Selection of a group from Assigned groups
- **Ribbon mandator**

![Image of mandator ribbon]

- **Add mandator > Select mandator > Assign**

![Image of selecting a mandator]

- **Ribbon Roles**
Highlight desired roles > Add roles

This will complete the assignment of mandators and roles to an Active Directory group. If required, this must be repeated for other groups, mandators or roles.
IIS settings - Authentication

**Note** If the setting of the Windows authentication is not available, the role feature must be installed if required:

- Start the Internet Information Services (IIS) Manager
Select the server > Sites > Default web site > Spider Web site > Authentication
Set all authentication types except the **Windows authentication** to **Disabled**, and set **Windows Authentication** to **Enabled**.

To ensure that all changes are correctly accepted, the IIS must be restarted with the `iisreset` command.
4.3.6 Info page - support.config

In the delivery state, there is no information about the support on the Info page which can be reached by a click on the Info button in the menu or in the login screen.

Support
Before calling our support we suggest you to check with our comprehensive product documentation and consult our knowledgebase.

Could not find support information. Please contact your administrator.

Copyright
Copyright © Zuq, Switzerland 2001 - 2017, Brainware Consulting & Development AG
A Company of brainwaregroup. All rights reserved.
http://www.brainwaregroup.com

To store your own information there, the file support.config in the path <InstallDir>\Spider\CoreServer_XX\Web\_settings must be edited.

This file contains an XML structure, which can be used to store language-specific information.

```
<Intro>
  <LanguageCode>DE</LanguageCode>
  <Text>Before contacting our helpdesk regarding your support request, please first refer to the product documentation and our knowledge base.</Text>
</Intro>
```

The intro allows to show a general text on the info page. In addition, there are the contact entries which can be used to configure one or more contact types.

```
<Contact>
  <LanguageCode>DE</LanguageCode>
  <Name>Knowledgebase</Name>
  <Icon>SupportKnowledgebase</Icon>
  <Text>Knowledgebase</Text>
  <Url></Url>
</Contact>
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LanguageCode</td>
<td>The language abbreviation to be entered can be found in the column &quot;639-1&quot; on the page <a href="https://en.wikipedia.org/wiki/List_of_ISO_639-1_codes">https://en.wikipedia.org/wiki/List_of_ISO_639-1_codes</a>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Name</td>
<td>Entry which defines the type of the resource to be shown.</td>
</tr>
<tr>
<td></td>
<td>Page (a web site)</td>
</tr>
<tr>
<td></td>
<td>Form (a form on a web site)</td>
</tr>
<tr>
<td></td>
<td>E-mail (an e-mail address)</td>
</tr>
<tr>
<td></td>
<td>Phone (a phone number)</td>
</tr>
<tr>
<td>Icon</td>
<td>The icon to be shown, see table below.</td>
</tr>
<tr>
<td>Text</td>
<td>The text to be displayed</td>
</tr>
<tr>
<td>URL</td>
<td>If an entry of the type Page, Form, or Email has been made in the Name field, the target URL may be entered here. Caution, for an e-mail address, a mailto: must be put in front!</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Icon code</th>
<th>Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>SupportKnowledgebase</td>
<td>📖</td>
</tr>
<tr>
<td>SupportPage</td>
<td>🎯</td>
</tr>
<tr>
<td>SupportForm</td>
<td>🗂️</td>
</tr>
<tr>
<td>SupportEmail</td>
<td>📩</td>
</tr>
<tr>
<td>SupportPhone</td>
<td>📞</td>
</tr>
</tbody>
</table>

**Important** You can use only one "Name" per language code! The combination of LanguageCode and Name must be unique.

```xml
<Contact>
  <LanguageCode>DE</LanguageCode>
  <Name>Page</Name>
  <Icon SupportPage></Icon>
  <Text>Support page</Text>
  <Url>https://support.brainwaregroup.com/</Url>
</Contact>

<Contact>
  <LanguageCode>DE</LanguageCode>
  <Name>Form</Name>
  <Icon SupportForm></Icon>
  <Text>Support form</Text>
  <Url>http://support.brainwaregroup.com/form/</Url>
</Contact>

<Contact>
  <LanguageCode>DE</LanguageCode>
  <Name>Email</Name>
  <Icon SupportEmail></Icon>
  <Text>E-mail</Text>
  <Url>mailto:support@brainwaregroup.com</Url>
</Contact>
```
4.3.7 Available languages - culture.config

The languages available in the web can be configured in the file culture.config (Path <InstallDir>\Spider\CoreServer_XX\Web\settings).

```xml
<?xml version="1.0" ?>
<culture>
    <availableCultures>
        <clear />
        <add cultureCode="en-GB" />
        <add cultureCode="en-US" />
        <add cultureCode="en-ZA" />
        <add cultureCode="de-DE" />
        <add cultureCode="de-CH" />
        <add cultureCode="de-AU" />
        <add cultureCode="yes-JP" />
    </availableCultures>
    <defaultCulture cultureCode="de-DE" />
</culture>
```
A list of available culture codes can be found in the table on https://msdn.microsoft.com/library/ee825488.aspx, in the column Language Culture Name.

<table>
<thead>
<tr>
<th>English (United Kingdom)</th>
<th>Info</th>
<th>Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>English (South Africa)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deutsch (Deutschland)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deutsch (Schweiz)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deutsch (Österreich)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>日本語 (日本)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The list can be edited by adding or deleting entries.

The entry `<defaultCulture cultureCode="" />` determines which language will be shown when a user opens the page.

**Important** Adding a new language in the file culture.config does not mean that there are any translations for this language. If there are no translations for the culture code, terms of the default culture will be shown automatically.

### 4.3.8 Settings in the Config table

Via the settings in the Config table, it is possible to adjust the behavior of Spider. Not all entries can be edited via the Spider admin or the web frontend.

<table>
<thead>
<tr>
<th>Area</th>
<th>Key</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>BrowserEnableAutocomplete</td>
<td>True</td>
<td>False</td>
</tr>
</tbody>
</table>

### 4.3.9 Display of advanced error messages

The exception handling implemented in Spider enables the display of error messages on a specific error page. Due to security reasons, the page will not show all information about an exception. To display detailed error messages of the IIS, Spider must be configured with the following settings.
Therefore, some files must be modified with an editor:

```xml
<?xml version="1.0" encoding="utf-8"?>
<!--
For DEBUG switch customErrors mode to "Off" (with upper-case "O") and httpErrors errorMode to "Detailed" and then restart the ApplicationPool in IIS. Without a restart the changes will not be applied!

(An ApplicationPool restart can also be achieved by saving the Web.config file without any changes. The IIS recognizes the file has been saved and then restarts the application pool.)

If you encounter an HTTP 500 error message, ensure that httpErrors existingResponse is set to "Auto"!
-->

<customErrors
    mode="On"
    defaultRedirect="~/Info/Error.aspx">
    <!-- NEVER redirect a 401 error! This will cause various problems in the application! -->

    <error statusCode="403" redirect="/Default.aspx"/>
    <error statusCode="404" redirect="/Default.aspx"/>
    <error statusCode="405" redirect="/Info/Error.aspx?Category=8"/>
    <error statusCode="406" redirect="/Info/Error.aspx?Category=8"/>
    <error statusCode="412" redirect="/Info/Error.aspx?Category=8"/>
    <error statusCode="500" redirect="/Info/Error.htm"/>
    <error statusCode="501" redirect="/Info/Error.htm"/>
    <error statusCode="502" redirect="/Info/Error.htm"/>
</customErrors>.

<?xml version="1.0" encoding="utf-8"?>
<!--
For DEBUG switch customErrors mode to "Off" (with upper-case "O") and httpErrors errorMode to "Detailed" and then restart the ApplicationPool in IIS. Without a restart the changes will not be applied!

(An ApplicationPool restart can also be achieved by saving the Web.config file without any changes. The IIS recognizes the file has been saved and then restarts the application pool.)

If you encounter an HTTP 500 error message, ensure that httpErrors existingResponse is set to "Auto"!
-->

<customErrors
    mode="Off"
    defaultRedirect="/Info/Error.aspx">
```
<error statusCode="403" redirect="/Default.aspx" />
<error statusCode="404" redirect="/Default.aspx" />
<error statusCode="405" redirect="/Info/Error.aspx?Category=8" />
<error statusCode="406" redirect="/Info/Error.aspx?Category=8" />
<error statusCode="412" redirect="/Info/Error.aspx?Category=8" />
<error statusCode="500" redirect="/Info/Error.htm" />
<error statusCode="501" redirect="/Info/Error.htm" />
<error statusCode="502" redirect="/Info/Error.htm" />

</customErrors>

httpErrors.config (..\Spider\CoreServer_XX\Web\Settings)

<?xml version="1.0" ?>
<!--
For DEBUG switch customErrors mode to "Off" (with upper-case "O") and httpErrors errorMode to "Detailed" and then restart the ApplicationPool in IIS. Without a restart the changes will not be applied!

(An ApplicationPool restart can also be achieved by saving the Web.config file without any changes. The IIS recognizes the file has been saved and then restarts the application pool.)

If you encounter an HTTP 500 error message, ensure that httpErrors existingResponse is set to "Auto"!
-->  
<httpErrors errorMode="Custom" defaultResponseMode="Redirect" existingResponse="Auto">
  <!-- NEVER redirect a 401 error! This will cause various problems in the application! -->
  <remove statusCode="403" subStatusCode="-1" />
  <remove statusCode="404" subStatusCode="-1" />
  <remove statusCode="405" subStatusCode="-1" />
  <remove statusCode="406" subStatusCode="-1" />
  <remove statusCode="412" subStatusCode="-1" />
  <remove statusCode="500" subStatusCode="-1" />
  <remove statusCode="501" subStatusCode="-1" />
  <remove statusCode="502" subStatusCode="-1" />

  <!-- Replace "/Spider/" in path attribute with the path of the application. "~" is not allowed here! -->
  <error statusCode="403" prefixLanguageFilePath="" path="/Spider/Default.aspx" responseMode="Redirect" />
  <error statusCode="404" prefixLanguageFilePath="" path="/Spider/Default.aspx" responseMode="Redirect" />
  <error statusCode="500" prefixLanguageFilePath="" path="/Spider/Info/Error.htm" responseMode="Redirect" />
  <error statusCode="501" prefixLanguageFilePath="" path="/Spider/Info/Error.htm" responseMode="Redirect" />
  <error statusCode="502" prefixLanguageFilePath="" path="/Spider/Info/Error.htm" responseMode="Redirect" />

</httpErrors>
<?xml version="1.0" ?>
<!--
For DEBUG switch customErrors mode to "Off" (with upper-case "O") and
httpErrors errorMode to "Detailed" and then restart the ApplicationPool
in IIS. Without a restart the changes will not be applied!

(An ApplicationPool restart can also be achieved by saving the
Web.config file without any changes. The IIS recognizes the file has
been saved and then restarts the application pool.)

If you encounter an HTTP 500 error message, ensure that httpErrors
existingResponse is set to "Auto"!
-->
<httpErrors errorMode="Detailed" defaultResponseMode="Redirect" existingResponse="Auto">
  <!-- NEVER redirect a 401 error! This will cause various problems in the application! -->
  <remove statusCode="403" subStatusCode="-1" />
  <remove statusCode="404" subStatusCode="-1" />
  <remove statusCode="405" subStatusCode="-1" />
  <remove statusCode="406" subStatusCode="-1" />
  <remove statusCode="412" subStatusCode="-1" />
  <remove statusCode="500" subStatusCode="-1" />
  <remove statusCode="501" subStatusCode="-1" />
  <remove statusCode="502" subStatusCode="-1" />

  <!-- Replace "/Spider/" in path attribute with the path of the application. "~" is not allowed here! -->
  <error statusCode="403" prefixLanguageFilePath="" path="/Spider/Default.aspx" responseMode="Redirect" />
  <error statusCode="404" prefixLanguageFilePath="" path="/Spider/Default.aspx" responseMode="Redirect" />
  <error statusCode="500" prefixLanguageFilePath="" path="/Spider/Info/Error.htm" responseMode="Redirect" />
  <error statusCode="501" prefixLanguageFilePath="" path="/Spider/Info/Error.htm" responseMode="Redirect" />
  <error statusCode="502" prefixLanguageFilePath="" path="/Spider/Info/Error.htm" responseMode="Redirect" />
</httpErrors>

**Attention** Please observe capital and small letters when changing settings in the files!
4.3.10 Encryption of the configuration

If the plain text information of the SQL access are stored in the configuration, the connection strings can be encrypted. In the Utilities folder \Spider\CoreServer_00\Utilities\Spider web.config Crypter.cmd) of the Spider instance, you can find a batch file which can be used for encrypting and decrypting.

Encryption

- Execution of Spider web.config Crypter.cmd
- Press button to continue

