Oracle® Fusion Middleware

WebCenter Forms Recognition Installation Guide

14c (14.1.1.0.0)

G55818-01

June 2025

Describes how to install WebCenter Forms Recognition

ORACLE®

Oracle Fusion Middleware Oracle WebCenter Forms Recognition Installation Guide, 14c (14.1.1.0.0)

G55818-01

Copyright © 2009, 2025, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.



Table of Contents

About Oracle WebCenter Forms Recognition 8
Oracle WFR API *8*
Prerequisites *8*
About the Oracle WebCenter Forms Recognition Process *8*
About the Oracle WebCenter Forms Recognition Database *10*
Install Oracle WebCenter Forms Recognition 10
Download the Setup Package *10*
About the Complete and Custom Installation Types *11*
Verify SQL Server Permissions *11*
Preparations for the Installation of an Oracle Database *11*
Create the Tablespace 11
Create the Database User 12
Install WebCenter Forms Recognition Attended *13*
Silent Installations *14*
Silent *Install.ini* Parameters 14
[General] 15
[Applications] 15
[OCR Engines] 16
[AutoServiceUpdate] ..... **Error! Bookmark not defined.**
[Database Configuration] 16
[DB Credentials] 17
Install an Additional Runtime Server Instance *17*
Oracle WebCenter Forms Recognition Subdirectories *18*
CONFIG Files *18*
Install the Database Manually *18*
Create the Oracle Database 19
Create the SQL Server Database 19
Modify the Database Connection Strings 19
Revoke Oracle User Rights 21
Install the Required Patch *21*
Install Interim 8bpp Grayscale Patch 21
Components Version Info Tool 21

Components General Info View *22*
Components Licensing Info View *22*
Review the Installed Components *22*
Review the Component License Information *22*
Manage the WebCenter Forms Recognition Components 23
Add or Remove WebCenter Forms Recognition Components *23*
Manually Register Components *23*
About the Oracle WebCenter Forms Recognition Core Service 23
Configuration for Web Verifier 24
Configure IIS for Web Verifier *24*
Role Services Configuration for Web Verifier in IIS 7.5 and Above 24
Common HTTP Features 24
Application Development 24
Health and Diagnostics 24
Create the Application Pool for Web Verifier in IIS 7.5 and Above 25
Configure Web Verifier in IIS 7.5 and Above 25
Configure a White Label Directory in IIS 25
Configure Web Verifier *26*
Modify the instanceName Value When Using Multiple Web Servers *26*
Modify the Database Connection Strings for Web Verifier 26
Configure Server Security for Web Verifier *27*
Add the User Context in SQL Server 27
Verify the IIS Identity 28
Set Permissions for WebCenter Forms Recognition Projects 28
Set Permissions for WebCenter Forms Recognition Bin Directory 28
Implement Single Sign-On Authentication *28*
About the Single Sign-On Authentication for Web Verifier 29
Enable the Single Sign-On Authentication 29
About the Single Sign-On Session and the Web Verifier Session 30
Modify the Web Verifier Session Timeout 30
Configure Windows Authentication *30*
About Windows Authentication for Web Verifier 30
Configure Windows Authentication in IIS 7.5 and Higher 30
Create a Windows Authentication Version of the Web.config File 30

Switch Back to Forms Authentication 31
Configure Cookies for Web Verifier *31*
About Web Verifier Performance *33*
Image Conversion 33
Delayed Validation 33
Use Traditional Chinese *34*
Access Web Verifier *34*
Additional Columns in Verifier or Web Verifier *34*
Display and Name Additional Verifier Columns: Oracle 34
Display and Name Additional Verifier Columns: SQL Server 35
Display Additional Web Verifier Columns 35
Change the Web Verifier Column Names 36
Configure Global Application Settings 36
About Workflow History Reporting *36*
Configure Workflow History Reporting: Oracle 36
Configure Workflow History Reporting: SQL Server 37
About Disabling Batch Deletion in Runtime Server and Designer *37*
Disable Batch Deletion: Oracle 38
Disable Batch Deletion: SQL Server 38
About Modifying the URL Expiration Time for Web Verifier *38*
Modify the URL Expiration Time: Oracle 38
Modify the URL Expiration Time: SQL Server 38
Configure WebCenter Forms Recognition Security 39
File System Security *39*
Recommended Accounts and Groups *40*
Configure Access to Project Data *41*
About the Service Account on a Domain Network *42*
About the Service Account for System Monitoring *42*
About INI File Encryption *42*
Encrypt a Password for a Database Connection String *43*
About User Password Encryption *43*
Change the Hashing Algorithm 44
Configure WebCenter Forms Recognition Runtime Components 44
About RTS Remote Administration MMC *44*

Configure the Runtime Service Manager Service *45*
Configure the RTS Remote Administration MMC Snap-In *45*
About the Desktop Heap Size 46
Modify the Desktop Heap Size *46*
Ideal Desktop Heap Size *46*
About Logging 47
Log Files *47*
Logging Levels *49*
Configure the Logging Level *49*
Configure the Location of the Application Log Files *49*
Configure the Retention Time of Application and Error Log Files *50*
OCR Engine Languages 51
Available OCR Engines *51*
Cleqs Barcode Engine 51
FineReader10 OCR Engine 51
FineReader11 OCR Engine 52
QualitySoft Barcode Engine 52
About Automated Update 52
Modify the Batch File *52*
Modify the Application Shortcuts for Verifier and Designer *52*
Automate Runtime Server Updates *53*
About Port Configuration 53
Configure a Different Port for Runtime Server *53*
File Permission Matrix 54
Web.config Options and Associated Resource File Parameters 57
About Navigation to Documents for Indexing *64*
Enable Navigation to Indexable Documents *64*
Registry Options 64
Create the Registry Key ErrorTraceDir *65*
Create the Registry Key HideBatchReleaseDialog *65*
Modify the Registry Key ErrorTrace - All *66*
Create the Registry Key MaximumDiskspaceUsageMB *66*
Create the Registry Key TotalDaysToKeepFiles *66*
Uninstall WebCenter Forms Recognition. 67

Troubleshooting 67

Windows could not start the WebCenter Forms Recognition Core Service on Local Computer Error. 0xffffffff: 0xffffffff 67

WebCenter Forms Recognition Services Won't Start Automatically 67

About Oracle WebCenter Forms Recognition

WebCenter Forms Recognition is a document processing system.

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

Oracle WebCenter Forms Recognition includes the following applications.

- Oracle WebCenter Forms Recognition Designer
- Oracle WebCenter Forms Recognition Runtime Server
- Oracle WebCenter Forms Recognition Verifier
- Oracle WebCenter Forms Recognition Web Verifier

For information about the document processing system, see About the Oracle WebCenter Forms Recognition Process.

Oracle WFR API

The Oracle WebCenter Forms Recognition setup package includes the Oracle WFR API installation files. For more information, see the *Oracle WebCenter Forms Recognition API Installation Guide*.

Prerequisites

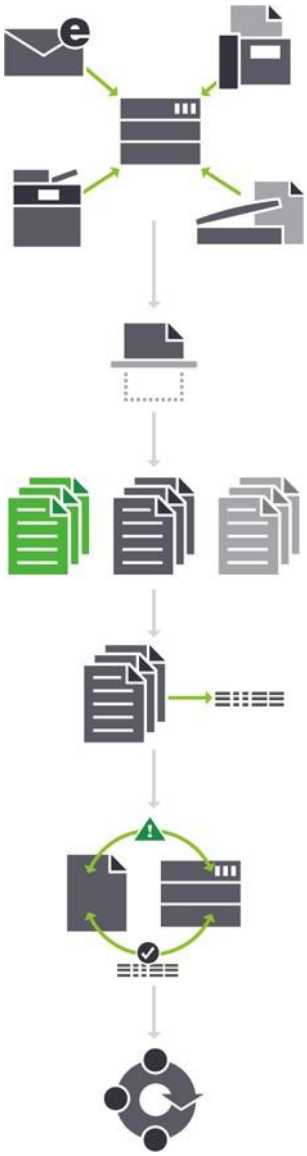
To verify your system requirements and database meet the minimum requirements for WebCenter Forms Recognition, refer to the *Oracle WebCenter Forms Recognition Technical Specifications Guide*. Before you install WebCenter Forms Recognition, verify the following prerequisites.

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

About the Oracle WebCenter Forms Recognition Process

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

WebCenter Forms Recognition forms a complete document processing system, as illustrated in the diagram below



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

Forms Recognition recognizes all eligible data values on the page.

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

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

About the Oracle WebCenter Forms Recognition Database

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

WebCenter Forms Recognition stores the following data in the database.

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

Install Oracle WebCenter Forms Recognition

To install WebCenter Forms Recognition, complete the following procedures.

- Download the Setup Package
- Optional. See About Help below for more information on how to modify the help file location.
- Optional. Complete one of the following substeps to verify database permissions.

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

  - Verify Oracle permissions
  - Verify SQL Server permissions
- Install WebCenter Forms Recognition Attended or Install WebCenter Forms Recognition Unattended
- If you did not install the database with the installation wizard, complete the steps in Install the Database manually.
- Optional. Encrypt the password for a database connection string.
- Configure Internet Information Services and Web Verifier, if the installation includes Web Verifier
- Configure WebCenter Forms Recognition Security
- Configure WebCenter Forms Recognition Runtime Components

Downloading the Setup Package

To obtain WebCenter Forms Recognition product installation files, complete the following steps.

