Oracle® WebCenter Forms Recognition

Installation Guide

11g Release 1 (11.1.1.8.0)

E50183-01

November 2013

WebCenter Forms Recognition

11g Release 1 (11.1.1.8.0)

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 software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency- specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software 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 which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

This software and documentation may provide access to or information on 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. 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.

Contents

1 About WebCenter Forms Recognition ... 6
2 System Requirements ... 7
2.1 Operating Systems ... 7
2.2 WebCenter Forms Recognition Database ... 7
2.3 IIS 7
2.4 Scripting Components ... 7
3 Hardware Requirements ... 8
3.1 Network Infrastructure ... 8
3.2 Hardware and Software Factors ... 8
3.3 Hardware Estimate – 500 PPD ... 9
3.3.1. Introduction – AP Packaged Project ... 9
3.3.2. Hardware Estimate – File System (Excl. Web Verifier & Database) ... 9
3.3.3. Hardware Estimate – Database (Excl. Web Verifier) ... 10
3.3.4. Hardware Estimate – Entire Application Suite ... 10
3.3.5. Hardware Estimate – Typical Development Environment ... 11
3.4 Hardware Estimate – 4000 PPD ... 11
3.4.1. Introduction – AP Packaged Project ... 11
3.4.2. Hardware Estimate – File System (Excl. Web Verifier & Database) ... 12
3.4.3. Hardware Estimate – Database (Excl. Web Verifier) ... 12
3.4.4. Hardware Estimate – Entire Application Suite ... 12
3.4.5. Web Verifier Server Hardware Sizing – Additional Information ... 13
3.5 Infrastructure Constraints ... 14
3.5.1. OCR Performance ... 14
3.5.2. Firewalls ... 14
3.6 RTS Remote Administration MMC ... 15
4 Pre-Installation of WebCenter Forms Recognition ... 16
4.1 Before Installing WebCenter Forms Recognition ... 16
4.1.1. Installation Checklist ... 16
4.2 Backward Compatibility ... 17
4.3 WebCenter Forms Recognition Database Checklist ... 17
4.3.1. WebCenter Forms Recognition Database ... 17
4.3.2. WebCenter Forms Recognition Oracle Database Checklist ... 17
4.3.3. WebCenter Forms Recognition SQL Server Checklist ... 18
4.4 Upgrading from Previous Versions ... 18
4.4.1. Upgrading from Oracle Forms Recognition Version 10.1.3.5.0 ... 18
4.5 Removing Oracle Forms Recognition Version 10.1.3.5.0 ... 18
5 Installing WebCenter Forms Recognition ... 20
5.1 Software Installation ... 20
5.1.1. Selecting Custom Installation ... 20
5.1.2. WebCenter Forms Recognition Database Setup ... 22
5.1.3. Completing the WebCenter Forms Recognition Setup ... 23
5.2 Manually Creating Database Objects (post install) ... 24
5.3 Configuring the WebCenter Forms Recognition Database (Post Install) ... 26
5.4 Cedar Workflow History Wrapper Component ... 26
5.5 Installing WebCenter Forms Recognition in a Workgroup Configuration ... 27
5.6 Installing WebCenter Forms Recognition in Standalone Mode ... 28
5.7 Checking the Installation ... 28
5.8 Migrating Existing Project Files to Version 11.1.1.8.0 ... 29
5.9 Removing WebCenter Forms Recognition Version 11.1.1.8.0 ... 29
5.10 Repairing a WebCenter Forms Recognition Installation ... 29

5.11 Adding or Removing Version 11.1.1.8.0 Components 30
5.12 Installing WebCenter Forms Recognition Service Packs / Service Updates 30
5.12.1. Current patch level 31
5.13 Password Encryption for Database Connection Strings in Core Config Files 31
5.14 INI File Encryption 32
5.14.1. INI File Encryption for Project Developer 33
5.14.2. INI File Encryption for Integrator 34
5.15 Silent Installations 34
5.15.1. Silent Install.ini 34
5.15.2. Automated Distribution of Service Updates on Verifier Workstations 37
5.16 Preparing Internet Information Server (post install) 37
5.16.1. Configuring IIS 6.0 38
5.16.2. Configuring IIS 7.0 41
5.16.3. Windows 2008 and above 44
5.16.4. Windows 2008 64bit R2 44
5.16.5. Enabling HTTP Compression on your Windows 2003 Server 44
5.16.6. IIS 6.0 Metabase Configuration - MetaBase.xml 45
6 Configuring Application 47
6.1 Configuring Application 47
6.1.1. Configuring WebCenter Forms Recognition Database connection string 47
6.1.2. Setting path to license file 47
6.1.3. Enable HTTP compression for IIS 6.0 and IIS 7.0 47
6.2 Server Security Configuration 47
6.2.1. Registering COM components 47
6.2.2. Setting Permissions for Oracle projects execution 49
6.2.3. Encrypting sections with aspnet_regiis tool 49
6.3 Client Security Configuration 50
6.4 Configuring Windows Authentication for Web Verifier 52
6.4.1. For IIS 7 52
6.4.2. For IIS 6 53
6.4.3. Changes to Web.config File 58
6.4.4. Reverting Back to Standard Authentication 59
6.5 Configuring SSL for Web Verifier 59
6.6 Configuring Additional Languages 59
6.7 Virus Check 60
6.8 Enabling New Columns for Batch View 60
6.9 Changing Custom Column Names 61
6.9.1. Custom Column Names for Web Verifier 61
6.9.2. Custom Column Names for Thick Verifier Client 61
7 Security 64
7.1 WebCenter Forms Recognition Security 64
7.1.1. Project Security 64
7.1.2. Project & Windows Authentication Security 64
7.2 File System Security 65
7.3 Access to Project Data 66
7.4 Accounts and File Access Security 67
7.5 Configuring the Service Account for WebCenter Forms Recognition 68
7.5.1. Running WebCenter Forms Recognition on a Domain Network 68
7.5.2. System Monitoring 69
7.5.3. Email Importing and Service User Accounts 69
8 Configuring Runtime Components 70
8.1 Configuring the Runtime Service Manager 70

8.2 Configuring the RTS RemoteAdmin MMC Snap-in 70
8.3 Advanced Logging 72
8.3.1. System Resource Logging 72
8.3.2. Crash / Failure Logging 73
9 Auto-Update 75
9.1 Description 75
9.1.1. How the Automatic Update Works 75
9.1.2. Manual Configuration of the Auto Update Function 76
9.2 Usage 77
10 Enabling Additional OCR Engine Languages 78
10.1 To Enable a Language for an OCR Engine 78
10.2 To add Input Language for Windows 7 78
10.3 To add Input Language for Windows XP 78
10.4 To add Input Language for Windows Vista 78
10.5 To add Input Language for Windows 2008 79
10.6 To add Input Language for Windows 2003 79
11 Workarounds 80
11.1 Running Multiple Web Verifier and RTS instances 80

1 About WebCenter Forms Recognition

WebCenter Forms Recognition is a product suite designed by Oracle Corporation, to automatically process incoming documents. It works with any document that is electronically available including scanned images, faxes, e-mails, and files. WebCenter Forms Recognition automatically classifies these documents and extracts meaningful information from them.

WebCenter Forms Recognition uses a trainable, self-learning algorithm that minimizes user definition and intervention tasks.

Within the WebCenter Forms Recognition suite, Designer enables you to customize the automatic processing of incoming documents, for example, which document classes are relevant in your enterprise as well as which information is to be extracted from the classified documents. All custom settings are saved in a WebCenter Forms Recognition project file.

To process large volumes of documents, WebCenter Forms Recognition organizes documents into batches, which are defined in the project file. The project files and stored settings are automatically forwarded to Runtime Server for production processing.

WebCenter Forms Recognition Runtime Server runs unattended as a server process in the background. Several mechanisms ensure that the system is stable, meaning that it can automatically recover from most error situations. Multiple instances of WebCenter Forms Recognition Runtime Server can be started simultaneously in a network or on a single machine. These instances cooperate and allow for optimal load distribution.

Batches that cannot be automatically processed in their entirety by the Runtime Server are forwarded to the quality assurance application, Verifier, for manual correction.

The Web Verifier application module allows users to verify documents with no software installed on the client side. Web Verifier can be used via a supported browser on any client machine to verify documents. This requires installation and configuration of the project and batches on the database platform. From version 11.1.1.8.0, WebCenter Forms Recognition features a newly implemented database platform for WebCenter Forms Recognition applications. It is possible to store project and authentication information in the WebCenter Forms Recognition database. This solution allows for central management of storage and backup and thus provides for easier security, better connectivity of your applications, and higher flexibility of your personnel.

2 System Requirements

2.1 Operating Systems

Using WebCenter Forms Recognition requires a complete and successful installation of the software on a server or workstation running one of the following operating systems:

- Microsoft Windows Server 2008 R2 (IPv4 and IPv6).
- Microsoft Windows 7

2.2 WebCenter Forms Recognition Database

The Web Verifier application module requires central management of project data in a database. The WebCenter Forms Recognition database has been certified to run on the following database platforms:

- Oracle 11g R2
- Microsoft SQL Server 2008 R2

Using WebCenter Forms Recognition will require .NET Framework 3.5 SP1 installed on the server or workstation.

2.3 IIS

Using WebCenter Forms Recognition 11.1.1.8.0 will require the following software applications installed on the server:

- Internet Information Server
- .NET Framework 3.5 SP1

For the client browser version side, Internet Explorer 7 and 8 have been certified with Forms Recognition 11.1.1.8.0 application.

2.4 Scripting Components

WebCenter Forms Recognition has been certified for the following supported Scripting component version:

- WinWrap version 9.0.0.56

3 Hardware Requirements

Before WebCenter Forms Recognition can be implemented, the underlying network must meet certain minimum platform and environment requirements.

This section includes information about, and instructions for, configuring basic network components.

3.1 Network Infrastructure

The technology infrastructure underlying WebCenter Forms Recognition consists of a set of scalable applications and services running on Microsoft Windows operating systems. These applications and services are deployed on a set of high-performance Intel-compatible servers and workstations.

Clients are supported on Intel-compatible workstations running Windows 7.

WebCenter Forms Recognition is a distributed two-tier application that is typically deployed across multiple Windows Server operating systems. These applications provide core system services when connected using an unimpeded high-speed, low-latency network infrastructure, such as Fast Ethernet (100BaseTX), using TCP/IP.

3.2 Hardware and Software Factors

When implementing a WebCenter Forms Recognition project, there are a number of dependencies that influence the hardware requirements for the solution.

This information is typically gathered during the requirements analysis phase of the project and used as a guideline to aid the project team members responsible for sizing the hardware and software for the implementation.

The hardware requirements provided in this document can be used as a guideline; it is not a recommended or required hardware configuration for an implementation of WebCenter Forms Recognition. The actual hardware and software configuration for an installation should be based on the client’s requirements.

Some factors to consider when sizing the hardware for a production environment are:

- Input volume – The number of documents/pages to process on a daily basis
- Completion Time – The required amount of time from when the document is scanned into the system, to when it is exported out of WebCenter Forms Recognition
- Complexity of input documents (single or multi-page TIFF, scanned resolution, document size, number of pages OCR’d per document, etc.)
- Output requirements (data extraction, validation, and export, number of documents processed per day, etc.)
- Complexity of workflow customization (scripting)
- Third-party software integration requirements (Oracle Financials, JD Edwards, CRM systems, etc.)
- Backup strategy
- Disaster recovery (backup, fault tolerance, up time, etc.)
- Network operating system platform
- Network environment
- Room for growth (increased in input/output and other system requirements)
- Users – The number of users (Web Verifier versus Verifier)

- Batch Retention Time – The time for a batch of documents to remain in the system after export
- Number of projects – Number of WebCenter Forms Recognition projects (per country, per solution, etc)

The following sections of the document are representations of some Hardware Scenario configuration.

3.3 Hardware Estimate – 500 PPD

3.3.1. Introduction – AP Packaged Project

Based on the standard Oracle AP Packaged Project, the following production system is recommended.

Assumptions:

- 1-3 page TIFF documents
- Document resolution of 300 dpi
- Average TIFF size of approximately 40KB
- Average WorkDoc size of approximately 21KB
- Minimum data extraction and validation (as per the project)
- Project size of less than 5 MB and less than 10 classes
- Cleanup of exported batches (1-3 days)

Note: Disk space requirement is implementation dependent; variables such as document complexity, scanned resolution, and document volume help determine the amount of disk space for a project. For example, persistent storage of TIFF images requires approximately 70 KB per page. In addition, approximately 100 KB per document are required to temporarily store WorkDocs with OCR results. If PDF file generation is enabled, another 100 KB per page are temporarily required.

3.3.2. Hardware Estimate – File System (Excl. Web Verifier & Database)

Machine Role		Hardware	Software Needed
WebCenter Forms Recognition Server (Primary) **- File Repository** **- OCR/Classify/Extract**	Required	Dual Core Xeon Class, 2.8 GHz CPU 4 GB RAM 20-40Gb Hard Disk Space	Windows 2008 R2 with the latest service pack WebCenter Forms Recognition Version 11.1.1.8.0
WebCenter Forms Recognition Designer **Project Design** **Class Training**	Optional	Pentium IV Class, 2.4 GHz CPU (2.8 GHz recommended) 1 GB RAM 10 GB hard drive (20 GB hard drive recommended)	Windows 7 WebCenter Forms Recognition Designer Version 11.1.1.8.0
WebCenter Forms Recognition Verifier, Advanced Verifier & Learnset Manager **Data Verification**	Required	Pentium Class, 2.4 GHz CPU (2.8 GHz recommended) 1 GB RAM 20 GB hard drive (10 GB minimum)	Windows 7 WebCenter Forms Recognition Verifier Version 11.1.1.8.0
WebCenter Forms Recognition Remote Admin **RTS Remote Admini-stration**	Optional	Pentium Class, 2.4 GHz 1 GB RAM [HD – Application install only <500Mb]	Windows 7 WebCenter Forms Recognition Version 11.1.1.8.0 RTS Remote Admin MMC Snap-in

Table 3-1: Recommended Configuration

3.3.3. Hardware Estimate – Database (Excl. Web Verifier)

Machine Role		Hardware	Software Needed
WebCenter Forms Recognition Server (Primary) **- File Repository** **- OCR/Classify/Extract** **Database Server**	Required	Quad Core Xeon Class, 2.8 GHz CPU 4 GB RAM 100Gb Hard Disk Space	Windows 2008 R2 with the latest service pack Oracle Database 10g or above, or SQL Server 2008 R2 .NET Framework 3.5 SP1 WebCenter Forms Recognition Version 11.1.1.8.0
WebCenter Forms Recognition Designer **Project Design** **Class Training**	Optional	Pentium IV Class, 2.4 GHz CPU (2.8 GHz recommended) 1 GB RAM 10 GB hard drive (20 GB hard drive recommended)	Windows 7 .NET Framework 3.5 SP1 WebCenter Forms Recognition Designer Version 11.1.1.8.0
WebCenter Forms Recognition Verifier, Advanced Verifier & Learnset Manager **Data Verification**	Required	Pentium Class, 2.4 GHz CPU (2.8 GHz recommended) 1 GB RAM 20 GB hard drive (10 GB minimum)	Windows 7 .NET Framework 3.5 SP1 WebCenter Forms Recognition Verifier Version 11.1.1.8.0
WebCenter Forms Recognition Remote Admin **RTS Remote Administration**	Optional	Pentium Class, 2.4 GHz 1 GB RAM [HD – Application install only <500Mb]	Windows 7 .NET Framework 3.5 SP1 WebCenter Forms Recognition Version 11.1.1.8.0 RTS Remote Admin MMC Snap-in

Table 3-2: Recommended Configuration

Note: When using Oracle as a database, it is required to have the 32-bit Oracle client installed on any workstation/server where WebCenter Forms Recognition communicates with the database (Designer, Verifier, etc).

3.3.4. Hardware Estimate – Entire Application Suite

The entire application suite comprises of Forms Recognition Runtime Server, Web Server, and Database.

Machine Role		Hardware	Software Needed
WebCenter Forms Recognition Server (Primary) **- File Repository** **- OCR/Classify/Extract** **Database Server** **Web Server**	Required	Quad Core Xeon Class, 2.8 GHz CPU 8 GB RAM 100Gb Hard Disk Space	Windows 2008 R2 with the latest service pack Oracle Database 10g or above, or SQL Server 2008 R2 WebCenter Forms Recognition Designer IIS 6 and above .NET Framework 3.5 SP1 WebCenter Forms Recognition Version 11.1.1.8.0
WebCenter Forms Recognition Designer **Project Design** **Class Training**	Optional	Pentium IV Class, 2.4 GHz CPU (2.8 GHz recommended) 1 GB RAM 10 GB hard drive (20 GB hard drive recommended)	Windows 7 .NET Framework 3.5 SP1 WebCenter Forms Recognition Designer Version 11.1.1.8.0
WebCenter Forms Recognition Verifier, Advanced Verifier & Learnset Manager **Data Verification**	Optional	Pentium Class, 2.4 GHz CPU (2.8 GHz recommended) 1 GB RAM 20 GB hard drive (10 GB minimum)	Windows 7 .NET Framework 3.5 SP1 WebCenter Forms Recognition Verifier Version 11.1.1.8.0
WebCenter Forms Recognition Web Verifier	Optional	Pentium Class, 2.4 GHz 2GB RAM	Windows 7 Supported Browser

Machine Role		Hardware	Software Needed
WebCenter Forms Recognition Remote Admin **RTS Remote Administration**	Optional	Pentium Class, 2.4 GHz 1 GB RAM [HD – Application install only <500Mb]	Windows 7 .NET Framework 3.5 SP1 WebCenter Forms Recognition Version 11.1.1.8.0 RTS Remote Admin MMC Snap-in

Table 3-3: Recommended Configuration

3.3.5. Hardware Estimate – Typical Development Environment

A typical development environment consists of one server which processes less than 500 pages per day. The specification below should be sufficient to house the Web Server, Database, and WebCenter Forms Recognition Runtime Server.