```
Adminstrator: Tools for En- or decrypting web.config sections

Tools for En- or decrypting web.config sections
(c) Copyright by brainwaregroup

Press any key to continue . . .
```
- Select whether to decrypt or encrypt

```
Administrator: Tools for En- or decrypting web.config sections

-- Please select an action to execute --

1. Encrypt Section
2. Decrypt Section
3. Exit

Select action to execute: 1
```

- Select the section to be encrypted

```
Administrator: Tools for En- or decrypting web.config sections

-- Please choose Section to encrypt --

1. connectionString
2. system.web/sessionState (Spider only)
3. Exit

Please choose Section to encrypt: 1
```
Enter the name of the IIS application

The connection strings of the Spider-Web application and/or the Spider IndexProxyApi can be processed.

Confirm summary by pressing a button

---

Action: encrypt
Architecture: AMD64
Section: connectionStrings
Application: Spider

This is the command that will be executed:
Path: C:\Windows\Microsoft.NET\Framework64\v4.0.30319
Command: aspnet_regiis.exe -pe connectionStrings /app /Spider"

Press any key to continue . . .
You can use the same procedure to decrypt the corresponding files.

**Example for encryption without the batch file**

```
%WINDIR%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -pe connectionStrings /app /<IIS application name>
```

**Example for decryption without the batch file**

```
%WINDIR%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -pd connectionStrings /app /<IIS application name>
```

**Example for encryption of the SessionState configuration without the batch file**

```
%WINDIR%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -pe system.web/sessionState /app /<IIS application name>
```

**Example for decryption of the SessionState configuration without the batch file**

```
%WINDIR%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -pd system.web/sessionState /app /<IIS application name>
```

**Example for decrypted file**

```xml
<?xml version="1.0" encoding="utf-8"?>
<connectionStrings>
  <add name="CoreConnectionString" connectionString="server=.;
    database=SpiderCore;
```
Integrated Security=True;
application name=Spider;
persist security info=True;
packet size=4096"
providerName="System.Data.SqlClient" />
</connectionStrings>

Example for encrypted file

```xml
<?xml version="1.0" encoding="utf-8"?>
<connectionStrings configProtectionProvider="RsaProtectedConfigurationProvider">
    <EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element">
        <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc" />
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
                <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />  
                <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                    <KeyName>Rsa Key</KeyName>
                </KeyInfo>
            </EncryptedKey>
        </KeyInfo>
    </EncryptedData>
</connectionStrings>
```

4.3.11 Error handling system

In general, the following will apply: Spider has a unified error handling system. However, due to the used technology (ASP.NET) it is only possible to handle certain error classes. Some exceptions are automatically handled by the web server (IIS) and it is not possible in our application to manipulate the view of these server responses. Microsoft gives the following information: "You cannot customize the following HTTP error messages: 400, 403.9, 411, 414, 500, 500.11, 500.14, 500.15, 501, 503, and 505."

Details: Configuring HTTP error responses in IIS 7
4.4  Update

This chapter describes the update of a Spider installation.

4.4.1  Start of the update

Start the installation by executing Spider 6.x Setup.exe.

At first, you are asked to select the language for the installation assistant. To do this, click on the desired language in the selection box and confirm your input with "OK".

After that, the installation assistant for Spider will open. This assistant will guide you through the setup installation in the selected language. Click on "Next" to start the installation.
4.4.2 Update

If an instance of Spider is already installed, you will be prompted to decide for one type of installation.

4.4.3 Selection of the Instance

Select the instance to be updated. If there is only one instance, it will be selected already in the selection field.
4.4.4 Database server

In the following step, the installation assistant will ask you to specify the name and the instance of a Microsoft SQL Server, on which the Spider databases are to be installed.

The user, with which the connection is established, can either be the logged-in (Windows) user or an SQL user.

To be able to use an SQL user, you must tick the check box Use SQL user for database connection and fill in the fields User name and Password with the desired data.
Note: The users have to be set up beforehand on the database server with the corresponding rights. Depending on the rights of the user, the subsequent dialogs will show different options.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL server name</td>
<td>Name of the SQL server, including instance name and port if required e.g. SQLSERVER\SQLINSTANZ,1234</td>
</tr>
<tr>
<td>Using SQL users for database connection</td>
<td>Select whether to use the logged-in domain user or an SQL user.</td>
</tr>
<tr>
<td>User name</td>
<td>Name of SQL user.</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the SQL user.</td>
</tr>
</tbody>
</table>

4.4.5 Index proxy server

If the index proxy server has not yet been configured so far, this can be made up for with each Spider update.

Next, you can select whether the index proxy shall be configured during the setup.

The Index Proxy Server is part of the Enterprise Services Infrastructure (ESI).
By ticking the check box, the dialog will be activated and the required data can be entered.

By ticking the check box, the dialog will be activated and the required data can be entered.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the index proxy</td>
<td>Activation of the dialog and query of the details</td>
</tr>
<tr>
<td>Name of the index proxy portal server</td>
<td>Name (FQDN) of the server, on which the index proxy is installed,</td>
</tr>
<tr>
<td>Port of the index proxy portal servers</td>
<td>Port (default: 7080) on which the index proxy reacts to requests</td>
</tr>
<tr>
<td>User name of the token service account</td>
<td>The client ID of the user which shall be used for the connection to the index proxy; the client ID has been created during the installation of the index proxy. Observe capital and small letters for the client ID!</td>
</tr>
<tr>
<td>Password of the token service account</td>
<td>Password belonging to the client ID.</td>
</tr>
</tbody>
</table>

After entering all data and selecting the **Next >** button, the connection to the index proxy will be checked.

If an error should occur, the following message will be displayed.

*The connection to the Index Proxy could not be verified, please check your entries and try again.*

Abort - Cancel check and change values
Retry - Try again with current values
Ignore - Continue setup without check
### Button Description

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abort</td>
<td>The check may be aborted to correct the values. Then the values will be rechecked.</td>
</tr>
<tr>
<td>Retry</td>
<td>New try with the current values</td>
</tr>
<tr>
<td>Ignore</td>
<td>The dialog can be closed without a positive check result. The installation will be carried out with the values specified in the dialog.</td>
</tr>
</tbody>
</table>

#### 4.4.6 Select updates

If the update is carried out for the first time, all products must be selected for update. The dialog is filled in already and cannot be changed anymore.

If one of the products has been updated earlier, it could happen that not all of the products are offered for updating.
If necessary, these products can nevertheless be selected for updating.

Please choose the updates that you want to be installed. Updates with the same version can be skipped.

- [ ] Core: 6.3.2.70 -> 6.3.2.70
- [x] Asset: 6.3.2.70 -> 6.3.2.70
- [x] Contract: 6.3.2.69 -> 6.3.2.70
- [x] Licence: 6.3.2.69 -> 6.3.2.70
### 4.4.7 Installation

The installation assistant will now install Spider. This can take some time. Please wait, until the installation is completed.

The successful completion of the installation will be shown in the progress dialog.
The setup has been completed successfully and can now be closed.

After completion of the installation, a log file will be written. For details to the log files, please refer to chapter Log files (on page 185).
5 Spider Web API

In this chapter
Technical information .............................................................. 113
Authentication ........................................................................... 115
Admin section ........................................................................... 116
Entity section ........................................................................... 117
Search section ........................................................................... 118
Report section ........................................................................... 120
Meta section ............................................................................... 122
Version information ................................................................. 124
Swagger .................................................................................... 125
Web API documentation ............................................................ 128
Spider Web API Explorer ........................................................... 132

As of Spider 6.4, a programming interface(Spider Web API) based on the REST standard will be provided. On the one hand, it is meant to improve the integration of the Spider and Columbus products with each other. On the other hand, however, it is mainly meant to improve the integration of Spider with the customer's existing systems and external systems. The Spider Web API allows for carrying out search queries and requesting reports as well as for creating, changing, assigning, disconnecting, and deleting objects. The Spider Web API is an regular feature of Spider 6.4 and available immediately after installation. The Spider Web API features its own documentation section with information on all functions, their parameters, and return values. The Spider Web API Explorer is provided for testing and development purposes. This makes it easier to get started with using the interface and is also intended to simplify the analysis possible errors. Swagger is provided for more substantial development tasks such as the construction of new interfaces.

5.1 Technical information

5.1.1 REST API

The Spider Web API is based on the principle of RESTful service. This means that each defined URL represents a resource on which one or multiple HTTP methods can be used. The HTTP methods GET, PUT, POST and DELETE are used to obtain, edit, add, and erase resources. The communication can be carried out via HTTP or HTTPS, depending on the customer's configuration. The Spider Web API receives and sends data in JSON format. The data is encoded in UTF-8.

5.1.2 Version management

The functions of the Spider Web API are versioned. The version of the requested function is specified in the URL. If the version is omitted in the URL, the newest version of the function will be used.

Example

Asset search without version specification

http(s)://{ServerName}/{SpiderApiInstance}/(Mandator)/search/asset

Asset search with version specification (V1)

http(s)://{ServerName}/{SpiderApiInstance}/v1/(Mandator)/search/asset

5.1.3 Tenant selection

Many functions of the Spider Web API require a tenant to perform. The designation or the ID of the tenant must then be included in the URL in the correct position.
For the list of the tenants available for the user, refer to the chapter **Mandator** (on page 122).

### 5.1.4 Request

Parameters may be added to any request sent to the Spider Web API. The possible parameters differ depending on the resource. However, the CultureCode parameter, which controls the language of notes and error messages as well translatable results, may be added to any request.

In general, the parameters are transmitted as URL parameters. Only the data and parameters used when creating and editing entities must be included in the request body.

**Example**

Request with parameters in the URL for an asset search:

```
GET http(s)://{ServerName}/{SpiderApiInstance}/{Mandator}/search/asset?culturecode=de&orderby=assetno&distinct=true
```

Request with parameters in the request body for editing the asset with the ID 5:

```
PUT http(s)://{ServerName}/{SpiderApiInstance}/{Mandator}/search/asset/5
with the body:

```
{
  "fields": {
    "AssetNo": "Test",
    "CPUCount": 1,
    "Status": 1
  }
}
```

### 5.1.5 Response

Each request sent to the Spider Web API results in a standardized response. This response includes a self-URL, the parameters of the request, the processing time of the request and, if available, notes and error messages which have been generated during execution of the request.

