Brainware Intelligent Capture Visibility

Installation and Setup Guide

Version: 4.0.x

Written by: Documentation Team, R&D
Date: Wednesday, July 10, 2024

Hyland

Documentation Notice

Information in this document is subject to change without notice. The software described in this document is furnished only under a separate license agreement and may only be used or copied according to the terms of such agreement. It is against the law to copy the software except as specifically allowed in the license agreement. This document or accompanying materials may contain certain information which is confidential information of Hyland Software, Inc. and its affiliates, and which may be subject to the confidentiality provisions agreed to by you.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright law, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Hyland Software, Inc. or one of its affiliates.

Hyland, HXP, OnBase, Alfresco, Nuxeo, and product names are registered and/or unregistered trademarks of Hyland Software, Inc. and its affiliates in the United States and other countries. All other trademarks, service marks, trade names and products of other companies are the property of their respective owners.

© 2024 Hyland Software, Inc. and its affiliates.

The information in this document may contain technology as defined by the Export Administration Regulations (EAR) and could be subject to the Export Control Laws of the U.S. Government including for the EAR and trade and economic sanctions maintained by the Office of Foreign Assets Control as well as the export controls laws of your entity’s local jurisdiction. Transfer of such technology by any means to a foreign person, whether in the United States or abroad, could require export licensing or other approval from the U.S. Government and the export authority of your entity’s jurisdiction. You are responsible for ensuring that you have any required approvals prior to export.

Table of Contents

Installation 5

Prerequisites for Installation *5*

Installation Process – 64 bit Version *5*

Post Installation Configuration 5

Request a License *5*

Deploy a Production License *6*

Access the Web Portal *6*

Visibility Sliding Menu *6*

Configure the Visibility Repository Database Connection *7*

Configure the Visibility Database Connection *8*

Deploy CAB files *9*

Set up Global Business Parameters *10*

prmImagePuller 10

prmExtractionFieldName 10

prmAmountFields 11

prmGenericClassName 11

prmParentClassName 11

prmSTPValue (Oracle Only) 12

prmUnknownValue (Oracle Only) 12

prmVerifyUser (Oracle Only) 12

Optional parameters 13

Populate updated project parameter values *13*

Configure the Adhoc Wizard *14*

Set up Communication with Mail Server *14*

Configure Visibility to pull images from Database *15*

Set up Organizations and User Accounts *16*

Add Organizations 16

Add Users and Roles 16

About privileges 16

Set up the Administrator Role 17

Set up the Users Role ... 17
Restrict Email Access ... 17
Add Users ... 18
Add Super Administrator Users ... 18
Configure LDAP Authentication for Visibility ... *19*
Create LDAP/LDAPS Authenticated Organization ... 19
Set Authentication mode to LDAP/LDAPS ... 19
Create Users ... 20
Map Users ... 20
Set Report Access Rights ... *21*
Set Report Access Rights for Administrator Roles ... 21
Set Report Access Rights for User Roles ... 21
Change the Default Admin Password ... *22*
Select User Dashboards ... *22*
Select Locale and Time Zone ... *22*
Deploy Portal Languages ... *22*
SiteMinder Authentication ... *23*
Enable Host Application authentication for the Organization ... 24
Map the Super-Admin User ... 24
Map Application Users ... 24
Configure SiteMinder ... 24
Data Management ... *25*
Enable Data Archiving (SQL Server) ... 25
Enable Data Archiving (Oracle) ... 26
Purge Document Script ... 26
Set up Archiving Parameters ... 26
prmTargetDBName (SQL Server only) ... 26
prmTargetDBServerAddress (SQL Server only) ... 27
prmDBLinkName (Oracle only) ... 27

Installation

Prerequisites for Installation

The Brainware Intelligent Capture reporting database must be populated with data and be accessible from the Visibility server. In addition, the Visibility Repository database must be created and be accessible from the Visibility server.

Installation Process – 64 bit Version

To install the Visibility server, complete the following steps.

1. Run **Setup.exe** from the **Visibility** installation folder.
2. From the **Welcome** screen, click **Next**.
3. Accept the EULA (End User License Agreement).
4. In the **Customer and Usage Details** screen, enter the **Certified Administrator's Name** and **Company Name**, then click **Next**.
5. When the **Installation Options** screen displays, it is recommended that you choose the **Custom Install** option and click **Next** to continue.
6. In the **Installation Location** screen, type or select the appropriate location path and click **Next**.
7. In the **Select Components to Install** screen, ensure that the **Desktop Studio (32-Bit)** option is checked, then click **Next**.

   Note:
   The **Visibility Report Server** and **Web Server** will run as 64-bit applications as 32-bit applications are no longer supported. However, the **Desktop Studio** is only supported as a 32-bit application.

8. In the **Configure Ports** screen, enter the **Portal Port** number that users will use to access the **Visibility** web portal, then click **Next**.
9. In the **Configure Timeout Values** screen, modify the defaults if needed, then click **Next**.
10. In the **Installations Preferences** review screen, click **Next**.
11. In the **Installation Complete** screen, respond to the prompts as needed, then click **Finish**.

Post Installation Configuration

Request a License

After installing Visibility 4.0, you need to request a new product license by modifying and providing the License.req file present in the <installFolder>\Hyland\Brainware Visibility\ReportEngine\bin folder. This new license will grant additional access to SMART Reports.

This procedure is not required for internal or partner development licenses that are used for demonstration purposes. A production license is only required for customer production environments.

To request a license, complete the following steps.

1. Open the **License.req** file in notepad and verify the following settings.
    - Number of "**CPUs**=" and "**OS**="
    - **"Licensee"** = Customer's Company Name used during the installation
    - **"Users"** = Number of RELs (Report Engine Licenses) customer ordered. Default order is 4. RELs are the number of concurrent reports that can be running at any given time. If your implementation has 20 users running reports and 4 RELs, the first four report requests will begin immediately and the other 16 will be placed in queue.
    - **"Location"** = City, State, Country
2. Email the modified **License.req** file to Hyland Software Technical Support group.