1. Contact the Oracle Technical Support group.
2. Save and unzip the installation files locally so you can access them during installation.

About the Complete and Custom Installation Types

When you install WebCenter Forms Recognition with an attended installation, you choose a complete or a custom installation type.

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

- FineReader 10
- FineReader 11
- QualitySoft

The custom installation type allows you to choose which applications, demo projects, and recognition engines you want to install.

Verifying SQL Server Permissions

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

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

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

Verifying Oracle Database Server Permissions

To use WebCenter Forms Recognition with an Oracle database, complete the following preparatory steps. You can use Windows authentication if the user performing the installation has the appropriate rights to the database server.

- As an administrator, create a new tablespace and user.

  N**ote**: The username must be all uppercase.
- Assign the following rights to the user
  - Insert, modify and delete data.
  - Create tables
  - Create views.

Preparations for the Installation of an Oracle Database

Creating the Tablespace

A default tablespace and a temporary tablespace are required to create the WebCenter Forms Recognition user and the schema. Complete the following steps.

1. Create the default tablespace according to the following example.

```
CREATE TABLESPACE WFR
    DATAFILE 'wfr.dat'
    SIZE 20M AUTOEXTEND ON;
```

2. Create the temporary tablespace according to the following example.

```
CREATE TEMPORARY TABLESPACE T_WFR
    TEMPFILE 'temp_WFR.dbf'
    SIZE 5M AUTOEXTEND ON;
```

Creating the Database User

To create the database user, complete the following steps.

Prerequisite

- The user needs a login, in the example `'IDENTIFIED BY PASSWORD'`

  If you want to use a different authentication type, see the Oracle documentation for more information.

- The user needs an unlimited quota on the default tablespace.

1. Create a user with password authentication according to the following example.

   Note: The user name must be written in capital letters.

```
CREATE USER WFRUSER
    IDENTIFIED BY <password>
    DEFAULT TABLESPACE WFR
    TEMPORARY TABLESPACE T_WFR
    QUOTA UNLIMITED ON WFR;
```

2. Grant the user the permissions required to create database objects according to the following example.

```
GRANT

    CONNECT,
    CREATE SESSION,
    CREATE TABLE,
    CREATE TYPE,
    CREATE INDEXTYPE,
    CREATE PROCEDURE,
    CREATE SEQUENCE,
    CREATE SYNONYM,
    CREATE PUBLIC SYNONYM,
    CREATE TRIGGER
TO WFRUSER;
```

Installing WebCenter Forms Recognition Attended

To install WebCenter Forms Recognition, complete the following steps.

1. Run **setup.exe**.

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

2. If .NET Framework 4.7.2 is not installed, complete one of the following substeps.

   - To allow setup.exe to install .NET Framework 4.7.2, select **Let the setup install .NET Framework Version 4.7.2 (Recommended)** and then click **Next**.

   - To cancel the setup and install the required .NET Framework manually, select **Abort setup** and then click **Next**. After installing .NET Framework, rerun **setup.exe** and proceed with the following steps.

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

3. In the **Setup Oracle WebCenter Forms Recognition** page, click **Next**.
4. In the **Installation Type** page, select **Complete** or **Custom** and click **Next**.
5. If you selected **Custom**, complete the following substeps. If you selected **Complete**, continue to the next step.
    1. In the **Installation Directory** page, accept the default or change the directory, and then click **Next**.
    2. In the **Feature Selection** page, clear any unrequired applications, demo projects, and recognition engines and then click **Next**.
    3. Click **Next**.
6. In the **Program Folder** page, accept the default program directory or select one of the existing directories and then click **Next**.
7. In the **Selected Install Options** page, verify your selections and then click **Next**.
8. In the **Database Setup Options** page, select one of the following options and then click **Next**.
    - Oracle
    - SQL Server
    - Do not install database

    Note: You can also create the database separately after the WebCenter Forms Recognition installation process.
9. For ORACLE or SQL Server, complete the following substeps.
    1. In the **Login Credentials** page, either select **Windows Authentication** or type the user ID and password and then click **Next**.
    2. In the **Database Server Information** page, in the **Database Server Name** field, type the database server name and then click **Next**.
10. In the **Performed Tasks** page, click **Next**.
11. Optional. In the **Icons on Desktop** page, select **Create desktop shortcuts for applications** and click **Finish**.

Silent Installations

To install WebCenter Forms Recognition on several machines concurrently, such as Verifier workstations, use the silent installation mode. To install WebCenter Forms Recognition silently, complete the following steps.

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

   Note: You can delete single parameters or complete sections, but you cannot move a parameter outside of its appropriate section.
3. Save and close the file.
4. From the *[drive:]\[setup directory]* directory, execute the **setupsilent.bat** file.

Silent *Install.ini* Parameters

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

- [General]

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

[General]

This section contains general installation parameters.

Path

The installation path, without a trailing backslash.

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

MoveComponentsIfRequired

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

0: Use existing component directory.

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

CreateDeskTopIcons

0: Default value – do not create desktop shortcuts.

1: Create desktop shortcuts.

[Applications]

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

Designer

0: Do not install Designer

1: Default value – Install Designer

Verifier

0: Do not install Verifier

1: Default value – Install Verifier

Runtime Server

0: Do not install Runtime Server

1: Default value – Install Runtime Server

Web Verifier

0: Do not install Web Verifier

1: Default value – Install Web Verifier

[OCR Engines]

Defines which OCR engines to install.

FineReader10

0: Do not install the FineReader10 engine

1: Default value – Install FineReader10 engine

FineReader11

0: Do not install the FineReader11 engine

1: Default value – Install FineReader11 engine

Cleqs

0: Do not install the Cleqs engine

1: Default value – Install Cleqs engine

QualitysoftBarcode

0: Do not install the QualitySoft engine

1: Default value – Install QualitySoft engine

[Additional]

Additional files to install.

Demo Files

0: Do not install the demo project files

1: Default value – Install the demo project files

[Database Configuration]

Settings for an existing database server.

DBServerType

1. Configure the Oracle database.
2. Configure the SQL Server database.
3. Default value – Do not configure a database.

UseDBConfIniFile

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

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

[DB Credentials]

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

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

The following options apply for SQL Server connections only.

SQLServerWindowsAuthent

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

1: Use Windows authentication for database access

SQLServerAdminUser

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

SQLServerAdminPassword

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

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

DBUserWindowsAuthent

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

1: Use Windows authentication for the database user

DBUserName

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

DBUserPassword

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

DatabaseServerPath

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

Installing an Additional Runtime Server Instance

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

1. Install WebCenter Forms Recognition without installing the database.
2. Copy the following configuration files from an existing installation to the new installation directory.
   - *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition* Web Server\Web.config
   - *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition*\bin\DstDsr.exe.config
   - *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition*\DstHost.exe.config
   - *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition*\DstSlm.exe.config
   - *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition*\bin\DstVer.exe.config
   - *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition*\bin\DstCoreSvc.exe.config

- *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition*\bin\DstWkBrw.exe.config

Oracle WebCenter Forms Recognition Subdirectories

Setup creates the following subdirectories in the installation directory.

- \Components\Bwe contains the WebCenter Forms Recognition Toolkit.
- \Components\Cairo contains the license file and the base components for imaging and recognition.
- \Components\Cedar contains the base components for document analysis.
- \Components\Tools contains the installation log file as well as several tools and utilities for WebCenter Forms Recognition, such as the SCBLibVersion.exe component version information tool
- Oracle\WebCenter Forms Recognition \bin contains the WebCenter Forms Recognition executables and the settings files.
- C:\Program Files (x86)\Oracle\WebCenter Forms Recognition\bin\LogRoot\Log contains the log files.
- \Oracle\WebCenter Forms Recognition Web Server contains the WebCenter Forms Recognition web components, the Web.config file, and other web libraries used by Web Verifier.
- \Projects contains demo projects.
- \License contains the shared runtime license file.

CONFIG Files

The following table provides a list of the CONFIG files used by the WebCenter Forms Recognition applications.

Application	**CONFIG files**
Designer	*C:\Program Files (x86)\Oracle\WebCenter Forms Recognition*\bin\DstDsr.exe.config
Learnset Manager	*C:\Program Files (x86)\Oracle\WebCenter Forms Recognition*\bin\DstSlm.exe.config
Runtime Server	*C:\Program Files (x86)\Oracle\WebCenter Forms Recognition*\bin\DstHost.exe.config
Verifier	*C:\Program Files (x86)\Oracle\WebCenter Forms Recognition*\bin\DstVer.exe.config
Core Service	*C:\Program Files (x86)\Oracle\WebCenter Forms Recognition*\bin\DstCoreSvc.exe.config
Workdoc Browser	*C:\Program Files (x86)\Oracle\WebCenter Forms Recognition*\bin\DstWkBrw.exe.config
Web Verifier	*C:\Program Files (x86)\Oracle\WebCenter Forms Recognition* Web Server\Web.config
Supervised Learning in Web Verifier	*C:\Program Files (x86)\Oracle\WebCenter Forms Recognition* \bin\Brainware.System.Project.exe.config

Installing the Database Manually

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

Complete the following steps.

