Brainware Intelligent Capture

Installation Guide

Version: 5.9.1

Written by: Documentation Team, R&D
Date: Monday, June 29, 2020

Hyland

Table of Contents

About Brainware Intelligent Capture ... 8
Brainware API ... *8*
Prerequisites ... *8*
About the Brainware Intelligent Capture process ... *9*
About the Brainware Intelligent Capture database ... *10*
Install Brainware Intelligent Capture ... 10
Download the setup package ... *11*
About the complete and custom installation types ... *11*
About Help files ... *11*
HelpLink parameters ... 11
Modify SetupType.ini for Help ... 12
Verify SQL Server permissions ... *12*
Verify Oracle permissions ... *13*
Install BIC attended ... *13*
Install BIC unattended ... *14*
Silent Install.ini parameters ... 15
[General] ... 15
[Applications] ... 16
[OCR Engines] ... 16
[Additional] ... 17
[AutoServiceUpdate] ... 17
[Database Configuration] ... 18
[DB Credentials] ... 18
Install an additional Runtime Server instance ... *19*
Brainware Intelligent Capture subdirectories ... *19*
Modify the application-specific HelpLink parameters ... *19*
CONFIG files ... *20*
Install the database manually ... *20*
Create a SQL Server database ... 20
Create an Oracle database ... 21

Modify the database connection strings 21
Modify the .NET configuration for Oracle 23
Components Version Info tool 23
Components General Info view *23*
Components Licensing Info view *23*
Review the installed components *24*
Review the component license information *24*
Manage the BIC components 24
Add or remove BIC components *24*
Manually register components *25*
Configuration for Web Verifier 25
Configure IIS for Web Verifier *25*
Role services configuration for Web Verifier in IIS 7.5 and above 26
Common HTTP Features 26
Application Development 26
Health and Diagnostics 26
Create an application pool for BIC in IIS 7.5 and above 26
Configure BIC in IIS 7.5 and above 27
Configure a white label directory in IIS 27
Configure Web Verifier *27*
Set the path to the license file 28
Modify the instanceName when using multiple web servers 28
Modify the database connection strings for Web Verifier 28
Configure server security for Web Verifier *29*
Add the user context in SQL Server 29
Verify the IIS settings 29
Set permissions for BIC projects 29
Configure Internet Explorer for Web Verifier *30*
Implement single sign-on authentication *30*
About the single sign-on authentication for Web Verifier 30
Enable the single sign-on authentication 30
About the single sign-on session and the Web Verifier session 31

Modify the Web Verifier session timeout ... 31
Configure Windows authentication ... *31*
About Windows authentication for Web Verifier ... 31
Configure Windows authentication in IIS 7.5 and higher ... 32
Create a Windows authentication-version of the Web.config file ... 32
Switch back to Forms authentication ... 32
Configure cookies for Web Verifier ... *33*
About Web Verifier performance ... *33*
Image conversion ... 33
Remote Matching Service ... 34
Delayed validation ... 34
Use Traditional Chinese ... *34*
Access Web Verifier ... *34*
Additional columns in Verifier or Web Verifier ... *35*
Display and name additional Verifier columns: SQL Server ... 35
Display and name additional Verifier columns: Oracle ... 36
Display additional Web Verifier columns ... 36
Change the Web Verifier column names ... 36
Configure global application settings ... 37
About workflow history reporting ... *37*
Configure workflow history reporting: SQL Server ... 37
Configure workflow history reporting: Oracle ... 38
About disabling batch deletion in Runtime Server and Designer ... *38*
Disable batch deletion: SQL Server ... 38
Disable batch deletion: Oracle ... 38
About modifying the URL expiration time for Web Verifier ... *39*
Modify the URL expiration time: SQL Server ... 39
Modify the URL expiration time: Oracle ... 39
Configure BIC security ... 39
File system security ... *40*
Recommended accounts and groups ... *41*
Configure access to project data ... *42*
About the service account on a domain network ... *43*

About the service account for system monitoring ... *43*
About the service account for email importing ... *43*
About INI file encryption ... *43*
Encrypt a password for a database connection string ... *43*
About user password encryption ... *44*
Change the hashing algorithm ... 45
Configure BIC Runtime Components ... 45
About RTS Remote Administration MMC ... *46*
Configure the Runtime Service Manager service ... *46*
Configure the RTS Remote Administration MMC Snap-in ... *46*
Configure the email import feature in Microsoft Outlook ... *47*
About the desktop heap size ... 48
Modify the desktop heap size ... *48*
Ideal desktop heap size ... *48*
About logging ... 49
Application log files ... *49*
Error log files ... *50*
OCR engine languages ... 50
Available OCR Engines ... *51*
Cleqs Barcode Engine ... 51
FineReader10 OCR Engine ... 51
FineReader11 OCR Engine ... 51
Kadmos 5 OCR Engine Client Edition ... 51
Kadmos 5 OCR Engine Server Edition ... 52
QualitySoft Barcode Engine ... 52
About automated update ... 52
Modify the batch file ... *52*
Modify the application shortcuts for Verifier and Designer ... *52*
Automate Runtime Server updates ... *53*
About port configuration ... 53
Configure a different port for Runtime Server ... *53*
File permission matrix ... 54
Web.config options and associated resource file parameters ... 57

About navigation to documents for indexing *64*
Example 64
Enable navigation to indexable documents *65*
Registry options 65
Create the registry key ErrorTraceDir *65*
Create the registry key HideBatchReleaseDialog *66*
Modify the registry key ErrorTrace - All *66*
Create the registry key MaximumDiskspaceUsageMB *67*
Create the registry key TotalDaysToKeepFiles *67*

About Brainware Intelligent Capture

Brainware Intelligent Capture (BIC) is a document processing system.

It combines optical character recognition (OCR), automatic data extraction from any document type, and validation of that data against known data sources for auto-processing to your ECM system and other core business applications.

Brainware Intelligent Capture includes the following applications.

- Brainware Intelligent Capture Designer
- Brainware Intelligent Capture Runtime Server
- Brainware Intelligent Capture Verifier
- Brainware Intelligent Capture Web Verifier

For information about the document processing system, see About the Brainware Intelligent Capture process.

Brainware API

The Brainware Intelligent Capture setup package includes the Brainware API installation files.

For more information, see the *Brainware API Installation Guide*.

Prerequisites

To verify your system requirements and database meet the minimum requirements for BIC, refer to the *Brainware Intelligent Capture Technical Specifications*. Before you install BIC, verify the following prerequisites.

- Ensure that you have local administrator rights and access to the Windows registry.
- Enable VBScript execution.
- Verify that you have installed Internet Information Services (IIS) on your server if your installation will include Web Verifier.
- If you use Oracle as a database, install a 32-bit Oracle client on any workstation or server where BIC communicates with the database, such as when using Designer or Verifier.
- Create the users and groups if you use the Microsoft-recommended resource rights assignment model.

About the Brainware Intelligent Capture process

Brainware Intelligent Capture (BIC) analyzes text from any media type. It uses artificial neural network techniques to automatically classify structured and unstructured documents and extract meaningful information from them. Once a sample based learning method is employed BIC can handle information that is similar to the samples without programming or extensive rule setting. BIC can operate at high speed and can be implemented on parallel hardware to further enhance performance.

BIC forms a complete document processing system, as illustrated in the diagram below

First, using capture, documents come into the process from a variety of sources.

Next, BIC recognizes all eligible data values on the page.

Then, BIC uses the extracted data to sort and classify the documents. Based on the document type, BIC extracts field-level and line item level data. It does this without templates, anchors, keywords or zones.

Finally, BIC can validate extracted data against your business application data to ensure accuracy before exporting it for workflow processing.

About the Brainware Intelligent Capture database

The BIC installation process allows you to create the required database on your Microsoft SQL Server or ORACLE server during the installation. You can also create the database separately after the BIC installation procedure.

BIC stores the following data in the database.

- Documents
- Batches
- Project references
- Web Verifier configuration
- Batch and document lock handling
- Users, groups, roles, and relationships
- Application level user licensing

Install Brainware Intelligent Capture

To install BIC, complete the following procedures.

- Download the setup package
- Optional. Modify the help file location
- Optional. Complete one of the following substeps to verify database permissions.

  Note:
  To create the database during BIC installation, you must have user credentials which have the proper permissions.

  - Verify SQL Server permissions
  - Verify Oracle permissions
- Install BIC attended or Install BIC unattended
- Optional. Modify the application-specific HelpLink parameters
- If you did not install the database with the installation wizard, complete the steps in Install the database manually.
- Optional. Encrypt the password for a database connection string.
- Copy the license file. For more information, see "Copy the license file to local license directories" in the *Brainware Intelligent Capture Product Licensing Guide*.
- Configure Internet Information Services and Web Verifier, if the installation includes Web Verifier

- Configure BIC security
- Configure BIC Runtime Components

Download the setup package

To obtain Perceptive product installation files, complete the following steps.

1. Contact the Hyland Software Technical Support group.
   For a list of Technical Support phone numbers, go to www.hyland.com/pswtscontact.
2. Save and unzip the installation files locally so you can access them during installation.

About the complete and custom installation types

When you install BIC with an attended installation, you choose a complete or a custom installation type.

The complete option installs Designer, Runtime Server, Verifier and Web Verifier in the *[drive:]\[Program directory]\[Installation directory]* and creates the Brainware Intelligent Capture program group. It also installs the following recognition engines.

- FineReader 10
- FineReader 11
- Kadmos 5
- QualitySoft

The custom installation type allows you to choose which applications, demo projects, and recognition engines you want to install. It also lets you select which programs you want to update automatically.

About Help files

By default, the Brainware Intelligent Capture products provide hosted product help, which enables you to always access the most recent information directly from the documentation website. If your company's network security does not allow users to open a URL, you can download static help through the Customer Portal. To implement static help instead of hosted help, you must modify the configuration.

The SetupType.ini file enables you to specify the path and file that the BIC application opens when you click Help in the Help menu of a particular product. You can place the files on a web server and specify the URL to the file that launches Help for that product or you can unzip the files on a local or a server drive, and use that file path.

HelpLink parameters

You can redirect product help from the default web URLs to a file on your system.

The HelpLink variable is a label that applies to a particular product. The products that provide help include: Designer, RTS, Verifier, Learnset Manager, and Web Verifier.

The syntax includes the HelpLink type, which defines the product, and the path to the static file location.

```
HelpLink = [path]/PIC.htm#5.9

HelpLink_Designer = [path]/PICD.htm
```

```
HelpLink_RTS = [path]/PICRS.htm

HelpLink_Verifier = [path]/PICV.htm

HelpLink_LSM = [path]/PICV.htm#Topics/Verifier/Working with the Learnset
Manager.htm

HelpLink_WebVerifier = [path]/PICWV.htm
```

For path, supply the URL or path (absolute or relative) to the launch file for that specific help project. The following examples show a URL, a network path, and a local path.

- `HelpLink_Designer = https://docs.mycompany.com/mypath/Designer/PICD.htm`
- `HelpLink_Designer = \\myserver\mypath\Designer\PICD.htm`
- `HelpLink_Designer = C:/mypath/Designer/PICD.htm`

Modify SetupType.ini for Help

To modify the SetupType.ini file, complete the following steps.