Deploy a Production License

After receiving a production license, you need to deploy it on the Visibility server using the following steps.

1. Stop the **Visibility Reporting Service**.
2. Delete the "work" folder located here: <Install Path>Hyland\Brainware Visibility\Jakarta\
3. Navigate to the folder <Install Path>\Hyland\Brainware Visibility\ReportEngine\bin\
4. Rename the file **ReportEngine.lic** to **ReportEngine.old**
5. Rename the license file received from Support to **ReportEngine.lic** and place it in this folder.
6. Restart the **Visibility Reporting Service**.

Access the Web Portal

Once the installation has been completed, restart your system and complete the following steps to access the Visibility Web Portal.

1. Click **Start** > **All Programs > Hyland > Brainware Visibility** > **Launch Portal**.
2. The web browser should display the **Login** page of the **Visibility Portal**. Enter the user credentials of **Admin** for the **User name** and **Admin** for the **Password**. The credentials are case sensitive.

Visibility Sliding Menu

Familiarize yourself with the Visibility sliding menu on the left side of the application window. This menu allows users to navigate quickly to the portal, providing access to the following areas.

- Navigate
- Explorer
- Home
- Alert
- Settings
- Info

Configure the Visibility Repository Database Connection

After the installation is completed, to configure a database connection for the Visibility repository, complete the following steps.

1. After logging in to **Visibility**, on the sliding menu click **Navigate > Administration > Configure**. The **Database** tabbed area appears, by default.
2. Click **Add**.
3. Modify the following options.
    - **Connection Name.** This is the name that a user can select if switching between databases. Make it a meaningful name. The name does not have to be the actual database name in the database server.
    - **Provider.** Select the provider for the repository database (MSSQL or Oracle).

      Note: To configure MS SQL Windows Authentication for the Visibility Portal, download and install the Microsoft JDBC driver for SQL Server. If using Integrated Security with MSSQL, **sqljdbc_auth.dll** (available from Microsoft's MSDN web site**)** must be placed in the **<install path>\Intellicus\ReportEngine\bin** directory and you must restart the Report Service. If using an Oracle database and the Oracle client is not installed on the report server machine, Visibility requires **ojdbc14.jar** for THIN connections.

      a) For SQL installations, select the **Driver Version**, **Authentication Mode**, and Driver Type For repository connections, always use Microsoft Driver Type.

      b) For Oracle installations, select the **Driver Type** and **Driver Version**.
    - For Windows Authentication connectivity, in the **Provider** list, select **MSSQL**, in the **Authentication Mode** list, click **Windows** and in the **Driver Type** list, click **JTDS**.
    - **Server.** Enter the IP address of the database server.
    - **Instance.** Enter the SQL server's instance name.
    - **Port.** Enter the port number used to connect to the database server.
    - **Database/SID.** Enter the SQL database name or the Oracle SID, depending on your environment.
    - **Username/Password.** Enter the credentials used to access the database.
    - **Blank.** When this option is selected, it enables **Integrated Security**.
    - **Runtime.** Leave unselected for repository connection. When selected, it requires the Visibility user to enter credentials at the time reports are run.
    - **Charset Encoding.** Multi-lingual support - For supporting I18n, you must select the UTF-8 option. If the database connection does not require multi-lingual support, leave this option blank.
    - **Is Default.** Leave this Unchecked - this option is selected for the Visibility reporting

database in another connection.

- **Is Repository.** Select this option. Repository connections are used to store information related to Visibility, such as entities like reports, categories, and users.

  Note:
  Hyland Software and Intellicus do not recommend using the default repository shipped with Visibility for production purposes. Therefore, a repository database must be established.

- **Read Only.** Allows only Select clause and Stored Procedures to run on the connection. This defaults to selected if the option **Is Repository** is selected.

4. Test the connection by clicking **Test** on the left side of the screen. You receive a connection message confirming the results of your test. If the test fails, revisit all the previous parameters entered before contacting customer support for further assistance.
5. To save the connection, click **Save** and then click **OK** on the message box that displays a request for you to restart the **Report Server**.
6. Restart the **Visibility Reporting Service**.

Configure the Visibility Database Connection

Once the installation has been completed, you must configure a database connection for the Brainware Intelligent Capture reporting database by completing the following steps.

1. After logging in to **Visibility**, on the sliding menu click **Navigate > Administration > Configure**. The **Database** tabbed area appears, by default.
2. Click **Add**.
3. Modify the following options.
   - **Connection Name.** This is the name that a user can select if switching between databases. Make it a meaningful name. It does not have to be the actual database name in the database server.
   - **Provider.** Select the provider for the reporting database (MSSQL or Oracle).

     Note:
     If using Integrated Security with MSSQL, sqljdbc_auth.dll (available from Microsoft's MSDN web site**)** must be placed in the <install path>\Intellicus\ReportEngine\bin directory and the Report Service must be restarted. If using an Oracle database and the Oracle client is not installed on the report server machine, Visibility requires **ojdbc14.jar** for THIN connections.

   - For SQL installations, select the **Driver Version**, **Authentication Mode** and **Driver Type**. For reporting database connections, Hyland recommends using "JTDS" Driver Type.
   - For Oracle installations, select the **Driver Type** and in the **Driver Version** box, type

12.2.0.1.0.

- **Server.** Enter the IP address of the database server.
- **Instance.** Enter the SQL server's instance name (leave blank if using "JTDS" driver type).
- **Port.** Enter the port number used to connect to the database server.
- **Database/SID.** Enter the SQL database name or the Oracle SID, depending on your environment.
- **Username/Password.** Enter the credentials used to access the database.
- **Blank.** When this option is selected, it enables **Integrated Security**.
- **Runtime.** When this option is selected, it requires the Visibility user to enter credentials at the time reports are run.
- **Charset Encoding.** Multi-lingual support - For supporting I18n, you must select UTF-8. If the database connection does not require multi-lingual support, leave this option blank.
- **Is Default.** Select this option if this connection is the default connection used for **Visibility** reporting.
- **Is Repository.** Do not select this option. This is for Repository Connections only.
- **Read Only.** Allows only Select clause and Stored Procedures to run on the connection.
- For Oracle installations, configure the **Pool Settings** as follows:

  - In the **Initial Connections** box, type *10*.