**Example**

An asset search returns the result

```
{
  "Count": 2204,
  "Result": [
    {
      "id": 2,
      "assetNo": "Access card-0002",
      "hostname": null,
      "assetType": "Access card",
      "status": "Active",
      "functionUnitID": null,
      "functionUnit": null
    }
  ],
  "IsResultTruncated": false,
  "Notifications": []
}
```
Authorized requests of the Spider Web API always return the HTTP status code 200. The only exception to this rule are successful requests for adding objects. These end with the HTTP status code 201.

Unauthorized requests return the HTTP status code 401.

## 5.2 Authentication

A token is used for the authentication of attempts to access the Spider Web API. This token is included with each request during its lifetime. Thanks to the token, it is not necessary to include the login data with each access.

### 5.2.1 Generation of tokens

The authentication token can be obtained via a GET request by means of basic authentication. The token is then returned in the header of the response.

For basic authentication, the username and the password can be included directly in the request URL.

```
http(s)://{UserName}:{Password}@{ServerName}/{SpiderApiInstance}/token
```

Alternatively, username and password can be transferred in the header of the request.

```
http(s)://{ServerName}/{SpiderApiInstance}/token
```

For this purpose, username and password are linked with a colon. The resulting text is converted to Base64 and transferred under Authorization.

Base64 converts **Username:Password** to **VXNlcm5hbWU6UGFzc3dvcmQ=** which must follows the keyword Basic under Authorization in the header.

```
Host: ServerName
User-Agent: WebAPI-Accessor
Authorization: Basic VXNlcm5hbWU6UGFzc3dvcmQ=
```

### 5.2.2 Use of tokens

The token must be included in the header of each subsequent request. The Spider Web API uses the token to identify the Spider user and the user's permissions.
Example

The token is transferred in the request header under Authorization.

```plaintext
Host: ServerName
User-Agent: WebAPI-Accessor
Authorization: Token ed901b25-2f7e-4461-86bd-604212f4e859
Content-Length: 220
Content-Type: application/json; charset=utf-8
```

5.2.3 Validity of tokens

For increased security, the token is only valid for a limited amount of time. The actual length in minutes can be set in the Spider Core Config. By default, it is set to 15 minutes.

After the token has expired, the token can no longer be used for authentication. The processing of requests which are already in progress will be continued. A new token can be generated via token generation.

5.2.4 Management of tokens

The tokens are centrally managed so that all Spider Web API instances can access the same tokens in a web farm scenario. This way, it is irrelevant to the user which instance processes the request.

Furthermore, multiple valid tokens may be assigned to one user since e.g. different services may access the Spider Web API with the same login at the same time.

5.3 Admin section

In the admin section of the Spider Web API, authorized users may list, read, link, and partially edit, add, or delete administrative Spider objects.

Restrictions

The admin section does not cover the same scope of functions as the Spider Web interface. Thus, there is no access to application forms, menu objects, role objects, Active Directory objects, password objects, and system message objects.

5.3.1 Mandator

Using the Spider Web API, tenants can be listed, read, edited, added, and deleted. Furthermore it is possible to assign a user to and disconnect a user from a tenant.

5.3.2 User

Using the Spider Web API, users can be listed, read, edited, added, and deleted. Furthermore it is possible to assign tenants, profiles, and business units to a user and disconnect these from a user accordingly.
5.3.3 Profile

Using the Spider Web API, profiles can be listed and read. Furthermore it is possible to assign users and business units to a profile and disconnect these from the profile accordingly. Deleting and adding of profiles is not provided for.

5.4 Entity section

In the entity section of the Spider Web API, users may access different Spider entities. The permission of a user with regard to entities and their fields is defined by the roles assigned to said user.

Limitation

Only entities whose technical designation is unique across all Spider applications can be addressed via the Spider Web API. Furthermore, access to certain entities is explicitly excluded since these e.g. only serve as a link between two other entities or have an administrative function.

5.4.1 Entity access

Depending on the permissions available, a user may read, edit, add, or delete entities. Custom entities are also available in the Spider Web API as long as they do comply with the restrictions. Note, however, that only business logic from assigned custom rules and not from custom kernel objects is applied here.

The objects are referred to via their technical designation and their ID. Typed objects can be addressed by the designation of their parent object.

Example

A server with the asset ID 1 can be displayed directly via the type.

http(s)://{ServerName}/{SpiderApiInstance}/{Mandator}/entity/server/1

Alternatively, the same result may be obtained via the parent object asset.

http(s)://{ServerName}/{SpiderApiInstance}/{Mandator}/entity/asset/1

5.4.2 Entity history access

For many entities, Spider maintains a change history. This change history may be filtered and listed based on change period and changed fields.

5.4.3 Entity document access

Many entities may be assigned to Spider documents. This is done within a folder structure which may be navigated with the Spider Web API. The different versions of the documents may be accessed as well. Furthermore, documents may be created and new versions may be added.

5.4.4 Entity reminder access

Some entities may be assigned to Spider reminders. These are to be created, displayed, edited, and deleted in the context of the entity.
5.4.5 Entity relationship access

Many entities in Spider are linked to each other. These links may be realized via relationship tables or via direct reference using a field of the entity. The Spider Web API may be used to list the entities assigned to a specific entity, establish new assignments, and disconnect existing assignments.

Restrictions

There are two special cases in which access to the relationships between entities is not possible in the Spider Web API:

- when the relationship exists between two entities of the same type (e.g. link between two contractors via a legal succession) or
- when the relationship has been realized via a typed relationship entity (e.g. link of two function units via a function unit relationship).

Relationship definition

The possibility of customizing entities and their relationships requires the list of possible entity relationships to be defined in an extendable way. This information can be found in the Spider Core database within the webapi.EntityRelationships table.

An entity relationship, in this case, is an unambiguous relationship from one entity to another entity. The return path from the other entity to the first entity is a separate relationship.

A relationship definition always consists of

- a MainEntity,
- a RelatedEntity,
- a search view,
- the field name of the MainEntityID in the search view
- and the application on whose database the search view must be executed.

Based on this information, it is possible to list the assigned entities.

Also, if required, the following takes place via a separate entity when creating a link:

- the name of the entity,
- the fieldname of the ID field of the MainEntity,
- the fieldname of the ID field of the RelatedEntity,
- are transferred to an SQL script for translating the ID value of the MainEntity (e.g. for determining the FunctionUnitID in case of a relationship from asset to employee),
- are transferred to an SQL script for translation of the ID value of the RelatedEntity.

By specifying this information, assignments can be created and resolved.

5.5 Search section

In the search section of the Spider Web API, users may access the search functions for the different Spider entities. The search result and the search fields can be influenced by the permissions of the user and the roles assigned to the user.

Example

Result of an asset search

```json
{
  "count": 201,
  "result": [
```
Limitation

Only entities whose technical designation is unique across all Spider applications can be addressed in the search section via the Spider Web API. Furthermore, access to certain entities is explicitly excluded since these e.g. only serve as a link between two other entities or have an administrative function.

5.5.1 Parameterization

The parameters of the search are transferred in the URL.

Example

A list of the first 100 assets with all fields sorted by the asset number.

```
http(s://{ServerName}/{SpiderApiInstance}/{Mandator}/search/asset?allfields=true&firstRow=1&maxRows=100&orderBy=assetno
```
5.6 Report section

In the report section of the Spider Web API, users may access the reports defined in Spider. A report may be accessed via its ID or its GUID.

Example

If the report "Assets with outdated Scandate" has the ID 1, it can be accessed as follows:

```
http(s)://{ServerName}/{SpiderApiInstance}/{Mandator}/report/1
```

Alternatively, the same report may be accessed via its GUID:

```
http(s)://{ServerName}/{SpiderApiInstance}/{Mandator}/report/3428E63A-882B-3C9D-D318-04AFA7DCCFBD
```
The report would deliver a similar result:

```json
{
  "meta": {
    "displayCategory": "Inventory",
    "displayName": "Assets with outdated scan date",
    "displayDescription": "Assets with outdated scan date (older than 90 days)",
    "guid": "3428e63a-082b-3c9d-d318-04afa7dccfbd",
    "category": "Inventory",
    "name": "Assets with outdated scan date",
    "description": "Assets, which have a scan date that is at least 90 days old",
    "id": 5,
    "applicationName": "Spider Asset",
    "applicationGuid": "38f96e97-c314-44b8-b137-c966d35a3ba0"
  },
  "count": 27,
  "result": [
    {
      "assetID": 222,
      "asset": "DP000001",
      "hostName": "heraetrdy",
      "assetStatus": "Active",
      "invLastScanDate": null,
      "swrUpdateDate": null
    }
  ],
  "isResultTruncated": false,
  "notifications": [],
  "duration": 553,
  "selfLink": "http://www.SpiderServer.com/SpiderWebApi/v1/0/report/3428e63a-
082b-3c9d-d318-04afa7dccfbd",
  "parameter": {
    "conditions": [],
    "maxRows": 1,
    "firstRow": 1,
    "orderBy": "",
    "distinct": false,
    "fields": [],
    "allFields": false,
    "cultureCode": null
  }
}
```

**Limitation**

The Spider Web API only allows access to query-based reports

### 5.6.1 Parameterization

The parameters of the report are transferred in the URL.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AllFields</td>
<td>This URL parameter must contain a Boolean value which defines whether all fields are to be included in the report. The value is false by default.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Condition | This URL parameter can be included in the URL multiple times. Each parameter includes a filter. A filter consists of  
- a logical link,  
- an flag for negation,  
- a field name,  
- a comparison type  
- and a comparison value.  
**Example**  
Report results must contain the text "srv" in the asset no.  
`condition=AND|AssetNo|LIKE|%srv%`  
Report results must not have an "Active" status.  
`Condition=AND|NOT|Status|=|Active` |
| CultureCode | This URL parameter must contain a text which represents a valid language code. This language setting is used for translatable results of the report. The default language is identical with the server language. |
| Distinct | The URL parameter must contain a Boolean value which defines whether lines are allowed to appear in the result twice. The value is false by default. |
| Fields | This URL parameter must contain a list of field names from the search separated by commas. The standard fields differ based on the search entity.  
The Fields parameter is ignored if the parameter AllFields is set to true. |
| FirstRow | This URL parameter must contain a numerical value which defines as of which line the result is to be transferred. The value is 1 by default. |
| MaxRows | This URL parameter must contain a numerical value which defines the maximum number of lines to be included in the result. The value is 500 by default. |
| OrderBy | This URL parameter must contain a field name which determines the sorting method. Optionally, the sorting direction can be defined by adding "ASC" for ascending order and "DESC" for descending order. By default, the sorting method is determined by the database. |

### 5.7 Meta section

In the meta section of the Spider Web API, users may access the meta data for the other sections.