1. Complete one of the following substeps.
   - Create the Oracle Database.
   - Create the SQL Server Database.
2. Modify the database connection strings.

Creating the Oracle Database

We recommend creating the WebCenter Forms Recognition database in a separate schema which is not shared with any other programs. To execute the creation scripts, use the owner of the schema created for WebCenter Forms Recognition. Complete the following steps.

1. To execute the installation scripts using **SQL Developer**, complete the following substeps.
   1. Configure a connection for the WebCenter Forms Recognition user.
   2. From the ***[drive:]\[setup directory]*\FirstPart\Database\CreationScripts\Oracle** directory, open the **BrwCreateDatabase.sql** script.
   3. Ensure that the connection is set to the WebCenter Forms Recognition user and then execute the script.
   4. From the ***[drive:]\[setup directory]*\FirstPart\Database\UpdateScripts\Oracle** directory, open the **BRW_Upgrade_Database.sql** script.
   5. Ensure that the connection is set to the WebCenter Forms Recognition user and then execute the script.
2. To execute the installation scripts using **SQL Plus**, complete the following substeps.
   1. Start **SQL Plus** and connect to the database as the WebCenter Forms Recognition user.
   2. From the ***[drive:]\[setup directory]*\FirstPart\Database\CreationScripts\Oracle** directory, execute the **BrwCreateDatabase.sql** script.
   3. From the ***[drive:]\[setup directory]*\FirstPart\Database\UpdateScripts\Oracle** directory, execute the **BRW_Upgrade_Database.sql** script.

Creating the SQL Server Database

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

1. Launch the **SQL Server Management Studio**.
2. Log on using an account with administrator rights.
3. Create a new database with a meaningful name, such as **Oracle WebCenter Forms Recognition**.
4. From the ***[drive:]\[setup directory]*\FirstPart\Database\CreationScripts\SQL Server** directory, execute the **BrwCreateDatabase.sql** script.
5. From the ***[drive:]\[setup directory]*\FirstPart\Database\UpdateScripts\SQL Server** directory, execute the **BRW_Upgrade_Database.sql** script against the WebCenter Forms Recognition database.
6. Review the **Messages** pane for errors.

   Note: If there are errors, you can rerun the script as often as required.

Modifying the Database Connection Strings

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

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

1. From the ***C:\Program Files (x86)\Oracle\WebCenter Forms Recognition*** **\bin** directory, open **DstDsr.exe.config** in a text editor.
2. Search for the `<connectionStrings>` element.

   Note: For information about password encryption, see Encrypt the password for a database connection string.
3. For a SQL Server database, modify the following values.
   - Set `Data Source`.
   - Set `Initial Catalog` to the SQL Server database catalog.
   - Set `User ID` to the SQL Server user ID.
   - Set `Password` to the SQL Server password.

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

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

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

   Note: To copy the connections string example as a single line, open this document in Acrobat Reader and copy and paste the string from there.
4. For an ORACLE database, modify the following values.
   - Set `Data Source`.
   - Set `User ID` to the service account user ID.
   - Set `Password` to the service account password.

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

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

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

Revoking Oracle User Rights

After creating or updating the Oracle database, you can revoke some of the permissions from the WebCenter Forms Recognition user because they are no longer needed. Complete the following step.

- Revoke the permissions according to the following example.

```
REVOKE
   CREATE TYPE,
   CREATE INDEXTYPE,
   CREATE PROCEDURE,
   CREATE SEQUENCE,
   CREATE SYNONYM,
   CREATE PUBLIC SYNONYM,
   CREATE TRIGGER
FROM WFRUSER;
```

Install the Required Patch

After installing WebCenter Forms Recognition, install the following required patches from the location ***[drive:]\[setup directory or installation media]*\Patches**.

1. Extract the **WFR 141100 Patch 6022.zip** file to any temporary directory.
2. Review and follow the steps mentioned in the **[extracted directory] \ *Readme*** text file.
3. Repeat the above steps [1-2] for the following patches in the same sequence:
   a. WFR 141100 Patch 6023.zip
   b. WFR 141100 Patch 6024.zip
   c. WFR 141100 Patch 6025.zip

Install Interim 8bpp Grayscale Patch

Install the Interim 8bpp Grayscale Patch if there are issues handling 8bpp grayscale images.

1. Navigate to the ***[drive:]\[setup directory]*\Patches** directory.
2. Extract the **Interim Grayscale Patch.zip** file to any temporary directory.
3. Review and follow the steps mentioned in the **[temporary directory] *Readme*** text file.

Components Version Info Tool

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

Components General Info View

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

See also: Reviewing the Installed Components.

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

Components Licensing Info View

This view lists licensable components and provides the following information.

See also: Review the Component License Information.

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

Reviewing the Installed Components

To review the installed components, complete the following steps.

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

Reviewing the Component License Information

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

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

Manage the WebCenter Forms Recognition Components

The WebCenter Forms Recognition installation process enables you to add or remove the following components.

- Oracle WebCenter Forms Recognition Designer
- Oracle WebCenter Forms Recognition Runtime Server
- Oracle WebCenter Forms Recognition Verifier
- Oracle WebCenter Forms Recognition Web Verifier

Adding or Removing WebCenter Forms Recognition Components

To modify an existing Oracle WebCenter Forms Recognition installation and to add or remove components, complete the following steps.

1. From **Windows Programs and Features**, select **Oracle WebCenter Forms Recognition** and then click **Change.**
2. In the **License Agreement** page, read and accept the End-User License Agreement (EULA), and then click **Next**.
3. In the **Setup** page, select **Modify** and then click **Next**.
4. In the **Feature Selection** page, select or clear the desired components and then click **Next**.
5. In the **Icons on Desktop** page, complete the following substeps.
    1. Optional. Select **Create desktop shortcuts for applications**.
    2. Click **Finish**.

Registering Components Manually

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

1. From the *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition\Components\Cairo* directory, execute the **RegCro.bat** file.
2. From the *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition\Components\Cedar* directory, execute the **RegCdr.bat** file.
3. From the *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition\Components\Bwe* directory, execute the **RegBwe.bat** file.

About the Oracle WebCenter Forms Recognition Core Service

The Oracle WebCenter Forms Recognition Core service is required to manage the shared license of WebCenter Forms Recognition.

- The service runs as a Windows Service under the **Network Service** account by default.
- The **DstCoreSvc.exe.config** file contains the database connection string.
- The Startup type of the service is set to Automatic (Delayed Start), so that the service starts automatically 2 minutes after other services have started. The administrator can modify the specific delay for a system in Windows Registry.
- The service starts automatically after installation and restarts according to the following rules.
    - The service restarts after 1 second if it stops working for the first time.

- The service restarts after 30 seconds if it stops working for the second time.
- The administrator must restart the service manually if it stops working for the third time on the same day.

Configuration for Web Verifier

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

- Configure IIS for Web Verifier
- Configure Web Verifier
- Configure Server Security for Web Verifier
- Optional. Implement single sign-on authentication
- Optional. Configure Windows Authentication
- Optional. Configure SSL. For information on how to configure SSL on your IIS machine, refer to https://support.microsoft.com.
- Optional. Configure Cookies for Web Verifier

Configuring IIS for Web Verifier

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

- To ensure that the required role services are enabled, see Role services are enabled.
- Create the Application Pool for Web Verifier in IIS 7.5 and Above
- Configure Web Verifier in IIS 7.5 and Above
- Configure a White Label Directory in IIS

Role Services Configuration for Web Verifier in IIS 7.5 and Above

Web Verifier requires the following role services in IIS.

Common HTTP Features

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

Application Development

- ASP.NET 4.x (The default version available on each of the supported version of Windows Sever)
- ASP.NET 4.8 (Windows Server 2022)
- ASP.NET 4.7 (Windows Server 2019)
- ASP.NET 4.6 (Windows Server 2016)
- .NET Extensibility
- ISAPI Extensions
- ISAPI Filters

Health and Diagnostics

- HTTP Logging
- Request Monitor

Creating the Application Pool for Web Verifier in IIS 7.5 and Above

To create the application pool for Web Verifier, complete the following steps.

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

      Note: Alternatively, you can specify a service account.
    - Load User Profile = True

Configuring Web Verifier in IIS 7.5 and Above

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

1. In the **Internet Information Services (IIS) Manager** window, in the left pane, expand **Sites > Default Web Site**.
2. Right-click **Default Web Site** and then click **Add Application**.
3. In the **Add Application** dialog box, complete the following substeps.
    1. In the **Alias** field, type `WebVerifier`.
    2. In the **Application pool** field, select the pool that was configured before, such as **WebVerifierPool**.
    3. In the **Physical path** field, type or browse to the ***C:\Program Files (x86)\Oracle\WebCenter Forms Recognition*Oracle WebCenter Forms Recognition Web Server** directory and then click **OK**.
4. In the **Internet Information Services (IIS) Manager** window, in the left pane, select **WebVerifier**.
5. In the middle pane, under **IIS**, double-click **Default Document**.
6. In the right pane, click **Add**.
7. In the **Add Default Document** dialog box, in the Name field, type `Login.aspx` and then click **OK**.