  - In the **Incremental Size** box, type *10*.

  - In the **Resubmit Time** box, type *5*.

  - In the **Max Connections** box, type *300*.

4. After all modifications are made, test the connection by clicking **Test** on the left side of the screen. You receive a connection message confirming the results of your test. If the test fails, revisit all the previous parameters entered before contacting customer support for further assistance.
5. To save the connection, click the **Save** button.

Next

You need to restart the report services after the databases are configured successfully.

Deploy CAB files

After the creation of the repository and reporting databases/connections, you need to deploy the CAB files that contains the Visibility Reports using the following steps.

1. Go to **Navigate > Repository > Deploy Repository Bundle**.
2. Under **Repository**, click **Deploy Repository Bundle**. The **Deploy Repository Bundle** area appears.

3. Select **Browse** and navigate to the .cab file for the installation (Oracle or SQL).
4. Click **Upload**, then click **Deploy**. Scroll down the page and ensure that all reports, queries, and parameters were added.
5. After the CAB files are deployed, restart the Visibility service.

Set up Global Business Parameters

After you deploy the CAB files, you need to set up and modify the global business parameters as described below.

prmImagePuller

You need to modify the default value of the prmImagePuller parameter based on the installation port that was selected at the time of installation. This is required to open the images for the scanned documents.

To modify this parameter, complete the following steps.

1. After logging on to **Visibility**, use the sliding menu to navigate to **Explorer > Capture > prmImagePuller**.
2. Select **Edit Parameter Details**. The **Parameter Object Editor** area appears.
3. Update the parameter's **Default Value** field to the port number used during installation.
4. Save the changes.

prmExtractionFieldName

Prerequisite

This step needs to be completed after processing documents through Brainware Intelligent Capture with reporting enabled for the appropriate fields to be available.

If you would like to define which fields are used to calculate the field extraction percentages in the dashboards and reports, update this parameter. The fields commonly included in this parameter are the fields located on the customer's Verifier screen. For example, if you process only US-based invoices, then GST, PST, and VAT should not be included in this parameter.

To modify this parameter, complete the following steps.

1. After logging on to **Visibility**, use the sliding menu to navigate to **Explorer > Capture > prmExtractionFieldName**.
2. Select **Edit Parameter Details**. The **Parameter Object Editor** area appears.
3. Click the **Verify SQL** button.
4. In the **Select Default Values** section, click **Selected** and then multi-select the specific values to included.
5. Save the changes.

prmAmountFields

Prerequisite

You must complete this step after processing documents through Brainware Intelligent Capture with reporting enabled for the appropriate fields to be available.

This parameter is used by the Missing Decimals report. This report should only be run on amount fields that are included within the reporting database.

To modify this parameter, complete the following steps.

1. After logging on to **Visibility**, use the sliding menu to navigate to **Explorer > Capture > prmAmountFields**.
2. Select **Edit Parameter Details**. The **Parameter Object Editor** area appears.
3. Click the **Verify SQL** button.
4. In the **Select Default Values** section, click **Selected** and then multi-select the specific amount fields you want to include.
5. Save the changes.

prmGenericClassName

Prerequisite

You must complete this step after processing documents through Brainware Intelligent Capture with reporting enabled for the appropriate fields to be available.

This parameter is used by the Classification Summary and Classification Detail reports. It should be configured to the generic class used within your project.

To modify this parameter, complete the following steps.

1. After logging on to **Visibility**, use the sliding menu to navigate to **Explorer > Capture > prmGenericClassName**.
2. Select **Edit Parameter Details**. The **Parameter Object Editor** area appears.
3. Click the **Verify SQL** button.
4. In the **Select Default Values** section, click **Selected** and then select the generic class name for your project.
5. Save the changes.

prmParentClassName

Prerequisite

You must complete this step after processing documents through Brainware Intelligent Capture with reporting enabled for the appropriate fields to be available.

This parameter is used by the Classification Summary and Classification Detail reports. It should be configured to the parent class of the generic class used within your project.

To modify this parameter, complete the following steps.

1. After logging on to **Visibility**, use the sliding menu to navigate to **Explorer > Capture > prmParentClassName**.
2. Select **Edit Parameter Details**. The **Parameter Object Editor** area appears.
3. Click the **Verify SQL** button.
4. In the **Select Default Values** section, click **Selected** and then select the parent class name of generic class for your project.
5. Save the changes.

prmSTPValue (Oracle Only)

This parameter is used in Oracle installations to return the default 'STP' value based on the column type within the Oracle database. If <%prmDocumentTbl%>.USEREXTRV column is of type nvarchar2 then default the value applies, otherwise prmUnknownValue needs to be updated to.

To modify this parameter, complete the following steps.

1. After logging on to **Visibility**, use the sliding menu to navigate to **Explorer > Capture > prmSTPValue**.
2. Select **Edit Parameter Details**. The **Parameter Object Editor** area appears.
3. Set the **Default Value** to `STP` for implementations where <%prmDocumentTbl%>.USEREXTRV is of type varchar2 or to `STP` for implementations where <%prmDocumentTbl%>.USEREXTRV is of type varchar2.
4. Save the changes.

prmUnknownValue (Oracle Only)

This parameter is used in Oracle installations to return the default 'UNKNOWN' value based on the column type within the Oracle database. If <%prmFieldsTbl%>.ContentV column is of type nvarchar2 then the default value applies, otherwise prmUnknownValue needs to be updated.

To modify this parameter, complete the following steps.