1. From the setup directory, open the **SetupType.ini** file with a text editor.
2. In the **SetupType.ini** file, in the [Help] section, specify the path for each HelpLink. The following lines show sample URLs to the hosted documentation.

   Example

   ```
   HelpLink_Designer =
   https://docs.mycompany.com/mypath/Designer/PICD.htm

   HelpLink_RTS = https://docs.mycompany.com/mypath/Runtime_
   Server/PICRS.htm

   HelpLink_Verifier =
   https://docs.mycompany.com/mypath/Verifier/PICV.htm

   HelpLink_WebVerifier = https://docs.mycompany.com/mypath/Web_
   Verifier/PICWV.htm
   ```

3. Save and close the file.

Verify SQL Server permissions

To use BIC with a SQL Server database, verify that your account has the following rights.

Note: You can use Windows authentication if the user performing the installation has the appropriate rights to the database server.

- Rights to create, modify, and delete tables.
- Rights to add, modify, and delete data.

Verify Oracle permissions

To use BIC with an ORACLE database, complete the following preparatory steps.

Note:
You can use Windows authentication if the user performing the installation has administrative rights to the database server.

1. As an administrator, create a new tablespace and user for the BIC database.

   Note:
   The user name must be all-uppercase.

2. Assign the following rights to the user.
   - Insert, modify, and delete data
   - Create tables
   - Create views

Install BIC attended

To install BIC, complete the following steps.

1. Run **setup.exe**.

   Note: The installation process is available in English and German. The language used depends on the regional settings of your system. The default language is English.

2. If .NET Framework 4.6 is not installed, complete one of the following substeps.
   - To allow setup.exe to install .NET Framework 4.6, select **Let the setup install .NET Framework Version 4.6 (Recommended)** and then click **Next**.

     Note:
     The .NET Framework installer automatically restarts the computer without further notification.

   - To cancel the setup and install the required .NET Framework manually, select **Abort setup** and then click **Next**. After installing .NET Framework, rerun **setup.exe** and proceed with the following steps.
3. In the **Setup Hyland Brainware Intelligent Capture** page, click **Next**.
4. In the **License Agreement** page, read and accept the End-User License Agreement (EULA), and then click **Next**.
5. In the **Installation Type** page, select **Complete** or **Custom** and click **Next**.
6. If you selected **Custom**, complete the following substeps. If you selected **Complete**, continue to the next step.
   1. In the **Installation Directory** page, accept the default or change the directory, and then

click **Next**.

2. In the **Feature Selection** page, clear any unrequired applications, demo projects, and recognition engines and then click **Next**.
3. Optional. In the **Configuration of Auto Update Feature** page, select the programs you want to update automatically.
4. The following option is currently not in use: Optional. In the **Shared network updates directory** field, type or browse to a path.

   Note: The path must exist. The installation process uses this path to create and configure the batch files required for the automated update feature.

5. Click **Next**.

7. In the **Program Folder** page, accept the default program directory or select one of the existing directories and then click **Next**.
8. In the **Selected Install Options** page, verify your selections and then click **Next**.
9. In the **WIBU-KEY Runtime-Kit** dialog box, click **Yes**.
10. In the **Database Setup Options** page, select one of the following options and then click **Next**.
    - SQL Server
    - Oracle
    - Do not install database

    Note: You can create the database separately after the BIC installation process.

11. For SQL Server or ORACLE, complete the following substeps.
    1. In the **Login Credentials** page, either select **Windows Authentication** or type the user ID and password and then click **Next**.
    2. In the **Database Server Information** page, in the **Database Server Name** field, type the database server name and then click **Next**.
12. In the **Performed Tasks** page, click **Next**.
13. Optional. In the **Icons on Desktop** page, select **Create desktop shortcuts for applications** and click **Finish**.

Install BIC unattended

To install BIC on several machines concurrently, such as Verifier workstations, use the silent installation mode.

To install BIC silently, complete the following steps.

1. From the *[drive:]\[setup directory]* directory, open the **Silent Install.ini** file with a text editor.
2. In the **Silent Install.ini** file, change the parameters according to your needs.

   Note: You can delete single parameters or complete sections, but you cannot move a parameter outside of its appropriate section.

3. Save and close the file.
4. From the *[drive:]\[setup directory]* directory, execute the **setupsilent.bat** file.

Silent Install.ini parameters

The following topics describe the parameters available in the Silent Install.ini file.

- [General]
- [Applications]
- [OCR Engines]
- [Additional]
- [AutoServiceUpdate]
- [Database Configuration]
- [DB Credentials]

[General]

This section contains general installation parameters.

Path

The installation path, without a trailing backslash.

Example

```
Path = C:\Program Files\YourCompanyName
```

EULA

End-user license agreement The following values are recognized:

“Accepted”

“Not Accepted”: Default value - the silent installation cancels.

MoveComponentsIfRequired

Indicates whether to use the existing component directory or to move any previous components to the new BIC directory prior to installation.

0: Use existing component directory.

1: Default value – Move components to the new directory.

CreateDeskTopIcons

0: Default value – do not create desktop shortcuts.

1: Create desktop shortcuts.

InstallWibuKey

0: Skip WIBU-key driver installation.

1: Default value - install WIBU-key drivers

StopIfDotNetIsNotFound

Web Verifier and the database connections require .NET Framework.

0: If the required .NET Framework is not present, the installation proceeds and automatically installs the required version.

1: Default value - Cancel the installation if the required .NET Framework version is not present.

[Applications]

Defines which applications to install.
To install only the extraction components, set all parameters in this section to 0.

Designer

0: Don’t install Designer

1: Default value – Install Designer

Verifier

0: Don’t install Verifier

1: Default value – Install Verifier

Runtime Server

0: Don’t install Runtime Server

1: Default value – Install Runtime Server

Web Verifier

0: Don’t install Web Verifier

1: Default value – Install Web Verifier

[OCR Engines]

Defines which OCR engines to install.

FineReader10

0: Don’t install the FineReader10 engine

1: Default value – Install FineReader10 engine

FineReader11

0: Don’t install the FineReader11 engine

1: Default value – Install FineReader11 engine

Kadmos5

0: Don’t install the Kadmos 5 engine

1: Default value – Install Kadmos 5 engine

Cleqs

0: Don’t install the Cleqs engine

1: Default value – Install Cleqs engine

QualitysoftBarcode

0: Don’t install the QualitySoft engine

1: Default value – Install QualitySoft engine

[Additional]

Additional files to install.

Demo Files

0: Don’t install the demo project files

1: Default value – Install the demo project files

[AutoServiceUpdate]

Defines whether the automatic service update feature installs.

ForDesigner

0: Default value – Don’t define an automatic service update for Designer.

1: Define an automatic service update for Designer.

ForVerifier

0: Default value – Don’t define an automatic service update for Verifier.

1: Define an automatic service update for Verifier.

NetworkUpdateFolder

The path where the automatic service update will look for updates.

The default value is an empty string.

[Database Configuration]

Settings for an existing database server.

DBServerType

1: Configure the SQL Server database

2: Configure the Oracle database

3: Default value – Don't configure a database

UseDBConfIniFile

Path and filename of a text file that contains the database connection string.

The default value is an empty string. If you do not define a file, the installer uses the credentials in the [DB Credentials] section. If the [DB Credentials] section does not exist, the DBServerType parameter defaults to 3.

[DB Credentials]

You can use this section instead of defining a file in the parameter UseDBConfIniFile.

Note: The database configuration skips, if the parameter UseDBConfIniFile contains an empty string.

The following options apply for SQL Server connections only.

SQLServerWindowsAuthent

0: Default value – Do not use Windows authentication for database access

1: Use Windows authentication for database access

SQLServerAdminUser

The DBA account name. The default value is an empty string.

SQLServerAdminPassword

The DBA account password. The default value is an empty string

The following options apply for both SQL Server and ORACLE connections.

DBUserWindowsAuthent

0: Default value – Do not use Windows authentication for database user

1: Use Windows authentication for the database user

DBUserName

The database user account name. The default value is an empty string.

DBUserPassword

The database user account password. The default value is an empty string.

DatabaseServerPath

The database name in the format <*MachineName*>\<*InstanceName*>. The default value is an empty string.

Install an additional Runtime Server instance

To install an additional Runtime Server instance and connect it to an existing database, complete the following steps.

1. Install BIC without installing the database.
2. Copy the following configuration files from an existing installation to the new installation directory.
    - *[Installation path]*\Brainware Intelligent Capture Web Server\Web.config
    - *[Installation path]*\Brainware Intelligent Capture\bin\DstDsr.exe.config
    - *[Installation path]*\Brainware Intelligent Capture\bin\DstHost.exe.config
    - *[Installation path]*\Brainware Intelligent Capture\bin\DstSlm.exe.config
    - *[Installation path]*\Brainware Intelligent Capture\bin\DstVer.exe.config
    - *[Installation path]*\Brainware Intelligent Capture\bin\DstWkBrw.exe.config

Brainware Intelligent Capture subdirectories

Setup creates the following subdirectories in the installation directory.

- \Components\Bwe contains the BIC Toolkit.
- \Components\Cairo contains the license file and the base components for imaging and recognition.
- \Components\Cedar contains the base components for document analysis.
- \Components\Tools contains the installation log file as well as several tools and utilities for BIC, such as the SCBLibVersion.exe component version information tool
- \Brainware Intelligent Capture\bin contains the BIC executables and the settings files.
- \Brainware Intelligent Capture\bin\Log contains the log files.
- \Brainware Intelligent Capture Web Server contains the BIC web components, the Web.config file, and other web libraries used by Web Verifier.
- \Projects contains demo projects.
- \License contains the shared runtime license file.

Modify the application-specific HelpLink parameters

You can modify the application-specific HelpLink parameters if required. Complete the following steps.

1. From ***[Installation path]*\Brainware Intelligent Capture\bin**, open the required configuration file, such as **DstDsr.exe.config** for Designer, in a text editor.
2. Search for the following line.

```
<add key="HelpLink"
```

3. Modify the `value` parameter according to your needs.

CONFIG files

The following table provides a list of the CONFIG files used by the BIC applications.

Application	CONFIG files
Designer	*[Installation path]*\Brainware Intelligent Capture\bin\DstDsr.exe.config
Runtime Server	*[Installation path]*\Brainware Intelligent Capture\bin\DstHost.exe.config
Learnset Manager	*[Installation path]*\Brainware Intelligent Capture\bin\DstSlm.exe.config
Verifier	*[Installation path]*\Brainware Intelligent Capture\bin\DstVer.exe.config
Web Verifier	*[Installation path]*\Brainware Intelligent Capture Web Server\Web.config
Workdoc Browser	*[Installation path]*\Brainware Intelligent Capture\bin\DstWkBrw.exe.config
Supervised Learning in Web Verifier	*[Installation path]*\Brainware Intelligent Capture\bin\Brainware.System.Project.exe.config

Install the database manually

If you did not install the database with the installation wizard, you can execute the scripts manually. Complete the following steps.

1. Complete one of the following substeps.
   - Create a SQL Server database.
   - Create an Oracle database.
2. Modify the database connection strings.
3. If you use Oracle as a database, modify the .NET configuration for Oracle.

Create a SQL Server database

To create a SQL Server database, complete the following steps.

1. Start the **SQL Server Management Studio**.
2. Log in using an account with administrator rights.
3. Create a new database with a meaningful name, such as **Brainware Intelligent Capture**.
4. From the ***[drive:]\[setup directory]*\FirstPart\Database\CreationScripts\SQL Server** directory, execute the **BrwCreateDatabase.sql** script.