Machine Role		Hardware	Software Needed
WebCenter Forms Recognition Server (Primary) **- File Repository** **- OCR/Classify/Extract** **- Database Server** **- Web Server**	Required	Quad Core Xeon Class, 2.8 GHz CPU 8 GB RAM 100Gb Hard Disk Space	Windows 2008 R2 with the latest service pack Oracle Database 10g or above, or SQL Server 2008 R2 IIS 6 and above .NET Framework 3.5 SP1 WebCenter Forms Recognition Designer WebCenter Forms Recognition Version 11.1.1.8.0

Table 3-4: Recommended Configuration

3.4 Hardware Estimate – 4000 PPD

3.4.1. Introduction – AP Packaged Project

Based on the standard Oracle AP Packaged Project, the following production system is recommended.

Assumptions:

- 1-3 page TIFF documents
- Document resolution of 300 dpi
- Average TIFF size of approximately 60KB
- Average WorkDoc size of approximately 60KB
- Minimum data extraction and validation (as per the project)
- Project size of less than 5 MB and less than 10 classes
- Cleanup of exported batches (1-3 days).
- All documents are provided at the start of the day

Disk space requirement is implementation dependent; variables such as document complexity, scanned resolution, and document volume help determine the amount of disk space for a project. For example, persistent storage of TIFF images requires approximately 70 KB per page. In addition, approximately 100 KB per document are required to temporarily store WorkDocs with OCR results. If PDF file generation is enabled, another 100 KB per page are temporarily required.

3.4.2. Hardware Estimate – File System (Excl. Web Verifier & Database)

Machine Role		Hardware	Software Needed
WebCenter Forms Recognition Server (Primary) - File Repository - OCR/Classify/Extract	Required	Quad Core Xeon Class, 2.8 GHz CPU 8GB RAM 200Gb Hard Disk Space	Windows 2008 R2 with the latest service pack WebCenter Forms Recognition Version 11.1.1.8.0
WebCenter Forms Recognition Designer Project Design Class Training	Optional	Pentium IV Class, 2.4 GHz CPU (2.8 GHz recommended) 1 GB RAM 10 GB hard drive hard drive recommended)	Windows 7 WebCenter Forms Recognition Designer Version 11.1.1.8.0
WebCenter Forms Recognition Verifier, Advanced Verifier & Learnset Manager Data Verification	Required	Pentium Class, 2.4 GHz CPU (2.8 GHz recommended) 1 GB RAM 20 GB hard drive (10 GB minimum)	Windows 7 WebCenter Forms Recognition Verifier Version 11.1.1.8.0
WebCenter Forms Recognition Remote Admin RTS Remote Administration	Optional	Pentium Class, 2.4 GHz 1 GB RAM [HD – Application install only <500Mb]	Windows 7 WebCenter Forms Recognition Version 11.1.1.8.0 RTS Remote Admin MMC Snap-in

Table 3-5: Recommended Configuration

3.4.3. Hardware Estimate – Database (Excl. Web Verifier)

Machine Role		Hardware	Software Needed
WebCenter Forms Recognition Server (Primary) - File Repository - OCR/Classify/Extract Database Server	Required	Quad Core Xeon Class, 2.8 GHz CPU 8 GB RAM 200Gb Hard Disk Space	Windows 2008 R2 with the latest service pack Oracle Database 10g or above, or SQL Server 2008 R2 .NET Framework 3.5 SP1 WebCenter Forms Recognition Version 11.1.1.8.0
WebCenter Forms Recognition Designer Project Design Class Training	Optional	Pentium IV Class, 2.4 GHz CPU (2.8 GHz recommended) 1 GB RAM 10 GB hard drive (20 GB hard drive recommended)	Windows 7 .NET Framework 3.5 SP1 WebCenter Forms Recognition Designer Version 11.1.1.8.0
Forms Recognition Verifier, Advanced Verifier & Learnset Manager Data Verification	Required	Pentium Class, 2.4 GHz CPU (2.8 GHz recommended) 1 GB RAM 20 GB hard drive (10 GB minimum)	Windows 7 .NET Framework 3.5 SP1 Forms Recognition Verifier Version 11.1.1.8.0
Forms Recognition Remote Admin RTS Remote Administration	Optional	Pentium Class, 2.4 GHz 1 GB RAM [HD – Application install only <500Mb]	Windows 7 .NET Framework 3.5 SP1 Forms Recognition Version 11.1.1.8.0 RTS Remote Admin MMC Snap-in

Table 3-6: Recommended Configuration

When using Oracle as a database, it is required to have the 32-bit Oracle client installed on any workstation/server where WebCenter Forms Recognition communicates with the database (Designer, Verifier, etc).

3.4.4. Hardware Estimate – Entire Application Suite

The entire application suite comprises of WebCenter Forms Recognition Runtime Server, Web Server, and Database.

Machine Role		Hardware	Software Needed
WebCenter Forms Recognition Server (Primary) **- File Repository** **- OCR/Classify/Extract** **Database Server**	Required	Quad Core Xeon Class, 2.8 GHz CPU 8 GB RAM 100Gb Hard Disk Space	Windows 2008 R2 with the latest service pack Oracle Database 10g or above, or SQL Server 2008 R2 IIS 6 and above .NET Framework 3.5 SP1 WebCenter Forms Recognition Version 11.1.1.8.0
WebCenter Forms Recognition Web Server	Required	Dual Core Xeon Class, 2.8 GHz CPU 4 GB RAM 50Gb Hard Disk Space 30Gb OS Hard Disk Space	Windows 2008 R2 with the latest service pack Oracle Database 10g or above, or SQL Server 2008 R2 WebCenter Forms Recognition Designer IIS 6 and above .NET Framework 3.5 SP1 WebCenter Forms Recognition Version 11.1.1.8.0
WebCenter Forms Recognition Designer **Project Design** **Class Training**	Optional	Pentium IV Class, 2.4 GHz CPU (2.8 GHz recommended) 1 GB RAM 10 GB hard drive (20 GB hard drive recommended)	Windows 7 .NET Framework 3.5 SP1 WebCenter Forms Recognition Designer Version 11.1.1.8.0
WebCenter Forms Recognition Verifier, Advanced Verifier & Learnset Manager **Data Verification**	Optional	Pentium Class, 2.4 GHz CPU (2.8 GHz recommended) 1 GB RAM 20 GB hard drive (10 GB minimum)	Windows 7 .NET Framework 3.5 SP1 WebCenter Forms Recognition Verifier Version 11.1.1.8.0
WebCenter Forms Recognition Web Verifier	Optional	Pentium Class, 2.4 GHz 2GB RAM	Windows 7 Supported browser
WebCenter Forms Recognition Remote Admin **RTS Remote Administration**	Optional	Pentium Class, 2.4 GHz 1 GB RAM [HD – Application install only <500Mb]	Windows 7 .NET Framework 3.5 SP1 WebCenter Forms Recognition Version 11.1.1.8.0 RTS Remote Admin MMC Snap-in

Table 3-7: Recommended Configuration

3.4.5. Web Verifier Server Hardware Sizing – Additional Information

Additional Web Server considerations depend on the number of Verifier users.

Number of Users	Memory	Processor
Per User	150Mb	Peak Load 100% of a 3GHz CPU
0-10 Users	4 Gb	Dual Core CPU
11-20 Users	8 Gb	Quad Core CPU

Table 3-8: Recommended Configuration

Factors which influence the metrics are:

- Project size and complexity
- Other software stored on the server
- Third party software integration

- Network connections
- Document Sizes
- Project Type

Machine Role	Hardware	Software Needed
WebCenter Forms Recognition Server (Primary) **Project File (.SDP)** **Batch Directory** **Stores Images** **Workdocs** **Input Directory** **Learnset**	Xeon Class, 2.4 GHz CPU 2 GB RAM Three or more 36 GB (40 GB recommended) + Hot Swappable hard drive RAID Controller (for fault tolerance)	Windows 2008 R2 with the latest service pack Microsoft .Net Framework 3.5 SP1 WebCenter Forms Recognition Version 11.1.1.8.0
WebCenter Forms Recognition RTS **Performs OCR** **Classification** **Data Extraction** **Export** **System Clean-up**	Dual Xeon Class, 2.8 GHz CPU 2 GB RAM (1 GB minimum) 40 GB hard drive	Windows 2008 R2 with the latest service pack Microsoft .Net Framework 3.5 SP1 WebCenter Forms Recognition Version 11.1.1.8.0
WebCenter Forms Recognition Designer **Project Design** **Class Training**	Pentium IV Class, 2.4 GHz CPU (2.8 GHz recommended) 1 GB RAM 10 GB hard drive (20 GB hard drive recommended)	Windows 7, or Windows 2008 R2 Microsoft .Net Framework 3.5 SP1 WebCenter Forms Recognition Designer Version 11.1.1.8.0
WebCenter Forms Recognition Verifier, Advanced Verifier & Learnset Manager **Data Verification**	Pentium Class, 2.4 GHz CPU (2.8 GHz recommended) 1 GB RAM 20 GB hard drive (10 GB minimum)	Windows 7, or Windows 2008 R2 Microsoft .Net Framework 3.5 SP1 WebCenter Forms Recognition Verifier Version 11.1.1.8.0
WebCenter Forms Recognition Remote Admin **RTS Remote Administration**	Pentium Class, 2.4 GHz CPU (2.8 GHz recommended) 1 GB RAM 10 GB hard drive	Windows 7, or Windows 2008 R2 WebCenter Forms Recognition Version 11.1.1.8.0 RTS Remote Admin MMC Snap-in
WebCenter Forms Recognition Web Verifier Server	Pentium Class, 2.4 GHz CPU (2.8 GHz recommended) 1 GB RAM 10 GB hard drive	Windows 7, or Windows 2008 R2 Microsoft .Net Framework 3.5 SP1 Internet Information Server (IIS) 6.0 or higher WebCenter Forms Recognition Version 11.1.1.8.0

Table 3-9: Recommended Configuration

3.5 Infrastructure Constraints

WebCenter Forms Recognition has been fully tested and is certified to work in most LAN environments. By adhering to the following infrastructure constraints, you can ensure a smooth implementation of the product suite.

3.5.1. OCR Performance

OCR is a processor-intensive task. To maximize OCR performance, we recommend that only one RTS OCR instance is active per CPU on a production server. Although it is possible to run multiple RTS OCR instances on a single CPU, doing so may impair the performance of OCR and the overall system.

3.5.2. Firewalls

WebCenter Forms Recognition is designed to work in a non-encapsulated LAN environment. A non-encapsulated LAN, in this context, is a LAN segment free of impediments such as firewalls and other traffic-filtering devices.

With multi-site network environments, it is the responsibility of the customer's IT personnel to ensure that an unobstructed communication path exists between the user community and host system.

3.6 RTS Remote Administration MMC

You can remotely administer WebCenter Forms Recognition Runtime Server, meaning that you can centrally manage multiple Runtime Servers from a single workstation on the network using a management console snap-in called the RTS Remote Administration MMC.

However, to use the RTS Remote Administration MMC snap-in, the administrator workstation must either reside on the same LAN segment as the RTS server services to be centrally administered or, in the case of a sub-netted network, a name resolution system must be in place to allow clients on one subnet to locate resources on another subnet.

Remote Administration by MMC requires one free configurable port number. The default port is 50607.

The Windows service WebCenter Forms Recognition Service Manager must be running in order to be able to connect by MMC to the Runtime Server service. Once the service is running, it is possible to start and stop each Runtime Server instance separately.

As long as the configured port is available in any TCP/IP network (or Internet across firewalls) and the main service is running, the MMC can be used to configure and maintain the Runtime Server instances.

4 Pre-Installation of WebCenter Forms Recognition

When you are ready to install WebCenter Forms Recognition, there are several steps you should take to ensure that the installation goes smoothly. This section includes information about the following:

- Backward compatibility with other Oracle applications
- Upgrading from previous versions of Forms Recognition
- Uninstalling Forms Recognition Version 10.1.3.5.0
- Installing WebCenter Forms Recognition Version 11.1.1.8.0 in standalone mode
- Installing WebCenter Forms Recognition Version 11.1.1.8.0
- Checking the installation
- Migrating existing project files to Version 11.1.1.8.0
- Uninstalling WebCenter Forms Recognition Version 11.1.1.8.0
- Repairing WebCenter Forms Recognition Version 11.1.1.8.0
- Adding or removing product components

4.1 Before Installing WebCenter Forms Recognition

Before starting the installation, make sure that you have local administrator rights on the target machine. During the installation, a number of DLLs will be copied to the Windows system directory and registered with the operating system. The WebCenter Forms Recognition database will be created on the Oracle Database or SQL Server servers. The install process requires administrative privileges and access to the Windows registry.

The installation media contains the following folders:

- .\Install contains the setup executables of the WebCenter Forms Recognition product suite.
- .\Install\doc contains WebCenter Forms Recognition product documentation.

4.1.1. Installation Checklist

The checklist below is designed to help you install and configure WebCenter Forms Recognition in your environment.

☐ If you are installing WebCenter Forms Recognition in a standalone mode (a non-network test or demo installation,) do only the steps outlined in section 5 Installing and skip the rest of the installation checklist.

☐ If you are upgrading from a previous version of Forms Recognition, read section 4.4 Upgrading from Previous Versions and do the steps outlined in that section before continuing with the installation checklist.

☐ If your organization uses other Oracle products, read section 4.2 Backward Compatibility before proceeding with the installation checklist.

☐ Read section 3 Hardware Requirements.

☐ Configure the Oracle Database or SQL Server software.

☐ If following the Microsoft recommended resource rights assignment model, create the users and groups.

☐ Install WebCenter Forms Recognition Version 11.1.1.8.0. (Section 5 Installing WebCenter Forms Recognition)

☐ Configure the Runtime Components. (Section 8 Configuring Runtime Components)

□ Configure the Runtime Service Manager (Section 8.1 Configuring the Runtime Service Manager).

□ Start the Runtime Service Manager.

□ Configure the RTS RemoteAdmin MMC snap-in (Section 8.2 Configuring the RTS RemoteAdmin MMC Snap-in).

□ Test the installation (See the WebCenter Forms Recognition ***Runtime Server User Guide***).

□ Configure license and project settings for an instance. (See the WebCenter Forms Recognition ***Runtime Server User's Guide***.)

□ Process a batch (minimum workflow steps: OCR, Classification, and Extraction).

□ If using Web Verifier, configure the IIS and .NET along with application security. (See section 6 Configuring Application)

4.2 Backward Compatibility

WebCenter Forms Recognition Version 11.1.1.8.0 is fully backward compatible with Version 10.1.3.5.0 of Oracle Forms Recognition, but not with earlier versions.

This version of WebCenter Forms Recognition is completely based on the Database platform. **Support of the file system has been discontinued.**

Note: Oracle recommends engaging Professional Services to ensure a successful and smooth installation of the software.

4.3 WebCenter Forms Recognition Database Checklist

4.3.1. WebCenter Forms Recognition Database

WebCenter Forms Recognition version 11.1.1.8.0 is able to store the following core information directly in the database, instead of the file system:

- Documents
- Batches (jobs)
- Images and document files in e-format
- Project references
- Users, groups, roles and relationships
- Verifier configuration (Web Verifier only)
- Batch/Document lock handling
- Application level user licensing

File system functionality is no longer supported. Customers with file system based batches that want to upgrade to version 11.1.1.8.0 will be required to upgrade to database based batches.

Prior to installation of WebCenter Forms Recognition, some care must be taken to make sure that the appropriate configuration steps have been taken.

4.3.2. WebCenter Forms Recognition Oracle Database Checklist

WebCenter Forms Recognition will need the following items taken care of prior to the installation of the software:

1. The 32-bit Oracle Database Client Libraries must be installed on all computers where WebCenter Forms Recognition will be run. This includes all Runtime Server instances, and all Verifier and Designer workstations.
2. Create a new Oracle instance for WebCenter Forms Recognition.
3. Create a new user with a password.
4. Assign sufficient rights to the above user:
   a. Allow for increased growth of data.
   b. Allow for insertion, modification, and deletion of data.
   c. Allow for table, views, etc. creation.
5. Administrative database accounts with rights to create, modify, and delete tables. Windows Authentication can be used if the user performing the installation has administrative rights to the database server.
6. A designated user database account that will be used by WebCenter Forms Recognition to access the database, add, modify, and delete data. Windows Authentication can be used if the user performing the installation has the appropriate rights to the database server.

4.3.3. WebCenter Forms Recognition SQL Server Checklist

WebCenter Forms Recognition will need to create the following items prior to the installation of the software:

1. An administrative database account with rights to create, modify, and delete tables. Windows Authentication can be used if the user performing the installation has administrative rights to the database server.
2. A designated user database account that will be used by WebCenter Forms Recognition to access the database, add, modify, and delete data. Windows Authentication can be used if the user performing the installation has the appropriate rights to the database server.

4.4 Upgrading from Previous Versions

4.4.1. Upgrading from Oracle Forms Recognition Version 10.1.3.5.0

Due to the WebCenter Forms Recognition database that has to be established during the setup process, Oracle Forms Recognition version 10.1.3.5.0 must be uninstalled prior to installation of version 11.1.1.8.0.

4.5 Removing Oracle Forms Recognition Version 10.1.3.5.0

It is recommended to uninstall any previous versions of Oracle Forms Recognition prior to installing Forms RecogWebCenter Forms Recognitionnition 11.1.1.8.0.

The uninstaller may not remove several registry entries and subdirectories adequately. For this reason, they must be removed manually. Please follow the procedure below to properly remove the older version of Oracle Forms Recognition before installing Version 11.1.1.8.0.

To remove previous versions of Oracle Forms Recognition:

1) Select *Start>Settings>Control Panel*.
2) Launch the *Add/Remove Program* wizard.
3) On the *Currently Installed Programs* list, select “Oracle Forms Recognition 10g Release 3 (10.1.3.5.0)”.
4) Click *Remove*.
5) Follow the on-screen instructions to remove the product.

6) Click *Finish*.

7) Save any permanent license files in the *…\<Application folder>\Component\Cairo directory before deleting the …\<Application folder>* folder.
Save the FineReader FRELF file if FineReader 8.1 or FineReader 10 is used.

8) Remove the …\<Application folder> subdirectory.

9) Restart the machine.

10) Install WebCenter Forms Recognition Version 11.1.1.8.0.