1. After logging on to **Visibility**, use the sliding menu and navigate to **Explorer > Capture > prmUnknownValue**.
2. Select **Edit Parameter Details**. The **Parameter Object Editor** area appears.
3. Click the **Edit Parameter Details** option.
4. Set the **Default Value** to `UNKNOWN` for implementations where <%prmFieldsTbl%>.ContentV is of type varchar2 or to `UNKNOWN` for implementations where <%prmFieldsTbl%>.ContentV is of type varchar2.
5. Save the changes.

prmVerifyUser (Oracle Only)

This parameter is used in Oracle installations to return the default 'STP' value within the Verifier user list based on the column type within the Oracle database. If <%prmDocumentTbl%>.USEREXTRV column is of type nvarchar2 then default the value applies, otherwise prmUnknownValue needs to be updated to.

To modify this parameter, complete the following steps.

1. After logging on to **Visibility**, use the sliding menu to navigate to **Explorer > Capture > Parameter Objects > prmAmount > Fields**.
2. Click the **Edit Parameter Details** option.
3. Set the **Default Value** to UNKNOWN for implementations where <%prmDocumentTbl%>.USEREXTRV is of type varchar2 or to UNKNOWN for implementations where <%prmDocumentTbl%>.USEREXTRV is of type varchar2.
4. Save the changes.

Optional parameters

The following parameters are optional and are used by almost all reports: **prmFieldsTbl, prmDocStatusDescTbl, prmDocStatusTbl, prmDocumentTbl, prmLPStatusTbl, PrmDELETEREPORTINGRECORDSProc**.

These parameters are used by almost all reports. The parameters are defaulted to the table names/stored procedures shipped with the Brainware Intelligent Capture solutions; however, they are configurable should you be using different table names than the defaults.

To modify these parameters, complete the following steps.

1. After logging in to **Visibility**, on the sliding menu click **Explorer**.
2. In the **Object Type** box, select the **Parameter Object** check box. The parameter objects appear under the existing categories.
    - You can also search for the required parameter object by typing the keyword in the **Name** box.
3. Under **Capture**, right-click the name of the required parameter and from the parameter object menu, select **Edit Parameter Details**. The **Parameter Object Editor** area appears.
4. Set the **Default Value** to the table name or stored procedure in your reporting data database.
5. Save the changes.

Populate updated project parameter values

After modifying the reporting database, you can populate the updated values for Project Parameter, Organization and User/Role under Manage Users. To populate updated project parameter values, complete the following steps.

1. Go to **Navigate > Administration > Manage Users > Organization > Modify**.
2. Click the **Preferences** tab and from the **Select Database** list, select the new database you want to use.
3. Click **Save**. The details are saved.
4. Click the **Data Restriction** tab and in the **Selected Values** area select the values you want to remove and click **<.**
5. On the **User/Role** tabbed page, select **Admin** and then click **Data Restrictions**.

6. Include relevant value(s) from the **Available Values** box to the **Selected Values** box.
7. Click **Save**. The details are saved.

Configure the Adhoc Wizard

The following procedure provides details on how to configure the default Adhoc Wizard settings. This is necessary to have newly created reports that use the same style sheet as the current adhoc reports. Additionally, you must enable the Show filter option so that Adhoc designers can use existing parameters within their reports.

To configure the Adhoc Wizard settings, complete the following steps.

1. After logging in to **Visibility**, use the sliding menu to navigate to **Navigate > Administration > Configure**. The **Databases** tabbed area appears, by default.
2. Click **Ad hoc Wizard > Data Source**.
3. Change the default template to **Classic**.
4. Select **Filters** on the left of the screen.
5. Select the **Show User Parameters** check box.
6. Select the **Show Run-Time Prompt** check box.
7. Save the configuration settings.

Set up Communication with Mail Server

If you want to send emails from the Visibility Report Server, you need to set up the Visibility server to communicate with your mail server.

To configure the SMTP server settings, complete the following steps.

1. After logging in to **Visibility**, use the sliding menu to navigate to **Navigate > Administration > Configure**. The **Databases** tabbed area appears, by default.
2. Click **Server > Scheduler and Mails** and update the following information.
    - Add the customer's company name to the beginning and add the customer's domain name within the email address. For example, enter `CompanyName Visibility Automated Reporting reportsdepartment@CompanyName.com`.
    - **SMTP Server.** Change the "127.0.0.1" to the IP address of the mail server.
    - **SMTP Authentication.** Select **Enable** or **Disable** based on your implementation requirements.
    - **SMTP Server User.** Enter the mail account's user name.
    - **SMTP Server Password.** Enter mail account's password.
3. To save the configuration settings, click **Save**.

Configure Visibility to pull images from Database

If the Brainware Intelligent Capture project is configured to store the images processed within a database, you need to configure Visibility to point to this database to retrieve the original images. To do this, you need to edit the ReportClient.properties file. This file is located in the following directory.

<Install Directory>\Hyland\Brainware Visibility\Jakarta\webapps\visibility\client\config

In the ReportClient.properties file, update the Configurable System Parameters section with the following settings.

```
[CONFIGURABLE SYSTEM PARAMETERS]

# Configuring file path for Intelligent Capture Visibility Image Puller.
# Set to File if the images are stored on a file server, or Database if
stored in the database tables
# SCAN_IMAGE_PATH=File/Database
# Default value=File
SCAN_IMAGE_PATH=Database

# If images are stored in the Database then specify the database connection
name to retrieve the images.
# If no connection name is specified then connection set in Visibility user
session will be used to retrieve the images.
SCAN_IMAGE_DB_NAME=(Leave blank to have Visibility use the currently
connected database)

# Determines whether decryption of the image name in the hyperlink is
required or not.
# NOTE: Image name encryption must be enabled in the Intelligent Capture
project file in order to use this option.
# Default value=Yes
DECRYPT_IMAGE_NAME=No (Configured to installation requirements)

# Determines what BRWDocument column is used to retrieve the image when
stored in the database.
# FILE_PATH will use DOCUMENT_LINK, FILE_PATH_DOCNUMBER will use
DOCUMENTNUMBER
## Syntax: SCAN_IMAGE_PARAM_NAME=[FILE_PATH / FILE_PATH_DOCNUMBER]
# Default value=FILE_PATH
SCAN_IMAGE_PARAM_NAME=FILE_PATH (Configured to installation requirements)

# This is to specify the Default text for the document if no extension is
present in the document name.
# Default value=.tif
SCAN_IMAGE_TYPE_DEFAULT=.tif (Configured to installation requirements)
```

Restart the Visibility Reporting Service after making changes to the ReportClient.properties file.