In addition to the lists of available tenants, entities, searches, and reports, this meta data, depending on the function, also includes information on the fields in searches and reports as well as information for creating and editing entities.

#### 5.7.1 Mandator

In the meta section, the user may call up a list of the tenants which have been assigned to them.

```
http(s)://{ServerName}/{SpiderApiInstance}/meta/mandator
```

#### 5.7.2 Admin

In the meta section, the user may call up the meta data for creating and editing tenants as well as users.

**Example**

The meta information required for creating a tenants can be obtained under:
The meta information for editing the user with the ID 5 can be obtained under:

http(s)://{ServerName}/{SpiderApiInstance}/meta/admin/user/5

### 5.7.3 Entity

In the meta section, the user may call up the entities available in the Web API. Additionally, there are functions for calling up the meta data for creating and editing.

**Example**

The list of possible entities is available under:

http(s)://{ServerName}/{SpiderApiInstance}/meta/entities

The meta information required for creating a manufacturer can be obtained under:

http(s)://{ServerName}/{SpiderApiInstance}/meta/entity/manufacturer

The meta information for editing the contract with the ID 5 can be obtained under:

http(s)://{ServerName}/{SpiderApiInstance}/meta/entity/contract/5

Furthermore, there is a list of available, related search field meta data and meta data for creating and editing relationships.

**Example**

The list of entities which can be linked to assets is available under:

http(s)://{ServerName}/{SpiderApiInstance}/meta/entity/asset/relationship

The required meta information for search fields of the list of software which is assigned to an asset:

http(s)://{ServerName}/{SpiderApiInstance}/meta/entity/asset/relationship/software

Furthermore, there is a list of Spider EntityTypes which are non-entities and their possible values.

**Example**

The list of EntityTypes used in a contract is available under:

http(s)://{ServerName}/{SpiderApiInstance}/meta/entity/contract/entityType

### 5.7.4 Search

In the meta section, the user may call up the entities available in the Web API as well as the related result fields.

**Example**

The list of possible search entities is available under:

http(s)://{ServerName}/{SpiderApiInstance}/meta/search

The field information for a manufacturer search can be obtained under:

http(s)://{ServerName}/{SpiderApiInstance}/meta/search/manufacturer
5.7.5 Report

In the meta section, the user may call up the reports available in the Web API as well as the related result fields.

Example

The list of possible reports is available under:

http(s)://{ServerName}/{SpiderApiInstance}/{Mandator}/meta/report

The field information for the report "Assets with outdated Scandate" can be obtained under:

http(s)://{ServerName}/{SpiderApiInstance}/{Mandator}/meta/search/3428E63A-882B-3C3D-D318-84AFA70CCFBD

5.8 Version information

If a user required information on the Spider version used, there are 2 resources from which this information can be obtained.

5.8.1 Simple version information

The simple version information provides a 4-part Spider build number and can be obtained under the following URL.

http(s)://{ServerName}/{SpiderApiInstance}/version

Example

{
   "build": "6.4.0.301",
   "notifications": [],
   "duration": 0,
   "parameter": null
}

5.8.2 Advanced version information

In addition to the build number, the advanced version information also provides the recognition version and the edition as well as information on whether the instance in question is a full update version. It can be obtained under the following URL.

http(s)://{ServerName}/{SpiderApiInstance}/versioninfo

Example

{
   "build": "6.4.0.301",
   "setup": "6.4.0-4154089",
   "edition": "Spider Enterprise",
   "recognition": "1.1805.2.2",
   "isFullUpdate": true,
   "settingsVersion": "6.4.0.301",
   "notifications": [],
   "duration": 267,
   "parameter": null
}
5.9 Swagger

The Spider Web API uses Swagger as interactive API documentation. Swagger is the largest framework of API developer tools for the OpenAPI Specification (OAS) and allows for development during the entire API lifecycle - from design and documentation to testing and publishing.

Swagger can be accessed under the following URL:

http(s)://{ServerName}/{SpiderApiInstance}/swagger/ui/index

5.9.1 OpenAPI Document

The OpenAPI document is a document (or a group of documents) which defines or describes an API. It can be read by humans as well as machines. The document can be used by a developer to automatically generate an interface to the Spider Web API.

The document may be called up via a URL which can be found in the header of the Swagger interface. The URL usually features the following structure:

http(s)://{ServerName}/{SpiderApiInstance}/swagger/docs/v1

5.9.2 Swagger UI

Via the Swagger UI, the user may directly access the functions of the Spider Web API.

**Note**

If you want to use Swagger in Internet Explorer, you must turn off the compatibility mode. Swagger is not compatible with Internet Explorer in compatibility mode.

**Token authentication**

A valid authentication is also required when accessing the functions from the Swagger UI. The user may generate a valid token under

http(s)://{ServerName}/{SpiderApiInstance}/swagger/ui/index#!/Token/Authenticate_Authenticate.

There, a valid basic authentication must be specified in the Authorization field. It has the format

"Basic {Base64 coding of "{{UserName}:{Password})"}

There are various tools and online resources available for encoding username and password to Base64 on the internet.
## Example

### Implementation Notes
The service returns an access token to be used for authentication at other services. It takes the user credentials given by the basic authentication information in the header. If those are verified by the Spider application the access token will be generated and returned inside the response's header.

### Response Class (Status 200)

**OK**

**Example Value**

```json
{
  "notifications": [
    {
      "category": "0",
      "message": "string"
    }
  ],
  "duration": "0",
  "selfLink": "string",
  "parameter": {
    "param1": "param1_value",
    "param2": "param2_value"
  }
}
```

### Response Content Type

- application/json

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
<th>Parameter Type</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>parameter.cultureCode</code></td>
<td></td>
<td></td>
<td>query</td>
<td>string</td>
</tr>
<tr>
<td>Authorization</td>
<td><code>Basic VGVzdGVyOlBhc3N3b3J0</code></td>
<td>The basic authorization information, e.g. <code>Basic TGFnaW86UGFzci5vcmQ=</code> (The second part is the combination of <code>user:login:password</code> encoded in Base64)</td>
<td>header</td>
<td>string</td>
</tr>
</tbody>
</table>

[Try it out]
After actuating the "Try it out!" button, the query is processed and the result is displayed. The generated access token is displayed in the response header section if processing was successful.

```plaintext
Curl

curl -X GET --header 'Accept: application/json' --header 'Authorization: Basic VGVzc09VY01RRc3NJBiY2Q=' 'http://srv-v-hh148/spider64api/token'

Request URL

http://srv-v-hh148/spider64api/token

Response Body

{
  "Notifications": [],
  "Duration": 120,
  "SelfLink": "http://srv-v-hh148/spider64api/token",
  "Parameter": null
}

Response Code

200

Response Headers

{ 
  "pragma": "no-cache",
  "date": "Wed, 30 Apr 2019 00:34:28 GMT",
  "server": "Microsoft-IIS/10.0",
  "x-aspmv-version": "6.0.0.0",
  "x-powered-by": "ASP.NET"
  "content-type": "application/json; charset=utf-8",
  "access-control-expose-headers": "Token,TokenExpiry",
  "cache-control": "no-cache",
  "token": "5337879c-d42f-4282-45c7-51e4835ed09ec"
}
```
In this example, the authorization text for other queries is "Token 5d37878d-42f2-d262-43e7-51e4819ed9ec" until the token expires.

### 5.10 Web API documentation

The Spider Web API features a non-interactive documentation. It contains websites with information on all functions, their parameters, and return values.

The documentation can be accessed under the following URL

http(s)://{ServerName}/{SpiderApiInstance}/help
**Example 1: Main page**

**Spider Web API Help Page**

**Introduction**

Spider WEB API - Custom your own Http Web API CRUD Requests.

**AdminEntity**

Mandatory Web Interface

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST v1/admin/{entityName}</td>
<td>The service creates a new admin entity.</td>
</tr>
<tr>
<td>POST admin/{entityName}</td>
<td>The service creates a new admin entity.</td>
</tr>
<tr>
<td>GET v1/admin/{entityName}/{entityID}?CultureCode=[CultureCode]</td>
<td>The service returns the fields of an admin entity.</td>
</tr>
<tr>
<td>GET admin/{entityName}/{entityID}?CultureCode=[CultureCode]</td>
<td>The service returns the fields of an admin entity.</td>
</tr>
<tr>
<td>PUT v1/admin/{entityName}/{entityID}</td>
<td>The service updates an admin entity.</td>
</tr>
<tr>
<td>PUT admin/{entityName}/{entityID}</td>
<td>The service updates an admin entity.</td>
</tr>
<tr>
<td>DELETE v1/admin/{entityName}/{entityID}?CultureCode=[CultureCode]</td>
<td>The service deletes an admin entity.</td>
</tr>
<tr>
<td>DELETE admin/{entityName}/{entityID}?CultureCode=[CultureCode]</td>
<td>The service deletes an admin entity.</td>
</tr>
</tbody>
</table>
Example 2: Detail view

Spider Help Page Home API

**POST v1/{mandator}/entity/{entityName}**

The service generates a new entity

**Request Information**

**URI Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>mandator</td>
<td>The mandator for whom the entity should be created.</td>
<td>string</td>
<td>Required</td>
</tr>
<tr>
<td>entity/Name</td>
<td>The name of the entity to be created.</td>
<td>string</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Body Parameters**

A parsed from the URL parameters.

**EntityFieldParameterModel**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fields</td>
<td></td>
<td>Dictionary of string [key] and Object [value]</td>
<td>None.</td>
</tr>
<tr>
<td>CultureCode</td>
<td></td>
<td>string</td>
<td>None.</td>
</tr>
</tbody>
</table>

**Request Formats**

application/json, text/json

Sample:

```json
{
    "fields": {},
    "cultureCode": "sample string 1"
}
```
Example 3: Return object

Response Formats

```json
Sample:
{
    "entities": [],
    "notifications": [],
    "duration": 1,
    "selfLink": "http://webap1helppage2.com",
    "parameters": {
        "cultureCode": "sample string 1"
    }
}
```
5.11 Spider Web API Explorer

In this chapter

| Expected users                                                                 | 132 |
| Authentication                                                                 | 132 |
| Session parameters (tenant, language, version)                                | 133 |
| Communication with the Spider Web API                                         | 133 |
| Web API Explorer sections                                                     | 135 |

The Spider Web API Explorer is a web application which allows for an easier access to all relevant functions of the Spider Web API for testing and development purposes.

Spider Web API Explorer allow data operations such as creating, searching, changing, and deleting data (CRUD: Create, Read, Update, Delete). You may select whether the results are displayed in JSON or HTML.

5.11.1 Expected users

The expected users of the Spider Web API Explorer are testers, quality assurance officers, business analysts, administrators, or software engineers who want to test the functions of the Spider Web API. Basic knowledge of Spider is required.