Note: Forms Recognition Runtime Server Settings and Verifier Settings files can be reused in the new version. It is recommended to save these prior to un-installation and reuse them when configuring a new Runtime Server or Verifier Workstation.

5 Installing WebCenter Forms Recognition

5.1 Software Installation

Note: You must first install .NET Framework 3.5 SP1 prior to installing WebCenter Forms Recognition.

To install WebCenter Forms Recognition:

1) Browse to the installation folder and run setup.exe.
2) English and German are the supported installation languages. The installer gets its language settings from the regional settings of the operating system. The installation defaults to English if a language other than English or German is detected.
3) Make sure that all WebCenter Forms Recognition applications are closed.
4) Click *Next* to continue.
5) Select the installation type:

   Complete:

   Installs WebCenter Forms Recognition Designer, Runtime Server, and Thick/Web Verifier. OCR Engines FineReader8.1, FineReader 10, Kadmos 5, Recognita, QualitySoft, and Cleqs Barcode.

Default Folder:	SystemDrive:\Program Files\Oracle.
Default Program Group:	WebCenter Forms Recognition.

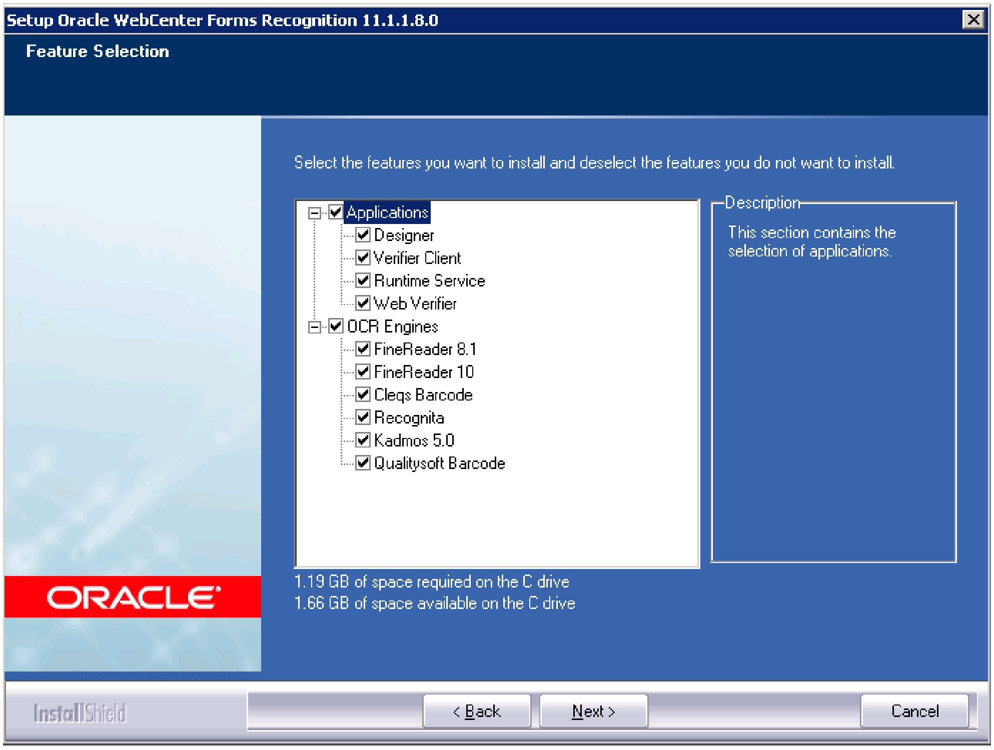
   Custom:

   Enables you to install only the components you will use.

6) For a complete installation choose *Complete* and press *Next*. This will run the typical installation and install all optional components. Go to section 5.1.2 to complete the setup.
7) For a custom installation choose *Custom* and press *Next*. Read the next chapter for details.

5.1.1. Selecting Custom Installation

If you selected *Custom* on the *Setup Type* screen, you can select the installation directory, the features and other components.



Setup Oracle WebCenter Forms Recognition 11.1.1.8.0

Feature Selection

Select the features you want to install and deselect the features you do not want to install.

- ☑ Applications
  - ☑ Designer
  - ☑ Verifier Client
  - ☑ Runtime Service
  - ☑ Web Verifier
- ☑ OCR Engines
  - ☑ FineReader 8.1
  - ☑ FineReader 10
  - ☑ Cleqs Barcode
  - ☑ Recognita
  - ☑ Kadmos 5.0
  - ☑ Qualitysoft Barcode

Description

This section contains the selection of applications.

1.19 GB of space required on the C drive
1.66 GB of space available on the C drive

Figure 5-1: Select or deselect applications and components.

For a custom installation:

1) First choose the installation directory.

2) In *Feature Selection* dialog box, select the desired applications.

3) In the OCR components list, you can select the optional components used for Barcode recognition and Handprint OCR.
Only components selected during the installation will be available. However, you can always add more components later. (See section 5.11 Adding or Removing Version 11.1.1.8.0 Components).

Optional Components	
Cleqs Barcode Engine:	Reads handwritten and machine-printed data and barcode information. It reads 18 types of barcodes.
FineReader8.1 OCR Engine:	Converts paper-based or scanned images into editable text. Supports English, German, Italian, French, and Spanish.
FineReader10 OCR Engine:	Converts paper-based or scanned images into editable text.
Kadmos5 OCR Engine:	Used for handwriting recognition.
Recognita Engine:	Supports 75 languages and more than 100 scanner models.
QualitySoft Barcode Engine	Support grayscale and color images. QualitySoft recognizes 19 different barcode types.

Table 5-1: List of available OCR components

4) Click *Next*.

The setup creates several subdirectories below the installation directory:

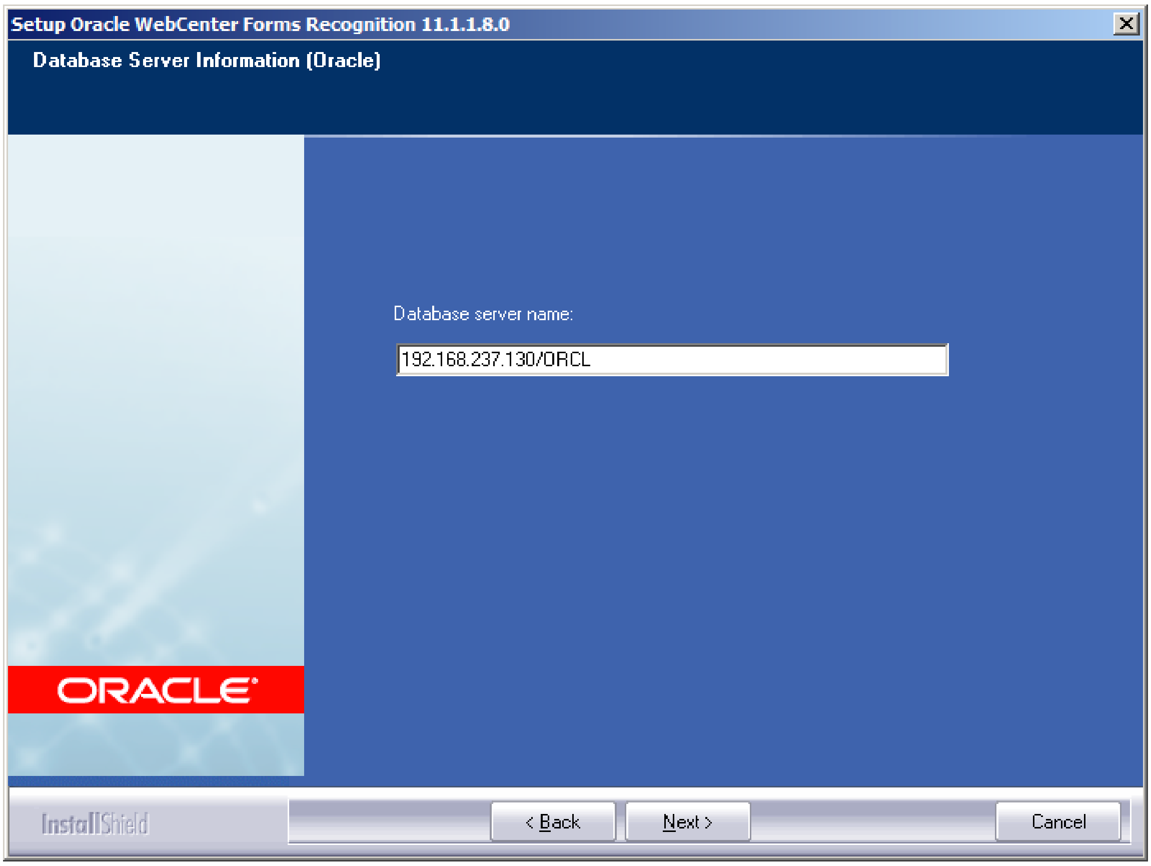
- **\Components\Cairo** contains the base components for imaging and recognition. In a complete installation there are several subdirectories with third party libraries: Accusoft, Cleqs Barcode, FineReader, Kadmos, Recognita, INSO, and LDF. This directory also contains the master license file.
- **\Components\Cedar** contains the base components for document analysis. There is one subdirectory for each supported language and a subdirectory with a third party library, FindLink.
- **\Components\Tools** contains the installation log file, component version information, and other tools/utilities for WebCenter Forms Recognition.
- **\Projects** contains the AP Packaged Project.
- \Forms Recognition**\bin** contains the WebCenter Forms Recognition Designer executable DstDsr.exe, the Runtime Server executables DstMgr.exe and DstHost.exe, the Supervised Learning Manager executable DstSlm.exe, and the Verifier executable DstVer.exe. It also contains the settings files.
- \WebCenter Forms Recognition**\bin\Log** contains the log files of the WebCenter Forms Recognition Runtime Server.
- \WebCenter Forms Recognition **Web Server** contains the WebCenter Forms Recognition Web components, the Web.Config file, and other web libraries used by the Web Verifier.

5.1.2. WebCenter Forms Recognition Database Setup

1) Now, the dialog box for the WebCenter Forms Recognition Database setup appears.
2) After selection of the desired server, click *Next*. If you want to end the installation without installing the Database, go to section 5.1.3 Completing the WebCenter Forms Recognition Setup, otherwise:

5.1.2.1. Oracle Database Setup

- Enter the Oracle Database username and password created in section 4.3.2 above
- Click *Next*.
- Enter the database server name. This must be entered as <database server name>/<instance name> as illustrated below



Setup Oracle WebCenter Forms Recognition 11.1.1.8.0

Database Server Information (Oracle)

Database server name: 192.168.237.130/ORCL

- Click Next.

5.1.2.2. SQL Server Setup

- Enter the name of your Database server.
- Enter your login credentials for the database, or use Windows authentication.
- Click *Next*.

3) The setup will search for the database server, connect with it and initialize WebCenter Forms Recognition database.

Very Important!

Please note, if you already have a WebCenter Forms Recognition database installed, this database will be overwritten by this installation process. In that case a notification would be displayed to remind you of deletion:

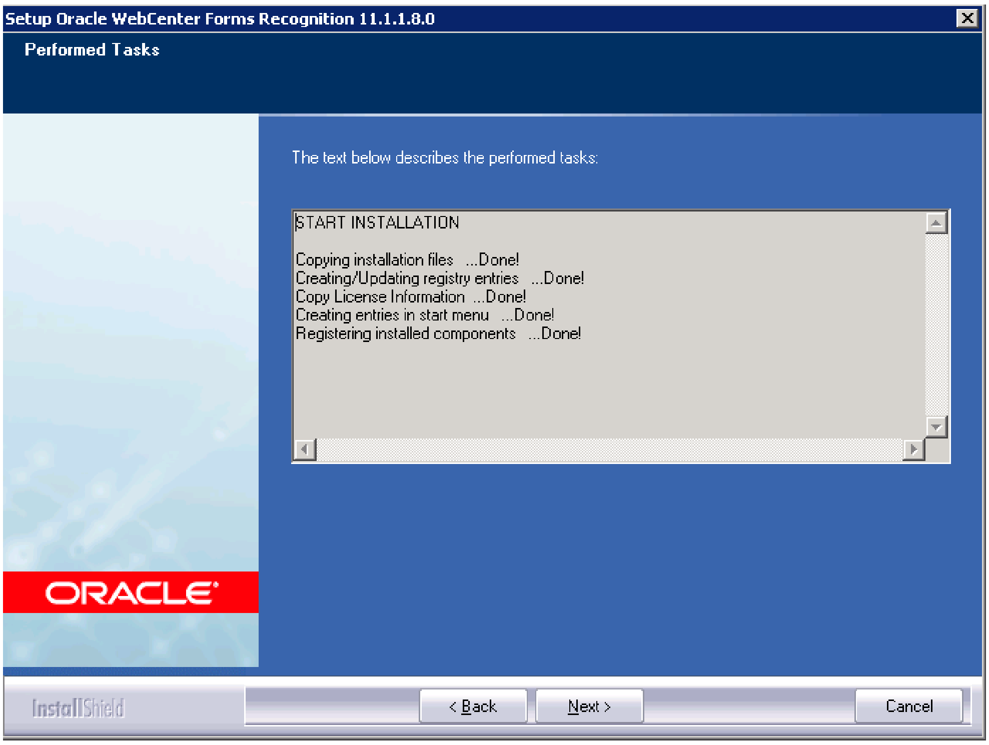
```
A WebCenter Forms Recognition Database has been detected.
If you continue the Database will be overwritten.
It is strongly recommended that the existing Database be backed up
before continuing.
```

If you want to save your existing Database, back it up before continuing. This applies for the installation of a new version on the same machine.

If you want to keep your current installation but want to install WebCenter Forms Recognition e. g. on an additional Runtime Server machine, you can keep your existing Database by copying all of the configuration files (web.config and .config files in \WebCenter Forms Recognition\bin) from the existing installation folder WebCenter Forms Recognition\bin to the new setup folder.

5.1.3. Completing the WebCenter Forms Recognition Setup

4) The final part of the installation confirms components that have been installed.



The text below describes the performed tasks:

```
START INSTALLATION

Copying installation files   ...Done!
Creating/Updating registry entries   ...Done!
Copy License Information  ...Done!
Creating entries in start menu   ...Done!
Registering installed components   ...Done!
```

Figure 5-2: Confirmation of installation steps.

5) Select *Next* to continue.

6) You will be presented with a screen to confirm if you want to have desktop icons created for WebCenter Forms Recognition application. Tick the checkbox if you want desktop icons.

7) Select *Finish*, to complete the installation.

Note: In version 11.1.1.8.0, French language is supported for Verifier, Web Verifier, and Learnset Manager. In order to enable French language, you have to select the language on the Formats tab of your system's Regional and Language Options.

5.2 Manually Creating Database Objects (post install)

It is also possible to install the database manually. This can be due to corporate policies. In such an instance, the following steps can be taken to install and configure the database manually:

1) Launch Windows Explorer and navigate to the installation folder. Navigate to <installerFolderLocation>\FirstPart\Database\CreationScripts.

   There are two folders, Oracle and SQL Server. Each folder contains database scripts to execute that will create the tables, views, indexes, and default data values.

2) Open the database configuration panel

   Oracle: SQLPlus or Oracle Management Console

- Follow the steps outlined earlier in this document in configuring the database prior to Oracle installation. (See section 4.3.2 WebCenter Forms Recognition Oracle Database Checklist)
- Log into the database with user account where the tables will be located.

- Run the database script to create the appropriate values.

SQLServer: Management Console.

- Log into the database with Administrator rights
- Create a new database
- Run the SQL scripts to create the appropriate values.

3) Navigate to
<installerFolderLocation>\FirstPart\Database\UpdateScripts
Again, you will find folders for the Oracle and SQL Server scripts.
4) Edit the Update Database script:
   - in Oracle script: TargetDBSchemaName
   - in MS SQL script: TargetDatabaseName

   Note: If you refrain from executing the steps outlined above, an error message will turn up on running of the Update Scripts.
5) Run the Update Database script.
6) Check that the database tables have been created correctly and no errors were reported on execution of the database scripts.
7) There are several configuration components that require modification. Navigate to the Oracle installation folder. By default this is located in Program Files\Oracle.
8) Navigate to the WebCenter Forms Recognition Web Server folder and open the Web.config file in Notepad.
9) Search for the connection string in the file.

   <connectionStrings></connectionStrings>
10) Modify the connection string to connect to the database.

Oracle Example

```
<connectionStrings>

<add name="Entities"
connectionString="metadata=res://*/Entity.ORAEntities.csdl|res://*/Entity.ORAEntities.ssdl|res://*/Entity.ORAEntities.msl;
provider=EFOracleProvider; Provider Connection String='Data Source=OracleServerName;User Id=Oracle;Password=Oracle'"
providerName="System.Data.EntityClient" />

</connectionStrings>
```

SQL Server Example

```
<connectionStrings>

<add name="Entities" connectionString="metadata=res://*/Entity.Entities.csdl|res://*/Entity.Entities.ssdl|res://*/Entity.Entities.msl;
provider=System.Data.SqlClient; provider connection string=&quot;Data Source=DBINSTANCE\SQLEXPRESS; Initial
Catalog=SQLServerDatabaseCatalog;Integrated Security=false;User
ID=Oracle;Password=Oracle;MultipleActiveResultSets=True&quot;" providerName="System.Data.EntityClient" />

  </connectionStrings>
```

11) Navigate to the WebCenter Forms Recognition\bin folder.
12) There are 6 other configuration files that require changing as with the web.config. These are DstDsr.exe.config, DstHost.exe.config, DstSlm.exe.config,

Brainware.System.Project.exe.config, DstVer.exe.config, and DstWkBrw.exe.config. Open each one in Notepad to make the appropriate changes below.

13) Search for the connection string in the file.

```
<connectionStrings></connectionStrings>
```

Modify the connection string to connect to the database. (Refer to Step 10 for examples)

14) For Oracle installation, it is required to make one more addition to the .NET installation for the Oracle connection string above to work.

- Navigate to the Windows folder using Windows Explorer
- Navigate to WINDOWS\Microsoft.NET\Framework\ v2.0.50727\CONFIG
- Open the machine.config file for editing and location the DbProviderfactories tag.
- Add the lines below and *do not delete any existing data.*

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

5.3 Configuring the WebCenter Forms Recognition Database (Post Install)

After the installation of WebCenter Forms Recognition there are additional configuration steps that are required.