Set up Organizations and User Accounts

Add Organizations

Visibility installs with a default organization named Intellica. You need to set up an organization for your company's users; however, the Intellica organization should not be deleted. To set up a new organization, complete the following steps.

1. After logging in to **Visibility**, use the sliding menu to navigate to **Navigate > Administration > Manage Users**. The **Databases** tabbed area appears, by default.
2. Click **Organization > Add** and complete the following substeps.
    1. Enter the **Organization Name**.
    2. Select the **Is Default** check box.
    3. Change the **Password Settings** under the **Advanced** tab based on your implementation's requirements.
3. Save the new organization.

Add Users and Roles

You can add and access users individually or use roles to help administer user access. Hyland recommends using at least the Administrator and User roles.

About privileges

Check privileges that you want to assign to the roles to configure system privileges. You can assign the following privileges.

- Suspend Role. Privileges for this role will be suspended. However, users continue to use privileges they have through other roles.
- Organization Admin. Users are granted all administration rights for the organization to which they belong. For example, creating users and giving them access rights.
- Access Over IM. Currently not available.
- Batch Scheduler Administrator. Users can view and create jobs, schedules, and tasks. If the scope is Organization, the user gains access to jobs, schedules, and tasks created by users belonging to the same organization. If the scope is Global, the user gains access to jobs, schedules, and tasks created by users who belong to any organization.
- Category Setup. User can view all public categories and create public categories. If the scope is Organization, the user gains access to categories created by users who belong to this organization. If the scope is Global, the user gains access to categories created by users belonging to any organization.
- Data Admin. Users can view and create Query objects and Parameter objects and work with Parameter Value Groups page. If the scope is Organization, the user gains access to parameter objects and query objects created by users who belong to the same organization. If the scope is Global, the user has access to parameter objects and query objects created by users belonging to

any organization.

- Deploy Repository Bundle. Users can deploy the repository bundle from Deploy Repository Bundle Portal page.
- Standard Report Designer. Users can design standard reports using desktop studio.
- Adhoc Report Designer. Users can design adhoc reports using Adhoc Wizard.
- Widget Designer. Users can design dashboard widgets. Widgets are placed on dashboards.
- Generate Link. Users can generate a link of any published report to share with non-Visibility users.

Set up the Administrator Role

To set up the Administrator Role, complete the following steps.

1. After logging in to **Visibility**, use the sliding menu to navigate to **Navigate > Administration > Manage Users**. The **Databases** tabbed area appears, by default.
2. Click **User/Role**, select the name of the organization for which you want to create an admin role and then click **Add Role**.
3. Enter **Administrators** under **Role Name** and enter **Visibility Administrators** in the **Role Description**.
4. Select the **Organization Admin** option.
5. Save the new **Role**.

Set up the Users Role

To set up the Users Role, complete the following steps.

1. After logging in to **Visibility**, use the sliding menu to navigate to **Navigate > Administration > Manage Users**. The **Databases** tabbed area appears, by default.
2. Click **User/Role**, select the name of the organization for which you want to create a user role and then click **Add Role**.
3. Enter `Users` under **Role Name** and enter `Basic Users` in the **Role Description**.

   Important Do not check the **Organization Admin** check box. This is for Administrators only.
4. Save the new role.

Restrict Email Access

Visibility allows you to restrict email capabilities from within the portal by assigning users to a role specifically named DisallowEmailing. You can create this role using the same steps required to create the Users role. If a user is assigned the DisallowEmailing role in Visibility, the user does not have Email options.

This access applies to:

- Email option on HTML toolbar on Report Viewer
- Email option on Report Run
- Direct access to ReportEmail.jsp

Note:
Remove all Schedule Reports rights to all users or the DisallowEmailing role if restricting email of published reports is required (**Navigate > Administration > Manage Users > AccessRights**).

Add Users

Adding users is similar to adding Roles in Visibility. The Administrators Role has the capability to add or delete users within the organization; therefore, it should only be assigned to Brainware Intelligent Capture Certified Administrators and/or the Department Manager.

To add a new user, complete the following steps.

1. After logging in to **Visibility**, use the sliding menu to navigate to **Navigate > Administration > Manage Users**. The **Databases** tabbed area appears, by default.
2. Click **User/Role > Add User**.
3. Enter the **User Name**, **Password**, and a brief description.
4. Add the user to the appropriate Role by selecting the **Role Name** check box.
5. Save the new **User**.

Add Super Administrator Users

You can only assign the role of Super Administrator at the user level. Super Administrator users have the capability to add and remove users, roles, queries, reports, and more from all organizations. They also have the ability to deploy the CAB files, create new database connections, and make changes to the server configuration settings. Only Brainware Intelligent Capture Certified Administrators should be assigned the Super Administrator role.

Note:
The Super Administrator role should not be assigned to any user for customer installations where Click Model Licensing is used.

To assign the Super Administrator role to a user, complete the following steps.

1. After logging in to **Visibility**, use the sliding menu to navigate to **Navigate > Administration > Manage Users**. The **Databases** tabbed area appears, by default.
2. Click **User/Role**.
3. Select the **Certified Admin** user.
4. Select the **Super Admin** check box.
5. Save the **User**.