5.11.2 Authentication

The authentication for access to the Web API Explorer is carried out via a Spider user account. In the Web API Explorer, users have the same permissions as in the Web API itself.

The API Explorer can be accessed under the following URL:

```text
http(s)://{ServerName}/{SpiderApiExplorerInstance}
```

Use your Spider account to log in.

```text
Username: SpiderUser
Password: ****

Remember me?
Log in
```
5.11.3  Session parameters (tenant, language, version)

After logging in, the session parameters are determined. Here, a tenant must be selected. At this time, it is also possible to select the language and the API version. By default, the latest version of the API is preselected. If no language is selected, English is used as the default API language.

The session parameters can be changed at any given time.

5.11.4  Communication with the Spider Web API

Communication with the Spider Web API via the HTTP / HTTPS protocol is protected by means of a token mechanism. The token is stored in the browser cache.

Response

The response page of the Spider API explorer consists of 2 tabs: HTML and JSON. Here, you may select whether the results are displayed in HTML or in JSON.

Response model

The following fields are returned:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>Duration of the query in seconds.</td>
</tr>
<tr>
<td>Selflink</td>
<td>Returns a URL of the query.</td>
</tr>
<tr>
<td>Notification</td>
<td>Returns the error messages from the kernel (category and message).</td>
</tr>
<tr>
<td>CultureCode</td>
<td>Returns the language used in the query.</td>
</tr>
</tbody>
</table>

The other fields depend on the query.

HTTP status code: The Spider Web API Explorer always receives HTTP status code 200 as response from the Spider Web API. Error messages are always included in the return object. Unauthorized requests return the HTTP status code 401.

Example:

The response to an asset search
1. HTML format:

Response

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>207 ms</td>
</tr>
<tr>
<td>SelfLink</td>
<td><a href="http://srv-v-hh149/Spider-FLEXENTAPI/0/search/Asset?s=10&amp;Firstrow=1&amp;OrderBy=AssetNo&amp;">http://srv-v-hh149/Spider-FLEXENTAPI/0/search/Asset?s=10&amp;Firstrow=1&amp;OrderBy=AssetNo&amp;</a></td>
</tr>
<tr>
<td>OrderBy</td>
<td>AssetNo</td>
</tr>
<tr>
<td>MaxRows</td>
<td>10</td>
</tr>
<tr>
<td>FirstRow</td>
<td>1</td>
</tr>
<tr>
<td>AllFields</td>
<td>Off</td>
</tr>
<tr>
<td>Distinct</td>
<td>Off</td>
</tr>
<tr>
<td>Count</td>
<td>100</td>
</tr>
<tr>
<td>IsResultTruncated</td>
<td>On</td>
</tr>
</tbody>
</table>

**Result**

<table>
<thead>
<tr>
<th>id</th>
<th>assetNo</th>
<th>hostname</th>
<th>assetType</th>
<th>status</th>
<th>functionUnitID</th>
</tr>
</thead>
<tbody>
<tr>
<td>65</td>
<td>CLIENT-SEKY002.domain.corp</td>
<td>CLIENT-SEKY002</td>
<td>Desktop</td>
<td>Active</td>
<td>65</td>
</tr>
<tr>
<td>86</td>
<td>CLIENT-TEKN002.domain.corp</td>
<td>CLIENT-TEKN002</td>
<td>Desktop</td>
<td>Active</td>
<td>86</td>
</tr>
<tr>
<td>11</td>
<td>ESXHOST003.domain.CORP</td>
<td>ESXHOST003</td>
<td>Server</td>
<td>Active</td>
<td>11</td>
</tr>
<tr>
<td>12</td>
<td>ESXHOST004 domain.CORP</td>
<td>ESXHOST004</td>
<td>Server</td>
<td>Active</td>
<td>12</td>
</tr>
<tr>
<td>10</td>
<td>ESXHOST005.domain.CORP</td>
<td>ESXHOST005</td>
<td>Server</td>
<td>Active</td>
<td>10</td>
</tr>
<tr>
<td>101</td>
<td>ESXHOST006.domain.corp</td>
<td>ESXHOST006</td>
<td>Server</td>
<td>Active</td>
<td>101</td>
</tr>
<tr>
<td>100</td>
<td>ESXHOST007</td>
<td>ESXHOST007</td>
<td>Server</td>
<td>Active</td>
<td>100</td>
</tr>
<tr>
<td>36</td>
<td>ESXHOSTC003.domain.CORP</td>
<td>ESXHOSTC003</td>
<td>Server</td>
<td>Active</td>
<td>36</td>
</tr>
<tr>
<td>35</td>
<td>ESXHOSTC004.domain.CORP</td>
<td>ESXHOSTC004</td>
<td>Server</td>
<td>Active</td>
<td>35</td>
</tr>
<tr>
<td>107</td>
<td>ESXHOSTZ002.domain.corp</td>
<td>ESXHOSTZ002</td>
<td>Server</td>
<td>Active</td>
<td>107</td>
</tr>
</tbody>
</table>
2. JSON format

Response in formatted Json

```json
{
    "Count": 100,
    "Result": [
    {
        "id": 2,
        "assetNo": "LAPTOP-OBST003.domain.corp",
        "hostname": "LAPTOP-OBST003",
        "assetType": "Laptop",
        "status": "Active",
        "functionUnitID": 2,
        "functionUnit": "LAPTOP-OBST003.domain.corp",
        "serialNo": "13JY21"
    }
    ],
    "IsResultTruncated": true,
    "Notifications": [],
    "Duration": 76,
    "Parameter": {
        "Conditions": [],
        "MaxRows": 1,
        "FirstRow": 1,
        "OrderBy": "",
        "Distinct": false,
        "Fields": null,
        "AllFields": false,
        "CultureCode": "en-US"
    }
}
```

5.11.5 Web API Explorer sections

There are three sections:

- Search API
- Report API
Entity API

Search API

Spider entities can be searched in the "Search API" section. **Search section** (on page 118)

The search can be accessed under the following URL:

http(s):/{ServerName}/{SpiderApiExplorerInstance}/search
Search API

Enter your API Request

Entities: Asset

Fields:
- AccountingApproachID int
- Actual book value € money
- Actual book value money
- Archived bit
- AssetNo nvarchar

OrderBy: AssetNo nvarchar

MaxRows: 1

FirstRow: 1

Distinct: 

AllFields: 

Conditions: 

Example: OR|NOT|assetno|like|%25

Send Request
Parameter

The parameters of the search are entered via the web front-end. For more detailed information, refer to chapter Parameterization (on page 119).

Response

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>76 ms</td>
</tr>
<tr>
<td>SelfLink</td>
<td><a href="http://srv-v-hh149/Spider-FLEXENTAPI/0/search/Asset?MaxRows=1&amp;Firstrow=1">http://srv-v-hh149/Spider-FLEXENTAPI/0/search/Asset?MaxRows=1&amp;Firstrow=1</a></td>
</tr>
<tr>
<td>MaxRows</td>
<td>1</td>
</tr>
<tr>
<td>FirstRow</td>
<td>1</td>
</tr>
<tr>
<td>AllFields</td>
<td>false</td>
</tr>
<tr>
<td>Distinct</td>
<td>false</td>
</tr>
<tr>
<td>Count</td>
<td>100</td>
</tr>
<tr>
<td>IsResultTruncated</td>
<td>true</td>
</tr>
<tr>
<td>Fields</td>
<td></td>
</tr>
<tr>
<td>Conditions</td>
<td></td>
</tr>
</tbody>
</table>

Response in formatted Json

```json
{
    "Count": 100,
    "Result": [],
    "id": 2,
    "assetNo": "LAPTOP-OBST003.domain.corp",
    "hostname": "LAPTOP-OBST003",
    "assetType": "Laptop",
    "status": "Active",
    "functionUnitID": 2,
    "functionunit": "LAPTOP-OBST003.domain.corp",
    "serialNo": "133PY21"
}
```

"IsResultTruncated": true,
"Notifications": [],
"Duration": 76,
"parameter": {
    "Conditions": [],
    "MaxRows": 1,
    "FirstRow": 1,
    "OrderBy": "",
    "Distinct": false,
    "Fields": null,
    "AllFields": false,
    "CultureCode": "en-US"
}
Report API

The "Report API" section allows searching for reports available for the selected tenant.

The Report API can be accessed under the following URL:
Report API

Enter your API Request

Report

Please select a Report

Fields

Autodesk - Assets with Autodesk Programs - 45 (Spider Asset)
Autodesk - Qualified Autodesk Inventory - 46 (Spider Asset)
Clearing - Double translations - 106 (Spider Localization)
Compliance - Product overlicensing - 73 (Spider Licence)
Compliance - Product underlicensing - 74 (Spider Licence)
Compliance - Productversion compliance - 72 (Spider Licence)
Compliance - Productversion compliance per Legal Entity - 71 (Spider Licence)
Compliance - Required Licenses per Device - 75 (Spider Licence)
Contracts - Contract overview - 97 (Spider Contract)
Contracts - Contracts according to contractual parties - 94 (Spider Contract)
Contracts - Contracts with missing dates - 95 (Spider Contract)
Contracts - Contracts with missing responsibilities - 95 (Spider Contract)
Contracts - Master agreements - 98 (Spider Contract)
Contracts - Overview of Contractual Parties - 93 (Spider Contract)
Contracts - Remaining time to maturity - 90 (Spider Contract)
### Parameter

The parameters of the Report API are entered via the web front-end analogously to the Search API. For more detailed information, refer to chapter Parameterization (on page 121).

### Entity API

The Entity section allows data operations (CRUD) such as creating, reading, changing, and deleting entities. For more detailed information, refer to chapter Entity section (on page 117).

The Entity API can be accessed under the following URL

<table>
<thead>
<tr>
<th>assetID</th>
<th>asset</th>
<th>hostName</th>
<th>assetStatus</th>
<th>invLastScanDate</th>
</tr>
</thead>
<tbody>
<tr>
<td>65</td>
<td>CLIENT-SEKY002.domain.corp</td>
<td>CLIENT-SEKY002</td>
<td>Active</td>
<td>29.05.2018 06:54:11</td>
</tr>
<tr>
<td>86</td>
<td>CLIENT-TEKN002.domain.corp</td>
<td>CLIENT-TEKN002</td>
<td>Active</td>
<td>29.05.2018 04:31:53</td>
</tr>
<tr>
<td>170</td>
<td>CLIENT-Test006.domain.corp</td>
<td>CLIENT-Test005</td>
<td>Active</td>
<td>29.05.2018 10:03:14</td>
</tr>
<tr>
<td>146</td>
<td>CLIENT-WITE05.domain.corp</td>
<td>CLIENT-WITE05</td>
<td>Active</td>
<td>15.03.2018 05:58:52</td>
</tr>
<tr>
<td>11</td>
<td>ESXHOST003.domain.CORP</td>
<td>ESXHOST003</td>
<td>Active</td>
<td>30.05.2018 01:04:21</td>
</tr>
<tr>
<td>12</td>
<td>ESXHOST004.domain.CORP</td>
<td>ESXHOST004</td>
<td>Active</td>
<td>30.05.2018 01:04:21</td>
</tr>
<tr>
<td>10</td>
<td>ESXHOST005.domain.CORP</td>
<td>ESXHOST005</td>
<td>Active</td>
<td>30.05.2018 01:04:21</td>
</tr>
<tr>
<td>101</td>
<td>ESXHOST006.domain.CORP</td>
<td>ESXHOST006</td>
<td>Active</td>
<td>30.05.2018 01:05:56</td>
</tr>
<tr>
<td>100</td>
<td>ESXHOST007.domain.CORP</td>
<td>ESXHOST007</td>
<td>Active</td>
<td>30.05.2018 01:05:56</td>
</tr>
<tr>
<td>121</td>
<td>ESXHOSTB001.domain.corp</td>
<td>ESXHOSTB001</td>
<td>Active</td>
<td>30.05.2018 01:06:52</td>
</tr>
</tbody>
</table>
The Entity API consists of six sections:

**Get Entity**

This section can be used to query entities.