Configuring a White Label Directory in IIS

If you are using a WebCenter Forms Recognition version that contains a white label (WL) directory inside the

Components\Cedar directory, create a WL virtual directory in IIS. Complete the following steps.

1. In the **Internet Information Services (IIS) Manager** window, in the left pane, open the tree view until **Web Verifier** displays.
2. Right-click **Web Verifier**, then click **Add Virtual Directory**.
3. In the **Add Virtual Directory** dialog box, complete the following substeps.
    1. In the **Alias** field, type `WL` as the name for the virtual directory.
    2. In the **Physical path** field, type or browse to the ***C:\Program Files (x86)\Oracle\WebCenter Forms Recognition*\Components\Cedar\WL** directory and then click **OK**.

Configuring Web Verifier

To configure Web Verifier, complete the following tasks.

1. Modify the instanceName Value When Using Multiple Web Servers.
2. Modify the Database Connection Strings for Web Verifier.
3. To enhance application performance, you can optionally enable HTTP compression. For more information, refer to Microsoft Technet.

Modifying the *instanceName* Value When Using Multiple Web Servers

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

1. From the *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition Web Server* directory, open **Web.config** in a text editor.
2. Search for the following lines.

```
<system.controllers>
<client instanceName="Web Verifier"
remoteObjectRenewalTimeout="180"></client>
```

3. Change `instanceName="Web Verifier"` to `instanceName="Web Verifier [xx]"` with xx being unique across the system.

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

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

Modifying the Database Connection Strings for Web Verifier

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

1. From the *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition Web Server* directory, open the **Web.config** file in a text editor.
2. Search for the `<connectionStrings>` element.
3. For a SQL Server database, to connect using Windows integrated security, modify the following values.
    - Set `Data Source` to the required data source.
    - Set `Initial Catalog` to the SQL Server database catalog.
    - Remove `User ID=<UserID>;Password=<UserPassword>;`.
    - Set `Integrated Security` to `SSPI`.

4. For a SQL Server database, to connect using SQL Server authentication, modify the following values.
    - Set `Data Source` to the data source.
    - Set `Initial Catalog` to the SQL Server database catalog.
    - Set `User ID` to the service account user ID.
    - Set `Password` to the service account password.
5. For an ORACLE database, modify the following values.
    - Set `Data Source` to the data source.
    - Set `User ID` to the service account user ID.
    - Set `Password` to the service account password.
6. Save and close the file.
7. Create a copy of the **Web.config** file and move it to *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition\bin*.
8. Rename the **Web.config** file copy to **Brainware.System.Project.exe.config**.

Configuring Server Security for Web Verifier

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

1. Add the User Context in SQL Server
2. Verify the IIS Identity
3. Set Permissions for WebCenter Forms Recognition Projects
4. Set Permissions for WebCenter Forms Recognition Bin Directory

Adding the User Context in SQL Server

To use Web Verifier, your users need access rights for the SQL Server database with the Web Verifier user context. The default user context is Network Service. You can change the default user context to a service account.

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

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

1. In **Microsoft SQL Server Management Studio**, in the left pane, click **Security > Logins**.
2. Right-click **Logins** and then click **New Login**.
3. In the **Login** dialog box, click **Search**.
4. In the **Select User or Group** dialog box, in the **Enter the object name to select** field, type either `IIS AppPool\WebVerifierPool` or the name of the user context, click **Check Names** and then click **OK**.
5. In the **Login Properties** dialog box, in the left pane, click **User Mapping**.
6. In the upper right pane, in the **Map** column, select the check box for the required database.
7. In the lower right pane, select the following database roles and then click **OK**.
    - db_datareader
    - db_datawriter

- db_runner

Verifying the IIS Identity

To verify that IIS run under the appropriate identity, complete the following steps.

1. In **Internet Information Services (IIS) Manager**, in the **Connections** pane, open the server node and then click **Application Pools**.
2. In the **Application Pools** pane, right-click **WebVerifierPool** and then click **Advanced Settings**.
3. In the **Advanced Settings** dialog box, under **Process Model**, verify that the **Identity** property has the value `ApplicationPoolIdentity` or the name of the service account.

Setting Permissions for WebCenter Forms Recognition Projects

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

To grant permission to the project directory, complete the following steps.

1. In **Windows Explorer**, right-click your projects directory and then click **Properties**.
2. In the **Properties** dialog box, on the **Security** tab, click **Edit**.
3. In the **Permissions** dialog box, click **Add**.
4. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select** field, type either `IIS AppPool\WebVerifierPool` or the name of the user context, click **Check Names** and then click **OK**.

Setting Permissions for WebCenter Forms Recognition Bin Directory

The Web Verifier application pool or the service account, if used, needs access to the Web Verifier installation directory.

To grant permission to the installation directory, complete the following steps.

1. In **Windows Explorer**, right-click the *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition Web Server* directory and then click **Properties**.
2. In the **Properties** dialog box, on the **Security** tab, click **Edit**.
3. In the **Permissions** dialog box, click **Add**.
4. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select** field, type either `IIS AppPool\WebVerifierPool` or the name of the user context, click **Check Names** and then click **OK**.
5. Repeat the previous steps for the *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition\bin\LogRoot* directory.

Removing the Server Header

If your installation is using Internet Information Services 10 or later, you can remove the server header from responses. Complete the following steps.

1. From the *[Installation path]\WebCenter Forms Recognition Web Server* directory, open Web.config in a text editor.
2. Search for the <security> element within the <system.webServer> element.

3. Uncomment the <security> element.
4. Save and close the file.

Redirecting Traffic to HTTPS and Enabling HSTS

After enabling SSL, you can configure Web Verifier to redirect insecure HTTP traffic to HTTPS and to send the HSTS header so that browsers automatically perform this redirection on future requests.

Complete the following steps.

1. Install Microsoft IIS URL Rewrite.
2. From the *[Installation path]\WebCenter Forms Recognition Web Server* directory, open Web.config in a text editor.
3. Search for the <rewrite> element within the <system.webServer> element.
4. Uncomment the <rewrite> element.
5. Save and close the file.

Implementing Single Sign-On Authentication

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

1. Enable the Single Sign-On Authentication.
2. Modify the Web Verifier Session Timeout.

About the Single Sign-On Authentication for Web Verifier

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

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

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

Enabling the Single Sign-On Authentication

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

1. From the *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition Web Server* directory, open **Web.config** in a text editor.
2. Search for the `<httpHeaderBasedSso>` element and complete the following substeps.
    1. Set the `enabled` attribute to `true`.
    2. Set the `loginHeader` attribute to the HTTP header attribute name that the SSO service returns.
    3. Set the `sessionHeader` attribute to the default session-ID header that the SSO service returns.

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

3. Save and close the file.

About the Single Sign-On Session and the Web Verifier Session

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

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

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

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

Modifying the Web Verifier Session Timeout

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

1. From the *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition Web Server* directory, open the **Web.config** file in a text editor.
2. Search for the `<sessionState>` element.
3. Set the `timeout` attribute, in minutes, according to your needs.

Configuring Windows Authentication

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

1. Configure Windows Authentication in IIS 7.5 and Higher .
2. Create a Windows Authentication Version of the Web.config File .
3. Switch Back to Forms Authentication.

About Windows Authentication for Web Verifier

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

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

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

Configuring Windows Authentication in IIS 7.5 and Higher

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

Prerequisite

Add the Windows user to the WebCenter Forms Recognition database.

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

Creating a Windows Authentication Version of the Web.config File

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

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

1. From the *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition Web Server* directory, create a backup of the **Web.config** file for the Forms authentication method.

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

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

Switching Back to Forms Authentication

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

1. Open **Administrative Tools** and then double-click **Internet Information Services (IIS) Manager**.
2. In the **Internet Information Services (IIS) Manager** window, in the left pane, open the tree view until **Web Verifier** displays.
3. Click **WebVerifier** and then, in the middle pane, under **IIS**, double-click **Authentication**.
4. In the **Authentication** pane, disable **Windows Authentication** and enable **Anonymous Authentication** and **Forms Authentication**.
5. Copy the backed up **Web.config** file to the ***C:\Program Files (x86)\Oracle\WebCenter Forms Recognition* Web Server** directory.
6. Restart any open browser sessions.

Implementing OAuth2.0 Authentication

This section describes how you can implement OAuth2.0 Authentication in the Web Verifier Client.
Support

Brainware Web Verifier Client Supports OAuth2.0 Authentication with Authorization flow type. Signature validation of access tokens is supported for RSA signature type. Client Secret setting supports shared secrets.
Refresh Tokens:

If configured to validate token Lifetime, Web Verifier will force a user to log out when their access token expires. Token lifetime can be extended by enabling refresh tokens. When refresh tokens are enabled, Web Verifier will attempt to use the refresh token to obtain a new access token before logging the user out. If the refresh token is expired or the refresh otherwise fails, the user will be logged out as normal. Refresh tokens can be enabled by adding ‘offline_access’ to the scope.