Configure LDAP Authentication for Visibility

LDAP servers (including Microsoft Active Directory) can be used to authenticate users. To configure LDAP authentication for Visibility you need to complete the following tasks:

- Create LDAP/LDAPS Authenticated Organization
- Set Authentication Mode to LDAP/LDAPS
- Create Users
- Map Users

Create LDAP/LDAPS Authenticated Organization

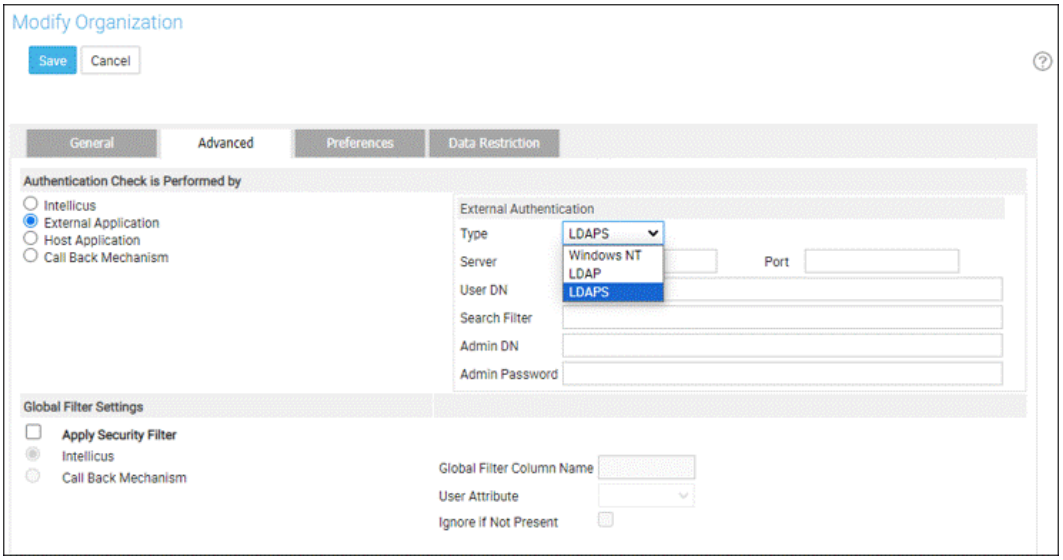
To add a new organization:

1. Click **Administration > Manage Users > Organization**.
2. Click **Add**.
3. Enter the relevant details in the **Organization Name** and **Description** fields.
4. Save the details.

Set Authentication mode to LDAP/LDAPS

To set the authentication mode to LDAP/LDAPS:

1. Click **Modify**.
2. Click the **Advanced** tab.
3. Under **Authentication Check is Performed by**, select **External Application**.
4. Under **External Authentication**, in the **Type** drop-down list, select `LDAP` or `LDAPS`.



5. Enter values for **Server**, Port, and User DN:

- Server = IP of the machine on which LDAP server is running.
- Port = Port on which LDAP server is running (default is 389 for LDAP and 636 for LDAPS)
- User DN = <%USER_ID%>@domain.com

> **Note:** The user DN is the distinguished name of a user on an LDAP server and format can differ between servers. For example: User DN = CN=<%USER_ID%>,CN=Users,DC=test,DC=co,DC=in

6. Click **Save**.

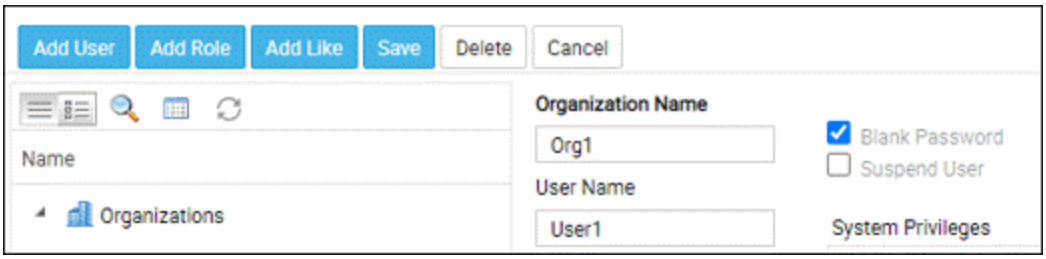
Create Users

To create users:

1. Click **Administration > Manage Users > User/Role**
2. Select the new organization created previously.
3. Click **Add User**.
4. In the **User Name** box, enter an appropriate user name.

> **Note:** This user name must match the user login name in the LDAP server.

5. Select the **Blank Password** check box.



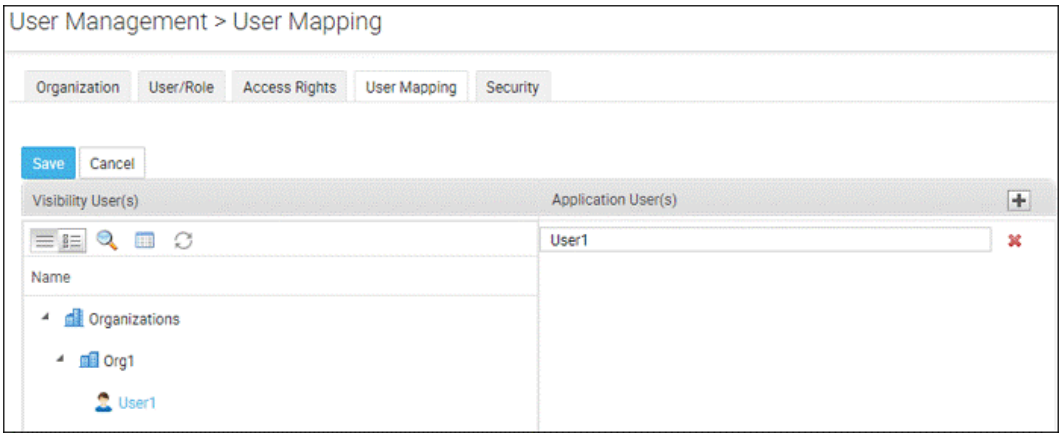
6. Click Save.