**Parameters**: name and ID of the entity.
**Example:** Querying an asset with ID=1 and having the result displayed in JSON.

![Spider Web API Explorer](image)

**Entity API**

Enter your API Request

- **Get**
- **Entities**
- **EntityID**

Send Request
Create Entity

This section can be used to create entities.

Parameters: Entity name, entity fields as JSON.

Example: Creating desktop entity:
1. Select desktop entity.
2. Enter usage data in JSON format:

```json
{"fields":
  {
    "Mandator":0,
    "AssetNo":"123456789",
  }
}
```
"HostName":"MyHostname",
"AssetStatusID":1,
"CommentStatus":"Just want to try to create a desktop",
"SerialNo":"12349875547945789",
}
}
3. Click <Send Request> button.
**Update Entity**

This section can be used to change entities.

**Parameter:** Entity name, entity fields as JSON and ID of the entity.

**Example:** Changing the host name of a desktop entity with ID=1

1. Select asset.
2. Enter usage data in JSON format:

   ```json
   {"fields": {
   "Hostname":"The hostname of My Test Desktop has changed"
   }}
   ``
3. Enter the ID of the entity.
4. Click <Send Request> button.

![Entity API](image)

**Result**

- **Duration**: 619 ms
- **SelfLink**: http://localhost/Spider/WebAPI/100/entity/Desktop/2886

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>The hostname of My Test Desktop has changed</td>
</tr>
</tbody>
</table>

**Delete Entity**

This section can be used to delete entities.
**Parameters:** name and ID of the entity.

**Example:** Deleting a desktop entity with ID=1

1. Select asset.
2. Enter the ID of the entity.
3. Click <Send Request> button.

---

**EntityType section**

This section belongs to the entity meta data. See chapter [Entity section](Page117) (on page 117), EntityTypes describe pre-defined states and values which individual fields of entities may assume.

**Parameters:** entity name and EntityType.

**Example:** Displaying EntityTypes available for assets:

1. Select asset.
2. Click <Send Request> button.

**Entity API**

Enter your API Request

- **Entity**
- **Get**
- **Create**
- **Update**
- **Delete**
- **Types**
- **TypeValues**

**Entities**
- Asset

**Types**
- AssetStatusID - AssetStatusID + (k

**Send Request**

**Response**

- **Duration**: 6 ms
- **SelfLink**: http://localhost/SpiderWebApi/100/meta/entity/Asset/entityType

**EntityTypes**

<table>
<thead>
<tr>
<th>Name</th>
<th>ColumnName</th>
<th>KeyColumn</th>
<th>ValueColumn</th>
<th>MandatorFilter</th>
<th>SCOObjectFilter</th>
<th>Translate</th>
</tr>
</thead>
<tbody>
<tr>
<td>AssetStatusID</td>
<td>AssetStatusID</td>
<td>ID</td>
<td>Name</td>
<td>False</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>CurrencyCode</td>
<td>CurrencyCode</td>
<td>Code</td>
<td>EntityTypeValue</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>MandatorID</td>
<td>MandatorID</td>
<td>ID</td>
<td>Name</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>PVD_FinancingType</td>
<td>FinancingType</td>
<td>Value</td>
<td>Text</td>
<td>False</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>PVD_ImportSource</td>
<td>ImportSourceID</td>
<td>Value</td>
<td>Text</td>
<td>False</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>PVD_DoSType</td>
<td>OsTypeID</td>
<td>Value</td>
<td>Text</td>
<td>False</td>
<td>True</td>
<td>False</td>
</tr>
</tbody>
</table>

**EntityTypeValues section**

EntityTypeValues are the defined states and values which individual fields of entities may assume.

**Parameters**: entity name and EntityType.

**Example**: Displaying available EntityValues for EntityType AssetStatusID:

1. Select asset.
2. Select EntityType AssetStatusID.
3. Click <Send Request> button.

### Entity API

**Enter your API Request**

- **Entity**
  - **Get**
  - **Create**
  - **Update**
  - **Delete**
  - **Types**

**Entities**
- Asset

**Types**
- AssetStatusID - AssetStatusID + 1

**Send Request**

### Response

- **Duration**: 46 ms
- **SelfLink**: http://localhost:SpiderWebApi/100/meta/entity/Asset/entityType/AssetStatusID

**HTML**

**EntityTypes**

<table>
<thead>
<tr>
<th>Name</th>
<th>ColumnName</th>
<th>KeyColumn</th>
<th>ValueColumn</th>
<th>MandatorFilter</th>
<th>SCOObjectFilter</th>
<th>Translate</th>
</tr>
</thead>
<tbody>
<tr>
<td>AssetStatusID</td>
<td>AssetStatusID</td>
<td>ID</td>
<td>Name</td>
<td>False</td>
<td>False</td>
<td>True</td>
</tr>
</tbody>
</table>

**EntityValues**

<table>
<thead>
<tr>
<th>id</th>
<th>name</th>
<th>initial</th>
<th>unknown</th>
<th>active</th>
<th>archive</th>
<th>defaultArchive</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Active</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>1. Asset is in operation</td>
</tr>
<tr>
<td>2</td>
<td>Disposed</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>2. Asset is not in operation</td>
</tr>
<tr>
<td>3</td>
<td>In repair</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>3. Asset is in repair</td>
</tr>
<tr>
<td>4</td>
<td>In stock</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>4. Asset is in stock</td>
</tr>
<tr>
<td>5</td>
<td>Inactive</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>5. Asset is not in stock</td>
</tr>
<tr>
<td>6</td>
<td>Stolen</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>6. Asset is not in stock</td>
</tr>
<tr>
<td>7</td>
<td>ActiveDefined</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>7. Asset is not in stock</td>
</tr>
<tr>
<td>8</td>
<td>NotReported</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>8. Asset is not in stock</td>
</tr>
</tbody>
</table>
6 Software Services (Catalogs and Recognition)

In this chapter
System requirements ................................................................. 152
Installation .................................................................................. 155
Advanced configuration ............................................................. 165
Update .......................................................................................... 169

6.1 System requirements

6.1.1 Application server

The installation of the Recognition can either be done on the system where Spider has been installed or on a separate system.

Additional services for the functionality of the Recognition are installed.

- EDC monitor
- Spider Data Receiver
- Software Recognition Center upload (optional)

The databases must be stored on the same server (and Instance), which is also used for storing the databases for Spider.

During the setup, the connection to the database server is prompted.

The following conditions must be observed:

- The setup has to be executed with administrative rights.
- Recognition (RC) and Spider Data Collector have to run on separate systems. These may also be separated virtual environments.
- On the Spider application server, the RC or the Spider Data Collector may be installed.
- Port for the communication of software recognition with Spider Data Collector(s) to be connected; the port can be selected freely. By default, port 1685 is used.
- In case of productive systems, the address and port for the upload to the software recognition center must be reachable from the server
  - Address: edcsrv1.brainwaregroup.com
  - Port: 1337

Note

Test systems without upload to the software recognition center.

Here, you can install software recognition and Spider Data Collector parallel.
6.1.2 Database server

A Microsoft SQL server, Version 2008 or later, is required as database server. For a successful setup, the following preconditions must be met on the database server.

The database server must be the same server on which the Spider databases are installed.

- You must activate the TCP/IP protocol in the "SQL Server Configuration" of the SQL server configuration manager.
- A database login for the SQL installation user is required.
- If the SQL installation user does not possess the right to create databases, it must be provided before starting the installation.

If the SQL installation user does not possess the rights to create other SQL logins on the database server, the required SQL login must be set up beforehand and made available for the setup. It is recommended to use the same user which has been used for the Spider installation, since the Spider services must also have access to the software recognition database.

- The SQL installation user will at least need the right to execute the SQL scripts for creating and changing the database objects as well as the database properties (Extended Properties) in the Spider databases.

Required database

To create databases during the installation, the SQL installation user will need the corresponding rights. If these cannot be granted, the product databases have to be created before execution of the setup. The setup supports the usage of empty databases which have been created beforehand. Especially if the databases shall not be created with default properties, the required databases can be provided using the desired settings.

The following databases are required for the installation:

- Spider Recognition

**Important** It is recommended to use the suffix (later in the example: "CoreServer_00_") used for the installation of Spider, also for the recognition database. This makes the identification on the SQL server easier.

Please note the following:

- The name can be chosen freely. The database name must not start with a number.
- All Spider databases must have the same Database collation. A case insensitive collation (CI collation) must be selected, e.g. SQL_Latin1_General_CP1_CI_AS.
- The databases must be completely empty before installation.

Required SQL user

If the SQL installation user does not have the permission to create new logins on the database server, this login must be created beforehand. An SQL user is required for the setup. The login data are requested during the installation. The user must be the same as the one used for the Spider installation, since the services of Spider must have access to the software recognition database.
Overview of required rights

Please refer to the table below for the rights required to execute the setup:

<table>
<thead>
<tr>
<th>Task</th>
<th>Rights to</th>
<th>Right(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating logins</td>
<td>Server</td>
<td>ALERT ANY LOGIN</td>
</tr>
<tr>
<td>Creating databases</td>
<td>Server</td>
<td>CREATE DATABASE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CREATE ANY DATABASE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ALTER ANY DATABASE</td>
</tr>
<tr>
<td>Creating extended properties</td>
<td>Database</td>
<td>ALTER</td>
</tr>
</tbody>
</table>
6.2 Installation

6.2.1 Start of the installation

Start the installation by executing Recognition Setup.exe

Please wait while Setup is loading...
unpacking data: 81%

At first, you are asked to select the language for the installation assistant. To do this, click on the desired language in the selection box and confirm your input with "OK".

After that, the installation assistant for Spider will open. This assistant will guide you through the setup installation in the selected language. Click on "Next" to start the installation.
6.2.2 License agreement

In the next step, you are asked to read and accept the license agreement before starting the installation. The setup can only be continued after accepting the license agreement.

6.2.3 License file

Select the matching license file to continue the setup. The setup cannot be continued without the license file.
Click on "..." Button:

Select the license and then click "Open".

The selected license will be loaded and its details are shown.
**Note**
If a license is found in the same directory which has been used to start the setup, it will be loaded automatically into the dialog (if valid).

### 6.2.4 Installation directory

In the following step, you can select a target directory for the installation. You may change the proposed default path.
6.2.5 Database server

In the following step, the installation assistant will ask you to specify the name and the instance of a Microsoft SQL Server, on which the recognition databases are to be installed.

The user, with which the connection is established, can either be the logged-in (Windows) user or an SQL user.

To use an SQL user, you must tick the check box **Use SQL user for database connection** and fill in the fields **User name** and **Password** with the desired data.
Note
The users have to be set up beforehand on the database server with the corresponding rights. Depending on the rights of the user, the subsequent dialogs will show different options.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL server name</td>
<td>Name of the SQL server, including instance name and port if required e.g. SQLSERVER\SQLINSTANZ,1234</td>
</tr>
<tr>
<td>Using SQL users for database connection</td>
<td>Select whether to use the logged-in domain user or an SQL user.</td>
</tr>
<tr>
<td>User name</td>
<td>Name of SQL user.</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the SQL user.</td>
</tr>
</tbody>
</table>

6.2.6 Database & Data Receiver

In this dialog, you can enter the data for the recognition database, the Core database of the Spider installation to be connected, the data directory, the recognition upload and the customer ID.

![Database & Data Receiver dialog](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>Select in the drop-down, whether a new database should be created, or select an existing (empty!) database</td>
</tr>
<tr>
<td>Core DB</td>
<td>Select the name of the Core database of the Spider installation to be linked</td>
</tr>
<tr>
<td>Data directory</td>
<td>The work directory in which the received data of the Data Collector(s) are stored and processed.</td>
</tr>
<tr>
<td>Port</td>
<td>Port used by the Data Receiver to receive the data of the connected Data Collectors (Default port: 1685)</td>
</tr>
<tr>
<td>Recognition Center Upload</td>
<td>Check box to determine whether unrecognized software shall be transferred to brainware-group for recognition.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload ID</td>
<td>ID (from the license file) used for identification prior to the upload to brainwaregroup.</td>
</tr>
<tr>
<td>Customer ID</td>
<td>Customer ID which will be transferred to the Data Collector(s) to ensure the identification at this installation of the recognition.</td>
</tr>
</tbody>
</table>

### 6.2.7 SQL login, service user

This user is used for access to the software recognition database.

The Spider services access also the recognition databases by using the Core server user databases!

The default system user «spider» or the user which has been used for the installation of Spider must be entered.

![SQL Login](image)

**Attention** When creating a new user, please make sure to grant the rights for Spider! To make sure that the Spider services can also access the recognition database, also the user used by the services must have the corresponding rights for using the recognition database.
6.2.8 Summary

The summary shows that:

- the version of software recognition
- the software recognition definitions
- the Data Receiver components and version
- the upload to the Spider Recognition Center with version
are installed.

6.2.9 Installation

The installation assistant will now install Recognition. This can take some time. Please wait, until the installation is completed.
The successful completion of the installation will be shown in the progress dialog.

![Progress Dialog](image)

The setup has been completed successfully and can now be closed.

![Recognition Setup](image)

After completion of the installation, a log file will be written. For details to the log files, please refer to chapter Log files (on page 185).
6.3 Advanced configuration

6.3.1 Data Receiver

The Data Receiver is the component which receives the deliveries of the Data Collector(s).

The port and the storage location of the received files can be changed.

The configuration is done in the file <Installation directory>\Recognition\DataReceiver\SpiderDataReceiver.cfg