1. Check the project file names. The project file name will be used to display the available project lists in Web Verifier.
2. Review the list of users in the projects.

- All usernames and passwords must be consistent throughout all project files.
- Each user must have their own username and password – user IDs cannot be shared.

3. Export the users from the project file into the WebCenter Forms Recognition database. This will now make users available to access projects via the Web Verifier.
4. Log into the User table (known in Oracle as USER_) and for each user; add a Forename and Surname into the WebCenter Forms Recognition database.
5. Create a Runtime Server instance for the project, or import existing Runtime Server settings, and configure again the WebCenter Forms Recognition database (creating a job and linking to the WebCenter Forms Recognition database).

You are now ready to use WebCenter Forms Recognition.

See Also:

For information on how to configure a project for a WebCenter Forms Recognition instance, or to migrate file system batches to the WebCenter Forms Recognition database, see the WebCenter Forms Recognition Runtime Server User's Guide.

5.4 Cedar Workflow History Wrapper Component

In order to achieve better compatibility of Visual Studio (VS) 6, Forms Recognition11.1.1.8.0 introduces an intermediate wrapper component for Workflow History related operations.

The component *Cedar Workflow History Wrapper* (CdrWH.dll) has to be installed and registered in \Oracle\Components\Cedar directory.

The component is a COM component created with VS 2008 (V9) C++ and wraps the currently available base component for Workflow History operations, which is the Cedar Database Access component (CdrDB.dll).

To access the Workflow History functionality, the CdrWH.dll should be used instead of the CdrDB.dll.

5.5 Installing WebCenter Forms Recognition in a Workgroup Configuration

A Windows workgroup, also referred to as peer-to-peer networking, is a network implementation of Windows-based operating systems (clients and servers) in which there is no central security authority (domain controller) responsible for user authentication or a central repository (such as Active Directory) for locating network resources.

In such a network, each machine is responsible for securing its resources, and users needing access to a resource located on a machine must have an account defined on that machine. Windows workgroup networking should only be used when you want to set up communication between a limited number of computers (less than 10) and the machines are not members of a Windows domain.

For an implementation of WebCenter Forms Recognition in corporate network environments that are standardized on network operating systems (servers) other than Windows –Novell Netware – a Windows workgroup setup may be the only choice. To install WebCenter Forms Recognition in Windows workgroup, perform the following steps (you must be logged on as an Administrator):

1) Create a user with the same name on each WebCenter Forms Recognition machine. Oracle recommends RTSsvc as the user name. (This does not apply to machines that will be used only as a Designer or Verifier workstation.)

2) Add the above user to the local Administrators group on each WebCenter Forms Recognition server.

3) Install WebCenter Forms Recognition on each machine by following the steps in Section 5.1 Software Installation.

4) Configure and start the Runtime Service Manager by performing the steps in Section 8.1 Configuring the Runtime Service Manager on each machine, with the following exception: Wherever a domain user is requested, add the user created in step 1 above.

5) Configure the RTS Remote Administration MMC snap-in by performing the steps in Section 8.2 Configuring the RTS RemoteAdmin MMC Snap-in on each machine.

6) Configure project settings on each machine and test the instance created in Step 5 above. You should (at a minimum) test the OCR, Classification, and Extraction workflow steps. For more information on how to configure project settings for a WebCenter Forms Recognition RTS instance, see the WebCenter Forms Recognition ***Runtime Server User's Guide.***

7) Once you have successfully tested each machine, test remote communication by adding a remote machine to the local MMC snap-in of one your servers. You can accomplish this by performing a subset of the steps (Steps 4 through 7) in Section 8.2 Configuring the RTS RemoteAdmin MMC Snap-in.

8) You should be able to administer the RTS instances (start, stop, change batch states, etc.) of the remote machine from the MMC snap-in of the local machine on which it was added.

5.6 Installing WebCenter Forms Recognition in Standalone Mode

WebCenter Forms Recognition can be deployed in a standalone mode. However, this implementation method is intended for test and demonstration purposes only. It should NOT be used in a production environment. Deployment of WebCenter Forms Recognition in standalone mode for production purposes would be deemed unsupported by Oracle.

In this setup, all WebCenter Forms Recognition components (applications, RTS, Remote Admin MMC snap-in, etc.) are installed and intended to be used on a single machine. Additionally, the integrated machine is not part of a Windows domain or is not intended to communicate with WebCenter Forms Recognition RTS instances running on other machine(s) in a network environment.

Using this setup, almost all of the configuration constraints (Windows domain, Users and Groups, etc.) can be ignored.

To install WebCenter Forms Recognition in a standalone mode:

1) Install WebCenter Forms Recognition Version 11.1.1.8.0 by following the steps in Section 5.5 Installing WebCenter Forms Recognition in a Workgroup Configuration.

2) Configure the RTS Remote Administration MMC snap-in by following the steps in Section 8.2 Configuring the RTS RemoteAdmin MMC Snap-in with one exception: In Step 6 of the procedure outlined, type LocalHost instead of the server name.

3) Configure project settings and test the instance created in step 4 above. You should (at a minimum) test the OCR, Classification, and Extraction workflow steps. For more information on how to configure project settings for a WebCenter Forms Recognition RTS instance, see the WebCenter Forms Recognition ***Runtime Server User's Guide***.

5.7 Checking the Installation

The installation was successful if WebCenter Forms Recognition runs without errors.

To check for the correct installation of components:

1) Open the installation directory.

2) Open *Components**Tools*.

3) Run SCBLibVersion.exe.

4) From the menu, select *View>Components General Info*. This displays a list of installed components:

5) Check the list for

- Completeness of components
- Homogeneity of build numbers
- Installation paths

6) All components Cro*.dll, Cdr*.dll and Bwe*.dll should have been registered automatically during the installation. If some of them seem to be missing, try to register them manually via the RegCro.bat, RegCdr.bat and BweReg.bat Windows batch files available in .\Components\Cairo, .\Components\Cedar and the corresponding .\Components\Bwe directories.

If the automatic registration does not work, try to register manually using the program regsvr32.exe from the Windows system directory.

If this does not help, create a copy of the components list using the command *File>Save* to file in the Oracle Component Version Info dialog box. Submit an error report, the components list, and the log files located in the ...\ Oracle\WebCenter Forms Recognition\\bin\Log folder to Oracle Customer Support.

5.8 Migrating Existing Project Files to Version 11.1.1.8.0

After you remove the earlier version of WebCenter Forms Recognition and install Version 11.1.1.8.0, project files designed in the earlier version must be converted to Version 11.1.1.8.0 formats before they can be used in the new version.

The conversion process is fully automated and is done by WebCenter Forms Recognition Designer. To convert Oracle Forms Recognition Version 10.1.3.5.0 project files to Version 11.1.1.8.0, do the following:

1) Launch WebCenter Forms Recognition Designer*.*

2) On the *Load Project* dialog box, browse to the project file location and double click on the project file that you want to convert. Login to the project using Administrator for User ID with the corresponding password.

3) Click *OK* to launch the automatic project conversion process. The conversion takes from a few seconds to a few minutes, depending on the size of the project.

4) Once the conversion is completed, click *Learn* (Light bulb) to relearn the project.

5) Save the project. The project is ready for use in WebCenter Forms Recognition Version 11.1.1.8.0.

Very Important!

Please note that a project and Learnset backup should always be taken.

See Also

For information on how to configure a project for a WebCenter Forms Recognition database, see the WebCenter Forms Recognition Designer User's Guide.

5.9 Removing WebCenter Forms Recognition Version 11.1.1.8.0

WebCenter Forms Recognition can be uninstalled by using the Windows Control Panel's *Add/ Remove* functionality. It is important to stop all running services using the Task Manager before uninstalling the application. To remove previous versions of WebCenter Forms Recognition:

1) Click *Start>Settings>Control* Panel.

2) Launch the *Add/Remove Program* wizard.

3) On the *Currently Installed Programs* list, select WebCenter Forms Recognition 11.1.1.8.0*.*

4) Click *Remove*.

5) Follow the on-screen instructions.

6) After un-installation, reboot your computer.

5.10 Repairing a WebCenter Forms Recognition Installation

The WebCenter Forms Recognition installer may be used to repair a copy of WebCenter Forms Recognition that has stopped working properly. Factors that could cause an installation to malfunction include:

- Accidental deletion of application files
- Missing registry entries
- Corrupted application files
- Malicious attacks on a machine housing WebCenter Forms Recognition

To repair WebCenter Forms Recognition:

1) Select *Start>Settings>Control* Panel.
2) Select *Add/Remove Program*.
3) In the *Currently Installed Programs* list on the *Add/Remove Programs* dialog box, select WebCenter Forms Recognition 11.1.1.8.0.
4) Click *Change*.
5) On the *Setup* dialog box, select *Repair* then click *Next*. This will reinstall all program components that were installed by the previous setup.
6) Click *Finish* when setup is completed.

5.11 Adding or Removing Version 11.1.1.8.0 Components

WebCenter Forms Recognition is a product suite consisting of the following applications:

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

The WebCenter Forms Recognition deployment utility, Setup.exe, uses a modular approach that enables you to add or remove applications from a machine.

To modify an existing WebCenter Forms Recognition installation:

1) Select *Start>Settings>Control* Panel.
2) Select *Add/Remove Program*.
3) In the *Currently Installed Programs* list, select WebCenter Forms Recognition 11.1.1.8.0.
4) Click *Change*.
5) On the *Setup* dialog box, select *Modify* and click *Next*.
6) In the *Select Components* dialog box, select or clear the desired components.
7) Click *Next*. Setup adds (if checked) or removes (if unchecked) the components.
8) Click *Finish* when setup completes.

5.12 Installing WebCenter Forms Recognition Service Packs / Service Updates

Interim updates, minor enhancements, and defect corrections for WebCenter Forms Recognition are typically released as a service pack. Service Packs for WebCenter Forms Recognition are self-extracting executables.

A Release Notes document detailing the product issues addressed and deployment instructions specific to that service pack accompanies each Service Pack release.

Generally, you can install the WebCenter Forms Recognition service packs as follows:

1) On the Windows Desktop, click *Start* → *Run*.
2) Browse to the location of the Service Pack executable.
3) Double click on the executable.
4) Follow the on-screen instructions.

Note: After installation of a service pack, launch the Register Web Server.bat in the WebCenter Forms Recognition Web Server\Bin folder and run the CdrReg.bat in the WebCenter Forms Recognition\Components\Cedar folder in order to register all of the new components. Only then, you will be able to open batches in Web Verifier*.*

The following steps are to be followed:

- Backup your project data before application of Service Updates or patches to your system.
- Backup the configuration of your IIS. To do this, open the IIS Manager under *Control Panel → Administration Tools → Internet Information Services*, right click on your local machine, and then select *All Tasks* and *Backup/Restore Configuration*.
- Before installation of a new patch, all RTS instances have to be stopped and all of the Forms Recognition applications have to be exited.
- After installation of a Web Verifier patch or Service Update, restart IIS. To do this, open the IIS Manager, right click on your local machine, go to *All Tasks*, and then click on *Restart IIS*.
- Perform standard sanity testing procedures.

5.12.1. Current patch level

If you want to check for the current version of the combined patch you are using, do the following:

1. Check the file version for the “Brainware.Verifier.WebClient.dll” in \WebCenter Forms Recognition\bin directory.
2. Check the highest file version of the “Cdr”*.dll” in \Components\Cedar and “Dst*.dll/exe in \WebCenter Forms Recognition\bin.

The highest of the version number is the installed patch.

5.13 Password Encryption for Database Connection Strings in Core Config Files

The application architecture of WebCenter Forms Recognition makes it very important to be able to hide sensitive security information, such as DB access password, stored in WebCenter Forms Recognition or custom project configuration files.

Password encryption is optional and configuration files with unencrypted passwords will still work with no issues.

Below are the steps to encrypt the database connection password for the core WebCenter Forms Recognition *.config files:

1. Open one of the WebCenter Forms Recognition config files you use, for example .\Application\bin\DstDsr.exe.config in a text editor.
2. Locate the connection string and the password part of the string, example:

```
<connectionStrings>

    <add name="Entities"
connectionString="metadata=res://*/Entity.Entities.csdl|res://*/Entity.Entities.ssdl|res://*
/Entity.Entities.msl;provider=System.Data.SqlClient;provider connection string=&quot;Data
Source=MYSQLSRV;Initial Catalog=DatabaseName;Integrated Security=false;User ID=alexey;
Password=MyPassword;MultipleActiveResultSets=True&quot;"
providerName="System.Data.EntityClient" />

  </connectionStrings>
```

3. Modify the password, replacing it with any amount of star signs, example:

```
<connectionStrings>

    <add name="Entities"
connectionString="metadata=res://*/Entity.Entities.csdl|res://*/Entity.Entities.ssdl|res://*
/Entity.Entities.msl;provider=System.Data.SqlClient;provider connection string=&quot;Data
Source=MYSQLSRV;Initial Catalog=DatabaseName;Integrated Security=false;User ID=alexey;
Password=********;MultipleActiveResultSets=True&quot;"
providerName="System.Data.EntityClient" />

  </connectionStrings>
```

*Note: The number of * is not important.*

4. Run the .Oracle\WebCenter Forms Recognition\bin\DstCrypt.exe tool with the following arguments:

a. DstCrypt.exe /text "MyPassword" >> my_encrypted_password.txt

b. You could add the line above to a new .bat file created in Oracle\WebCenter Forms Recognition\bin\ directory and double click on it - this should produce a new file with the name "my_encrypted_password.txt" in the same directory where the executable is located.

5. Open the resulting text file:

a. It will contain a text like in the example below. Copy its red part that represents the encrypted password:

```
Text MyPassword encoded to
Y652CeXVdMtdNtbnBD2itCEmfFFyHf9IGsN2psi6svy/MsKp8nKUgv2P7M37uu5rNo3V7wkH5795A5z6WGox/KEm60l
6AG9flX+B5miOQg7iOgJCBqoHrsAbICHzm2EJbCkaMp1oUcvtP+8hpeJVMlBpD+QkfLlithUXINhWaCM=
```

6. Locate the "appSettings" section of your DstDsr.exe.config file and add the new "EncrPwd" key to this section, assigning the red encrypted sequence above to the value of the key. Example:

```
   <appSettings>

       <add key="EncrPwd"
Y652CeXVdMtdNtbnBD2itCEmfFFyHf9IGsN2psi6svy/MsKp8nKUgv2P7M37uu5rNo3V7wkH5795A5z6WGox/KEm60l
6AG9flX+B5miOQg7iOgJCBqoHrsAbICHzm2EJbCkaMp1oUcvtP+8hpeJVMlBpD+QkfLlithUXINhWaCM=

  </appSettings>
```

7. Save your DstDsr.exe.config file.

8. When required, apply steps 1-7 to the other core configuration files, which represent different applications. These are:

a. For Runtime Server application: .\Application\bin\DstHost.exe.config

b. For Learnset Manager tool: .\Application\bin\DstSlm.exe.config

c. For Designer application: .\Application\bin\DstDsr.exe.config

d. For Thick Verifier application: .\Application\bin\DstVer.exe.config

e. For Supervised Learning nomination feature of Web Verifier application: .\Application\bin\Brainware.System.Project.exe.config

f. For Web Verifier application: .\Application Web Server\web.config

Note: corrupted or incorrect encryption key or an incorrect password in the web.config file will entail a 'Login failed' error message when trying to open the Web Verifier application.

5.14 INI File Encryption

WebCenter Forms Recognition allows the user to encrypt a password within the open text INI file. RSA encryption is used which contains a public key and a private key.

Public Key: provides customer or PS integrated, for user who wants to encrypt text in INI file. It is distributed to PS teams and customer service for generating an encrypted passwords.

Example:

```
<RSAKeyValue><Modulus>vJ+W7SuXuvOrWVoy4tPrbfLCuoHElo750cpTuEzLPk6iz6bHAodPVgLFaOEK+XMMS2G5z+696
1vuQsDGUt+O1Ag1PiTXCa6rrAaeCaaDO4HI8Mmpw0OkUZEfCZpTTYCYQPfZ1gokwomF6VDSB9dlUS430IT0gctQY1b5iM4M
qT0=</Modulus><Exponent>AQAB</Exponent></RSAKeyValue>
```

Private Key: held by project owner/ developer only.