Configuring Web Verifier Client for OAuth2 Authentication

To configure Brainware for OAuth2.0, find the **OAuth2Settings** and **secureSettings** sections in web.config and update the following values.

Settings	Description
OAuth2ClientId*	The client ID provided by your IdP provider.
OAuth2ClientSecret	When using client secret, enter the client secret provided your IdP provider; otherwise, leave blank.
OAuth2Enabled*	Enter True to enable OAuth2 authentication.
OAuth2DiscoveryUrl*	The discovery endpoint of your authorization provider.
OAuth2RequireHttps	Enter True to indicate that you require OAuth2 connections to use https. This is recommended for production environments.
OAuth2RedirectUrl*	The URL of the hosted Web Verifier login page.
OAuth2Scope	Set to ‘offline_access’ to enable refresh tokens; otherwise leave blank.
OAuth2ValidateLifetime	Enter True to indicate that the Web Verifier will validate the lifetime of the returned access token. When the token expires, the user will be logged out. If using refresh tokens Web Verifier will attempt to refresh the users token before logging them out.Enter False to indicate that the token lifetime will be ignored.
OAuth2ClockSkew	Enter the duration in minutes, a user session is still valid after the token expires.This can be used to account for clock differences between the Web Verifier server and the IdP server.
OAuth2PKCEMehtod	Set to S256 to enable PKCE; leave blank to disable PKCE.
OAuth2ValidateSignature	Set to True to validate the token signature; recommended for production environments.

* Indicates mandatory fields

Encrypting the ClientId and ClientSecret for OAuth2 Authentication

Items in the **secureSettings** section can be encrypted using the following command. Replace / webverifier if you are encrypting for another location.

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319/aspnet_regiis -pe
```

```
"secureSettings" -app "/webverifier" -prov
"RsaProtectedConfigurationProvider"
```

By Default, Client Id and Client Secret are included in **secureSettings**, but any of the **OAuth2Settings** settings can be encrypted by moving the value to **SecureSettings**. If the same value appears in **secureSettings** and **OAuth2Settings**, the **OAuth2Settings** value will take precedence. This can be used to temporarily replace encrypted settings for testing purposes.

For more information on encrypting web.config, including how to decrypt values and how to control the encryption key so that it can be reused on other machines, please refer to the ASP.NET documentation from Microsoft.

Configuring Cookies for Web Verifier

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

Prerequisite

Configure SSL on the server.

1. From the *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition Web Server* directory, open the **Web.config** file in a text editor.
2. In the `<configuration>` element, search for the following line.
   `<system.web>`
3. Under `<system.web>`, add the following line: `<httpCookies requireSSL="true" />`
4. To apply forms authentication, search for the following line.
   `<forms loginUrl="Login.aspx" defaultUrl="BatchView.aspx" />`
5. Add the `requireSSL` attribute.
   ```
   <forms loginUrl="Login.aspx" defaultUrl="BatchView.aspx"
   requireSSL="true" />
   ```
6. Save and close the file.
7. Optional. To prevent other applications from accessing Web Verifier cookies, deploy Web Verifier in one of the following ways.
   - As the root level website.
   - As the only web application under a website in IIS.

About Web Verifier Performance

Consider the following information to improve Web Verifier performance.

Image Conversion

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

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

For more information, see "About display formats" and "Set display format" in the *Oracle WebCenter Forms Recognition Runtime Server User's Guide*.

Delayed Validation

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

For more information, see "About delayed validation" and "Modify the validation rules for a field" in the *Oracle WebCenter Forms Recognition Designer User's Guide*.

Using Traditional Chinese

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

To change to Traditional Chinese, complete the following steps.

1. From the *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition Web Server\bin\Resources* directory, create a backup copy of the **zho** directory.
2. Copy all files from the *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition Web Server\bin\Resources\cmn* directory to the *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition Web Server\bin\Resources\zho* directory.
3. From the *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition Web Server* directory, open the **Web.config** file in a text editor.
4. Search for the following line.

   ```
   <add key="LanguageDisplayName_ZHO" value="中文简体" />
   ```

5. Modify the line as follows.

   ```
   <add key="LanguageDisplayName_CMN" value="中文繁體" />
   ```

6. Save and close the file.
7. Restart any open browser sessions.

Accessing Web Verifier

To access Web Verifier, in your browser, type `http://localhost/WebVerifier/login.aspx`.

Additional Columns in Verifier or Web Verifier

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

You can add the following columns to batch view.

- ExternalGroupId
- ExternalBatchId
- TransactionId
- TransactionType

Displaying and Naming Additional Verifier Columns: Oracle

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

- External group ID

  ```
  exec sp_SetGlobalApplicationSetting
  ('SysAppBatchColumnExternalGroupId', '[Column header name, for
  example User Group]', 1)
  ```

- External batch ID

```
exec sp_SetGlobalApplicationSetting
('SysAppBatchColumnExternalBatchId', '[Column header name, for
example Batch Group]', 1)
```

- Transaction ID

```
exec sp_SetGlobalApplicationSetting
('SysAppBatchColumnTransactionId', '[Column header name, for example
Transaction]', 1)
```

- Transaction type

```
exec sp_SetGlobalApplicationSetting
('SysAppBatchColumnTransactionType', '[Column header name, for
example Transaction Type], 1)
```

Displaying and Naming Additional Verifier Columns: SQL Server

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

- External group ID

```
exec sp_SetGlobalApplicationSetting
'SysAppBatchColumnExternalGroupId', '[Column header name, for example
User Group]', True
```

- External batch ID

```
exec sp_SetGlobalApplicationSetting
'SysAppBatchColumnExternalBatchId', '[Column header name, for example
Batch Group]', True
```

- Transaction ID

```
exec sp_SetGlobalApplicationSetting 'SysAppBatchColumnTransactionId',
'[Column header name, for example Transaction]', True
```

- Transaction type

```
exec sp_SetGlobalApplicationSetting
'SysAppBatchColumnTransactionType', '[Column header name, for example
Transaction Type]', True
```

Display Additional Web Verifier Columns

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

For more information on the event, see “PostImportBatch” in the *Oracle WebCenter Forms Recognition Scripting User’s Guide*. To display additional columns in Web Verifier, complete the following steps.

1. From the *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition Web Server* directory, open the **Web.config** file in a text editor.
2. Search for the following elements and set the `visible` attribute to `true` for the columns you want to display.
    - externalGroupIdColumn

- externalBatchNameColumn
- transactionIdColumn
- transactionTypeColumn

3. Save and close the file.
4. Restart any open browser sessions.

Change the Web Verifier Column Names

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

1. From the *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition Web Server\bin\resources\[language code]* directory, open the **Brainware.Verifier.WebClient.resx** file in a text editor.
2. Search for the following `<data name=>` elements.
   - TEXT_EXTERNALBATCH_NAME
   - TEXT_EXTERNAL_GROUP_ID
   - TEXT_TRANSACTION_ID
   - TEXT_TRANSACTION_TYPE
3. Set the `<value>` attributes with the names you want to display.
4. Save and close the file.
5. Restart any open browser sessions.

Configure Global Application Settings

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

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

About Workflow History Reporting

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

Configure Workflow History Reporting: Oracle

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

- For documents

```
exec sp_SetGlobalApplicationSetting
('SysAppHistoryReportingActivatedForDocument', 'True', 1)
```

- For fields

```
exec sp_SetGlobalApplicationSetting
('SysAppHistoryReportingActivatedForField', 'True', 1)
```

- For fields and table cells

```
exec sp_SetGlobalApplicationSetting
('SysAppHistoryReportingActivatedForTableCell', 'True', 1)
```

- For classification

```
exec sp_SetGlobalApplicationSetting
('SysAppHistoryReportingActivatedForClass', 'True', 1)
```

- For OCR and document separation

```
exec sp_SetGlobalApplicationSetting
('SysAppHistoryReportingActivatedForPage', 'True', 1)
```

- For learning

```
exec sp_SetGlobalApplicationSetting
('SysAppHistoryReportingActivatedForLearning', 'True', 1)
```

Configure Workflow History Reporting: SQL Server

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

- For documents

```
exec sp_SetGlobalApplicationSetting
'SysAppHistoryReportingActivatedForDocument', 'True', True
```

- For fields

```
exec sp_SetGlobalApplicationSetting
'SysAppHistoryReportingActivatedForField', 'True', True
```

- For fields and table cells

```
exec sp_SetGlobalApplicationSetting
'SysAppHistoryReportingActivatedForTableCell', 'True', True
```

- For classification

```
exec sp_SetGlobalApplicationSetting
'SysAppHistoryReportingActivatedForClass', 'True', True
```

- For OCR and document separation

```
exec sp_SetGlobalApplicationSetting
'SysAppHistoryReportingActivatedForPage', 'True', True
```

- For learning

```
exec sp_SetGlobalApplicationSetting
'SysAppHistoryReportingActivatedForLearning', 'True', True
```

About Disabling Batch Deletion in Runtime Server and Designer

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

Disable Batch Deletion: Oracle

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

- For Designer

```
exec sp_SetGlobalApplicationSetting
('SysAppBatchDeletionDisabledInDesigner', 'True', 1)
```

- For Runtime Server

