Brainware Intelligent Capture Visibility

Installation and Setup Guide

Version: 3.2.x

Written by: Product Knowledge, R&D
Date: September 2018

Table of Contents

Installation

Prerequisites for Installation

The 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 – 32 bit Version

To install the Visibility server, complete the following steps.

1. Run **Setup.exe** as Administrator 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**.
5. In the **Installation Options** screen, it is recommend that you choose the **Express Install** option and click **Next**.

   Note Use the **Custom Install** option if you are changing the location of the installed objects or want to customize the implementation.
6. In the **Configure Ports** screen, enter the **Portal Port** number that users will use to access the **Visibility** web portal.

   Note If you are installing **Visibility** on the same server as IIS, change the default port from 80 to the appropriate port.
7. In the **Installations Preferences** review screen, click **Next.**
8. In the **Installation Complete** screen, respond to the prompts as needed, then click **Finish.**

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, 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**.

   Note If you are installing **Visibility** on the same server as IIS, you will need to change the default port from 80 to the appropriate port.

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, you need to request a production license by modifying and providing the License.req file present in the <*InstallFolder*>\ReportEngine\bin folder. 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**.
1. Delete the “work” folder located here: <*Install Path*>\Jakarta\
2. Navigate to the folder <*Install Path*>\ReportEngine\bin\
   - Rename the file **ReportEngine.lic** to **ReportEngine.old**
   - Rename the license file received from Support to **ReportEngine.lic** and place it in this folder.
3. Restart the **Visibility Reporting Service**.

Access the Web Portal

Once the installation has been completed, 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 3.0 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.

- Portal Navigation
- Report Categories
- Data Model (Repository)
- User Favorites
- Home

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**, use the sliding menu to navigate to **Navigation** > **Administration** > **Configure** and select the **Databases** tab.
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 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.

     1. For SQL installations, select the **Driver Version**, **Authentication Mode**, and **Driver Type** For repository connections, always use "Microsoft" Driver Type.
     2. For Oracle installations, select the **Driver Type** and **Driver Version**.

   - **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 Intelligent Capture reporting database by completing the following steps.

1. After logging in to **Visibility**, use the sliding menu to navigate to **Navigation** > **Administration** > **Configure** and select the **Databases** tab.
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 **Driver Version**.
   - **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.

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.

Deploy CAB files

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

1. After logging in to **Visibility**, use the sliding menu to navigate to **Navigation** > **Repository** > **Deploy Repository Bundle**.
2. Select **Browse** and navigate to the **.cab** file for the installation (Oracle or SQL).
3. Click **Upload**, then click **Deploy**. Scroll down the page and ensure that all reports, queries, and parameters were added.
4. After all CAB files are deployed, restart the Visibility service.

   Note Capture category CAB is required for all implementations. Repeat this process for any additional CAB files you want to deploy. Some CAB files include the deleting of older report objects. If these objects were not present when the CAB file was deployed, you receive a warning next to the report object to be deleted. In such cases, this warning can be ignored.

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 in to **Visibility**, use the sliding menu to navigate to **Data Model** > **Capture** > **Parameter Objects** > **prmImagePuller**.
2. Select the **Edit Parameter Details** option.
3. Update the parameter's **Default Value** field to the port number used during installation.
4. Save the changes.

prmExtractionFieldName

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 in to **Visibility**, use the sliding menu to navigate to **Data Model** > **Capture** > **Parameter Objects** > **prmExtractionFieldName**.
2. Click the **Edit Parameter Details** option.
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.

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

prmAmountFields

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 in to **Visibility**, use the sliding menu to navigate to **Data Model** > **Capture** > **Parameter Objects** > **prmAmountFields**.
2. Click the **Edit Parameter Details** option.
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.

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

prmGenericClassName

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 in to **Visibility**, use the sliding menu to navigate to **Data Model** > **Capture** > **Parameter Objects** > **prmGenericClassName**.
2. Click the **Edit Parameter Details** option.
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.

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

prmParentClassName

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 in to **Visibility**, use the sliding menu to navigate to **Data Model** > **Capture** > **Parameter Objects** > **prmParentClassName**.
2. Click the **Edit Parameter Details** option.
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.

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

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 in to **Visibility**, use the sliding menu to navigate to **Data Model** > **Capture** > **Parameter Objects** > **prmAmountFields**.
2. Click the **Edit Parameter Details** option.
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 .

To modify this parameter, complete the following steps.