Example:

```
<RSAKeyValue><Modulus>vJ+W7SuXuvOrWVoy4tPrbfLCuoHElo750cpTuEzLPk6iz6bHAodPVgLFaOEK+XMMS2G5z+696
1vuQsDGUt+O1Ag1PiTXCa6rrAaeCaaDO4HI8Mmpw0OkUZEfCZpTTYCYQPfZ1gokwomF6VDSB9dlUS430IT0gctQY1b5iM4M
qT0=</Modulus><Exponent>AQAB</Exponent><P>8SRHEvT5Bn2paRHSDR9yCQb7WGYE9PbeHzuqwH6iWa0LNYJrSrhhU
eCEpwlPLQWQq10KmMZgG0+Br4nuBMmMHQ==</P><Q>yD7l9fjB/MJWYaV3LcEzY286Q+Xvo74i6THvHkKqB1NKYGcN9xF9d
8XbiUQNgBZ/4F02T6mFeYDO32KFVRXHoQ==</Q><DP>nRDTFn7nwRmSgfRwi8minkyk5DQ3IFO35EIZ+x3Ao4Z52ZWkStwD
z6/c12vR3XJVg7irkU0NBlzoDK1bklSw5Q==</DP><DQ>B3xieGmORva05/2ZkPpSA3ubAALOjJ6FC5a0S7tOQ+vXMfdoTD
45JIsfA+ipYIp2yVpyt1OtC7fHBA7Y0S95QQ==</DQ><InverseQ>4S1xqlXK9f1rawGCbFWOVp6lz1fCoQ8RfyDE87/G/p
UilHRJV2acBAcngY3c/MRMKrXQb8lx99k7dENUYc8ywQ==</InverseQ><D>KAL6cwkCQKgbuvKFRNSLZmFOqV2JpB5kI/p
1U+0GWAs6Qi4wnPqy+53O3naOa2faPctXLSKJqvlvSz21VDMUCsyphvOSxBtc1cZHJp4ueQPA7u+qrIJaDY1RhlAVoqNfCJ
FX6+McVJ+I/X+mZOCtdUaCuAoNn014UYOaMujYDQE

=</D></RSAKeyValue>
```

Below is the new connection string parameter:

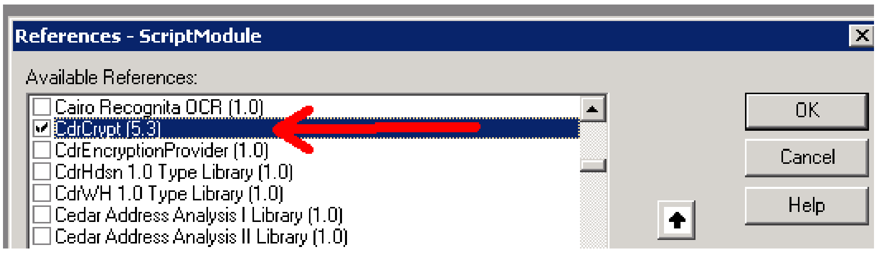
```
SQL_VL_01_ConnectionString=Provider=SQLOLEDB.1;Persist  Security  Info=True;User  ID=sa;Initial
Catalog=MyData;Data Source=10.4.0.19

SQL_VL_01_ConnectionPassword=MyEncryptedPassword
```

5.14.1. INI File Encryption for Project Developer

The idea of coding is to locate the code that calls Database Connection from the INI file, so that you can read the new line in the INI file with an encrypted line text. The password then can be decrypted by using a Private Key. At last, you append the password to the end of the Connection String in the INI file.

As a project developer, you can select the CdrCrypt ScriptModule in the Reference section of Project File Script Page.



References - ScriptModule

Available References:

- ☐ Cairo Recognita OCR (1.0)
- ☑ CdrCrypt (5.3)
- ☐ CdrEncryptionProvider (1.0)
- ☐ CdrHdsn 1.0 Type Library (1.0)
- ☐ CdrWH 1.0 Type Library (1.0)
- ☐ Cedar Address Analysis I Library (1.0)
- ☐ Cedar Address Analysis II Library (1.0)

Figure 5-3: Script Module References

Example script of the encrypted password:

```
  Dim theCedarCryptographyHelper As New CdrCrypt.RSACodecInt

  Dim strEncryptedPassword As String

  Dim strOpenPassword As String

  Dim strPrivateKey As String

  strPrivateKey =
"<RSAKeyValue><Modulus>vJ+W7SuXuvOrWVoy4tPrbfLCuoHElo750cpTuEzLPk6iz6bHAodPVgLFaOEK+XMMS2G5z+69
61vuQsDGUt+O1Ag1PiTXCa6rrAaeCaaDO4HI8Mmpw0OkUZEfCZpTTYCYQPfZ1gokwomF6VDSB9dlUS430IT0gctQY1b5iM4
MqT0=</Modulus><Exponent>AQAB</Exponent><P>8SRHEvT5Bn2paRHSDR9yCQb7WGYE9PbeHzuqwH6iWa0LNYJrSrhh
UeCEpwlPLQWQq10KmMZgG0+Br4nuBMmMHQ==</P><Q>yD7l9fjB/MJWYaV3LcEzY286Q+Xvo74i6THvHkKqB1NKYGcN9xF9
d8XbiUQNgBZ/4F02T6mFeYDO32KFVRXHoQ==</Q><DP>nRDTFn7nwRmSgfRwi8minkyk5DQ3IFO35EIZ+x3Ao4Z52ZWkStw
Dz6/c12vR3XJVg7irkU0NBlzoDK1bklSw5Q==</DP><DQ>B3xieGmORva05/2ZkPpSA3ubAALOjJ6FC5a0S7tOQ+vXMfdoT
D45JIsfA+ipYIp2yVpyt1OtC7fHBA7Y0S95QQ==</DQ><InverseQ>4S1xqlXK9f1rawGCbFWOVp6lz1fCoQ8RfyDE87/G/
pUilHRJV2acBAcngY3c/MRMKrXQb8lx99k7dENUYc8ywQ==</InverseQ><D>KAL6cwkCQKgbuvKFRNSLZmFOqV2JpB5kI/
p1U+0GWAs6Qi4wnPqy+53O3naOa2faPctXLSKJqvlvSz21VDMUCsyphvOSxBtc1cZHJp4ueQPA7u+qrIJaDY1RhlAVoqNfC
JFX6+McVJ+I/X+mZOCtdUaCuAoNn014UYOaMujYDQE=</D></RSAKeyValue>"

  strEncryptedPassword = DicVal("01" & "ConnectionPassword", "SQL")

  If Len(strEncryptedPassword) > 0 Then

    strOpenPassword = theCedarCryptographyHelper.Decode(strEncryptedPassword, strPrivateKey)

  End If
  If Len(strOpenPassword) > 0 Then
    strConnection = strConnection + ";Password=" + strOpenPassword
  End If
```

5.14.2. INI File Encryption for Integrator

As an integrator, you simply need to add the encrypted customer password, and encrypt the password similarly to Config files.

Run the following command in the Oracle\WebCenter Forms Recognition\bin folder:

```
DstCrypt.exe /text “MyPassword" /key
"<RSAKeyValue><Modulus>vJ+W7SuXuvOrWVoy4tPrbfLCuoHElo750cpTuEzLPk6iz6bHAodPVgLFaOEK+XMMS2G5z+69
61vuQsDGUt+O1Ag1PiTXCa6rrAaeCaaDO4HI8Mmpw0OkUZEfCZpTTYCYQPfZ1gokwomF6VDSB9dlUS430IT0gctQY1b5iM4
MqT0=</Modulus><Exponent>AQAB</Exponent></RSAKeyValue>" >> my_encrypted_custom_password.txt
```

The my_encrypted_custom_password.txt will now contain the encrypted text string for the password.

And then, add the encrypted password to the ConnectionPassword INI tag.

```
SQL_VL_01_ConnectionPassword=puejB5SQNCFGgwe6MRoWc1G1y7qX8xSAhgUZjhN6JolhYdKIxla7vLMU4bYmG9V3Ay
xualp/ObgXRqnSAmGsGF1FPZXktRmf58SXbnCDXmYrYgp8eS3IaqiLUPrhTiRCvfr8ZsMtK+3usmahfxpESUOQ7MZf36suW
V4V3sBf9Xw=
```

5.15 Silent Installations

A Silent Install mode is provided for situations where the same configuration of WebCenter Forms Recognition is to be installed on several machines, for example, Verifier workstations. The use of a configuration file removes the necessity to go through the installation dialog on each machine.

5.15.1. Silent Install.ini

The configuration settings for the silent installation are read from the “Silent Install.ini” file in the WebCenter Forms Recognition installation directory. The directory contains an example file, which must be edited before performing a silent installation.

The file contains seven sections – General, Applications, OCR Engines, Additional, AutoServiceUpdate, Database Configuration, and DB Credentials.

It’s allowed to delete single entries or complete sections.

However, it's not allowed to use options without the section name. If any information is deleted from the "Silent Install.ini" file, the Setup uses the DEFAULT values as described.

Name	Description
[General]	Determines how and where WebCenter Forms Recognition is to be installed.
Path =	Indicates where the application should be installed. The pathname should not have a final backslash. Example: Path = C:\Program Files\your company name.
MoveComponentsIfRequired =	If an older version of the application is installed, this indicates whether to use the existing component folder or whether to move the old components into the new directory prior to installation. 0: Use existing component folder. 1: Move components to the new path.
CreateDeskTopIcons =	0: Don’t create desktop shortcuts. 1: Create desktop shortcuts.
InstallWibuKey =	0: Skip Wibukey driver installation. 1: Install Wibukey drivers.
StopIfDotNetIsNotFound = #	0: If .Net Framework 3.5 SP1 is not found on the system the installation proceeds. The Features (WebVerifier, Database Connection...) will not be installed. 1 (DEFAULT): If .Net Framework 3.5 SP1 is not found on the system the installation will be aborted.
[Applications]	Defines which applications are to be installed. Note that it is permissible to skip all applications if, for example, only the extraction components are to be installed.
Designer =	0: Skip installation of the Designer application. 1: Install the Designer application.
Verifier =	0: Skip installation of the Verifier application. 1: Install the Verifier application.
Runtime Service =	0: Skip installation of the Runtime Server application. 1: Install the Runtime Server application.
Web Verifier=	0: To skip installation of WebVerifier application (Thin Client) 1 (DEFAULT): Install WebVerifier application (See also option StopIfDotNetIsNotFound)
[OCR Engines]	Defines which OCR engines are to be installed. It is permissible to skip all the engines.
FineReader8.1 =	0: Skip installation of ABBYY FineReader 8.1. 1: Install ABBYY FineReader 8.1.

Name	Description
FineReader10 =	0: Skip installation of ABBYY FineReader 10. 1: Install ABBYY FineReader 10.
Kadmos5 =	0: Skip installation of Kadmos 5 engine. 1: Install Kadmos 5 engine.
Recognita =	0: Skip installation of Recognita engine. 1: Install Recognita engine.
QualitySoft	0: Skip installation of QualitySoft engine. 1: Install QualitySoft engine.
Cleqs =	0: Skip installation of Cleqs engine. 1: Install Cleqs engine.
[Additional]	Additional files to install.
Demo Files =	0: Skip installation of the demo project files. 1: Install demo project files.
[AutoServiceUpdate]	Defines the installation of automatic ServiceUpdate (will be skipped if ForDesigner and ForVerifier are skipped)
ForDesigner =	0 (DEFAULT): Skip definition of ServiceUpdate for Designer Application. 1: Defines Shortcut for Designer start with automatic ServiceUpdate
ForVerifier = #	0 (DEFAULT): Skip definition of ServiceUpdate for Verifier Application. 1: Defines Shortcut for Verifier start with automatic ServiceUpdate.
NetworkUpdateFolder = "*"	Path where automatic ServiceUpdate looks for Updates. (DEFAULT empty string)
[Database Configuration]	Configures Existing DatabaseServer (See also option StopIfDotNetIsNotFound).
DBServerType = #	1: SQL Server database will be configured. 2: Oracle Server database will be configured. 3 (DEFAULT): No database will be configured.
If there is any wrong information for the following options DBServerType will be set to 3	
UseDBConfIniFile = "*"	Text file name that contains Database Connection String. If this option is empty, credentials will be taken from [DB Credentials] section. If there is neither a config file nor a [DB Credentials] section, DBServerType will be set to 3 (no database) internally. (DEFAULT empty string).

Name	Description
[DB Credentials]	This section can be used instead of a config file (See Option UseDBConfIniFile). (DEFAULT database cofiguration will be skipped, if option UseDBConfIniFile is not set).
Only for SQL Server Usage (See Option DBServerType and UseDBConfIniFile)	
SQLServerWindowsAuthent =	0 (DEFAULT): No Windows Authentication will be used for DBA. 1: Windows Authentification will be used for DBA.
SQSqlerverAdminUser = "*"	DBA account name (See also option SQLServerWindowsAuthent) (DEFAULT empty string).
SQLServerAdminPassword = "*"	DBA account password (See also option SQLServerWindowsAuthent) (DEFAULT empty string).
For both Database Server Types (See Option DBServerType and UseDBConfIniFile)	
DBUserWindowsAuthent = #	0 (DEFAULT): No Windows Authentication will be used for DB user. 1: Windows Authentification will be used for DB user.
DBUserName = "*"	DB user account name (See also option DBUserWindowsAuthent) (DEFAULT empty string).
DBUserPassword = "*"	DB user account password (See also option DBUserWindowsAuthent) (DEFAULT empty string).
DatabaseServerPath = "*"	Name of the database. Ususal it is build like <MachineName>\<InstanceName> (DEFAULT empty string).

Table 5-2: Options for "silent install.ini"

An example "Silent Install.ini" INI-file is available in the root setup directory.

5.15.2. Automated Distribution of Service Updates on Verifier Workstations

Silent Installation can also be used to install service packs and service updates automatically on Verifier workstations when updates become available in a pre-defined network folder by running a batch file with the following content:

```
Call “Silently Install Latest Service Update.bat”
Call “C:\Program Files\Oracle\WebCenter Forms Recognition\DstVer.exe”
```

5.16 Preparing Internet Information Server (post install)

One of the preconditions for working with WebCenter Forms Recognition Web Verifier is the installation of the Internet Information Server. Windows 2003 Server works with IIS 6.0, Windows 2008 Server with IIS 7.0.

Perform the installation of the appropriate IIS application version. Please use the following links for more information:

- For Windows 2003 Server and IIS 6.0

http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/750d3137-462c-491d-b6c7-5f370d7f26cd.mspx?mfr=true

- For Windows Server 2008 or Windows Server 2008 R2 and IIS 7.0/IIS 7.5

http://learn.iis.net/page.aspx/29/installing-iis-7-on-windows-server-2008-or-windows-server-2008-r2/

5.16.1. Configuring IIS 6.0

The Internet Information Server is used for executing the WebCenter Forms Recognition Web-Verifier. The IIS configuration is presented below.

- Run IIS manager (*Start → Control Panel → Administrative tools – Internet Information Services*)
- Extend *Web Sites*.
- Right click on *Default Web Site* node, then choose *New → Virtual Directory*

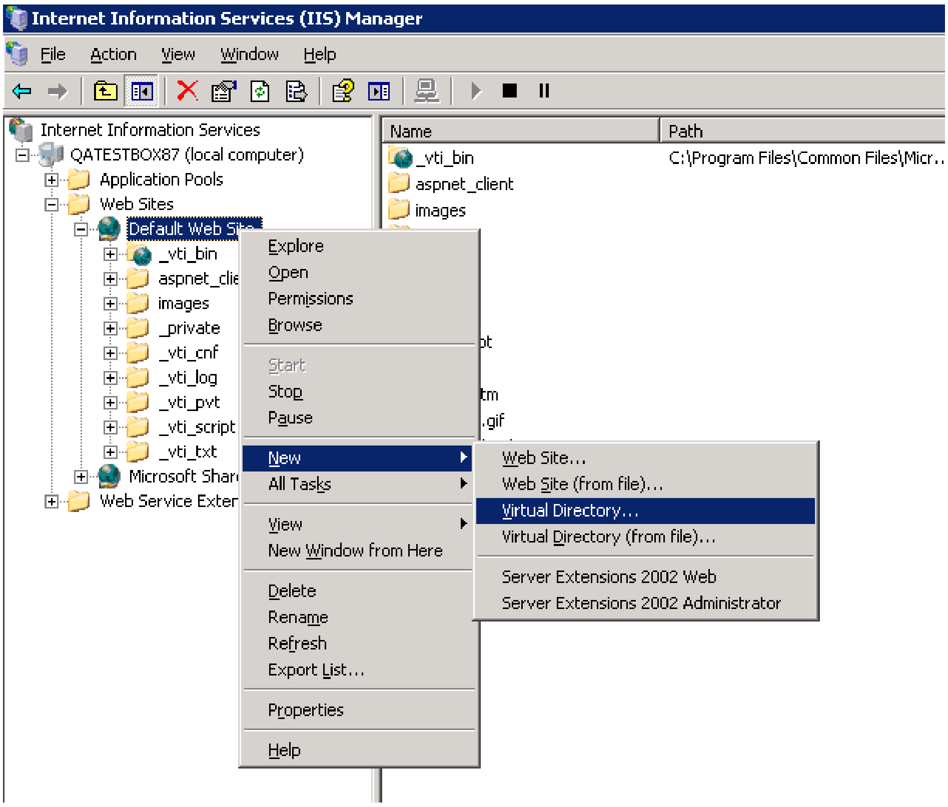
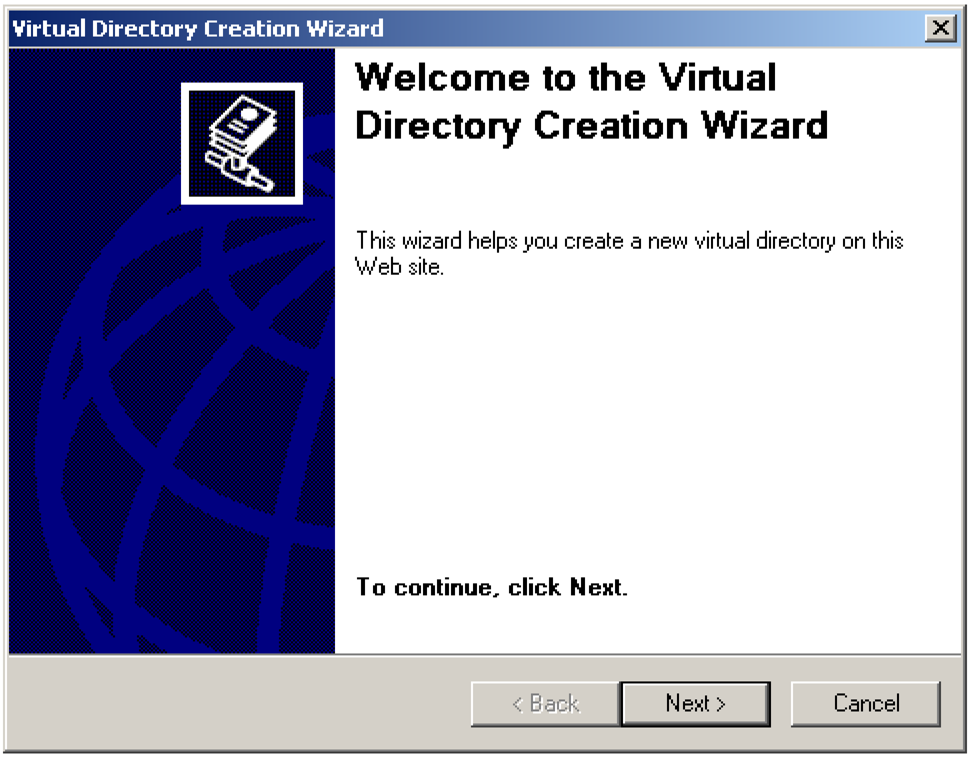


Figure 5-4: IIS 6.0 manager

- In the dialog window click *Next*.