5. From the ***[drive:]\[setup directory]*\FirstPart\Database\UpdateScripts\SQL Server** directory, open the **BRW_Upgrade_Database.sql** script.
6. In the **BRW_Upgrade_Database.sql** script, search for the term `TargetDatabaseName` and change the term to the name of your BIC database.
7. Execute the **BRW_Upgrade_Database.sql** script.

Create an Oracle database

To create an Oracle database, complete the following steps.

1. As an administrator, create a new tablespace and user for the BIC database.

   Note:
   The user name must be all-uppercase.

2. Start **SQL*Plus or the ORACLE Management Console**.
3. From the ***[drive:]\[setup directory]*\FirstPart\Database\CreationScripts\Oracle** directory, execute the **BrwCreateDatabase.sql** script.
4. From the ***[drive:]\[setup directory]*\FirstPart\Database\UpdateScripts\Oracle** directory, open the **BRW_Upgrade_Database.sql** script.
5. In the **BRW_Upgrade_Database.sql** script, search for the term `TargetDBSchemaName` and change it to the name of the user associated to the BIC database.
6. Execute the **BRW_Upgrade_Database.sql** script.

Modify the database connection strings

To modify the database connection strings for Web Verifier, see “Modify the database connection strings for Web Verifier”.

To modify the database connection strings for all BIC components, except Web Verifier, complete the following steps.

1. From the ***[Installation path]*\Brainware Intelligent Capture\bin** directory, open **DstDsr.exe.config** in a text editor.
2. Search for the `<connectionStrings>` element.

   Note:
   For information about password encryption, see Encrypt the password for a database connection string.

3. For a SQL Server database, modify the following values.
   - Set `Data Source`.
   - Set `Initial Catalog` to the SQL Server database catalog.
   - Set `User ID` to the SQL Server user ID.
   - Set `Password` to the SQL Server password.

   Example

```
<connectionStrings>
<add name="Entities"

connectionString="metadata=res://*/Entity.Entities.csdl|res://*/Entity
.Entities.ssdl|r
es://*/Entity.Entities.msl; provider=System.Data.SqlClient;provider
connection
string=&quot;Data Source=<DataSource>;Initial
Catalog=<SQLServerDatabaseCatalog>;Integrated Security=false;User

ID=<UserId>;Password=<UserPassword>;MultipleActiveResultSets=True&quo
t;"
providerName="System.Data.EntityClient" />
</connectionStrings>
```

Note: To copy the connections string example as a single line, open this document in Acrobat Reader and copy and paste the string from there.

4. For an ORACLE database, modify the following values.
   - Set `Data Source`.
   - Set `User ID` to the service account user ID.
   - Set `Password` to the service account password.

   Example

```
<connectionStrings>
<add name="Entities"

connectionString="metadata=res://*/Entity.ORAEntities.csdl|res://*/Ent
ity.ORAEntities.
ssdl|res://*/Entity.ORAEntities.msl; provider=EFOracleProvider;
Provider Connection
String='Data Source=<OracleServerName\InstanceName>;User
ID=<UserID>;Password=<UserPassword>'"
providerName="System.Data.EntityClient" />
</connectionStrings>
```

Note: To copy the connections string example as a single line, open this document in Acrobat Reader and copy and paste the string from there.

5. Save and close the file.
6. Repeat the previous steps for the following configuration files.
   - Brainware.System.Project.exe.config
   - DstSlm.exe.config
   - DstVer.exe.config

- DstHost.exe.config
- DstWkBrw.exe.config

Modify the .NET configuration for Oracle

If you use BIC with an Oracle database, complete the following steps.

1. From *<drive>:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\CONFIG*, open **machine.config** in a text editor.
2. Search for the `<system.data>` element.
3. Under the `<DbProviderFactories>` element, verify or add the following element.

   Example

   ```
   <add name="EF Oracle Data Provider" invariant="EFOracleProvider"
   description="EF
   Provider for Oracle" type="EFOracleProvider.EFOracleProviderFactory,
   EFOracleProvider, Version=1.0.0.0, Culture=neutral,
   PublicKeyToken=def642f226e0e59b"/>
   ```

   Note: To copy this example as a single line, open this document in Acrobat Reader and copy and paste the string from there.

4. Save and close the file.

Components Version Info tool

The Components Version Info tool provides information about the installed DLLs and the components that require an entry in the license file to be available.

Components General Info view

This view lists the installed primary DLLs and provides the following information.

See also: Review the installed components.

- Name. Name of the installed DLL.
- Description. Description of the DLL.
- Build. Build number of the DLL.
- Product version. Version of the DLL.
- Date. Compilation date and time.
- Build Date Time. Date and time the build was created.
- Install Directory. Path to the component location.

Components Licensing Info view

This view lists licensable components and provides the following information.

See also: Review the component license information.

- Component Name. Name of the component.
- Component Type. Type of the component.
- Status. License status of the component.
- License File Path. License file location.
- License Files. License file name.
- Expires. License expiration date for component.
- Version. Version number.
- Customer. Customer name.
- Customer ID. Customer ID.
- Serial. Serial number.

Review the installed components

To review the installed components, complete the following steps.

1. Start the **Components Version Info** tool.
2. To display the list of installed components, click **View > Components General Info**.
3. Optional. To copy the displayed information to the clipboard, click **File > Copy to Clipboard**.
4. Optional. To save the displayed information to a file, click **File > Save to File**.

Review the component license information

To review the component license information, complete the following steps.

1. Start the **Components Version Info** tool.
2. To display the license information, click **View > Components Licensing Info**.

Manage the BIC components

The BIC installation process enables you to add or remove the following components.

- Brainware Intelligent Capture Designer
- Brainware Intelligent Capture Runtime Server
- Brainware Intelligent Capture Verifier
- Brainware Intelligent Capture Web Verifier

Add or remove BIC components

To modify an existing Brainware Intelligent Capture installation and to add or remove components, complete the following steps.

1. From **Windows Programs and Features**, select **Brainware Intelligent Capture** and then click **Change**.
2. In the **License Agreement** page, read and accept the End-User License Agreement (EULA), and then click **Next**.
3. In the **Setup** page, select **Modify** and then click **Next**.

4. In the **Feature Selection** page, select or clear the desired components and then click **Next**.
5. In the **Icons on Desktop** page, complete the following substeps.
    1. Optional. Select **Create desktop shortcuts for applications**.
    2. Click **Finish**.

Manually register components

The installation process automatically registers the Cro*.dll, Cdr*.dll, and Bwe*.dll components. For troubleshooting purposes, you can manually register these components. To register the components, complete the following steps.

1. From the *[Installation path]\Brainware Intelligent Capture\Components\Cairo* directory, execute the **RegCro.bat** file.
2. From the *[Installation path]\Brainware Intelligent Capture\Components\Cedar* directory, execute the **RegCdr.bat** file.
3. From the *[Installation path]\Brainware Intelligent Capture\Components\Bwe* directory, execute the **RegBwe.bat** file.

Configuration for Web Verifier

Your Internet Information Server (IIS) executes Web Verifier. To configure IIS and Web Verifier, complete the following tasks as necessary.

- Configure IIS for Web Verifier
- Configure Web Verifier
- Configure server security for Web Verifier
- Configure Internet Explorer for Web Verifier
- Optional. Implement single sign-on authentication
- Optional. Configure Windows authentication
- Optional. Configure SSL. For information on how to configure SSL on your IIS machine, refer to http://support.microsoft.com.
- Optional. Configure cookies for Web Verifier

Configure IIS for Web Verifier

To configure IIS for Web Verifier, complete the following tasks.

- Ensure that the required role services are enabled.
- Create an application pool for BIC in IIS 7.5 and above
- Configure BIC in IIS 7.5 and above
- Configure a white label directory in IIS

Role services configuration for Web Verifier in IIS 7.5 and above

Web Verifier requires the following role services in IIS.

Common HTTP Features

- Static Content
- Default Document
- Directory Browsing
- HTTP Errors

Application Development

- ASP.NET 4.6 (ASP.NET 4.5 for operating system earlier than Windows Server 2016)
- .NET Extensibility
- ISAPI Extensions
- ISAPI Filters

Health and Diagnostics

- HTTP Logging
- Request Monitor

Create an application pool for BIC in IIS 7.5 and above

To create an application pool, complete the following steps.

1. Start **Internet Information Services (IIS) Manager**.
2. In the **Internet Information Services (IIS) Manager** window, in the left pane, right-click the local computer and then click **Switch to Content View**.
3. In the middle pane, right-click **Application Pools** and then click **Add Application Pool**.
4. In the **Add Application Pool** dialog box, complete the following substeps.
    1. In the **Name** field, type `WebVerifierPool`.
    2. From the **.NET CLR version** list, select **.NET CLR v4.0.30319** and then click **OK**.
5. In the left pane, click **Application Pools**.
6. In the middle pane, right-click **WebVerifierPool** and then click **Advanced Settings**.
7. In the **Advanced Settings** dialog box, provide the following settings and then click **OK**.
    - Enable 32-Bit Applications = True
    - Managed Pipeline Mode = Integrated
    - Identity = NetworkService
    - Load User Profile = True

Configure BIC in IIS 7.5 and above

To configure BIC in IIS 7.5 and above, complete the following steps.

1. Start **Internet Information Services (IIS) Manager**.
2. In the **Internet Information Services (IIS) Manager** window, in the left pane, expand **Sites > Default Web Site**.
3. Right-click **Default Web Site** and then click **Add Application**.
4. In the **Add Application** dialog box, complete the following substeps.
    1. In the **Alias** field, type `WebVerifier`.
    2. In the **Application pool** field, select the pool that was configured before, such as **WebVerifierPool**.
    3. In the **Physical path** field, type or browse to the ***[Installation path]*\Brainware Intelligent Capture Web Server** directory and then click **OK**.
5. In the **Internet Information Services (IIS) Manager** window, in the left pane, select **WebVerifier**.
6. In the middle pane, under **IIS**, double-click **Default Document**.
7. In the right pane, click **Add**.
8. In the **Add Default Document** dialog box, in the Name field, type `Login.aspx` and then click **OK**.

Configure a white label directory in IIS

If you are using a BIC version that contains a white label (WL) directory inside the Components\Cedar directory, create a WL virtual directory in IIS. Complete the following steps.

1. In the **Internet Information Services (IIS) Manager** window, in the left pane, open the tree view until **Web Verifier** displays.
2. Right-click **Web Verifier**, then click **Add Virtual Directory**.
3. In the **Add Virtual Directory** dialog box, complete the following substeps.
    1. In the **Alias** field, type `WL` as the name for the virtual directory.
    2. In the **Physical path** field, type or browse to the ***[Installation path]*\Brainware Intelligent Capture\Components\Cedar\WL** directory and then click **OK**.

Configure Web Verifier

To configure Web Verifier, complete the following tasks.

1. Set the path to the license file.
2. Modify the instanceName when using multiple web servers.
3. Modify the database connection strings for Web Verifier.
4. To enhance application performance, you can optionally enable HTTP compression. For more information, refer to Microsoft Technet.

Set the path to the license file

To set the path to the license file, complete the following steps.

1. From the *[Installation path]\Brainware Intelligent Capture Web Server* directory, open **Web.config** in a text editor.
2. Search for the following line.