1. After logging in to **Visibility**, use the sliding menu to navigate to **Data Model** > **Capture** > **Parameter Objects** > **prmUnknownValue.**
2. Click the **Edit Parameter Details** option.
3. 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.
4. **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 in to **Visibility**, use the sliding menu to navigate to **Data Model** > **Capture** > **Parameter Objects** > **prmAmountFields**.
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**, use the sliding menu to navigate to **Data Model** > **Capture** > **Parameter Objects** > **Parameter Name**.
2. Click the **Edit Parameter Details** option.
3. Set the **Default Value** to the table name or stored procedure in your reporting data database.
4. **Save** the changes.

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 two “Show filter” options 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 **Navigation** > **Administration** > **Configure** and select the **Ad hoc Wizard** tab.
2. Select **Data Source** on the left of the screen.
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 **Navigation** > **Administration** > **Configure** and select the **Server** tab.
2. Select **Scheduler and Mails** on the left of the screen and update the following information.
   - **Email From Address.** 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 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>\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 **Navigation** > **Administration** > **Manage Users** and select the **Organization** tab.
2. Click the **Add** button on the left side of the panel 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.

Add Roles

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.

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

1. After logging in to **Visibility**, use the sliding menu to navigate to **Navigation** > **Administration** > **Manage Users** and select the **User/Role** tab
2. Select the **CompanyName** organization in the left tab and 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**.

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

1. After logging in to **Visibility**, use the sliding menu to navigate to **Navigation** > **Administration** > **Manage Users** and select the **User/Role** tab.
2. Select the **CompanyName** organization in the left tab and 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 through the DisallowEmailing Role

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 (**Navigation** > **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 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 **Navigation** > **Administration** > **Manage Users** and select the **User/Role** tab
2. Click the **Add User** button.
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 new CAB files, create new database connections, and make changes to the server configuration settings. Only 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 **Navigation** > **Administration** > **Manage Users** and select the **User/Role** tab.
2. Select the **Certified Admin** user.
3. Select the **Super Admin** check box.
4. Save the **User**.

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 and User 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 **Data Model**.
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.

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

1. In the **Data Model**, after selecting multiple report categories, select **Access Rights**.
2. Expand the **CompanyName** organization and select the **Admin** check box.
3. Select the **Full** radio button in the **Access Rights** window
4. 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 **Navigation** > **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 **Navigation** > **Dashboards** > **Preferences**.
3. 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 in to Visibility 3.0.
2. Navigate to **Navigation** > **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.
   <Installed Path>\Brainware Visibility\Jakarta\webapps\visibility\client\lang folder
4. Add locale entries for each new language in the **localeconfigurations.xls** file located in the following directory.
   <Installed Path>\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.
   <Installed Path>\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><![CDATA[ja_JP]]></VALUE>
</OPTION>
```

6. Delete the **work** folder in the following directory.
   <Installed Path>\Brainware Visibility\Jakarta
7. Restart **Report Server** and **Web Server**.

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 **Navigation** > **Administration** > **Manage Users** and select the **Organization** tab
2. Select the company Organization 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 **Navigation** > **Administration** > **Manage Users** and select the **User Mapping** tab.
2. Select the company 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 **Navigation** > **Administration** > **Manage Users** and select the **User Mapping** tab.
2. Select the company 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*>/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.

```
# 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

Data Archiving (Optional)

Visibility can be configured to use data archiving for reporting database. This is an optional configuration.

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 the DB link, refer to Oracle database product documentation for more details.
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 Patch

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

1. Download the patch script file, **Purge Document_Patch_<SQL or Oracle>.sql**.
2. Log in to the reporting database.
3. Execute the patch 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 in to **Visibility**, use the sliding menu to navigate to **Data Model** > **Capture** > **Parameter Objects** > **prmTargetDBName**.
2. Select the **Edit Parameter Details** option.
3. Update the parameter's **Default Value** field to the port number used during installation.
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 in to **Visibility**, use the sliding menu to navigate to **Data Model** > **Capture** > **Parameter Objects** > **prmTargetDBServerAddress**.
2. Select the **Edit Parameter Details** option.
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 in to **Visibility**, use the sliding menu to navigate to **Data Model** > **Capture** > **Parameter Objects** > **prmDBLinkName**.
2. Select the **Edit Parameter Details** option.
3. Update the parameter’s **Default Value** field to the port number used during installation.
4. Save the changes.