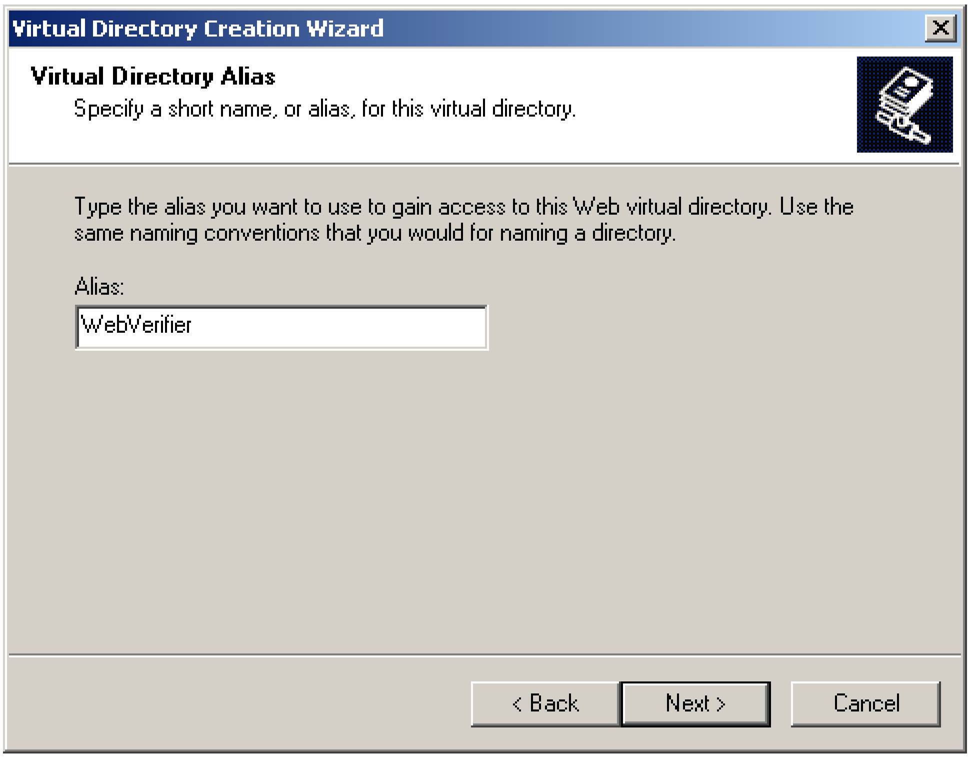
Welcome to the Virtual Directory Creation Wizard

This wizard helps you create a new virtual directory on this Web site.

To continue, click Next.

Figure 5-5: Virtual Directory Creation Wizard

- Type in the Alias you want to use to gain access to this Web virtual directory. Click *Next*.



Virtual Directory Alias

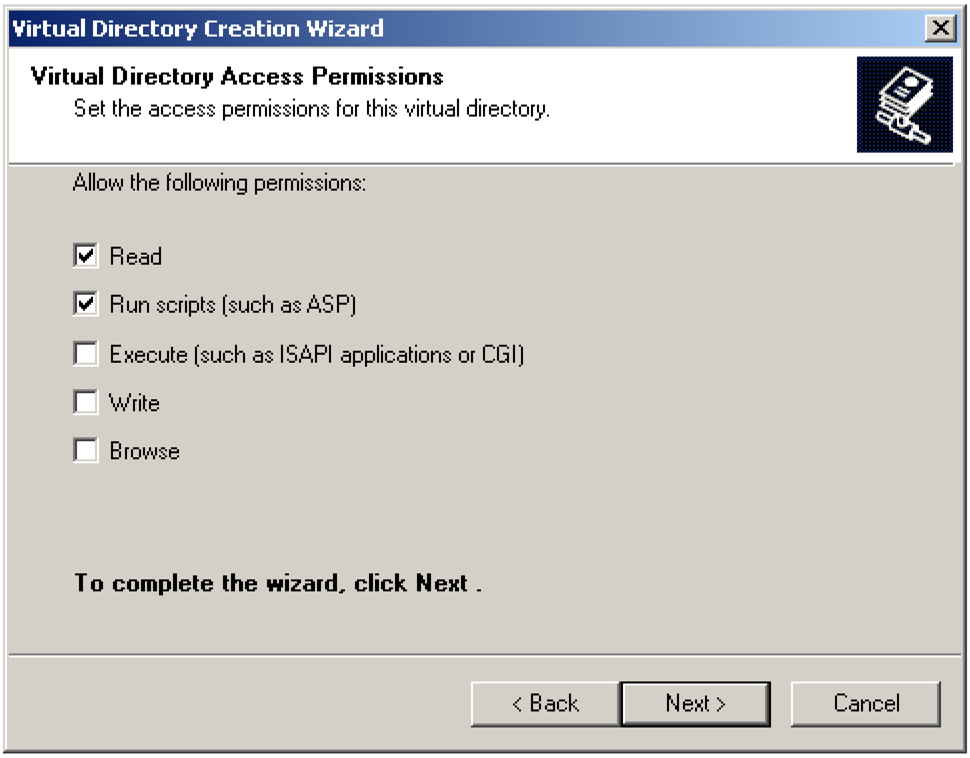
Specify a short name, or alias, for this virtual directory.

Type the alias you want to use to gain access to this Web virtual directory. Use the same naming conventions that you would for naming a directory.

Alias: WebVerifier

Figure 5-6: Alias for the Web virtual directory

- Select the path to the directory with the installed WebCenter Forms Recognition Web Server and click *Next*.
- Set the permissions as shown in the screenshot below. Click *Next*.



Virtual Directory Creation Wizard

Virtual Directory Access Permissions

Set the access permissions for this virtual directory.

Allow the following permissions:

☑ Read

☑ Run scripts (such as ASP)

□ Execute (such as ISAPI applications or CGI)

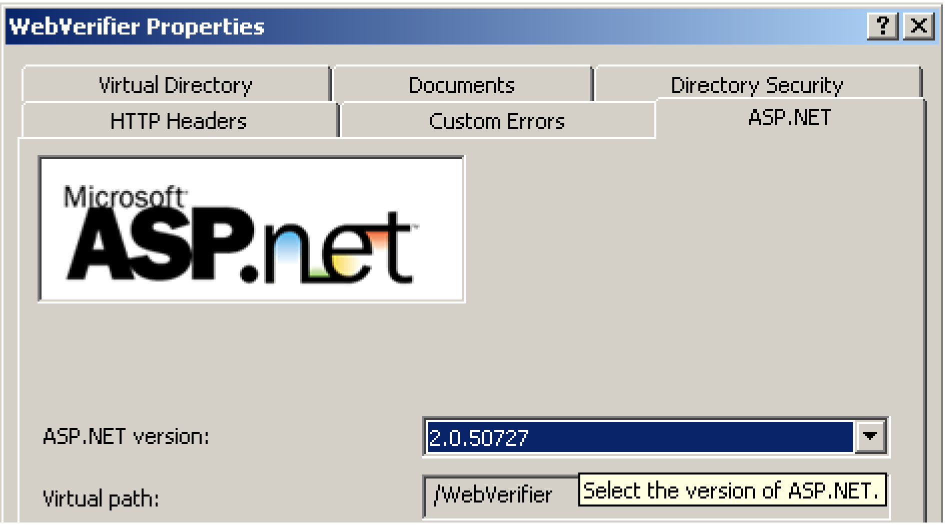
□ Write

□ Browse

To complete the wizard, click Next .

Figure 5-7: Virtual Directory Access Permissions

- Press *Finish*.
- Right click on the Web Verifier node then select *Properties*.
- In the dialog window, open the *ASP.NET* tab.
- Check the ASP.net version. If it is not a v.2.0 – set it to v.2.0.



WebVerifier Properties

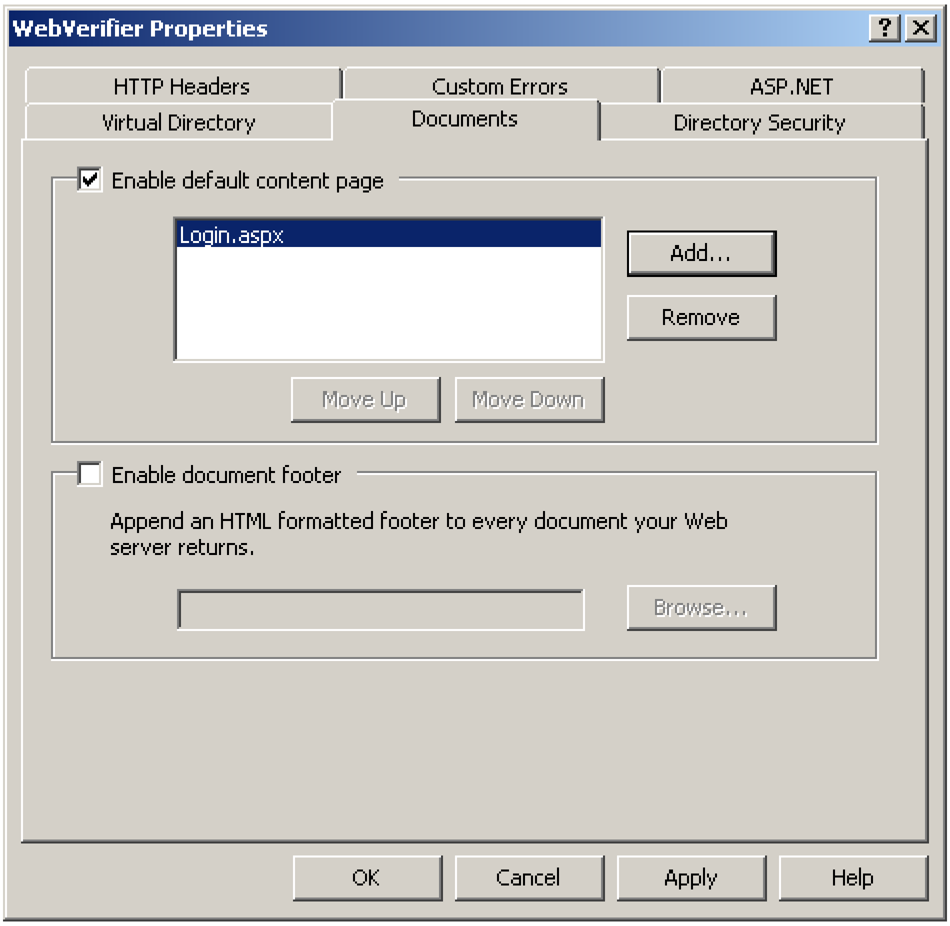
ASP.NET version: 2.0.50727

Virtual path: /WebVerifier

Select the version of ASP.NET.

Figure 5-8: Setting the ASP.net version number

- Select the *Documents* tab. Remove all default content pages, and add Login.aspx to the list.



☑ Enable default content page

Login.aspx

□ Enable document footer

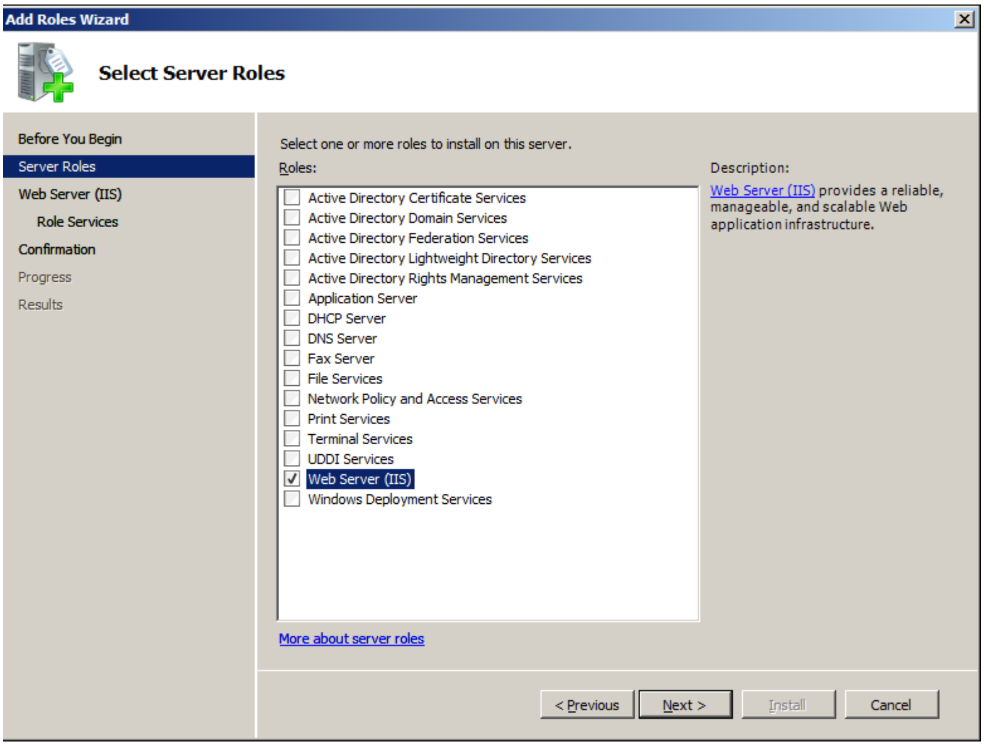
Append an HTML formatted footer to every document your Web server returns.

Figure 5-9: Documents tab – setting Login.aspx as default content page

- Click *OK*.
- Right-click the Web Verifier node and select New, and then click Virtual Directory.
- The Virtual Directory Creation Wizard appears.
- Click Next.
- In the Alias box, type “WL” as the name for the virtual directory.
- In the Path box, type or browse to the physical directory in which the virtual directory resides, which is the Components\Cedar\WL folder.
- Complete the Virtual Directory Creation wizard.
- The WebCenter Forms Recognition Web Verifier application will be accessible by the address http://localhost/WebVerifier/login.aspx

5.16.2. Configuring IIS 7.0

- Run Server Manager (*Start → Administrative tools → Server Manager*)
- Extend the Roles directory.
- Click *Add Roles*.
- Select *Web Server (IIS)*.
- You will be asked to install other required features.
- Click *Add Required Features*.
- Now you will be able to select the Server Roles.



Select Server Roles

Select one or more roles to install on this server.

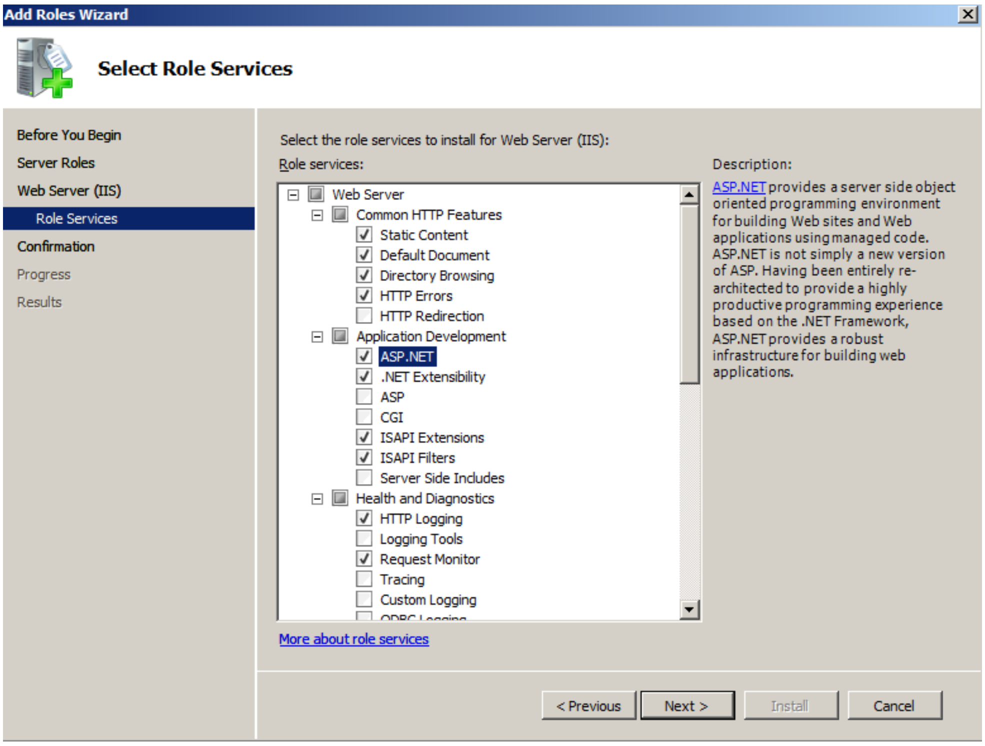
Roles:

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- □ File Services
- □ Network Policy and Access Services
- □ Print Services
- □ Terminal Services
- □ UDDI Services
- ☑ Web Server (IIS)
- □ Windows Deployment Services

Description:
Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Figure 5-10: Selecting Server Roles

- Click *Next*.
- Continue by clicking *Next*
- Select the Role Services as follows:



Select Role Services

Select the role services to install for Web Server (IIS):

Role services:

- ▣ Web Server
  - ▣ Common HTTP Features
    - ☑ Static Content
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - □ HTTP Redirection
  - ▣ Application Development
    - ☑ ASP.NET
    - ☑ .NET Extensibility
    - □ ASP
    - □ CGI
    - ☑ ISAPI Extensions
    - ☑ ISAPI Filters
    - □ Server Side Includes
  - ▣ Health and Diagnostics
    - ☑ HTTP Logging
    - □ Logging Tools
    - ☑ Request Monitor
    - □ Tracing
    - □ Custom Logging
    - □ ODBC Logging

Description:
ASP.NET provides a server side object oriented programming environment for building Web sites and Web applications using managed code. ASP.NET is not simply a new version of ASP. Having been entirely re-architected to provide a highly productive programming experience based on the .NET Framework, ASP.NET provides a robust infrastructure for building web applications.

Figure 5-11: Complete selection for role services

- Confirm by clicking *Next*.

- Click *Install* to install the selected roles, role services, and features.