   ```
   <project licensePath="[Installation path]\Brainware Intelligent Capture\License\Runtime.lic"
   ```
3. Set the `licensePath` value to your license file location.
4. Save and close the file.

Modify the instanceName when using multiple web servers

To ensure that the instanceName value in the Web.config is unique across all web servers accessing the same BIC database, complete the following steps.

1. From the *[Installation path]\Brainware Intelligent Capture Web Server* directory, open **Web.config** in a text editor.
2. Search for the following XML elements.

   ```
   <system.controllers><client instanceName="Web Verifier" remoteObjectRenewalTimeout="180"></client>
   ```
3. Change `instanceName="Web Verifier"` to `instanceName="Web Verifier [xx]"` with xx being unique across the system.

   Example `instanceName="Web Verifier 01"` for the first server.

   Example `instanceName="Web Verifier 02"` for the second server.

Modify the database connection strings for Web Verifier

To modify the database connection string, complete the following steps.

1. From the *[Installation path]\Brainware Intelligent Capture Web Server* directory, open the **Web.config** file in a text editor.
2. Search for the `<connectionStrings>` element.
3. For a SQL Server database, modify the following values.
   - Set **Data Source** to the data source.
   - Set **Initial Catalog** to the SQL Server database catalog.
   - Set **User ID** to the service account user ID.
   - Set **Password** to the service account password.
4. For an ORACLE database, modify the following values.
   - Set **Data Source** to the data source.
   - Set **User ID** to the service account user ID.
   - Set **Password** to the service account password.
5. Save and close the file.

6. Create a copy of the **Web.config** file and move it to *[Installation path]\Brainware Intelligent Capture\bin*.
7. Rename the **Web.config** file copy to **Brainware.System.Project.exe.config**.

Configure server security for Web Verifier

To configure server security for Web Verifier, complete the following tasks as necessary.

1. Add the user context in SQL Server
2. Verify the IIS settings
3. Set permissions for BIC projects

Add the user context in SQL Server

To use Web Verifier, your users need access rights for the SQL Server database with the Web Verifier user context. The default user context is Network Service.

Note: If you log in to the SQL Server using Windows authentication, you need to add the domain username to the SQL Server database in addition to the NT Authority/Network Service.

To add the Network Service user context to the SQL Server, complete the following steps.

1. In **Microsoft SQL Server Management Studio**, in the left pane, click **Security > Logins**.
2. Right-click **Logins** and then click **New Login**.
3. In the **Login** dialog box, click **Search**.
4. In the **Select User or Group** dialog box, in the **Enter the object name to select** field, type `NETWORK SERVICE`, click **Check Names** and then click **OK**.
5. In the **Login** dialog box, in the left pane, click **Server Roles**.
6. In the right pane, under **Server roles**, select **sysadmin** and then click **OK**.

Verify the IIS settings

To verify that the IIS runs under NT Authority\Network Service, complete the following steps.

1. In **Internet Information Services (IIS) Manager**, in the **Connections** pane, open the server node and then click **Application Pools**.
2. In the **Application Pools** pane, right-click **Web Verifier Pool** and then click **Advanced Settings**.
3. In the **Advanced Settings** dialog box, under **Process Model**, verify that the **Identity** property has the value `NetworkService`.

Set permissions for BIC projects

BIC stores all projects in a file system directory. To enable Web Verifier to load projects, you must assign appropriate permissions for the project directory.

To grant permission to the Network Service user for the project directory, complete the following steps.

1. In **Windows Explorer**, right-click your projects directory and then click **Properties**.
2. In the **Properties** dialog box, on the **Security** tab, click **Edit**.

3. In the **Permissions** dialog box, click **Add**.
4. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select** field, type `NETWORK SERVICE`, click **Check Names** and then click **OK**.

Configure Internet Explorer for Web Verifier

To configure Internet Explorer for Web Verifier, complete the following steps.

1. In **Internet Explorer**, click **Tools > Internet Options**.
2. In **Internet Options** dialog box, on the **Security** tab, click **Custom level**.
3. In the **Security Settings** dialog box, under **ActiveX controls and plug-ins**, enable the following settings.
   - Binary and script behaviors
   - Run ActiveX controls and plug-ins
4. Under **Scripting**, enable the following settings.
   - Active scripting
   - Allow status bar updates via script

   Note: This setting allows Web Verifier to display information on batches, documents, current filters, and page numbers in the Internet Explorer status bar.

Implement single sign-on authentication

To enable single sign-on authentication, complete the following tasks as necessary.

1. Enable the single sign-on authentication.
2. Modify the Web Verifier session timeout.

About the single sign-on authentication for Web Verifier

Web Verifier supports single sign-on (SSO) user authentication. SSO intercepts the login request and either gathers the user credentials, or accepts the user as already authenticated.

BIC provides the SSO functionality as a generic solution. It works with any SSO implementation and configuration that provides the user credential information through an HTTP header. SSO support was tested using Shibboleth 2.x which builds on SAML 2.0 standards.

For information on configuring the SSO service provider, refer to your provider's product documentation.

Enable the single sign-on authentication

To enable single sign-on authentication, complete the following steps.

1. From the *[Installation path]\Brainware Intelligent Capture Web Server* directory, open **Web.config** in a text editor.
2. Search for the `<httpHeaderBasedSso>` element and complete the following substeps.
   1. Set the `enabled` attribute to `true`.

2. Set the `loginHeader` attribute to the HTTP header attribute name that the SSO service returns.
3. Set the `sessionHeader` attribute to the default session-ID header that the SSO service returns.

Example

```
<httpHeaderBasedSso loginHeader="remoteuser" enabled="true"
sessionHeader="ShibSessionID" />
```

3. Save and close the file.

About the single sign-on session and the Web Verifier session

Using SSO involves two different sessions: the SSO session and the Web Verifier session.

To prevent verifier data loss, the SSO session should have a longer timeout than the Web Verifier session.

The SSO and Web Verifier sessions renew with every server request, such as field validation or opening a batch. The sessions do not renew with client-side actions, such as zooming in on an image or typing a value into a form field without validating it.

For details on how to configure the SSO session timeout, refer to your SSO provider documentation.

Modify the Web Verifier session timeout

To modify the Web Verifier session timeout, complete the following steps.

1. From the *[Installation path]\Brainware Intelligent Capture Web Server* directory, open the **Web.config** file in a text editor.
2. Search for the `<sessionState>` element.
3. Set the `timeout` attribute, in minutes, according to your needs.

Configure Windows authentication

To configure Windows authentication, complete the following tasks as necessary.

1. Configure Windows authentication in IIS 7.5 and higher .
2. Create a Windows authentication-version of the Web.config file .
3. Switch back to Forms authentication.

About Windows authentication for Web Verifier

Web Verifier allows you to log in using Windows authentication instead of Forms authentication.

After you configure this option, your users will only be able to log in with Windows authentication.

However, you can use the re-login menu option to login with an account other than your Windows user account, for example as an administrator, to perform certain administrative tasks.

Configure Windows authentication in IIS 7.5 and higher

To configure Windows authentication for the Web Verifier in IIS 7.5 and higher, complete the following steps.

Prerequisite

Add the Windows user to the BIC database.

1. In the **Internet Information Services (IIS) Manager** window, in the left pane, open the tree view until **Web Verifier** displays.
2. Click **Web Verifier** and then, in the middle pane, under **IIS**, double-click **Authentication**.
3. In the **Authentication** pane, enable **Windows Authentication** and disable all other authentication methods.
4. Restart any open browser sessions.

Create a Windows authentication-version of the Web.config file

We recommend maintaining two versions of the Web.config file to simplify switching between the default Forms authentication and Windows authentication methods.

To create a copy of the default Web.config file and modify it for Windows authentication, complete the following steps.

1. From the *[Installation path]\Brainware Intelligent Capture Web Server* directory, create a backup of the **Web.config** file for the Forms authentication method.

   Note: You can store this backup Web.config for Forms authentication in any directory.

2. Open the original **Web.config** file in a text editor.
3. Complete the following substeps.
   1. Search for the following line.
      `<authentication mode="Forms">`
   2. Replace `Forms` with `Windows`.
      `<authentication mode="Windows">`
   3. Remove the following line.
      `<forms loginUrl="Login.aspx" defaultUrl="BatchView.aspx" />`
   4. Under the `<authorization>` node, replace the `<deny users="?"/>` element with an `<allow users="?"/>` element.
   5. Under the `<pages>` node, add an `<pages enableSessionState="true">` element.
   6. Remove all `<location path=>` nodes.
   7. Save and close the file.

Switch back to Forms authentication

To switch from Windows authentication mode back to default Forms authentication, complete the following steps.

1. Open **Administrative Tools** and then double-click **Internet Information Services (IIS) Manager**.

2. In the **Internet Information Services (IIS) Manager** window, in the left pane, open the tree view until **Web Verifier** displays.
3. Click **WebVerifier** and then, in the middle pane, under **IIS**, double-click **Authentication**.
4. In the **Authentication** pane, disable **Windows Authentication** and enable **Anonymous Authentication** and **Forms Authentication**.
5. Copy the backed up **Web.config** file to the ***[Installation path]*\Brainware Intelligent Capture Web Server** directory.
6. Restart any open browser sessions.

Configure cookies for Web Verifier

To ensure that the browser sends cookies over a secure https network only, complete the following steps.

Prerequisite

Configure SSL on the server.

1. From the *[Installation path]\Brainware Intelligent Capture Web Server* directory, open the **Web.config** file in a text editor.
2. In the `<configuration>` element, search for the following line.
   ```
   <system.web>
   ```
3. Under `<system.web>`, add the following line.
   ```
   <httpCookies requireSSL="true" />
   ```
4. To apply forms authentication, search for the following line.
   ```
   <forms loginUrl="Login.aspx" defaultUrl="BatchView.aspx" />
   ```
5. Add the `requireSSL` attribute.
   ```
   <forms loginUrl="Login.aspx" defaultUrl="BatchView.aspx"
   requireSSL="true" />
   ```
6. Save and close the file.
7. Optional. To prevent other applications from accessing Web Verifier cookies, deploy Web Verifier in one of the following ways.
   - As the root level website.
   - As the only web application under a website in IIS.

About Web Verifier performance

Consider the following information to improve Web Verifier performance.

Image conversion

Opening documents in Web Verifier that failed during classification or extraction may cause performance issues. The Runtime Server properties provide the following settings to convert failed images to PNG to speed up the loading time.

- Convert image to display format after failed classification
- Convert image to display format after failed extraction

For more information, see "About display formats" and "Set display format" in the *Brainware Intelligent Capture Runtime Server Help*.

Remote Matching Service

The Remote Matching Service (RMS) is an implementation of the Associative Search Engine. RMS is capable of supporting large search data pools and is highly recommended for BIC installations including Web Verifier.

For more information, see "Associative Search Engine" in the *Brainware Intelligent Capture Designer Help*.

Delayed validation

The "Allow delayed validation" feature increases the validation performance in Verifier and Web Verifier by reducing the number of server requests.

For more information, see "About delayed validation" and "Modify the validation rules for a field" in the *Brainware Intelligent Capture Designer Help*.

Use Traditional Chinese

If you choose Chinese as UI language, Web Verifier uses Simplified Chinese by default.

To change to Traditional Chinese, complete the following steps.