```
exec sp_SetGlobalApplicationSetting
('SysAppBatchDeletionDisabledInRTS', 'True', 1)
```

Disable Batch Deletion: SQL Server

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

- For Designer

```
exec sp_SetGlobalApplicationSetting
'SysAppBatchDeletionDisabledInDesigner', 'True', True
```

- For Runtime Server

```
exec sp_SetGlobalApplicationSetting
'SysAppBatchDeletionDisabledInRTS', 'True', True
```

About Modifying the URL Expiration Time for Web Verifier

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

Modify the URL Expiration Time: Oracle

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

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

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

Modify the URL Expiration Time: SQL Server

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

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

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

Configure WebCenter Forms Recognition Security

To configure WebCenter Forms Recognition security, review the following topics and complete the tasks as necessary.

1. File System Security
2. Recommended Accounts and Groups
3. Configure Access to Project Data
4. About the Service Account on a Domain Network
5. About the Service Account for System Monitoring
6. About INI File Encryption
7. Encrypt a Password for a Database Connection String
8. About User Password Encryption
9. Change the Hashing Algorithm

File System Security

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

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

The following table lists the available file permissions.

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

Full Control	Allows the user or group to change the files permissions and to take ownership of the file. Includes all other file permissions.

The following table lists the available directory permissions.

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

Recommended Accounts and Groups

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

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

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

The following table lists the groups and accounts recommended for each WebCenter Forms Recognition implementation.

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

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

Group / Account Name	Permission Type: Shared	Permission Type: NTFS	Directory/Objects Assigned On
Oracle WebCenter Forms Recognition	Full Control	Full Control	C:\Program Files*[company]*\ *[ProjectName]*
Oracle WebCenter Forms Recognition Users	Change	Modify	C:\Program Files*[company]*\ *[ProjectName]*

Configure Access to Project Data

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

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

To configure the access rights to the WebCenter Forms Recognition project directory, complete the following steps.

1. In **Windows Explorer**, right-click your projects directory and then click **Properties**.

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

About the Service Account on a Domain Network

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

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

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

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

About the Service Account for System Monitoring

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

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

About INI File Encryption

WebCenter Forms Recognition allows password encryption in INI files for database strings by using RSA encryption. RSA encryption requires a public and a private key.

For more information, see “Password encryption for database connection strings” in the *Oracle WebCenter Forms Recognition Scripting User’s Guide*.

Encrypt a Password for a Database Connection String

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

1. In the ***C:\Program Files (x86)\Oracle\WebCenter Forms Recognition*\bin** directory, create a new batch file and give it a meaningful name, such as **CreateEncryptedPassword.bat**.
2. Copy one of the following options to the batch file, replacing `MyPassword` with the password you want to encrypt.

Notes:

- The maximum character length for a password to encrypt using **RSA-1024** is 30.
- The maximum character length for a password to encrypt using **RSA-3072** is 280.
  - To encrypt the password using the internal RSA-3072 key, use the following option.

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

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

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

3. Save and close the file.
4. In **Windows Explorer**, double-click the batch file.
5. From ***C:\Program Files (x86)\Oracle\WebCenter Forms Recognition*\bin**, open **EncryptedPassword.txt** in a text editor and copy the encrypted password to the clipboard.
6. Open the required configuration file in a text editor.
7. Search for the `<connectionStrings>` element.
8. In the `<add name>` element, set password as an asterisk.

   Example

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

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

   Example

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

10. Save and close the file.

About User Password Encryption

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

WebCenter Forms Recognition stores only the hash values in the database to authenticate the user. The following hashing algorithms are available.

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

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

Change the Hashing Algorithm

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

Note: For more information about the possible hashing algorithms, see About User Password Encryption.

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

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

Example

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

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

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

Example

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

Configure WebCenter Forms Recognition Runtime Components

To configure WebCenter Forms Recognition runtime components, review the following topics and complete the tasks as necessary.

1. About RTS Remote Administration MMC
2. Configure the Runtime Service Manager Service
3. Configure the RTS Remote Administration MMC Snap-In

About RTS Remote Administration MMC

Before you can use WebCenter Forms Recognition, you must configure the Runtime Service Manager (RTS).

The RTS Remote Administration Microsoft Management Console (MMC) snap-in enables you to start and

stop multiple Runtime Servers remotely from a single workstation on the network. The WebCenter Forms Recognition installation creates a default console, called Runtime Server Administration that you can use to configure the RTS Remote Administration MMC snap-in.

Configure the Runtime Service Manager Service

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

Prerequisite

Verify that the WebCenter Forms Recognition RTSsvc domain user exists.

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

Configure the RTS Remote Administration MMC Snap-In

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

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

   Note: The default port number is 50607.
3. Verify one of the following prerequisites.
   - The administration workstation resides on the same LAN segment as the RTS services.
   - In a sub-netted network, a name resolution system is in place to allow clients on one subnet to locate resources on another subnet.
4. Start **Oracle WebCenter Forms Recognition Runtime Service**.
5. In the **Runtime Server Administration** window, in the left pane, right-click **Runtime Server Administration** and click **New RTS Group**.
6. In the **New Group** dialog box, type a group name and click **OK**.
7. Open the **Runtime Server Administration** node, right-click the newly created group, and then click **New Machine**.
8. In the **Group Management** dialog box, complete the following substeps.
   1. From the **Domains** list, select the required domain and then click **Search**.
   2. In the left pane, select the required machines, click **>>** and then click **OK**.

9. In the **Runtime Server Administration** window, complete the following substeps.
    1. In the left pane, right-click the newly added machine and then click **License**.
    2. In the **License Information** dialog box, verify or change the license path and then click **OK**.
    3. In the left pane, right-click the newly added machine and then click **New > RTS Instance**.
    4. In the **New RTS Instance** dialog box, type an instance name and then click **OK**.

About the Desktop Heap Size

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

Modify the Desktop Heap Size

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

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

   Note: For information about the appropriate heap size, see Ideal Desktop Heap Size.
5. Reboot the server.

Ideal Desktop Heap Size

Determine the ideal desktop heap size with the following table.

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

About Logging

WebCenter Forms Recognition creates new log files daily in the log directory.

You can configure the logging level, location, and retention time for your application log files.

The default log directory is *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition\bin\LogRoot\Log*. **Notes**

- Application users must have permission to write to the log directory.
- When the database or the specified `LogOutDir` is inaccessible or no `LogOutDir` is defined, logging automatically redirects to the default log directory.
- If the default log directory is inaccessible, the application redefines the default log directory as the first writable location listed.
    1. `%TMP%\DstLog`
    2. `%TEMP%\DstLog`
    3. `%USERPROFILE%\DstLog`
    4. `%WINDIR%\Temp\DstLog`
- If an application is unable to write to the log file, a warning appears in the system logs.

Log Files

Each application log file contains the following information.

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

The following log files are available in the log directory.

Application log file	Description
V_*.log	Verifier messages including custom script errors.
VA_*.log	Advanced Verifier messages.
VL*.log	Local Verifier messages.
H_*.log	Runtime Server Host (DstHost) messages for a single RTS instance. **Note:** The standard Runtime Server log files include system level resource information and, in case of a system failure, special error logs.
L_*.log	Learnset Manager messages, such as when the user triggers document learning, or backs up the learnset.
D_*.log	Designer messages including script errors.
U_*.log	Web Verifier and external application messages.
S_*.log	Service Manager (DstMgr) messages, such as start and end of service, restart, or failures.
M_*.log	System Monitoring (DstEvent) messages. Holds all system messages and can log error messages across all server machines and hosts.

Component log file	Description
I_*.log	Component log files for all applications.

Error log file	Description
C_*.log	In the event of system or application failures, WebCenter Forms Recognition creates an additional error log file named **C_ <Process ID>_yyyymmdd.log**.

Logging Levels

The following application logging levels are available.

Logging level	Description
0	No logging.
1	Log only errors.
2	Log errors and warnings.
3	Log errors, warnings, and information.

Configure the Logging Level

To configure the logging level, complete the following step in your WebCenter Forms Recognition database.

Note: The specified `LogTraceLevel` does not apply to Runtime Server instances. For more information about setting the logging level for an RTS instance, see "Define logging levels" in the *Oracle WebCenter Forms Recognition Runtime Server User's Guide*.

- Update the following command with the desired logging level and then execute the command.
  - **For Oracle**

    ```
    exec sp_SetGlobalApplicationSetting ('LogTraceLevel', '[logging level]', 1)
    ```

    Example

    ```
    exec sp_SetGlobalApplicationSetting ('LogTraceLevel', '1', 1)
    ```
  - **For SQL Server**

    ```
    exec sp_SetGlobalApplicationSetting 'LogTraceLevel', '[logging level]', True
    ```

    Example

    ```
    exec sp_SetGlobalApplicationSetting 'LogTraceLevel', '1', True
    ```

Configure the Location of the Application Log Files

To configure the location of the application log files, complete the following step in your WebCenter Forms Recognition database.

Notes

- Update the following command with the desired log file directory and then execute the command. To revert to the default setting, set LogOutDirto an empty string.
  - **For Oracle**

    ```
    exec sp_SetGlobalApplicationSetting ('LogOutDir', '[log file location]', 1)
    ```

Example