- Check the *Result* overview and finish by clicking on *Close*.
- Now run IIS manager *(Start → Administrative tools → Internet Information Services (IIS) Manager*)

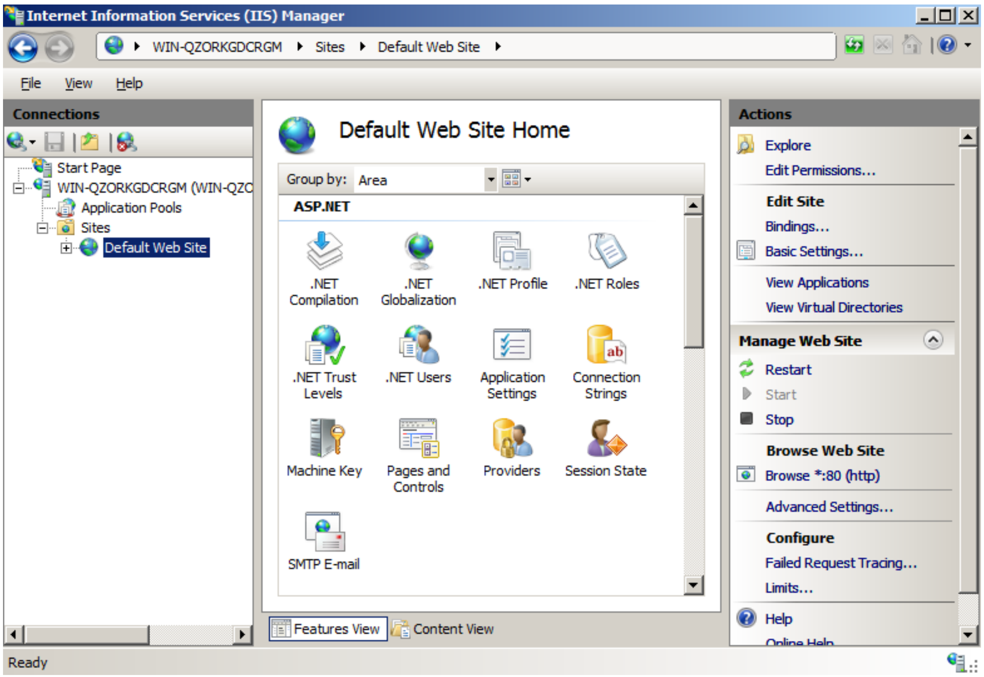
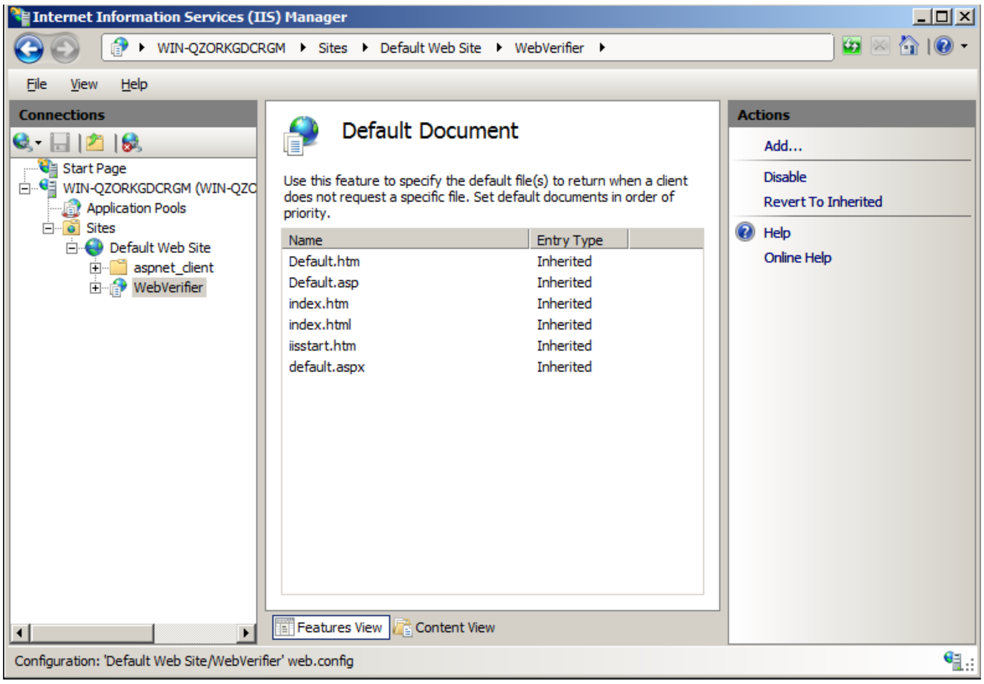


Figure 5-12: IIS Manager

- Right click *Default Web Site*.
- Select the *Add Application* menu item.
- In the dialog window, enter the Alias you want to use to gain access to this Web virtual directory, usually WebVerifier. Set the *Physical path* to the directory with the installed WebCenter Forms Recognition Web Server and then click *OK*.
- Double click the *Default Document* icon for the WebVerifier application.



Default Document

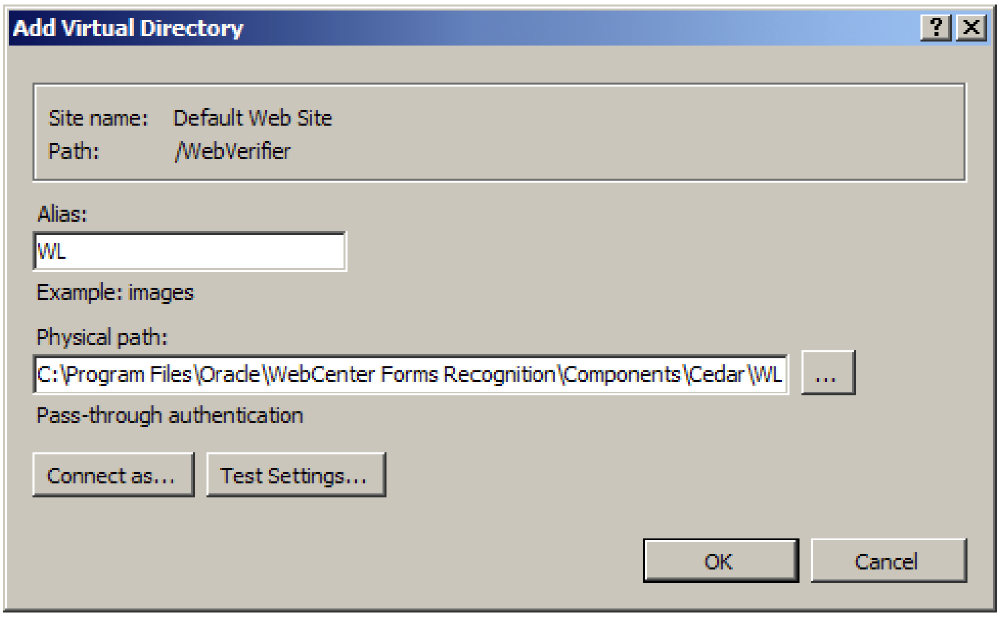
Use this feature to specify the default file(s) to return when a client does not request a specific file. Set default documents in order of priority.

Name	Entry Type
Default.htm	Inherited
Default.asp	Inherited
index.htm	Inherited
index.html	Inherited
iisstart.htm	Inherited
default.aspx	Inherited

Configuration: 'Default Web Site/WebVerifier' web.config

Figure 5-13: Setting the Default Document II

- Click *Add…* and add Login.aspx to the list.
- Right click on Web Verifier node, then choose Add Virtual Directory.
- In the dialog box, enter “WL” (without quotes) in the Alias field as the name for the virtual directory.
- Set the Physical Path field to the ..\Components\Cedar\WL subfolder of the WebCenter Forms Recognition installation directory.



Add Virtual Directory

Site name: Default Web Site
Path: /WebVerifier

Alias:
WL

Example: images

Physical path:
C:\Program Files\Oracle\WebCenter Forms Recognition\Components\Cedar\WL

Pass-through authentication

- Click OK.
- The WebCenter Forms Recognition Web Verifier application will be accessible by the address http://localhost/WebVerifier/login.aspx .

5.16.3. Windows 2008 and above

Disable DEP with following command:

* bcdedit.exe /set {current} nx AlwaysOff

Note: The server must be rebooted after this command has been applied.

5.16.4. Windows 2008 64bit R2

The following steps are required in order to configure IIS 7.5 for your operating system:

1. Create an application pool or change defaultAppPool with the following advanced properties:
   * Enable 32-bit applications = True
   * Managed pipeline mode = Integrated
   * Identity is set to NetworkService
2. Assign the Web Verifier application to this application pool so that the application can run under 32-bit mode.
3. Disable DEP with following command:
   * bcdedit.exe /set {current} nx AlwaysOff

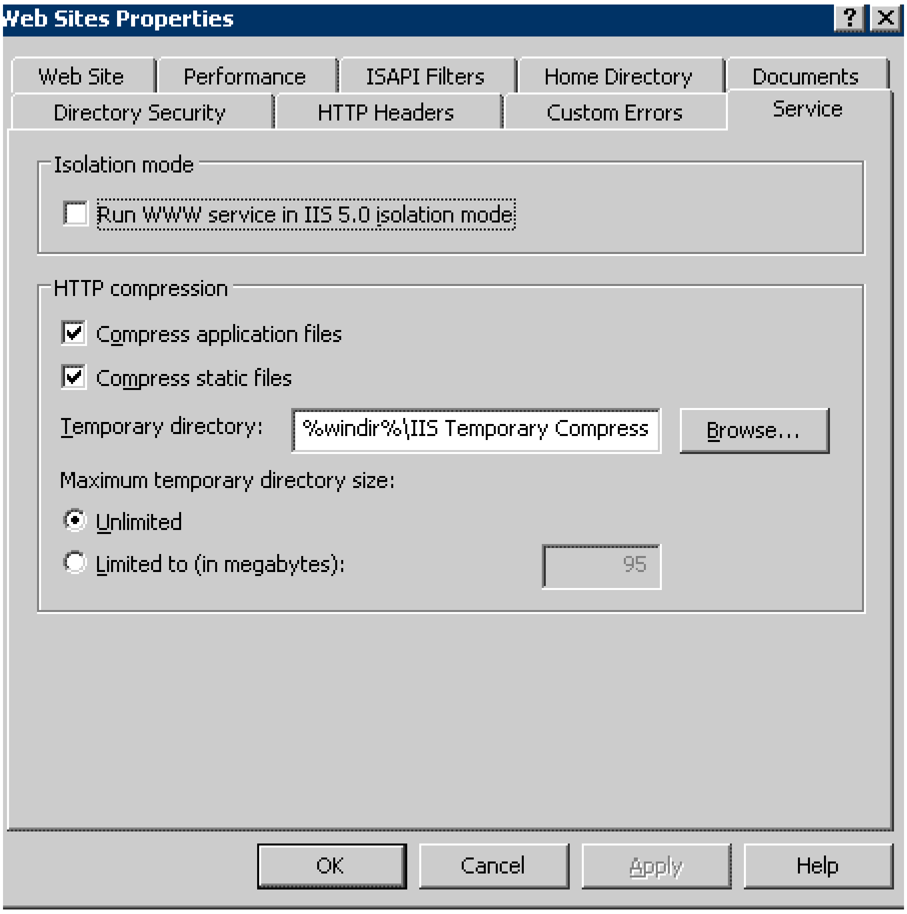
   Note: The server must be rebooted after this command has been applied.

5.16.5. Enabling HTTP Compression on your Windows 2003 Server

To more efficiently use available bandwidth, enable IIS HTTP compression. HTTP compression provides faster transmission time between compression-enabled browsers and

IIS. HTTP compression allows faster page serving to clients and lower server costs due to lowered bandwidth.

- Open up IIS and right click on *Web Sites* node, and go to *Properties*.
- Go to *Service* tab. (See figure below)



Isolation mode

□ Run WWW service in IIS 5.0 isolation mode

HTTP compression

☑ Compress application files

☑ Compress static files

Temporary directory: %windir%\IIS Temporary Compress

Maximum temporary directory size:

● Unlimited

○ Limited to (in megabytes): 95

Figure 5-14: The Web Sites Properties dialog box

- Set up values as shown in figure above.

Compress application files: Check this to compress application files. It works only if you have *Compress static files* checked.

Compress static files: Check this to compress static files. Selecting this option will activate the Temporary directory text box.

Temporary directory: You can leave this at the default, which is %windir%\IIS Temporary Compressed Files, or set it to a custom folder. This is where temporary compressed static files will be stored.

Maximum temporary directory size: This option enables you to set the maximum size of the temporary directory. Once the size limit is reached, newly added files will replace the oldest files.

- Next, go to *Web Service Extensions*. Right click on the right panel, and then click *Add a new Web service extension*. You can enter any name for the extension, but HTTP Compression is recommended.
- Click *Add…*, Choose *C:\WINDOWS\system32\inetsrv\gzip.dll*, and then click *OK*.
- Check *Set extension status to Allowed box*, and then click *OK*.

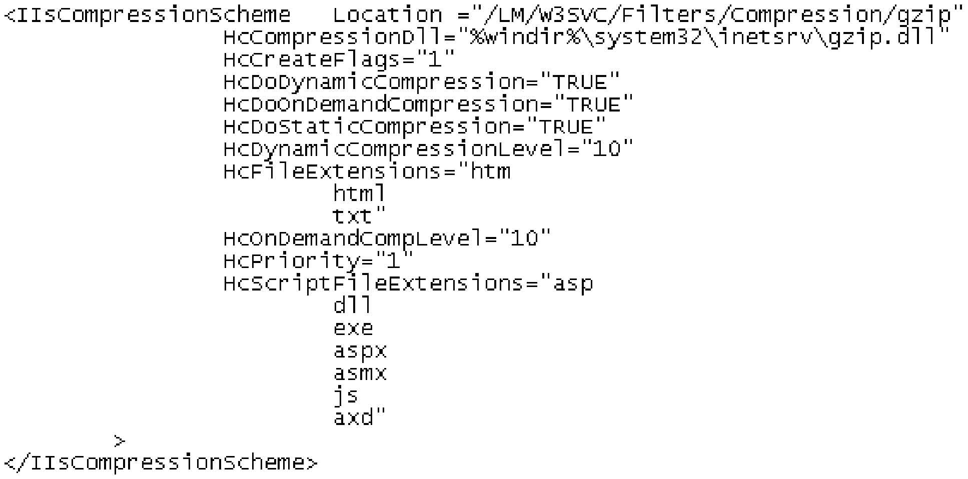
5.16.6. IIS 6.0 Metabase Configuration - MetaBase.xml

- Open Windows Explorer and go to *C:\Windows\System32\inetsrv*.
- Find MetaBase.xml and make a backup copy.

- Now open up MetaBase.xml in a text editor. Find the <IIsCompressionScheme/> section. Be careful, there are two sections here: one for **deflate** and one for **gzip**. Select the section for **gzip**. (See Figure 5-15) The Location attribute of this element will have the following value:
  Location ="/LM/W3SVC/Filters/Compression/gzip". Look for the HcScriptFileExtensions section. As default, it should contain: asp, dll, and exe. This is where you add any extensions you want to be compressed for dynamic files. For instance, you can add the extension aspx.

Note: Use a list format for the file extensions as in the sample below using a new line for each extension and indenting them using tabs.

For Web-Verifier this section should look as follows:



```
<IIsCompressionScheme   Location ="/LM/W3SVC/Filters/Compression/gzip"
                HcCompressionDll="%windir%\system32\inetsrv\gzip.dll"
                HcCreateFlags="1"
                HcDoDynamicCompression="TRUE"
                HcDoOnDemandCompression="TRUE"
                HcDoStaticCompression="TRUE"
                HcDynamicCompressionLevel="10"
                HcFileExtensions="htm
                        html
                        txt"
                HcOnDemandCompLevel="10"
                HcPriority="1"
                HcScriptFileExtensions="asp
                        dll
                        exe
                        aspx
                        asmx
                        js
                        axd"
        >
</IIsCompressionScheme>
```

Figure 5-15: MetaBase.xml

- Save this document by opening IIS and right click on the top node, *Internet Information Services*, and then check *Enable Direct Metabase Edit*.
- The final step is to exit IIS and to restart by right clicking *Internet Information Services* node, and then click *All Tasks, Restart IIS*.

6 Configuring Application

6.1 Configuring Application

There are some main configuration parameters to be accounted for. See 0 for more information**.**

6.1.1. Configuring WebCenter Forms Recognition Database connection string

- Open the application configuration file (WebCenter Forms Recognition Web Server\web.config)
- Find the following string:

```
<connectionStrings>

<add name="Entities"
connectionString="metadata=res://*/Entity.Entites.csdl|res://*/Entity.Entites.ssdl|res://*/
Entity.Entites.msl;provider=System.Data.SqlClient;provider connection string=&quot;Data
Source=NEO\SQLSERVER2005;Initial Catalog=Oracle_verifier_work;Integrated
Security=false;User ID=developer; Password=123456;MultipleActiveResultSets=True&quot;"
providerName="System.Data.EntityClient" />
```

- Modify the connection string in accordance with your database settings.
- Replace the connection string within the Brainware.System.Project.exe config file by the one configured within the web.config file.

Note: These two connection string entries must be identical in order to assure the availability of all Web Verifier functionalities associated with the Knowledge base.

6.1.2. Setting path to license file

- Open the application configuration file (Oracle\Forms Recognition Web Server\web.config)
- Find the following string:

```
<project.controller>

<project licensePath="{app_root}\License\Runtime.lic" ...

</project.controller>
```

- Modify the `licensePath` value in accordance with the location of your license file.

6.1.3. Enable HTTP compression for IIS 6.0 and IIS 7.0

In order to enhance your application performance and to save server costs, it is recommended you enable HTTP compression in the context of the Internet Information Services.

Please use the following links for detailed information.

For IIS 6.0:

http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/d52ff289-94d3-4085-bc4e-24eb4f312e0e.mspx?mfr=true

For IIS 7.0:

http://technet.microsoft.com/en-us/library/cc771003.aspx

6.2 Server Security Configuration

6.2.1. Registering COM components

After applying a patch, locate and run the 'Register Web Server.bat' as administrator. It is located in the WebCenter Forms Recognition Web Server\bin\ folder. For registering this component:

- Right click on the Register Web Server.bat file.
- Select *Open* from the context menu.