1. From the *[Installation path]\Brainware Intelligent Capture Web Server\bin\Resources* directory, create a backup copy of the **zho** directory.
2. Copy all files from the *[Installation path]\Brainware Intelligent Capture Web Server\bin\Resources\cmn* directory to the *[Installation path]Brainware Intelligent Capture Web Server\bin\Resources\zho* directory.
3. From the *[Installation path]\Brainware Intelligent Capture Web Server* directory, open the **Web.config** file in a text editor.
4. Search for the following line.
   ```
   <add key="LanguageDisplayName_ZHO" value="中文简体" />
   ```
5. Modify the line as follows.
   ```
   <add key="LanguageDisplayName_CMN" value="中文繁體" />
   ```
6. Save and close the file.
7. Restart any open browser sessions.

Access Web Verifier

To access Web Verifier, complete the following step.

- In your browser, type `http://localhost/WebVerifier/login.aspx`.

Additional columns in Verifier or Web Verifier

You can display additional columns in Verifier and Web Verifier. If you display the external group ID column, verify that the group ID matches the group ID you created for the users.

You can add the following columns to batch view.

- ExternalGroupId
- ExternalBatchId
- TransactionId
- TransactionType

Display and name additional Verifier columns: SQL Server

To display additional Verifier columns from a SQL database, in Microsoft SQL Server Management Studio, in your BIC database, modify and execute any of the following commands.

- External group ID
```
exec sp_SetGlobalApplicationSetting
'SysAppBatchColumnExternalGroupId', '[Column header name, for example
User Group]', True
```
- External batch ID
```
exec sp_SetGlobalApplicationSetting
'SysAppBatchColumnExternalBatchId', '[Column header name, for example
Batch Group]', True
```
- Transaction ID
```
exec sp_SetGlobalApplicationSetting 'SysAppBatchColumnTransactionId',
'[Column header name, for example Transaction]', True
```
- Transaction type
```
exec sp_SetGlobalApplicationSetting
'SysAppBatchColumnTransactionType', '[Column header name, for example
Transaction Type]', True
```

Display and name additional Verifier columns: Oracle

To display additional Verifier columns from an Oracle database, from the SQL*Plus or ORACLE Management Console, in your BIC database, execute any of the following commands.

- External group ID
  ```
  exec sp_SetGlobalApplicationSetting
  ('SysAppBatchColumnExternalGroupId', '[Column header name, for example
  User Group]', 1)
  ```
- External batch ID
  ```
  exec sp_SetGlobalApplicationSetting
  ('SysAppBatchColumnExternalBatchId', '[Column header name, for example
  Batch Group]', 1)
  ```
- Transaction ID
  ```
  exec sp_SetGlobalApplicationSetting ('SysAppBatchColumnTransactionId',
  '[Column header name, for example Transaction]', 1)
  ```
- Transaction type
  ```
  exec sp_SetGlobalApplicationSetting
  ('SysAppBatchColumnTransactionType', '[Column header name, for example
  Transaction Type], 1)
  ```

Display additional Web Verifier columns

The PostImportBatch event in the project script displays additional Web Verifier columns.

For more information on the event, see “PostImportBatch” in the *Brainware Intelligent Capture Scripting Help*.

To display additional columns in Web Verifier, complete the following steps.

1. From the *[Installation path]\Brainware Intelligent Capture Web Server* directory, open the **Web.config** file in a text editor.
2. Search for the following elements and set the `visible` attribute to `true` for the columns you want to display.
   - externalGroupIdColumn
   - externalBatchNameColumn
   - transactionIdColumn
   - transactionTypeColumn
3. Save and close the file.
4. Restart any open browser sessions.

Change the Web Verifier column names

To change the display names for any additional columns in Web Verifier, complete the following steps.

1. From the *[Installation path]\Brainware Intelligent Capture Web Server\bin\resources\[language code]* directory, open the **Brainware.Verifier.WebClient.resx** file in a text editor.
2. Search for the following `<data name=>` elements.
   - TEXT_EXTERNALBATCH_NAME

- TEXT_EXTERNAL_GROUP_ID
- TEXT_TRANSACTION_ID
- TEXT_TRANSACTION_TYPE

3. Set the `<value>` attributes with the names you want to display.
4. Save and close the file.
5. Restart any open browser sessions.

Configure global application settings

To configure global application settings, complete the following tasks as necessary.

1. Optional. Configure workflow history reporting for SQL Server or Oracle.
2. Optional. Disable batch deletion for SQL Server or Oracle.
3. Optional. Modify the URL expiration time for SQL Server or Oracle.

About workflow history reporting

You can activate the workflow history reporting for documents, fields, table cells, classification, learning, and OCR and document separation. Changing these settings takes immediate effect and applies to all users.

Configure workflow history reporting: SQL Server

To configure workflow history reporting for SQL Server, in Microsoft SQL Server Management Studio, in your BIC database, execute any of the following commands.

- For documents
```
exec sp_SetGlobalApplicationSetting
'SysAppHistoryReportingActivatedForDocument', 'True', True
```
- For fields
```
exec sp_SetGlobalApplicationSetting
'SysAppHistoryReportingActivatedForField', 'True', True
```
- For fields and table cells
```
exec sp_SetGlobalApplicationSetting
'SysAppHistoryReportingActivatedForTableCell', 'True', True
```
- For classification
```
exec sp_SetGlobalApplicationSetting
'SysAppHistoryReportingActivatedForClass', 'True', True
```
- For OCR and document separation
```
exec sp_SetGlobalApplicationSetting
'SysAppHistoryReportingActivatedForPage', 'True', True
```
- For learning
```
exec sp_SetGlobalApplicationSetting
'SysAppHistoryReportingActivatedForLearning', 'True', True
```

Configure workflow history reporting: Oracle

To configure workflow history reporting for Oracle, in SQL*Plus or Oracle Management Console, in your BIC database, execute any of the following commands.

- For documents
```
exec sp_SetGlobalApplicationSetting
('SysAppHistoryReportingActivatedForDocument', 'True', 1)
```
- For fields
```
exec sp_SetGlobalApplicationSetting
('SysAppHistoryReportingActivatedForField', 'True', 1)
```
- For fields and table cells
```
exec sp_SetGlobalApplicationSetting
('SysAppHistoryReportingActivatedForTableCell', 'True', 1)
```
- For classification
```
exec sp_SetGlobalApplicationSetting
('SysAppHistoryReportingActivatedForClass', 'True', 1)
```
- For OCR and document separation
```
exec sp_SetGlobalApplicationSetting
('SysAppHistoryReportingActivatedForPage', 'True', 1)
```
- For learning
```
exec sp_SetGlobalApplicationSetting
('SysAppHistoryReportingActivatedForLearning', 'True', 1)
```

About disabling batch deletion in Runtime Server and Designer

You can disable batch deletion in Runtime Server and Designer. Changing these settings takes immediate effect and applies to all users.

Disable batch deletion: SQL Server

To disable batch deletion for SQL Server, in Microsoft SQL Server Management Studio, in your BIC database, execute any of the following commands.

- For Designer
```
exec sp_SetGlobalApplicationSetting
'SysAppBatchDeletionDisabledInDesigner', 'True', True
```
- For Runtime Server
```
exec sp_SetGlobalApplicationSetting
'SysAppBatchDeletionDisabledInRTS', 'True', True
```

Disable batch deletion: Oracle

To disable batch deletion for Oracle, in SQL*Plus or Oracle Management Console, in your BIC database, execute any of the following commands.

- For Designer
```
exec sp_SetGlobalApplicationSetting
('SysAppBatchDeletionDisabledInDesigner', 'True', 1)
```
- For Runtime Server
```
exec sp_SetGlobalApplicationSetting
('SysAppBatchDeletionDisabledInRTS', 'True', 1)
```

About modifying the URL expiration time for Web Verifier

You can modify the URL expiration time for Web Verifier. Changing these settings takes immediate effect and applies to all users.

Modify the URL expiration time: SQL Server

To modify the URL expiration time for SQL Server, in Microsoft SQL Server Management Studio, in your BIC database, complete the following step.

- Execute the following command, specifying the expiration time in seconds for the second parameter.

```
exec sp_SetGlobalApplicationSetting
'SysAppUrlSignatureExpirationPeriod', '300', True
```

Modify the URL expiration time: Oracle

To modify the URL expiration time for Oracle, in SQL*Plus or Oracle Management Console, in your BIC database, complete the following step.

- Execute the following command, specifying the expiration time in seconds for the second parameter.

```
exec sp_SetGlobalApplicationSetting
('SysAppUrlSignatureExpirationPeriod', '300', 1)
```

Configure BIC security

To configure BIC security, review the following topics and complete the tasks as necessary.

1. File system security
2. Recommended accounts and groups
3. Configure access to project data
4. About the service account on a domain network
5. About the service account for system monitoring
6. About the service account for email importing
7. About INI file encryption
8. Encrypt a password for a database connection string
9. About user password encryption
10. Change the hashing algorithm

File system security

Although BIC provides application-level security, the BIC applications rely on the integrated Windows file system security to control access to application and project data in SDP, DAT, and WDC files.

BIC uses a combination of shared and file and directory permissions to control the access of users, groups, and applications to directories and files.

The following table lists the available file permissions.

File Permission	Access Granted
Read	Allows the user or group to read the file and view its attributes, ownership, and permissions.
Write	Allows the user or group to overwrite the file, change its attributes, and view its ownership and its permissions.
Read and Execute	Allows the user or group to execute the file. Includes the Read permissions.
Modify (CHANGE)	Allows the user or group to modify and delete the file. Includes the Read, Write, and Read and Execute permissions.
Full Control	Allows the user or group to change the files permissions and to take ownership of the file. Includes all other file permissions.

The following table lists the available directory permissions.

Directory Permission	Access Granted
Read	Allows the user or group to view the files, folders, and subfolders of the parent folder and to view the folder attributes, ownership, and permissions.
Write	Allows the user or group to create new files and folders within the parent folder, view folder ownership and permissions, and change folder attributes.
List Folder Content	Allows the user or group to view the files and subfolders in the folder.
Read and Execute	Allows the user or group to navigate through all files and subfolders. Includes the Read and List Folder Contents permissions.
Modify	Allows the user to delete the folder.

Directory Permission	Access Granted
(CHANGE)	Includes the Write and Read and Execute permissions.
Full Control	Allows the user or group to change the folder permissions and to take ownership of the folder. Includes all other folder permissions.

Recommended accounts and groups

To control access to BIC project data, we recommend a combination of Discretionary Access Control (DAC) and Role-based Access Control (RBAC).

The DAC model allows the system administrators to control which users can access objects and resources and the operations they can perform.

The RBAC model, also known as non-discretionary model, grants access based on the rights and permissions of roles and groups. The users inherit their rights and permissions from their assigned roles and groups.

The following table lists the groups and accounts recommended for each BIC implementation.

Group / Account Name	Purpose
BIC Project Users	Global group containing all users designated as BIC project designer or data verifier. Add this group to the BIC Users group.
BIC Admin	Global group containing all users designated as a BIC system administrator. Add this group to the BIC group on all RTS servers and RTS remote administration workstations.
BIC	Local group used to grant access to local BIC resources. Create this group on all RTS server and RTS remote administration workstations.
BIC Users	Local group used to grant access to the project directory. Create this group on the BIC server on which the project directory resides.
BIC RTSsvc	Service account used to start the BIC service manager. Add this user to the BIC Admin group and the local administrators group on all BIC servers and remote administration workstations.