```
exec sp_SetGlobalApplicationSetting ('LogOutDir', 'C:\Program
Files (x86)\Brainware\Log Files', 1)
```

- **For SQL Server**

```
exec sp_SetGlobalApplicationSetting 'LogOutDir', '[log file
directory]', True
```

Example

```
exec sp_SetGlobalApplicationSetting 'LogOutDir', 'C:\Program
Files (x86)\Brainware\Log Files', True
```

Configure the Retention Time of Application and Error Log Files

To configure the retention time of application and error log files, complete the following step in your WebCenter Forms Recognition database.

Notes

- The specified `LogTotalDaysToKeepFiles` does not apply to Runtime Server instances. For more information about deleting log files for Runtime Server, see "Delete log files" in the *Oracle WebCenter Forms Recognition Runtime Server User's Guide*.
- Each WebCenter Forms Recognition application deletes its own file.
- Cleaning is done once per day.
- To determine whether a file is to be deleted, the cleaning process uses the creation time of the file, which is part of the file name.
- If this setting is not configured, no files are deleted.
- To revert to the default setting, set `LogTotalDaysToKeepFiles` to 0.

- Update the following command with the desired number of days and then execute the command.
  - **For Oracle**

```
exec sp_SetGlobalApplicationSetting ('LogTotalDaysToKeepFiles',
'[Number of Days]', 1)
```

Example

```
exec sp_SetGlobalApplicationSetting ('LogTotalDaysToKeepFiles',
'5', 1)
```

  - **For SQL Server**

```
exec sp_SetGlobalApplicationSetting 'LogTotalDaysToKeepFiles',
'[Number of Days]', True
```

Example

```
exec sp_SetGlobalApplicationSetting 'LogTotalDaysToKeepFiles',
'5', True
```

OCR Engine Languages

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

Supported OCR languages		
Bulgarian	Italian	Romanian
Chinese Simplified *	Japanese *	Russian *
Chinese Simplified + English *	Japanese + English *	Slovak
Czech	Korean *	Slovenian
Danish	Korean + English * **Note:** Only with FineReader 11	Spanish
Digits	KoreanHangul	Swedish
Dutch	Latvian	Thai *
English	Lithuanian	Turkish
Estonian	Norwegian	Ukrainian *
Finnish	NorwegianBokmal	Vietnamese *
French	NorwegianNynorsk	CMC7
German	Polish	E13B
Greek *	Portuguese Brazilian	
Hungarian	Portuguese Standard	

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

Available OCR Engines

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

Cleqs Barcode Engine

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

FineReader10 OCR Engine

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

FineReader11 OCR Engine

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

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

QualitySoft Barcode Engine

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

About Automated Update

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

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

Note: This feature is not available for all versions of WebCenter Forms Recognition. For details, refer to the appropriate *Oracle WebCenter Forms Recognition Release Notes*.

Modify the Batch File

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

Prerequisite

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

1. From the ***C:\Program Files (x86)\Oracle\WebCenter Forms Recognition*Oracle WebCenter Forms Recognition\bin** directory, open the **AutoInstall.bat** file in a text editor.
2. Search for the following line.