```plaintext
; OTB Connection Settings:
; ------------------------
; OTBPort - default setting is "80"

[Connection]
OTBPort=1685

; General settings:
; -----------------
; DataDirectory - is the data directory to save files in that should be uploaded - default if not set is the folder where the EDCRV.exe is installed (environment variables are resolved)

[General]
DataDirectory=C:\Recognition\Data\DataReceiver
```

<table>
<thead>
<tr>
<th>Section</th>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection</td>
<td>OTBPort</td>
<td>Port used by the Data Receiver to listen to the connections of the Data Collector(s)</td>
</tr>
<tr>
<td>General</td>
<td>DataDirectory</td>
<td>Path used to store the received files.</td>
</tr>
</tbody>
</table>

**Attention**

If variable DataDirectory is adapted, the Service "Spider Data Receiver" must be restarted. Only then, the change will become active.

In addition, the configuration of the EDC monitor (on page 166) has to be adapted to make sure that it can find the files to be processed.

**SSL Secured Transmission**

Communication with the Spider Data Collector can be secured by SSL (RSA 2048Bit).

The superior Data Receiver provides the SSL mechanism for the subordinate Data Collectors.

Upon installation of the Data Receiver the necessary files are generated and placed in: %ProgramData%\Columbus

SSL usage can be enabled by setting the following registry keys.

```plaintext
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Brainware\Columbus\7\ "OTBEncryptionUseSSL"="1"
"OTBEncryptionForceUseSSL"="0"
```
6.3.2 EDC Monitor

The EDC monitor is responsible for the import of the files received by the Data Receiver into the recognition database.

The configuration of the EDC monitor is stored in the file <installation path>\Recognition\EDCMonitor\EDCMonitor.exe.config.

```xml
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <connectionStrings>
    <!-- Connection string to the software recognition database -->
    <add name="SoftwareRecognitionConnectionString" connectionString="server=server.domain.local; database=Recognition; uid=Spider; pwd=abcde; application name=SpiderEDCMonitor;Persist Security Info=True" />
  </connectionStrings>
  <appSettings>
    <!-- Working directory of the EDC monitor
    Has to be the path where EDCMonitor.exe is located -->
    <add key="EDCMonitorWorkingDirectory" value="C:\Program Files\Spider\Recognition\EDCMonitor" />
    <!-- Working directory of Data Receiver.
    Following files are expected in the directory:
    * SpiderDataReceiver.cfg
    * SpiderDataReceiverRegister.csv
    * SpiderDataReceiverConnection.csv -->
    <add key="DataReceiverWorkingDirectory" value="C:\Program Files\Spider\Recognition\DataReceiver" />
    <!-- Location, where files are committed to software recognition.
    The data directory of the EDC server and this directory should be located on the same HDD. -->
    <add key="SoftwareRecognitionImportDirectory" value="C:\RecognitionData\EDC monitor" />
    <!-- Delay between monitoring processes (in minutes). -->
    <add key="Interval" value="1" />
    <!-- Directory where log files will be written
    Standard: %ProgramData%\brainwaregroup\EDCMonitor\Logs -->
    <add key="FeedbackDirectory" value="C:\ProgramData\brainwaregroup\EDCMonitor\Logs" />
  </appSettings>
</configuration>
```

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connectionStrings</td>
<td>Data for the connection to the recognition database; if Integrated Security is used, uid=...,pwd=...; must be replaced by &quot;IntegratedSecurity = True.&quot;</td>
</tr>
<tr>
<td>appSettings. EDCMonitorWorkingDirectory</td>
<td>Path used to store the file EDCMonitor.exe.</td>
</tr>
<tr>
<td>appSettings. DataReceiverWorkingDirectory</td>
<td>Path used to store the file SpiderDataReceiver.exe and its configuration file.</td>
</tr>
<tr>
<td>appSettings. SoftwareRecognitionImportDirectory</td>
<td>Path used by the EDC monitor to store its files.</td>
</tr>
<tr>
<td>appSettings. Interval</td>
<td>Interval in which the EDC monitor is activated, detects new files and imports them if required.</td>
</tr>
<tr>
<td>appSettings. FeedbackDirectory</td>
<td>Path used to store the log files.</td>
</tr>
</tbody>
</table>
6.3.3 Operation with domain account

Prepare SQL server

The setup is carried out according to the description for setting up Spider [Prepare SQL server](on page 54).

In addition, the user must be given new or additional rights for the recognition database.

- Entering the **Roles memberships** for the recognition database by setting the tick on **Map** and selecting the membership in the lower part of the dialog.

<table>
<thead>
<tr>
<th>Database</th>
<th>Database role membership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recognition</td>
<td>public, sr_user</td>
</tr>
</tbody>
</table>

![Database roles membership](image)
Folder permissions

In order to enable the access to the stored files, the user can either be given administrative rights on the computer on which the EDC monitor is installed, or you can give the folder access rights to the EDC monitor directly or via its group membership.

<table>
<thead>
<tr>
<th>Folder</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation directory of the EDC monitor C:\Program Files\Spider\Recognition\EDCMonitor</td>
<td>Modify</td>
</tr>
<tr>
<td>Installation directory of the data receiver C:\Program Files\Spider\Recognition\DataReceiver</td>
<td>Modify</td>
</tr>
<tr>
<td>Data directory Database &amp; Data Receiver (on page 160)</td>
<td>Modify data directory and all subfolders</td>
</tr>
</tbody>
</table>

Adapt the service account

The setup is done according to the setup of Spider Adapt the service account (see "" on page 64).

The service to be adapted is the External Data Collector - Monitor

Adapt the connection string

The file ConnectionStrings.config is used for the access of the service.

Storage location of the connection string

<table>
<thead>
<tr>
<th>Component</th>
<th>Storage location</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDC monitor</td>
<td>C:\Program Files\Spider\Recognition\EDCMonitor\EDCMonitor.exe.config</td>
</tr>
</tbody>
</table>

The entries uid=... and pwd=... must be replaced by Integrated Security=True.

ConnectionStrings.config