The following table lists the groups and accounts, assigned permissions, and the directories and objects on which you need to apply the permissions for each BIC implementation.

Group / Account Name	Permission Type: Shared	Permission Type: NTFS	Directory/Objects Assigned On
Brainware Intelligent Capture	Full Control	Full Control	C:\Program Files*[company]*\ *[ProjectName]*
Brainware Intelligent Capture Users	Change	Modify	C:\Program Files*[company]*\ *[ProjectName]*

Configure access to project data

BIC uses a hierarchical file structure to store project-related data, where the project directory is at the highest level.

All BIC components including services, applications, license engines, and users need appropriate access rights to the project directory and its subfolders.

To configure the access rights to the BIC project directory, complete the following steps.

1. In **Windows Explorer**, right-click your projects directory and then click **Properties**.
2. In the **Properties** dialog box, on the **Sharing** tab, click **Advanced Sharing**.
3. In the **Advanced Sharing** dialog box, select **Share this folder**.
4. In the **Share name** box, type a name for the share and then click **Permissions**.
5. In the **Permissions for Projects** dialog box, complete the following substeps.
    1. Click **Add**.
    2. In the **Select Users, computers, Service Accounts or Groups** dialog box, in the **Enter the object names to select** field, type the local BIC group name and click **OK**.
    3. Repeat the previous steps to add the local administrators and BIC users group names.
    4. For the local BIC group and the local administrators group, select **Full Control**.
    5. For the local BIC users group, select **Change**.
    6. Select the **Everyone** group, click **Remove** and then click **OK**.
6. In the **Properties** dialog box, on the **Security** tab, complete the following substeps.
    1. Add the local BIC group and the local administrators group with **Full Control** permission.
    2. Add the local BIC users group with **Change** permission.
    3. Select the **Everyone** group, click **Remove** and then click **OK**.

About the service account on a domain network

The Runtime Server service utilizes a Windows service to manage the Runtime Server instances and the document processing.

When running BIC on multiple servers located on a domain network, we recommend assigning a domain user to the Runtime Server service against the Windows service. This allows BIC to communicate with all servers running the service across the domain.

The service account, used in BIC, needs permissions for any file or directory shares across the servers to allow the Runtime Server service to access all project-related files.

Note: Do not use the service account to log into the system, either locally or through Remote Desktop. You can configure the Security Settings for the “Deny log on locally” and “Deny log on through Remote Desktop Services” policies in Windows on the system running the services.

About the service account for system monitoring

You can use the System Monitoring service to send emails to selected users for any Runtime Server errors or warnings.

The service user account used for System Monitoring needs sufficient rights on the server and domain to send emails.

About the service account for email importing

BIC provides the ability to import emails, automatically download emails from a mailbox, and import the emails into the BIC system. The Runtime Server service needs sufficient access rights to access the mailbox and to download emails.

About INI file encryption

BIC allows password encryption in INI files for database and SAP connection strings by using RSA encryption. RSA encryption requires a public and a private key.

For more information, see “Password encryption for database connection strings” in the *Brainware Intelligent Capture Scripting Help*.

Encrypt a password for a database connection string

Password encryption in CONFIG files is optional, but highly recommended. To provide an encrypted password for the database connection in a configuration file, complete the following steps.

1. In the ***[Installation path]*\Brainware Intelligent Capture\bin** directory, create a new batch file and give it a meaningful name, such as **CreateEncryptedPassword.bat**.
2. Copy one of the following options to the batch file, replacing `MyPassword` with the password you want to encrypt.

   Note:

The maximum character length for a password to encrypt using **RSA-1024** is 30.

The maximum character length for a password to encrypt using **RSA-3072** is 280.

- To encrypt the password using the internal RSA-3072 key, use the following option.

  ```
  DstCrypt.exe /text "MyPassword" >> EncryptedPW_
  InternalKeys3072.txt
  ```

- To encrypt the password using the internal RSA-1024 key, use the following option.

  ```
  DstCrypt.exe /text "MyPassword" /keysize "1024" >> EncryptedPW_
  InternalKeys1024.txt
  ```

3. Save and close the file.
4. In **Windows Explorer**, double-click the batch file.
5. From ***[Installation path]*\Brainware Intelligent Capture\bin**, open **EncryptedPassword.txt** in a text editor and copy the encrypted password to the clipboard.
6. Open the required configuration file in a text editor.
7. Search for the `<connectionStrings>` element.
8. In the `<add name>` element, set password as an asterisk.

   Example

   ```
   <add name="Entities" Password=*>
   ```

9. In the `<appSettings>` element, add a line with your encrypted password according to the following example.

   Example

   ```
   <appSettings>
   <add key="EncrPwd" value="The_encrypted_Password"/>
   </appSettings>
   ```

10. Save and close the file.

About user password encryption

For security reasons and to ensure unfeasibility of password decryption, user passwords are encrypted using a one-way hashing algorithm.

BIC stores only the hash values in the database to authenticate the user.

The following hashing algorithms are available.

- SHA-256 (default value)
- SHA-512

Note:
If the hashing algorithm is changed, the system updates the database with the recalculated hash value as soon as the user logs in to a BIC application.

Change the hashing algorithm

To change the hashing algorithm, complete one of the following steps.

Note:
For more information about the possible hashing algorithms, see About user password encryption.

- For a **SQL Server** database, in **Microsoft SQL Server Management Studio**, in your BIC database, update the following command with the desired hashing algorithm and then execute the command.

  ```
  exec sp_SetGlobalApplicationSetting 'SysAppHashingAlgorithm', '
  [hashing algorithm]', True
  ```

  Example

  ```
  exec sp_SetGlobalApplicationSetting 'SysAppHashingAlgorithm', 'SHA-
  512', True
  ```

- For an **Oracle** database, from the **SQL*Plus or ORACLE Management Console**, in your BIC database, update the following command with the desired hashing algorithm and then execute the command.

  ```
  exec sp_SetGlobalApplicationSetting ('SysAppHashingAlgorithm', '
  [hashing algorithm]', 1)
  ```

  Example

  ```
  exec sp_SetGlobalApplicationSetting ('SysAppHashingAlgorithm', 'SHA-
  512', 1)
  ```

Configure BIC Runtime Components

To configure BIC runtime components, review the following topics and complete the tasks as necessary.

1. About RTS Remote Administration MMC
2. Configure the Runtime Service Manager service
3. Configure the RTS Remote Administration MMC Snap-in
4. Configure the email import feature in Microsoft Outlook

About RTS Remote Administration MMC

Before you can use BIC, you must configure the Runtime Service Manager (RTS).

The RTS Remote Administration Microsoft Management Console (MMC) snap-in enables you to start and stop multiple Runtime Servers remotely from a single workstation on the network. The BIC installation creates a default console, called Runtime Server Administration that you can use to configure the RTS Remote Administration MMC snap-in.

Configure the Runtime Service Manager service

To configure the Runtime Service Manager service, complete the following steps.

Prerequisite

Verify that the BIC RTSsvc domain user exists.

1. Log in to **Windows** using an account with administrator rights.
2. In **Windows Services**, right-click the **Brainware Intelligent Capture Runtime Service Manager** service and then click **Properties**.
3. In the **Brainware Intelligent Capture Service Manager Properties** dialog box, on the **General** tab, set the **Startup type** according to your needs.
4. On the **Log On** tab, select **This account** and then click **Browse**.
5. In the **Select User** dialog box, click **Locations**.
6. In the **Locations** dialog box, select the domain that has the required account and then click **OK**.
7. In the **Select User** dialog box, in the **Enter the object name to select** box, type the domain user name, such as `BIC RTSsvc`, click **Check Names**, and then click **OK**.
8. Type the password for the user in the **Password** and the **Confirm password** fields and then click **OK**.

Configure the RTS Remote Administration MMC Snap-in

To configure the snap-in, complete the following steps.

1. Verify that the **Brainware Intelligent Capture Runtime Service Manager** service is running. This lets you connect by MMC to the machine.
2. Identify one free configurable port available in any TCP/IP network or the Internet across firewalls.

   Note: The default port number is 50607.

3. Verify one of the following prerequisites.
   - The administration workstation resides on the same LAN segment as the RTS services.
   - In a sub-netted network, a name resolution system is in place to allow clients on one subnet to locate resources on another subnet.
4. Start **Brainware Intelligent Capture Runtime Service**.
5. In the **Runtime Server Administration** window, in the left pane, right-click **Runtime Server Administration** and click **New RTS Group**.

6. In the **New Group** dialog box, type a group name and click **OK**.
7. Open the **Runtime Server Administration** node, right-click the newly created group, and then click **New Machine**.
8. In the **Group Management** dialog box, complete the following substeps.
    1. From the **Domains** list, select the required domain and then click **Search**.
    2. In the left pane, select the required machines, click **>>** and then click **OK**.
9. In the **Runtime Server Administration** window, complete the following substeps.
    1. In the left pane, right-click the newly added machine and then click **License**.
    2. In the **License Information** dialog box, verify or change the license path and then click **OK**.
    3. In the left pane, right-click the newly added machine and then click **New > RTS Instance**.
    4. In the **New RTS Instance** dialog box, type an instance name and then click **OK**.

Configure the email import feature in Microsoft Outlook

You can optionally configure BIC to import emails from Microsoft Outlook. To configure the email import feature, complete the following steps.

1. In **Windows Control Panel**, click **Mail**.
2. In the **Mail** dialog box, click **Add**.
3. In the **New Profile** dialog box, type `RTS_Import` and then click **OK**.
4. In the **Add New Account** dialog box, select **Manually configure server settings or additional server types** and then click **Next**.
5. In the **Choose Service** page, select **Microsoft Exchange or compatible service**.
6. In the **Server Settings** page, complete the following substeps.
    1. In the **Server** field, type the name of your Microsoft Exchange Server.
    2. Clear the **Use Cached Exchange Mode** check box.
    3. In the **User Name** field, type the user name and then click **Next**.
7. To create the account and close the wizard, click **Finish**.
8. In the ***[Installation path]*\Brainware Intelligent Capture** directory, create a new batch file that contains the following line and then run the file.
   ```
   DstHost.exe /TestMailUI
   ```
9. In the **Outlook login** dialog box, complete the following substeps.
    1. In the **User name** field, type *[domain name]\[user name]* and in the **Password** field, type the password.
    2. Select **Remember my credentials** and then click **OK**.
10. From the ***[Installation path]*\Brainware Intelligent Capture\bin\Log** directory, open the latest **I_*[YYYYMMDD]*_DistillerRuntimeServiceHost_*[PID]*.log** file and check for a success or error message, such as `Managed to open the folder 'Inbox'.`
11. In the ***[Installation path]*\Brainware Intelligent Capture** directory, create a new batch file that

    ```
    DstHost.exe /TestMail
    ```

Note: This writes a message to the log file, but does not open the **Outlook login** dialog box.

About the desktop heap size

If you run more than 10 concurrent Web Verifier sessions or Runtime Service instances, modify the Windows desktop heap size to prevent internal memory issues.

Modify the desktop heap size

To modify the desktop heap size, complete the following steps.