```
SET SHAREDNETFOLDER
=\\YourNetworkInstallServerName\YourInstallShareName
```

3. Modify `\\YourNetworkInstallServerName\YourInstallShareName` to your shared network directory.
4. Save and close the file.

Modify the Application Shortcuts for Verifier and Designer

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

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

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

Automate Runtime Server Updates

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

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

1. To stop the RTS service, in *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition\bin* directory, run **Stop RTS running as NT Service.bat**.

   Note: Verify that RTS is not actively processing documents before you stop the service.
2. In *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition\bin* directory, run **AutoInstall.bat**
3. To start the RTS service, in *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition\bin* run **Start RTS running as NT Service.bat**.

About Port Configuration

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

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

Configure a Different Port for Runtime Server

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

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

File Permission Matrix

The following tables list the various file permissions used within WebCenter Forms Recognition.

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

The following table lists the required NTFS permissions.

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

Common Folder	Administrators Developers Learnset Manager Advanced Verifiers	x	x	x	x	x	x	-
	Standard Verifiers RTS Service User	-	-	-	-	-	-	x
Global Project	Administrators	x	x	x	x	x	x	-
	Developers Learnset Manager RTS Service User							
	Advanced Verifiers Standard Verifiers	-	-	x	x	x	-	-
Local Project	Administrators Developers	x	x	x	x	x	x	-
	Learnset Manager RTS Service User Standard Verifiers	-	-	-	-	-	-	x
	Advanced Verifiers	x	x	x	x	x	x	-
Local Learnset	Administrators Developers	x	x	x	x	x	x	-

	Learnset Manager RTS Service User Standard Verifiers	-	-	-	-	-	-	x
	Advanced Verifiers	x	x	x	x	x	x	-
Global Learnset	Administrators Developers Learnset Manager RTS Service User	x	x	x	x	x	x	-
	Advanced Verifiers Standard Verifiers	-	-	x	x	x	x	-
ASE Pool	Administrators Developers RTS Service User	x	x	x	x	x	x	-
	Learnset Manager Advanced Verifiers Standard Verifiers	-	-	x	x	x	-	-
ASSA CSV File	Administrators Developers RTS Service User	x	x	x	x	x	x	-
	Learnset Manager	-	-	-	-	-	-	x

	Advanced Verifiers Standard Verifiers							

Web.config Options and Associated Resource File Parameters

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

For more information about the event options, refer to the *Oracle WebCenter Forms Recognition Scripting User's Guide*.

Option	Description
ADOCommandExecutionTimeOut	Defines the timeout, in seconds, for executing stored procedures in the database. Possible values Any valid integer
AllowAccessToDocumentsToIndexOnly	For more information, see About Navigation to Documents for Indexing. Possible values True: Enable navigation to indexable documents only False: Enable navigation to out-of-workflow documents. The default value is False.
BatchViewPageSize	Defines the number of batches per page that display in the Web Verifier batch list. Possible values Any valid integer The default value is 20.
client script mode	Defines the parameter to compress the script file that is sent to the browser from the server. Possible values Test: Testing or debugging of Web Verifier client side script on browser. Release: Used in production environment to minimize the file size of the client side script that assists in improving page loading performance.
cacheScripts in the <clientScript> element	Defines the Ext. script caching behavior. Possible values True: Used in *Ext.Loader.setConfig* parameter to enable caching. False: Used in *Ext.Loader.setConfig* parameter to disable caching.

ClientSideDocumentCacheSize	Defines the number of pages to cache in the current document. Possible values Any valid integer The default value is 0.
connectionStrings	The database connection string.
convertedScriptCaching	Add this configuration in the <*project.controller*>\<*project*> node along with *mpdDistance* and *mpdThreshold*. Possible values True: Enables script conversion caching to reduce initial project loading time. False: Disables script conversion caching to slow down initial project loading time. The default value is True. **Note:** You also need to set this value to "true" in the *Brainware.system.project.exe.config* setting to enable script conversion caching.
DialogWidth	Defines the default width, in pixels, of message boxes in Web Verifier. Possible values Any valid integer The default value is 400.
document cacheSize in the <document.controller> element	Specifies the number of workdoc objects to pre-load. This accelerates opening documents within the batch. You cannot disable pre-loading, but minimize the number of pre-loaded documents to 2, that means one current and one pre-loaded. Possible values Any valid integer The default value is 5.

document maxPagesToPreload in the <document.controller> element	Defines the number of document pages to pre-load. First and last pages always pre-load, and remaining cache slots fill with pages that have field candidates starting from the lower index. The following actions take place on page images when a document loads in the background. - Pre-load the page - Convert the page to PNG - Save the page to the database Possible values Any valid integer The default value is 5.
DocumentViewPageSize	Defines the number of folders for Verifier to display in the document tree view when using Show Selected Batch mode. Additional batches display in subsequent navigation panels. Possible values Any valid integer The default value is 10.
EnableProfiler	Whether to enable the Web Verifier profiler. The profiler collects and records the duration of user actions, such as commands and their internal sub-operations. Possible values True / False The default value is False.
externalGroupIdColumn	Whether the external group ID column displays in Web Verifier. Possible values True / False The default value is False.
externalBatchNameColumn	Whether the external batch name column displays in Web Verifier. Possible values True / False The default value is False.

focusChanged	Whether to enables the focusChanged event for fields in the verification view. The event triggers when the user presses the Enter key in a field. The setting has no effect on the FocusChanged event if the <mouseClicked> attribute is set to true. Possible values True / False The default value is True.
HelpLink	Links to Web Verifier Help.
httpHeaderBasedSso	Controls the single sign-on (SSO) user authentication mode.
login header in the <httpHeaderBasedSso> element	Corresponds to the HTTP header attribute name that contains the SSO authenticated user name. The SSO service uses this attribute to send the user name.
Enabled in the <httpHeaderBasedSso> element	Whether to use the Web Verifier SSO feature. Possible values True / False The default value is False.
sessionHeader in the <httpHeaderBasedSso> element	The provider-dependent name of the HTTP header that the SSO service uses to send the user session ID.
inactiveUserTimeout	Unchangeable attribute. **Note:** This attribute does not control the user session timeout. The `<sessionState Timeout>` parameter controls the user session timeout.
inspectionTimeOut	Unchangeable attribute. **Note:** This attribute does not control the user session timeout. The `<sessionState Timeout>` parameter controls the user session timeout.
instanceName	The instanceName value displays in the batch list column “Last Module". **Note:** The instanceName value must be unique across all installed Web Verifier servers accessing the same database.

itemCopied	Whether to enable the itemCopied event. Possible values True / False The default value is False.
LanguageDisplayName*_[ISO]*	Customizes the language display names in the language selection menu. Replace *[ISO]* by the three letter directory name in *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition* Web Server\Bin\Resources. Example for Simplified Chinese `<add key="LanguageDisplayName_ZHO" value="中文简体"/>`
level	Defines the tracing level. Possible values DEBUG: Trace all information and error messages. ERROR: Trace error messages only.
loadInSeparateProcess	Unchangeable attribute.
mouseClicked	Whether to enable the mouseClicked event on fields and tables in the verification view in indexing mode. Possible values True / False The default value is False.
pathToProjectExe	The location of the Designer program Brainware.System.Project.exe. In typical installations, it is not required to modify this value. Possible values A valid non-UNC path ending with a “\”. The default value is *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition*\Bin\.
ReinitScriptEngineAfterScriptErrors	Whether to recover the script engine after a script error in Web Verifier. Possible values True / False The default value is False.

remoteObjectRenewalTimeout	Defines, in seconds, the time to lapse before renewing remote object references. The lower the number the faster unused objects free memory. Increase this value in the event of errors caused by long-running commands, such as field validation. Possible values Any valid integer more than or equal to 30. The default value is 30.
SavePageImageToDatabase	Specifies if page images extracted from document file blobs needs to be saved back to the database. Possible values True / False
timeout in the <sessionState> element	Defines, in minutes, the amount of time a user can be inactive before the session ends. Specify a value less than that of the SSO session. For details, see the product documentation of your SSO provider. Possible values Any valid integer. The default value is 20.
ShowExtendedErrorMessages	Whether to enable stack trace information for Web Verifier error messages. Error messages display in the trace log file. Possible values True / False The default value is False.

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

SYSTEM_LONG_DATE_FORMAT	The XML key available in each Brainware.Verifier.WebClient.resx file located in *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition* Web Server\Bin\Resources*[language code]*.
	The key contains the date pattern for the last access date column in the batch list for the respective language.
	To use the default system date pattern, leave the value element empty. The time format uses a 24-hour clock.
	For Traditional and Simplified Chinese, use the date format in the following example without any Chinese characters.
	Example for Chinese
	`<data name="SYSTEM_LONG_DATE_FORMAT"`
	`xml:space="preserve">`
	`<value>yyyy-MM-dd, hh:mm:ss</value>`
	`</data>`

transactionIdColumn	Whether the transaction ID batch column displays in Web Verifier. Possible values True / False The default value is False.
transactionTypeColumn	Whether the transaction type batch column displays in Web Verifier. Possible values True / False The default value is False.
tabPressed	Whether to enable the tabPressed event on fields and tables in the verification view in indexing mode. Possible values True / False The default value is False.
tableCellSelected	Whether to enable the tableCellSelected event. Possible values True / False The default value is False.
usePath	Possible values True: Use the pathToProjectExe parameter. False: Use the current directory instead of the pathToProjectExe parameter. The default value is True.

waitLoadTimeOut	Defines the timeout for the initial loading of the project.exe.

About Navigation to Documents for Indexing

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

Example

Workflow settings: 550 -> 700

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

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

Enable Navigation to Indexable Documents

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

1. From the *C:\Program Files (x86)\Oracle\WebCenter Forms Recognition Web Server* directory, open **Web.config** in a text editor.
2. Search for `<appSettings>`.
3. Add the following line.
   ```
   <add key="AllowAccessToDocumentsToIndexOnly" value="true" />
   ```
4. Save and close the file.
5. In Web Verifier, activate the **Disable navigation to valid documents** option.

Registry Options

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

Key	Description
ErrorTraceDir	Provides the possibility to change the component log file location. The setting does not affect the core product log file location.
HideBatchReleaseDialog	Allows you to enable or disable the Batch Release dialog box within Verifier, where the workflow does not require prompting users to the next task. The registry value determines the next action carried out by users. The default action of the Batch Release dialog box is to verify the next invalid batch. When WebCenter Forms Recognition suppresses the dialog, this value is maintained. To change to a different action, use the Batch Release dialog box once, then change the setting accordingly and click OK. The default value is 0.

ErrorTrace - All	Defines the trace level. The default value is 1.
MaximumDiskspaceUsageMB	Defines the disk space in MB allocated for component level logs.
TotalDaysToKeepFiles	Defines the number of days the WebCenter Forms Recognition server retains the component log files.

Create the Registry Key *ErrorTraceDir*

To create the registry key, complete the following steps.

1. In **Windows Registry Editor**, complete one of the following substeps.
   - For a 32-bit machine, navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\ErrorTrace*.
   - For a 64-bit machine, navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Oracle\ErrorTrace*.
2. In the right pane, right-click and then click **New > String Value**.
3. In the **Name** field, type `ErrorTraceDir` and then click **OK**.
4. Right-click the **ErrorTraceDir** key and then click **Modify**.
5. In the **Edit String** dialog box, in the **Value data** field, type the path and then click **OK**.

   Note: The path must exist and the service account / user needs write permission to the path.
6. Restart all WebCenter Forms Recognition applications and services.

Create the Registry Key *HideBatchReleaseDialog*

To create the registry key, complete the following steps.

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

Modify the Registry Key *ErrorTrace - All*

To modify the value, complete the following steps.

1. In **Windows Registry Editor**, complete one of the following substeps.
   - For a 32-bit machine, navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\ErrorTrace*.
   - For a 64-bit machine, navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Oracle\ErrorTrace*.
2. In the right pane, right-click **All** and then click **Modify**.
3. In the **Edit DWORD (32-bit) Value** dialog box, in the **Value data** field, complete one of the following steps and then click **OK**.
   - To turn off logging, type `0`.
   - To log only errors, type `1`.
   - To log errors and warnings, type `2`.
   - To log errors, warnings, and information, type `3`.

Create the Registry Key MaximumDiskspaceUsageMB

To create the registry key, complete the following steps.

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

Create the Registry Key *TotalDaysToKeepFiles*

To create the registry key, complete the following steps.

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

- To deactivate the option, type zero: `0`.
- Type the number of days.

Uninstall WebCenter Forms Recognition.

Perform the following steps to uninstall WebCenter Forms Recognition from the system:

1. Stop the following windows services:
   - ABBY SDK 10 Licensing Service.
   - ABBY SDK 11 Licensing Service.
   - WebCenter Forms Recognition Core Service.
   - WebCenter Forms Recognition Runtime Service Manager.
   - WebCenter Forms Recognition System Monitoring.
2. Close all the WebCenter Forms Recognition applications such as Designer, Verifier, and so on.
3. Stop the Internet Information Services (IIS) Server.
4. Run setup.exe as an administrator from the Installation Media directory.
   - Click **Remove (Remove all installed features).**
   - Click **Yes** when asked to completely remove the application and all of its features.
   - Click **Yes, I want to restart my computer now**.
   - Click **Finish.**
5. After restart, delete the *Program Files (x86)\Oracle\WebCenter Forms Recognition* directory.

Troubleshooting

Windows could not start the WebCenter Forms Recognition Core Service on Local Computer Error. 0xffffffff: 0xffffffff

This error message is seen during start of WebCenter Forms Recognition Core Service in Windows Services. Review the recent CS Log files. It generally happens when WFR Core Service could not connect to database for multiple reasons:

1. Verify using the UDL Method if the connectivity to database is fine. You can also use the following command to test the 32-bit OLEDB connectivity.

   ```
   C:\Windows\syswow64\rundll32.exe "C:\Program Files (x86)\Common Files\System\Ole DB\oledb32.dll",OpenDSLFile C:\Test.udl
   ```

2. Make sure the password for the database account configured in WFR has not been expired.
3. For Oracle database, make sure the 32-bit client libraries are installed for the same version as the database server version.
4. Review the connection string in config files located at C:\Program Files (x86)\Oracle\WebCenter Forms Recognition\Bin\bin\.

WebCenter Forms Recognition Services Won’t Start Automatically

If you observe that some or all of the WebCenter Forms Recognition Services would not start automatically, then repeat the following steps for each of the following services:

- WebCenter Forms Recognition Core Service. (Required, must be Up and Running automatically)

- WebCenter Forms Recognition Runtime Service Manager (Optional).
- WebCenter Forms Recognition System Monitoring (Optional).

1. Open Windows **Services**.
2. Locate the corresponding WebCenter Forms Recognition service.
3. Right-click the selected service and click **Properties**.
4. Change the **Startup Type** to **Automatic (Delayed Start)**.

   Note: The service will be up and running in around 2 mins after (re)starting the Windows Operating System.
5. Click **OK** to save the changes.
6. [Optional] Manually start the services which are required for current login/session.