Map Users

To map users:

1. Click **Administration > Manage Users > User Mapping**
2. In the **Organization** drop-down list, select the Organization authenticated by the LDAP server.
3. Click the add icon (+) next to **Application User(s)**.
4. Select the relevant Visibility user from the list of users.
5. Enter an appropriate user name.

> **Note:** This value should match the Visibility User Name in the **Application User** column.



6. Click **Save**.

Repeat these steps for all users in the LDAP authentication Organization.

Once configured, the users will be required to provide LDAP credentials on the host application login screen.

Set Report Access Rights

Report access rights can be configured at the Report Category or individual report level for Users/Roles. Hyland recommends setting report access rights for Roles and then adding Users to the respective roles. How customers choose to administer report access rights is their choice. Installers need to configure report access rights on the Administrators and Users roles.

Set Report Access Rights for Administrator Roles

To set report access rights for administrator roles, complete the following steps.

1. After logging in to **Visibility**, use the sliding menu to navigate to **Explorer**.
2. Press Ctrl and multi-select the **Report Categories** for which you want to configure access. For example, you can select Accounts Payable, Custom, Capture, and Verifier.
3. Right-click a category name and select **Access Rights**.
4. Expand the **CompanyName** organization and select the **Admin** check box.
5. Select the **Full** radio button in the **Access Rights** window.
6. Save the changes.

Set Report Access Rights for User Roles

To set report access rights for user roles, complete the following steps.

1. After logging in to **Visibility**, use the sliding menu to navigate to **Explorer**.
2. Press Ctrl and multi-select the **Report Categories** for which you want to configure access. For example, you can select Accounts Payable, Custom, Capture, and Verifier.
3. Right-click a category name and select **Access Rights**.
4. Expand the **CompanyName** organization and select the check box next to the users role.

5. Select the **Full** radio button in the **Access Rights** window.
6. Save the changes.

> **Note:**
> Full access is required for users to view, schedule, and print the reports. This does not give the Users role the access to change or delete the original report.

Change the Default Admin Password

The default Admin password for the Intellica organization must be changed after the installer has completed setting up the CompanyName organization. To change the password, complete the following steps.

1. Log in to **Visibility** as **Admin** using the Intellica organization.
2. Navigate to **Navigate** > **Personalization** > **Preferences** and expand **User Preferences**.
3. Enter the **Current Password** and the **New Password**, then click **Change**.
4. Log out of **Visibility** and log back in using the new credentials to verify the change.

Select User Dashboards

When a new user first accesses the Visibility portal, they need to configure their Dashboard preference. The default Visibility Capture CAB includes an Intelligent Capture Dashboard in the Capture category. To use this Dashboard, complete the following steps.

1. Log in to **Visibility** as a user.
2. Navigate to **Navigate > Personalization > Preferences** and expand **Dashboard Preferences**.
3. In the **Available Dashboard(s)** area, expand the **Capture** category and select the **Intelligent Capture Dashboard**.
4. Press **>** to move the **Intelligent Capture Dashboard** into the **Selected Dashboards** list.
5. Click **Save**.
6. Navigate to **Navigation** > **Dashboards** > **View** to display the **Intelligent Capture Dashboard**.

Select Locale and Time Zone

When a new user first accesses the Visibility portal, they need to configure their locale and time zone preferences. If user does not select locale and time zone under the user's personal preferences, then the default locale and default time zone specified in user preferences will be applied. To set locale and time zone preferences, complete the following steps.

1. Log on to Visibility 4.0.
2. Navigate to **Navigate** > **Personalization** > **Preferences** and expand **User Preferences**.
3. Select the **Default Locale** and **Time Zone**.
4. Click **Save**.

Deploy Portal Languages

Portal languages in Visibility allow users to activate and enable a locale based on their preferences. To add a

portal language to visibility, complete the following steps.

1. Stop **Report Server** and **Web Server**.
2. Download the portal language files.

   Note:
   These files have a .XLS extension

3. Copy these files and paste them in the following directory. folder.

   Example

   ```
   <Installed Path>\Hyland\Brainware
   Visibility\Jakarta\webapps\visibility\client\lang
   ```

4. Add locale entries for each new language in the **localeconfigurations.xls** file located in the following directory.

   Example

   ```
   <Installed Path>\Hyland\Brainware Visibility\ReportEngine\Config\i18n
   ```

   Note:
   Although you can add information to all columns for a locale entry, we recommend you add information to the following columns before saving: **Input date style**, **Output date style**, **Input time style**, and **Output time style**.

5. Add locale entries in the **ReportServerProperties.xml** file located in the following directory.

   Example

   ```
   <Installed Path>\Hyland\Brainware Visibility\ReportEngine\Config
   ```

   Note:
   This enables listing the above locale(s) under the **Default Locale** box under the **User Preferences** section in **Visibility**. To add a locale entry in the **DEFAULT_LOCAL** section, enter the desired locale value and save the file.

   ```
   <OPTION DISPLAY_TEXT="Japanese(Japan)">
      <VALUE><
   ```

SiteMinder Authentication

Visibility can be configured to use SiteMinder for user authentication. This is an optional configuration. For SiteMinder authenticated Users, the Visibility Login Screen is bypassed. There should be a User with Super-Admin access privileges who can perform any administrative activity like creating users in Visibility, mapping application users with those Visibility users, and providing access privileges prior to enabling the SiteMinder Authentication.

Enable Host Application authentication for the Organization

To use SiteMinder authentication, you must set the Authentication mode for the default Organization to Host Application.

To change the Organization Authentication settings, complete the following steps.

1. After logging in to **Visibility**, use the sliding menu to navigate to **Navigate** > **Administration** > **Manage Users**. The **Organization** tab is selected, by default.
2. Select the Organization Name on the left and click **Modify**.
3. Select the **Advanced** tab.
4. Select **Host Application** in **Authentication Check is Performed by**.
5. Click **Save**.