1. Start Windows Registry Editor and back up the registry settings.
2. Navigate to *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems*.
3. In the right pane, right-click the **Windows** entry, and then click **Modify**.
4. In the **Edit String** dialog box, in the editing field, modify the third argument of the **SharedSection** parameter, which defines the desktop heap size.

   Note: For information about the appropriate heap size, see Ideal desktop heap size.

5. Reboot the server.

Ideal desktop heap size

Determine the ideal desktop heap size with the following table.

Number of concurrent Web Verifier or Runtime Server instances	Desktop heap size in KB
1 - 10	Operating system default value
11 - 24	1024
25 - 36	1536
37 - 48	2048
49 - 60	2560
61 - 72	3072

About logging

The standard Runtime Server log files include system level resource information and, in case of a system failure, special error logs.

Application log files

Each log file contains the following information.

Entry Nr.	Description
1	Type of message such as Info, Warning, or Error
2	Severity of message
3	Time logged
4	Process ID (PID)
5	Overall used/available physical memory in KB
6	Overall used/available virtual memory in KB
7	Used physical/virtual memory by this RTS instance in KB
8	Number of process handles used by this RTS instance
9	GDI resources/UserObjects used by this RTS instance
10	Message text

The following log files are available in the *[Installation path]\Brainware Intelligent Capture\bin\Log directory*.

Log file name	Description
V_*.log	Verifier messages including custom script errors.
VA_*.log	Advanced Verifier messages.
VL*.log	Local Verifier messages.
H_*.log	Runtime Server Host (DstHost) messages for a single RTS instance.
L_*.log	Learnset Manager messages, such as when the user triggers document learning, or backs up

Log file name	Description
	the learnset.
D_*.log	Designer messages including script errors.
U_*.log	Web Verifier and external application messages.
S_*.log	Service Manager (DstMgr) messages, such as start and end of service, restart, or failures.
I_*.log	Component log files for all applications.
M_*.log	System Monitoring (DstEvent) messages. Holds all system messages and can log error messages across all server machines and hosts.

Error log files

In the event of system or application failures, BIC creates an additional error log file named C_<Process ID>_ yyyymmdd.log.

OCR engine languages

The following table lists the OCR engine languages supported by FineReader 10 and 11.

Supported OCR languages		
Bulgarian	Italian	Romanian
Chinese Simplified *	Japanese *	Russian *
Chinese Simplified + English *	Japanese + English *	Slovak
Czech	Korean *	Slovenian
Danish	Korean + English * **Note:** Only with FineReader 11	Spanish
Digits	KoreanHangul	Swedish
Dutch	Latvian	Thai *

Supported OCR languages		
English	Lithuanian	Turkish
Estonian	Norwegian	Ukrainian *
Finnish	NorwegianBokmal	Vietnamese *
French	NorwegianNynorsk	CMC7
German	Polish	E13B
Greek *	Portuguese Brazilian	
Hungarian	Portuguese Standard	

*: These languages require support of double byte and extended ASCII character sets. To avoid performance loss, do not use more than one DBCS language in a project.

Available OCR Engines

The following optional OCR engines are available, but require separate licensing.

Cleqs Barcode Engine

Reads handwritten and machine-printed data and bar code information. It reads 18 types of bar codes.

FineReader10 OCR Engine

Supports Chinese, Korean and Japanese characters in addition to English, German, Italian, French, and Spanish characters. Converts paper-based or scanned images to editable text.

FineReader11 OCR Engine

Supports OCR of several additional languages and features several improvements in the OCR output quality relative to FineReader 10.

- Receipt Mode
- Improved auto-orientation
- Improved OCR of amounts with leading or trailing asterisks
- Improved OCR of amounts with leading dollar sign

Kadmos 5 OCR Engine Client Edition

Used for handwriting recognition.

Kadmos 5 OCR Engine Server Edition

A server edition capable of processing for multiple users and on multiple processors is available by additional licensing.

QualitySoft Barcode Engine

Supports both grayscale and color images and recognizes 19 different bar code types.

About automated update

You can enable your system to automate updates to your BIC workstations. The automated update feature compares the build level files in the shared network directory and local update directory, and if required, an update performs before the application starts.

If you did not configure the automated update feature during the installation process, you can configure the feature manually.

Note: This feature is not available for all versions of BIC. For details, refer to the appropriate *Brainware Intelligent Capture Release Notes*.

Modify the batch file

To modify the batch file to automate updates, complete the following steps on each BIC server and workstation.

Prerequisite

Determine a shared network directory on a server to incorporate the update files. All BIC workstations must have access permissions to this directory.

1. From the ***[Installation path]*\Brainware Intelligent Capture\bin** directory, open the **AutoInstall.bat** file in a text editor.
2. Search for the following line.
   ```
   SET SHAREDNETFOLDER
   =\\YourNetworkInstallServerName\YourInstallShareName
   ```
3. Modify `\\YourNetworkInstallServerName\YourInstallShareName` to your shared network directory.
4. Save and close the file.

Modify the application shortcuts for Verifier and Designer

To set up Designer and Verifier to run the automated update feature each time they start, complete the following steps.

1. In the **Windows** start menu, right-click the **Designer** application and then click **Properties**.
2. On the **Shortcut** tab, in the **Target** field, change **DstDsr.exe** to **DstDsr_AutoUpdate.bat** and then click **OK**.
3. In the **Windows** start menu, right-click the **Verifier** application and then click **Properties**.

4. On the **Shortcut** tab, in the **Target** field, change **DstDsr.exe** to **DstDsr_AutoUpdate.bat** and then click **OK**.

Automate Runtime Server updates

To configure the automated update for Runtime Server, you can create a Windows task.

In Windows Task Scheduler, create a new task that executes the following steps.

1. To stop the RTS service, in *[Installation path]\Brainware Intelligent Capture\bin* directory, run **Stop RTS running as NT Service.bat**.

   Note: Verify that RTS is not actively processing documents before you stop the service.

2. In *[Installation path]\Brainware Intelligent Capture\bin* directory, run **AutoInstall.bat**
3. To start the RTS service, in *[Installation path]\Brainware Intelligent Capture\bin* run **Start RTS running as NT Service.bat**.

About port configuration

In case of a conflict in port assignments or for the purpose of firewall configuration, you can change the port the Runtime Server uses for the TCP/IP communication channel.

The Runtime Server service, the instance processes, and the MMC use the same Port registry setting. The default port is 50607.

Configure a different port for Runtime Server

To configure a different port for Runtime Server, complete the following steps.

1. In **Windows** registry, complete one of the following substeps.
   - For a 32-bit machine, navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Hyland_BW\Services`.
   - For a 64-bit machine, navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hyland_BW\Services`.
2. In the right pane, right-click and then click **New > DWORD (32-bit) Value**.
3. In the **Name** field, type `Port`.
4. Right-click the **Port** key and then click **Modify**.
5. In the **Edit DWORD (32-bit) Value** dialog box, in the **Value** data field, type the number of an available port and then click **OK**.
6. Restart **Brainware Intelligent Capture Runtime Server** service.
7. Repeat the previous steps on all BIC servers.

File permission matrix

The following tables list the various file permissions used within BIC.

Role/Group	Description
Administrators	Users with full access rights to all application modules and features.
Developers	Users that develop, maintain, and enhance projects.
Learnset Manager	Typically one single user responsible for maintaining the project learnsets.
Advanced Verifiers	Several users responsible for identifying documents for improvements to the project learnset.
Standard Verifiers	Users responsible for document correction.
RTS Service User	The service account responsible for running the service for automatic document processing. Configured only on the server machines.

The following table lists the required NTFS permissions.

Directory	Groups	Full Control	Modify	Read & Execute	List Folder Content	Read	Write	No Access
License Share	Administrators Developers Learnset Manager Advanced Verifiers Standard Verifiers RTS Service User	-	-	x	x	x	x	-
Common Folder	Administrators	x	x	x	x	x	x	-

Directory	Groups	Full Control	Modify	Read & Execute	List Folder Content	Read	Write	No Access
	Developers Learnset Manager Advanced Verifiers							
	Standard Verifiers RTS Service User	-	-	-	-	-	-	x
Global Project	Administrators Developers Learnset Manager RTS Service User	x	x	x	x	x	x	-
	Advanced Verifiers Standard Verifiers	-	-	x	x	x	-	-
Local Project	Administrators Developers	x	x	x	x	x	x	-
	Learnset Manager RTS Service User Standard Verifiers	-	-	-	-	-	-	x
	Advanced Verifiers	x	x	x	x	x	x	-

Directory	Groups	Full Control	Modify	Read & Execute	List Folder Content	Read	Write	No Access
Local Learnset	Administrators Developers	x	x	x	x	x	x	-
	Learnset Manager RTS Service User Standard Verifiers	-	-	-	-	-	-	x
	Advanced Verifiers	x	x	x	x	x	x	-
Global Learnset	Administrators Developers Learnset Manager RTS Service User	x	x	x	x	x	x	-
	Advanced Verifiers Standard Verifiers	-	-	x	x	x	x	-
ASE Pool	Administrators Developers RTS Service User	x	x	x	x	x	x	-
	Learnset Manager Advanced Verifiers Standard Verifiers	-	-	x	x	x	-	-

Directory	Groups	Full Control	Modify	Read & Execute	List Folder Content	Read	Write	No Access
ASSA CSV File	Administrators Developers RTS Service User	x	x	x	x	x	x	-
	Learnset Manager Advanced Verifiers Standard Verifiers	-	-	-	-	-	-	x

Web.config options and associated resource file parameters

This topic lists Web.config file options you can modify to enable, disable, or customize features.

For more information about the event options, refer to the *Brainware Intelligent Capture Scripting Guide*.

Option	Description
ADOCommandExecutionTimeOut	Defines the timeout, in seconds, for executing stored procedures in the database. Possible values Any valid integer
AllowAccessToDocumentsToIndexOnly	For more information, see About navigation to documents for indexing. Possible values True: Enable navigation to indexable documents only False: Enable navigation to out-of-workflow documents. The default value is False.
BatchViewPageSize	Defines the number of batches per page that display in the Web Verifier batch list. Possible values Any valid integer The default value is 20.

Option	Description
client script mode	Defines the parameter to compress the script file that is sent to the browser from the server. Possible values Test: Testing or debugging of Web Verifier client side script on browser. Release: Used in production environment to minimize the file size of the client side script that assists in improving page loading performance.
cacheScripts in the <clientScript> element	Defines the Ext. script caching behavior. Possible values True: Used in *Ext.Loader.setConfig* parameter to enable caching. False: Used in *Ext.Loader.setConfig* parameter to disable caching.
ClientSideDocumentCacheSize	Defines the number of pages to cache in the current document. Possible values Any valid integer The default value is 0.
connectionStrings	The database connection string.
convertedScriptCaching	Add this configuration in the *<project.controller>\<project>* node along with *mpdDistance* and *mpdThreshold*. Possible values True: Enables script conversion caching to reduce initial project loading time. False: Disables script conversion caching to slow down initial project loading time. The default value is True. **Note:** You also need to set this value to "true" in the *Brainware.system.project.exe.config* setting to enable script conversion caching.
DialogWidth	Defines the default width, in pixels, of message boxes in Web Verifier. Possible values Any valid integer

Option	Description
	The default value is 400.
document cacheSize in the <document.controller> element	Specifies the number of workdoc objects to pre-load. This accelerates opening documents within the batch. You cannot disable pre-loading, but minimize the number of pre-loaded documents to 2, that means one current and one pre-loaded. Possible values Any valid integer The default value is 5.
document maxPagesToPreload in the <document.controller> element	Defines the number of document pages to pre-load. First and last pages always pre-load, and remaining cache slots fill with pages that have field candidates starting from the lower index. The following actions take place on page images when a document loads in the background. • Pre-load the page • Convert the page to PNG • Save the page to the database Possible values Any valid integer The default value is 5.
DocumentViewPageSize	Defines the number of folders for Verifier to display in the document tree view when using Show Selected Batch mode. Additional batches display in subsequent navigation panels. Possible values Any valid integer The default value is 10.
EnableProfiler	Whether to enable the Web Verifier profiler. The profiler collects and records the duration of user actions, such as commands and their internal sub-operations. Possible values True / False The default value is False.