```xml
<?xml version="1.0" encoding="utf-8"?>
<configuration>
<connectionStrings>
    <!-- Connection string to the software recognition database -->
    <add name="SoftwareRecognitionConnectionString" connectionString="server=<SQLServer>;
```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <connectionStrings>
    <!-- Connection string to the software recognition database -->
    <add name="SoftwareRecognitionConnectionString" connectionString="server=<SQLServer>;
      database=Recognition;
      uid=Spider;
      pwd=abcde;
      application name=SpiderEDCMonitor;
      Persist Security Info=True" />
  </connectionStrings>
  ...
</configuration>

Note After all adaptations have been done, the service must be restarted to activate the changes.

6.4 Update

6.4.1 Start of the update

Start the installation by executing Recognition Setup.exe

At first, you are asked to select the language for the installation assistant. To do this, click on the desired language in the selection box and confirm your input with "OK".
After that, the installation assistant for Spider will open. This assistant will guide you through the setup installation in the selected language. Click on "Next" to start the installation.

6.4.2 License agreement

In the next step, you are asked to read and accept the license agreement before starting the installation. The setup can only be continued after accepting the license agreement.
6.4.3 License file

Select the matching license file to continue the setup. The setup cannot be continued without the license file.

Click on "..." Button:

Select the license and then click "Open".
The selected license will be loaded and its details are shown.

**Note** If a license is found in the same directory which has been used to start the setup, it will be loaded automatically into the dialog (if valid).
6.4.4 Installation directory

During the update, the selection of the installation directory is prevented. An update is only possible in the existing path.

6.4.5 Database server

During an update, it is not possible to change the previously used SQL server.
The user, with which the connection is established, can either be the logged-in (Windows) user or an SQL user. To use an SQL user, you must tick the check box **Use SQL user for database connection** and fill in the fields **User name** and **Password** with the desired data.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL server name</td>
<td>Name of the SQL server, not to be changed!</td>
</tr>
<tr>
<td>Using SQL users for database connection</td>
<td>Select whether to use the logged-in domain user or an SQL user.</td>
</tr>
<tr>
<td>User name</td>
<td>Name of SQL user.</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the SQL user.</td>
</tr>
</tbody>
</table>
6.4.6 Summary

If the update is carried out for the first time, all products must be selected for update. The dialog is filled in already and cannot be changed anymore.

If one of the products has been updated earlier, it could happen that not all of the products are offered for updating. These products can nevertheless be selected for updating.
6.4.7 Installation

The installation assistant will now install Recognition. This can take some time. Please wait, until the installation is completed.

The successful completion of the installation will be shown in the progress dialog.
The setup has been completed successfully and can now be closed.

After completion of the installation, a log file will be written. For details to the log files, please refer to chapter Log files (on page 185).
7 Data center module (nova ratio appliance)

In this chapter
- Sizing of the virtual machine ................................................................. 178
- Launching of the appliance ..................................................................... 179
- Setting up the data center module .......................................................... 182

7.1 Sizing of the virtual machine

The sizing of the virtual machine depends on many parameters. The following data, which distinguish among four application scenarios, could serve as a guideline:

- **TEST:**
  Usage of the Datacenter appliance as a temporary test system

- **SMALL:**
  Usage of the Datacenter appliance in an environment with up to 1,000 systems

- **MEDIUM:**
  Usage of the Datacenter appliance in an environment with 1,000 to 5,000 systems

- **LARGE:**
  Usage of the Datacenter appliance in an environment with 5,000 to 10,000 systems

In case of environments with more than 10,000 systems, it is not possible to give any generalized specifications.

The following specifications are given for each of these scenarios:

- **# CPU threads:** Number of CPU threads for the appliance
- **Memory RAM:** Main memory for the appliance
- **Disc space:** File system size of the appliance
- **Network:** Number of network interfaces

<table>
<thead>
<tr>
<th>Sizing</th>
<th>TEST</th>
<th>SMALL</th>
<th>MEDIUM</th>
<th>LARGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of systems</td>
<td></td>
<td>up to 1.000</td>
<td>1.000 to 5.000</td>
<td>5.000 to 10.000</td>
</tr>
<tr>
<td># CPU threads</td>
<td>2</td>
<td>4</td>
<td>12</td>
<td>16</td>
</tr>
<tr>
<td>Memory RAM in GB</td>
<td>4</td>
<td>10</td>
<td>20</td>
<td>32</td>
</tr>
<tr>
<td>File system size in GB</td>
<td>150</td>
<td>250</td>
<td>500</td>
<td>750</td>
</tr>
<tr>
<td># of gigabit network interfaces</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
7.2 Launching of the appliance

7.2.1 Import of the VM

The virtual machine is available as an appliance for VMware. Please find below a short description of how to integrate the virtual machine into an existing VCenter environment by means of the vSphere client. Select "Virtual Machine..." under File -> New.

![Configuration screen](image)

Then select "User-defined" as configuration.

The following settings are self-explanatory. Please make sure to select the item "Existing virtual hard disc" under "Select hard disc".

![Configuration settings](image)

Now you can select the VM, which has previously been stored on the configured Datastore, by clicking on "Next". For using the import by web client, VMware offers its own KB article with video guide under the following address: [https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2032904](https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2032904)
7.2.2 Operating system users

For the operation of the appliance AND the Application, users have been created on the operating system level:

<table>
<thead>
<tr>
<th>User</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>erunbook</td>
<td>erunbook</td>
</tr>
<tr>
<td>root</td>
<td>nova123</td>
</tr>
</tbody>
</table>

By default, the appliance is provided with the host name "vm-spider-inv". The network settings are configured so that an IP address is assigned to the server via DHCP. A short illustration on how these settings can be adjusted to customer-specific environments is given below.

7.2.3 Adaptation of the host name

The host name may be changed by using the command "hostname". The call is executed under the root user and works immediately, however, only until the next restart of the appliance:

```
root@vm-spider-inv:~# hostname <new hostname>
```

In order to make the change of the host name permanent, the file /etc/hostname has to be adapted with a text editor under the root user. This can be carried out with e.g. the vi editor:

```
root@vm-spider-inv:~# vi /etc/hostname
<new hostname>
:x
```

7.2.4 Adaptation of the IP address

By default, the IP address of the appliance is set to use DHCP. To use a static IP address, the following adaptations in the file /etc/network/interface must be made under the root user:

```
root@vm-spider-inv:~# vi /etc/network/interface
```

In the delivery state of the appliance, the section "The primary Network interface" appears as follows:

```
# The primary network interface
auto eth0
iface eth0 inet dhcp
#iface eth0 inet static
#address 172.19.120.99
#netmask 255.255.255.0
#gateway 172.19.120.1
#dns-nameservers 172.19.120.1
```

To use a static IP address, the DHCP line has to be commented out. The lines "iface", "address", "netmask", "gateway" and "dns-nameservers" must be activated and filled with the desired values.

In the following example, the appliance shall use the IP address 172.19.120.99. The routing is done via gateway 172.19.120.1, the subnet mask is set to 255.255.255.0 and the system with IP address 172.19.120.1 will be used as DNS server:

```
# The primary network interface
auto eth0
#iface eth0 inet dhcp
iface eth0 inet static
address 172.19.120.99
netmask 255.255.255.0
gateway 172.19.120.1
dns-nameservers 172.19.120.1
```
After changing these files, the network services of the appliance have to be restarted:

```
root@vm-spider-inv:~# systemctl restart ifup@eth0
```

After this command, please use the `ifconfig` command to make sure that all settings have been applied correctly

```
root@vm-spider-inv:~# ifconfig
```

---

### 7.2.5 Creating a certificate

The tool for creating or updating an eRunbook certificate is already installed on the eRunbook server. On the eRunbook server, go to the directory `/opt/erunbook/product/tools` and run the script `erunbook_gen_SSL_certificate.sh` as user erunbook.

To create the certificate, some information is requested. Please note that the FQDN of the eRunbook server is expected in the query of the "common name" (in bold in the illustration).

```
erunbook@vm-dev-mj:~ > cd /opt/eRunbook/product/tools
erunbook@vm-dev-mj:~/product/tools ./erunbook_gen_ssl_certificate.sh
```

```
writing RSA key
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:Germany
Locality Name (eg, city) []:Koblenz
Organization Name (eg, company) [Internet Widgits Pty Ltd]:nova ratio AG
Organizational Unit Name (eg, section) []:eRunbook Dev
Common Name (eg, YOUR name) []:vm-dev-mj.novaratio
Email Address []:.

Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []:.
An optional company name []:.

Signature ok
subject=/C=DE/ST=Germany/L=Koblenz/O=nova ratio AG/OU=eRunbook Dev/CN=vm-dev-mj.novaratio
Getting Private key
```

Finally, the web browser has to be restarted. A script is available to start the Apache web server. This script is located in the directory `/opt/erunbook/product/admin/` and will be called with the parameter "restart"::

```
erunbook@vm-dev-mj:~/product/tools > cd /opt/eRunbook/product/admin/
erunbook@vm-dev-mj:~/product/admin > ./eRunbook_apache restart
```

The new erunbook certificate is created with the name "httpd.server.crt" and can be found in the directory `/opt/erunbook/software/additional/etc`

The certificate created in this way is a "self-signed SSL certificate". This means that web browsers will usually ask for a confirmation before granting access to the pages of this web server.
7.3 Setting up the data center module

In this chapter

General information .................................................................................................................. 182
Registration ............................................................................................................................... 182
Tenant assignment ..................................................................................................................... 183

7.3.1 General information

For the following configuration steps, in some cases, direct actions may be carried out on the data center module via an API. The creation or deletion of a tenant from spider results in multiple actions in the data module. Depending on the equipment used and the workload of the data center module, a single task executed in the background may take several minutes to complete.

Multi-platform inventory management may be carried out via the Columbus Datacenter Inventory. You may select whether the delivery of the inventory data is carried out to a Spider Data Collector (SDC) end point or a Columbus infrastructure server. From here, the inventory management files are delivered to the recognition module as Columbus Datacenter Container (cdc) file.

After the data center module has been set up, the *.cdc files may be processed with the next data delivery. This is usually done once per day and may take some time, depending on the size of the covered system landscape.

7.3.2 Registration

In order to enable processing of the inbound raw files in *.cdc format, the access to a data center module (nova ratio appliance) must be configured. This is done via the technical connection parameters of an API.

For this purpose, a data center module menu item is provided in the main menu of the system section.

Clicking this menu item will provide access to a connection page via which the data center module may be set up. Technically, only one data center module is set up. In case of multitenancy systems, it may be necessary to set up multiple data center modules for load distribution reasons.
A data center module may be set up via the "Create" ribbon button. In addition to a name for internal reference, the URL to the API as well as the access data of the technical user must be entered.

After registration, the data center module details page is displayed. In the left section, configured data center modules are displayed. The details for the first existing data center module are automatically loaded when accessing the page. For the currently selected data center module, you may use the "Test" button to immediately test the connectivity.

### 7.3.3 Tenant assignment

A data center module is able to process the data of multiple tenants. Conversely, a tenant is always assigned to one data center module.

Therefore, the assignment of a data center module takes place in the context of the affected tenant.
The setup page is accessed via the data center module tab.

Any previously configured access to a data center module will be available via a selection field. The selection must be confirmed by clicking "Save". This will start the setup of the tenant in the data center module in the background.

This completes the tenant setup. If inventory data related to the tenant is delivered for the data center module, this data is automatically transferred to the data center module for processing. In Spider, the results will be displayed after a processing run.

- Systems
- Software from the data center software detection
- Oracle data
8 Log files

In this chapter

Brainware.log ................................................................. 185
Smart-Inspect log files (*.sil) ............................................ 185

Log files are written for the installation and the update of all setups as well as the services. Please refer to the table to see where to find these.

<table>
<thead>
<tr>
<th>Product</th>
<th>Path to the log file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spider Installation / Update</td>
<td>%ProgramData%\brainwaregroup\Logs</td>
</tr>
<tr>
<td>Recognition Installation / Update</td>
<td></td>
</tr>
<tr>
<td>Software catalog</td>
<td></td>
</tr>
<tr>
<td>Spider Services</td>
<td>%ProgramData%\brainwaregroup\CoreServer_xx&lt;Service name&gt;</td>
</tr>
<tr>
<td>Spider Data Receiver</td>
<td>%Windir%\</td>
</tr>
<tr>
<td>Spider Data Collector</td>
<td></td>
</tr>
<tr>
<td>EDC monitor</td>
<td>%ProgramData%\brainwaregroup\EDCMonitor\Logs</td>
</tr>
</tbody>
</table>

8.1 Brainware.log

The log file Brainware.log will be rewritten periodically. Older revisions will be renamed with Brainware_0.log, Brainware_1.log, Brainware_2.log, etc.

This file is a plain text file which may be edited with any text editor.

8.2 Smart-Inspect log files (*.sil)

The *.sil files have the SmartInspect format. These files cannot be read immediately. You will need a (free-of-charge) tool of the company Gurock Software GmbH.

The SmartInspect redistributable console can be downloaded under SmartInspect Redistributable Console.