Map the Super-Admin User

An application user with Super-Admin access privileges needs to be mapped to a Visibility Super-Admin user. Once mapped, the application user can perform administrative activities based on the Visibility Super-Admin user.

To map the application admin user to the Visibility Super-Admin, complete the following steps.

1. Go to **Navigate** > **Administration** > **Manage Users** and select the **User Mapping** tab.
2. Select the Organization and the Visibility Super-Admin user.
3. Click **+** to add the application user for the selected **Visibility** user.
4. Enter the name of the application user.
5. Click **Save**.

Map Application Users

Each application user needs to be mapped to Visibility user to access Visibility. When reporting requests come from host application users, they can carry out tasks based on the Visibility users / roles to which they are mapped.

To map the application users to Visibility users, complete the following steps for each user.

1. Go to **Navigate** > **Administration** > **Manage Users** and select the **User Mapping** tab.
2. Select the Organization and the Visibility user.
3. Click the **+** to add application user for the selected Visibility user.
4. Enter the name of the application user.
5. Click **Save**.

Configure SiteMinder

To enable SiteMinder Integration, configure the following settings within ReportClient.properties (`<Install_Path>/Hyland/Brainware Visibility/Jakarta/webapps/visibility/client/config/`).

- SITEMINDER_AUTHENTICATION - Option to enable/disable SiteMinder authentication. Set this property to "ENABLE" to enable the SiteMinder Authentication.
- HOSTAPP_USER - This value defines the field name for the User ID that is contained in the HTTP Header.
- DEFAULT_ORGANIZATION - This value defines the name of default Organization present in Repository.
- LOGIN_PAGE_URL - This value defines the URL of SiteMinder login page.

Result

```
Set Siteminder Authentication as [ENABLE / DISABLE]
# Default value=DISABLE
SITEMINDER_AUTHENTICATION=DISABLE

# This is to specify the field name for the User ID contained in the HTTP
Header
# Default value=""
HOSTAPP_USERID=

# This is to specify the default organization name
# Default value=""
DEFAULT_ORGANIZATION=HostOrg

# This is to specify the SiteMinder login page URL
# Default value=""
LOGIN_PAGE_URL=https://smlogin.companyname.com/siteminderagent/SSOlogin.fcc
```

Restart the Visibility Reporting Service after making these changes.

Data Management

Visibility can be configured to archive data or purge data from the reporting database. This is not required, but may be needed to keep the size of the reporting database manageable.

Enable Data Archiving (SQL Server)

Execute the following steps to enable data archiving on SQL Server database.

1. Identify Source SQL Server Database and Target SQL Server Database.
2. All the tables to be archived must exist in a target database, and table definitions must match with that of source database.
3. Enable windows network Distributed Transaction Coordinator (DTC) access and configure Windows Firewall between source and target database servers - if applicable. To enable DTC access and configure Windows Firewall refer to product documentation for more details.
4. Create a linked server for target database on source database. To create linked server refer to SQL Server database product documentation for more details.
5. Download and Execute the script, **Archive Reporting Documents_SQL.sql**, on source database.

Enable Data Archiving (Oracle)

Execute the following steps to enable data archiving on an Oracle database.

1. Identify Source Oracle Database and Target Oracle Database.
2. All the tables to be archived must exist in a target database, and table definitions must match with that of source database.
3. Create a DB link(`ARCHIVALDBLINK`) for target the database on the source database. To create DB link, execute the below script on source database:

   ```
   CREATE DATABASE LINK ARCHIVALDBLINK     CONNECT TO _username_   IDENTIFIED
   BY _passwd_     USING '$_ORACLE_SID_'
   ```

   Example

   Here the `_username_, _passwd_` and `$_ORACLE_SID_` should be of target database.
4. Download and execute the script, **Prerequisite_Archive Reporting Documents_Oracle.sql**, on source database.
5. Download and execute the script, **Archive Reporting Documents_Oracle.sql**, on source database.

Purge Document Script

Visibility can optionally be configured to enable purging of reporting documents from the reporting database. This will allow a user with Organizational Admin privileges to run a report which will permanently remove data from the reporting database based on user specified parameters.

After deployment of the CAB file from the repository, you need to run the corresponding script for the Purge Document report using the following steps.

1. Download the script file, **Purge Document_Patch_<SQL or Oracle>.sql**.
2. Log on to the reporting database.
3. Execute the script.

Set up Archiving Parameters

prmTargetDBName (SQL Server only)

This parameter is used by the Archive Reporting Documents report. It should be configured to the target database name into which the archived data would be stored.

To modify this parameter, complete the following steps.

1. After logging on to **Visibility**, use the sliding menu to navigate to **Explorer > Capture > prmTargetDBName**.
2. Select **Edit Parameter Details**. The **Parameter Object Editor** area appears.
3. Update the parameter's **Default Value** field to the target database name.
4. Save the changes.

prmTargetDBServerAddress (SQL Server only)

This parameter is used by the Archive Reporting Documents report. It should be configured to the ip address or FQDN of the database server host.

To modify this parameter, complete the following steps.

1. After logging on to **Visibility**, use the sliding menu to navigate to **Explorer > Capture > prmTargetDBServerAddress**.
2. Select **Edit Parameter Details**. The **Parameter Object Editor** area appears.
3. Update the parameter's **Default Value** field to the port number used during installation.
4. Save the changes.

prmDBLinkName (Oracle only)

This parameter is used by the Archive Reporting Documents report. It should be configured to the database link name created for target database that would be used to store the archived data.

To modify this parameter, complete the following steps.

1. After logging on to **Visibility**, use the sliding menu to navigate to **Explorer > Capture > prmDBLinkName**.
2. Select **Edit Parameter Details**. The **Parameter Object Editor** area appears.
3. Update the parameter's **Default Value** field to the port number used during installation.
4. Save the changes.