Option	Description
externalGroupIdColumn	Whether the external group ID column displays in Web Verifier. Possible values True / False The default value is False.
externalBatchNameColumn	Whether the external batch name column displays in Web Verifier. Possible values True / False The default value is False.
focusChanged	Whether to enables the focusChanged event for fields in the verification view. The event triggers when the user presses the Enter key in a field. The setting has no effect on the FocusChanged event if the <mouseClicked> attribute is set to true. Possible values True / False The default value is True.
HelpLink	Links to Web Verifier Help.
httpHeaderBasedSso	Controls the single sign-on (SSO) user authentication mode.
login header in the <httpHeaderBasedSso> element	Corresponds to the HTTP header attribute name that contains the SSO authenticated user name. The SSO service uses this attribute to send the user name.
Enabled in the <httpHeaderBasedSso> element	Whether to use the Web Verifier SSO feature. Possible values True / False The default value is False.
sessionHeader in the <httpHeaderBasedSso> element	The provider-dependent name of the HTTP header that the SSO service uses to send the user session ID.
inactiveUserTimeout	Unchangeable attribute. **Note:** This attribute does not control the user session timeout.

Option	Description
	The `<sessionState Timeout>` parameter controls the user session timeout.
inspectionTimeOut	Unchangeable attribute. **Note:** This attribute does not control the user session timeout. The `<sessionState Timeout>` parameter controls the user session timeout.
instanceName	The instanceName value displays in the batch list column “Last Module". **Note:** The instanceName value must be unique across all installed Web Verifier servers accessing the same database.
itemCopied	Whether to enable the itemCopied event. Possible values True / False The default value is False.
LanguageDisplayName_*[ISO]*	Customizes the language display names in the language selection menu. Replace *[ISO]* by the three letter directory name in *[Installation path]*\Brainware Intelligent Capture Web Server\Bin\Resources. Example for Simplified Chinese `<add key="LanguageDisplayName_ZHO" value="中文简体"/>`
licensePath	The location of the shared license file. Possible values Any valid path The default value is *[Installation path]*\License\Runtime.lic.
level	Defines the tracing level. Possible values DEBUG: Trace all information and error messages. ERROR: Trace error messages only.

Option	Description
loadInSeparateProcess	Unchangeable attribute.
mouseClicked	Whether to enable the mouseClicked event on fields and tables in the verification view in indexing mode. Possible values True / False The default value is False.
pathToProjectExe	The location of the Designer program Brainware.System.Project.exe. In typical installations, it is not required to modify this value. Possible values A valid non-UNC path ending with a "\". The default value is *[Installation path]*\Brainware Intelligent Capture\Bin\.
ReinitScriptEngineAfterScriptErrors	Whether to recover the script engine after a script error in Web Verifier. Possible values True / False The default value is False.
remoteObjectRenewalTimeout	Defines, in seconds, the time to lapse before renewing remote object references. The lower the number the faster unused objects free memory. Increase this value in the event of errors caused by long-running commands, such as field validation. Possible values Any valid integer more than or equal to 30. The default value is 30.
SavePageImageToDatabase	Specifies if page images extracted from document file blobs needs to be saved back to the database. Possible values True / False
timeout in the <sessionState> element	Defines, in minutes, the amount of time a user can be inactive before the session ends. Specify a value less than that of the SSO session. For details, see the product documentation of your SSO provider. Possible values

Option	Description
	Any valid integer. The default value is 20.
ShowExtendedErrorMessages	Whether to enable stack trace information for Web Verifier error messages. Error messages display in the trace log file. Possible values True / False The default value is False.

slogan	A text message that displays on the Web Verifier browser header, such as corporate messages, announcements, or the corporate slogan.
	Possible values
	The default value is an empty string.
	Example
	`<verifier.webclient>`
	`<company slogan="This is a slogan" />`

SYSTEM_LONG_DATE_FORMAT	The XML key available in each Brainware.Verifier.WebClient.resx file located in *[Installation path]*\Brainware Intelligent Capture Web Server\Bin\Resources\ *[language code]*.
	The key contains the date pattern for the last access date column in the batch list for the respective language.
	To use the default system date pattern, leave the value element empty. The time format uses a 24-hour clock.
	For Traditional and Simplified Chinese, use the date format in the following example without any Chinese characters.
	Example for Chinese
	`<data name="SYSTEM_LONG_DATE_FORMAT"`
	`xml:space="preserve">`
	`<value>yyyy-MM-dd, hh:mm:ss</value>`
	`</data>`

transactionIdColumn	Whether the transaction ID batch column displays in Web Verifier. Possible values

Option	Description
	True / False The default value is False.
transactionTypeColumn	Whether the transaction type batch column displays in Web Verifier. Possible values True / False The default value is False.
tabPressed	Whether to enable the tabPressed event on fields and tables in the verification view in indexing mode. Possible values True / False The default value is False.
tableCellSelected	Whether to enable the tableCellSelected event. Possible values True / False The default value is False.
usePath	Possible values True: Use the pathToProjectExe parameter. False: Use the current directory instead of the pathToProjectExe parameter. The default value is True.
waitLoadTimeOut	Defines the timeout for the initial loading of the project.exe.

About navigation to documents for indexing

Indexable documents are documents with states from enabled workflow input states. The Web.config option `AllowAccessToDocumentsToIndexOnly` and the Web Verifier option “Disable navigation to valid documents” control the navigation to indexable documents.

Example

Workflow settings: 550 -> 700

A batch includes documents with states 550, 600, and 700.

If you set `AllowAccessToDocumentsToIndexOnly` to `True` and activate the "Disable navigation to valid documents" option in Web Verifier, you cannot access documents with state 600 or 700.

Enable navigation to indexable documents

To enable navigation to indexable documents only, complete the following steps.

1. From the *[Installation path]\Brainware Intelligent Capture Web Server* directory, open **Web.config** in a text editor.
2. Search for `<appSettings>`.
3. Add the following line.
   ```
   <add key="AllowAccessToDocumentsToIndexOnly" value="true" />
   ```
4. Save and close the file.
5. In Web Verifier, activate the **Disable navigation to valid documents** option.

Registry options

You can create or modify the following keys in the Windows registry to enable, disable, or customize features.

Key	Description
ErrorTraceDir	Provides the possibility to change the component log file location. The setting does not affect the core product log file location.
HideBatchReleaseDialog	Allows you to enable or disable the Batch Release dialog box within Verifier, where the workflow does not require prompting users to the next task. The registry value determines the next action carried out by users. The default action of the Batch Release dialog box is to verify the next invalid batch. When BIC suppresses the dialog, this value is maintained. To change to a different action, use the Batch Release dialog box once, then change the setting accordingly and click OK. The default value is 0.
ErrorTrace - All	Defines the trace level. The default value is 1.
MaximumDiskspaceUsageMB	Defines the disk space in MB allocated for component level logs.
TotalDaysToKeepFiles	Defines the number of days the BIC server retains the component log files.

Create the registry key ErrorTraceDir

To create the registry key, complete the following steps.

1. In **Windows Registry Editor**, complete one of the following substeps.
   - For a 32-bit machine, navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Hyland_*

BW\ErrorTrace.

- For a 64-bit machine, navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hyland_BW\ErrorTrace*.

2. In the right pane, right-click and then click **New > String Value**.
3. In the **Name** field, type `ErrorTraceDir` and then click **OK**.
4. Right-click the **ErrorTraceDir** key and then click **Modify**.
5. In the **Edit String** dialog box, in the **Value data** field, type the path and then click **OK**.

   Note: The path must exist and the service account / user needs write permission to the path.

6. Restart all BIC applications and services.

Create the registry key HideBatchReleaseDialog

To create the registry key, complete the following steps.

1. In **Windows Registry Editor**, complete one of the following substeps.
   - For a 32-bit machine, navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Hyland_BW\Cedar* .
   - For a 64-bit machine, navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hyland_BW\Cedar*.
2. In the right pane, right-click and then click **New > DWORD (32-bit) Value**.
3. In the **Name** field, type `HidebatchReleaseDialog` and then click **OK**.
4. Right-click the **HidebatchReleaseDialog** key and then click **Modify**.
5. In the **Edit DWORD (32-bit) Value** dialog box, in the **Value data** field, complete one of the following steps and then click **OK**.
   - To display the confirmation screen, type zero: `0`.
   - To hide the confirmation screen, type `1`.
6. Restart all BIC applications.

Modify the registry key ErrorTrace - All

To modify the value, complete the following steps.

1. In **Windows Registry Editor**, complete one of the following substeps.
   - For a 32-bit machine, navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Hyland_BW\ErrorTrace*.
   - For a 64-bit machine, navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hyland_BW\ErrorTrace*.
2. In the right pane, right-click **All** and then click **Modify**.
3. In the **Edit DWORD (32-bit) Value** dialog box, in the **Value data** field, complete one of the following steps and then click **OK**.
   - To log only errors, type `1`.
   - To log only errors and warnings, type `2`.

- To log only errors, warnings, and information, type `3`.

Create the registry key MaximumDiskspaceUsageMB

To create the registry key, complete the following steps.

1. In **Windows Registry Editor**, complete one of the following substeps.
   - For a 32-bit machine, navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Hyland_BW\ErrorTrace* .
   - For a 64-bit machine, navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hyland_BW\ErrorTrace* .
2. In the right pane, right-click and then click **New > DWORD (32-bit) Value**.
3. In the **Name** field, type `MaximumDiskspaceUsageMB`.
4. Right-click the **MaximumDiskspaceUsageMB** key and then click **Modify**.
5. In the **Edit DWORD (32-bit) Value** dialog box, in the **Value data** field, complete one of the following steps and then click **OK**.
   - To deactivate the option, type zero: `0`.
   - Type the appropriate value in megabyte.

Create the registry key TotalDaysToKeepFiles

To create the registry key, complete the following steps.

1. In **Windows Registry Editor**, complete one of the following substeps.
   - For a 32-bit machine, navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Hyland_BW\ErrorTrace* .
   - For a 64-bit machine, navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hyland_BW\ErrorTrace*.
2. In the right pane, right-click and then click **New > DWORD (32-bit) Value**.
3. In the **Name** field, type `TotalDaysToKeepFiles`.
4. Right-click the **TotalDaysToKeepFiles** key and click **Modify**.
5. In the **Edit DWORD (32-bit) Value** dialog box, in the **Value data** field, complete one of the following steps and then click **OK**.
   - To deactivate the option, type zero: `0`.
   - Type the number of days.