6.2.1.1. Preparing the User Context

It is necessary for the user of the user context in which the Web Verifier is running in IIS to have the proper rights to access the database. By default, the Web Verifier runs under the NETWORK SERVICE user context, hence the same should be allowed to access the database.

If you select *Windows Authentication* during the installation of WebCenter Forms Recognition, you will need to add the domain username to the SQL Server DB additionally to the NT AUTHORITY\NETWORK SERVICE.

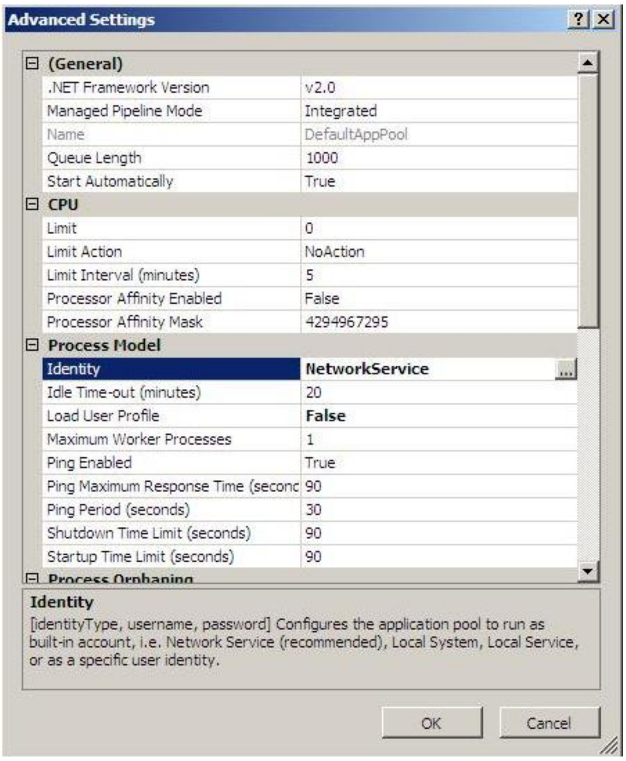
Steps to add NETWORK SERVICE to SQL server:

1. Open Microsoft SQL Server Management Studio.
2. Expand the local computer name, select *Security* → *Logins*.
3. Right click *Logins*, select *New Login*.
4. On *Login Properties*, under *General*, click *Search*. Enter NETWORK SERVICE and then click *Check Names*. Click *OK*.
5. Select *sysadmin* (*public* is selected by default) for Server Roles. Click *OK*.
6. The **NT AUTHORITY \NETWORK SERVICE** has been added to SQL server.

After adding Network Service to SQL server, make sure that the IIS is running under NT AUTHORITY \NETWORK SERVICE by opening the IIS Manager.

To open IIS Manager from *Start* menu:

1. Click *Start*, and then select *Control Panel*.
2. Select *Administrative Tools*, and then click *Internet Information Services (IIS) Manager*.
3. In the Connections panel, expand the server node and click *Application Pools.*
4. On *Application Pools*, select the application pool which you want to specify an identity, and then click *Advanced Settings* in the *Actions* panel.
5. For the identity property, the built-in account should be NetworkService.



Advanced Settings

(General)	
.NET Framework Version	v2.0
Managed Pipeline Mode	Integrated
Name	DefaultAppPool
Queue Length	1000
Start Automatically	True
CPU	
Limit	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Process Model	
Identity	**NetworkService**
Idle Time-out (minutes)	20
Load User Profile	**False**
Maximum Worker Processes	1
Ping Enabled	True
Ping Maximum Response Time (seconc	90
Ping Period (seconds)	30
Shutdown Time Limit (seconds)	90
Startup Time Limit (seconds)	90
Process Orphaning	

Identity
[identityType, username, password] Configures the application pool to run as built-in account, i.e. Network Service (recommended), Local System, Local Service, or as a specific user identity.

Figure 6-1: Identity.

6. If it does not contain NetworkService, click *Set…* to open the *Application Pool Identity* dialog box.

7. Select the Built-in account option and select NetworkService account from the list.

6.2.2. Setting Permissions for Oracle projects execution

All Oracle projects are located in a filesystem folder. The Web Verifier sources this path from the WebCenter Forms Recognition database. Oracle projects are loaded by the “Brainware.System.Project.exe” process. This process cannot load the projects until it has the appropriate permissions for the projects folder. In this case, it is necessary to grant permission to the “Network Service” Windows user for this folder by performing the following steps:

- Select the projects folder.
- Right click on the folder and select *Properties*.
- In the dialog window, select the *Security* tab.
- Add the *Network service* user to the list.

6.2.3. Encrypting sections with aspnet_regiis tool

If you want to protect the data stored in the configuration file perform the following steps:

Pre-configuring:

- Find the “Brainware.System.AppConfiguration.dll” file in the WebCenter Forms Recognition\bin\ directory.
- Register this assembly in the GAC using the

  gacutil -I Brainware.System.AppConfiguration.dll command.

Encryption of the web.config file:

- Use the **aspnet_regiis** command-line tool. This tool is located at: ***C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe***

- For encrypting a particular section of the configuration file, you can use the **-pe** option when executing the aspnet_regiis tool.

For example, for encryption of the connectionStrings section use:

aspnet_regiis -pe connectionStrings -app/MyApp

*Note: The **"-app"** option is used to specify the application's virtual path.*

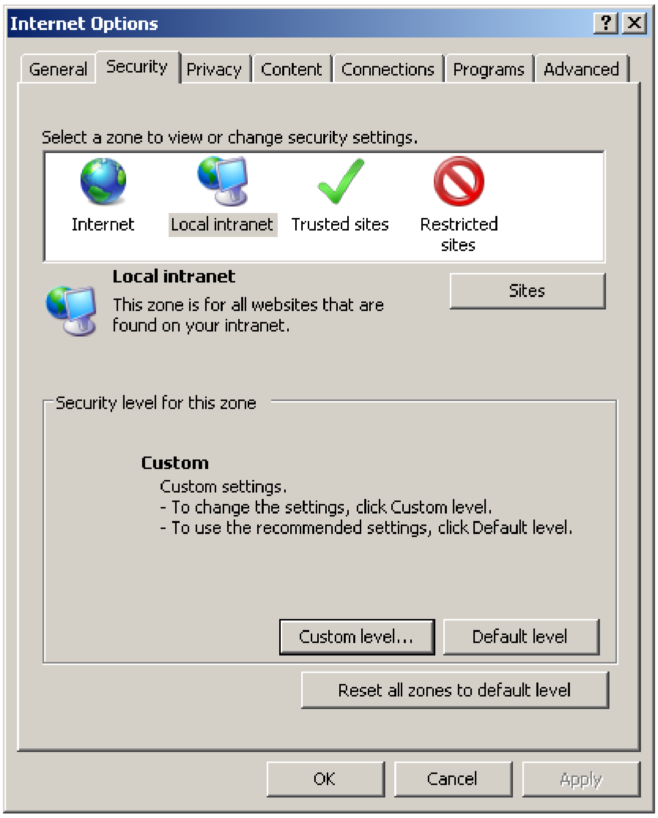
Decryption of the web.config file:

- For decryption of a configuration section, use the following command: **aspnet_regiis -pd connectionStrings -app/MyApp**

6.3 Client Security Configuration

This section describes security configuration for the client side.

- Open your Internet Browser. Select *Tools* → *Internet Options,* and then select the *Security* tab. Click *Custom Level…*



Select a zone to view or change security settings.

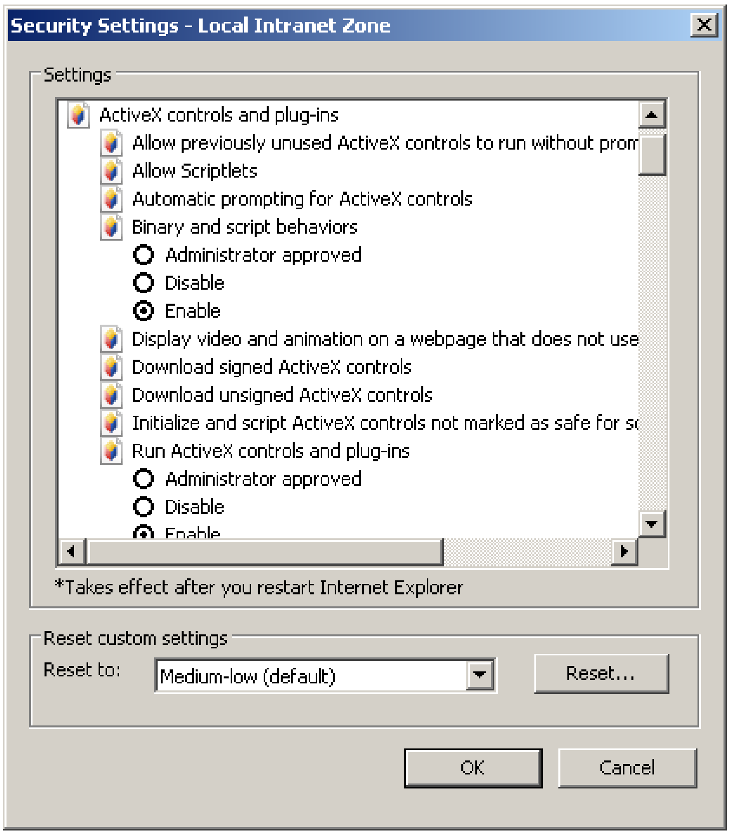
Local intranet
This zone is for all websites that are found on your intranet.

Security level for this zone

Custom
Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

Figure 6-2: Internet Browser – Security tab

- Check for the configuration settings (See the screenshots below)
- ActiveX controls and plug-ins:
- *Binary and script behaviors* setting should be *Enable.*
- *Run ActiveX controls and plug-ins* setting should be *Enable*.



Security Settings - Local Intranet Zone

Settings

ActiveX controls and plug-ins
- Allow previously unused ActiveX controls to run without prom
- Allow Scriptlets
- Automatic prompting for ActiveX controls
- Binary and script behaviors
  - ○ Administrator approved
  - ○ Disable
  - ● Enable
- Display video and animation on a webpage that does not use
- Download signed ActiveX controls
- Download unsigned ActiveX controls
- Initialize and script ActiveX controls not marked as safe for sc
- Run ActiveX controls and plug-ins
  - ○ Administrator approved
  - ○ Disable
  - ● Enable

*Takes effect after you restart Internet Explorer

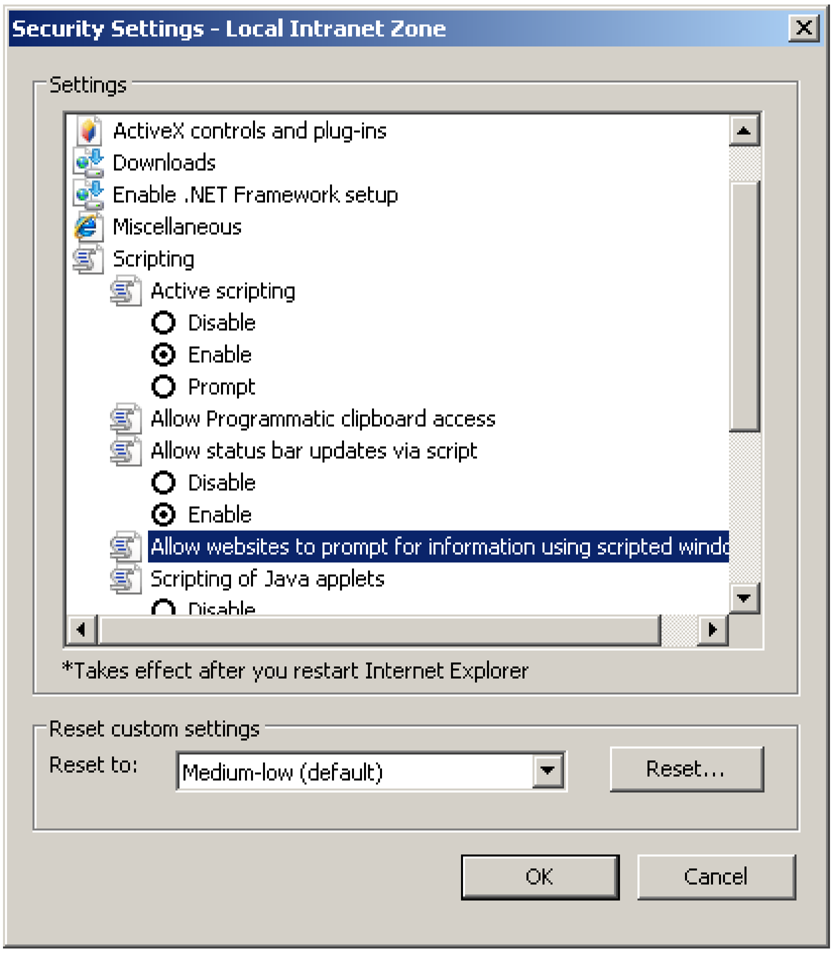
Reset custom settings

Reset to: Medium-low (default)

Figure 6-3: Custom level configuration settings – ActiveX controls and plug-ins

- Scripting
- *Active scripting* setting should be *Enable*.
- *Allow status bar updates via script* setting should be *Enable*.

Note: Only if allowing status bar updating via script is enabled, will the information on batches, documents, current filters and page number be displayed.



Security Settings - Local Intranet Zone

Settings

ActiveX controls and plug-ins
Downloads
Enable .NET Framework setup
Miscellaneous
Scripting
Active scripting
○ Disable
● Enable
○ Prompt
Allow Programmatic clipboard access
Allow status bar updates via script
○ Disable
● Enable
Allow websites to prompt for information using scripted windc
Scripting of Java applets
○ Disable

*Takes effect after you restart Internet Explorer

Reset custom settings

Reset to: Medium-low (default)

Figure 6-4: Custom level configuration settings – Scripting

6.4 Configuring Windows Authentication for Web Verifier

The Web Verifier application allows you to login with your Windows user account. In this case, the password that is shared with Windows will be used to login into Web Verifier.

To use this option, you first need to configure the server.

Note: Only Windows Authentication access will be possible after this option is configured. However, when logged in to Web Verifier via Windows Authentication, it will be possible to use the re-login menu option to login e.g. as an administrator in order to perform certain administrative tasks.

Prerequisites which apply to both, IIS 6 and IIS 7

- Before starting to configure IIS, make sure that the Web Verifier application is working properly using an existing project user account.
- Back up the web.config file.

6.4.1. For IIS 7

To configure Windows Authentication access to Web Verifier with IIS 7:

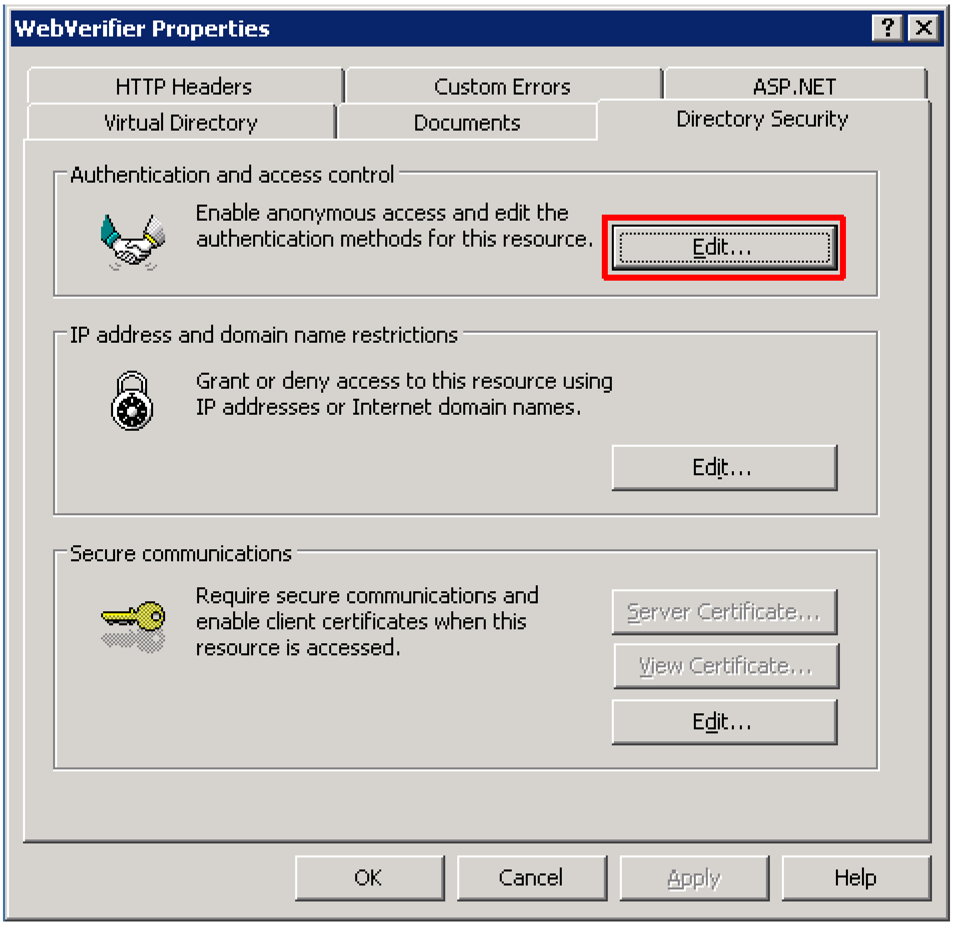
1. Open “Authentication” settings in IIS group for the WebVerifier application.
2. Enable “Windows Authentication” and disable all other authentication methods.
3. Close all of the running browser sessions prior to access the Web Verifier application.
4. Add the Windows user to the database. Please refer to the **Designer User Guide** for information on how to do this.

Note: In IIS 7, Error Pages will be configured automatically.

6.4.2. For IIS 6

To configure Windows Authentication to Web Verifier with IIS6:

1. Open the WVC application properties.
2. Go to *Directory Security* tab, *Authentication and access control* section and press the *Edit* button.



WebVerifier Properties

Authentication and access control

Enable anonymous access and edit the authentication methods for this resource.

IP address and domain name restrictions

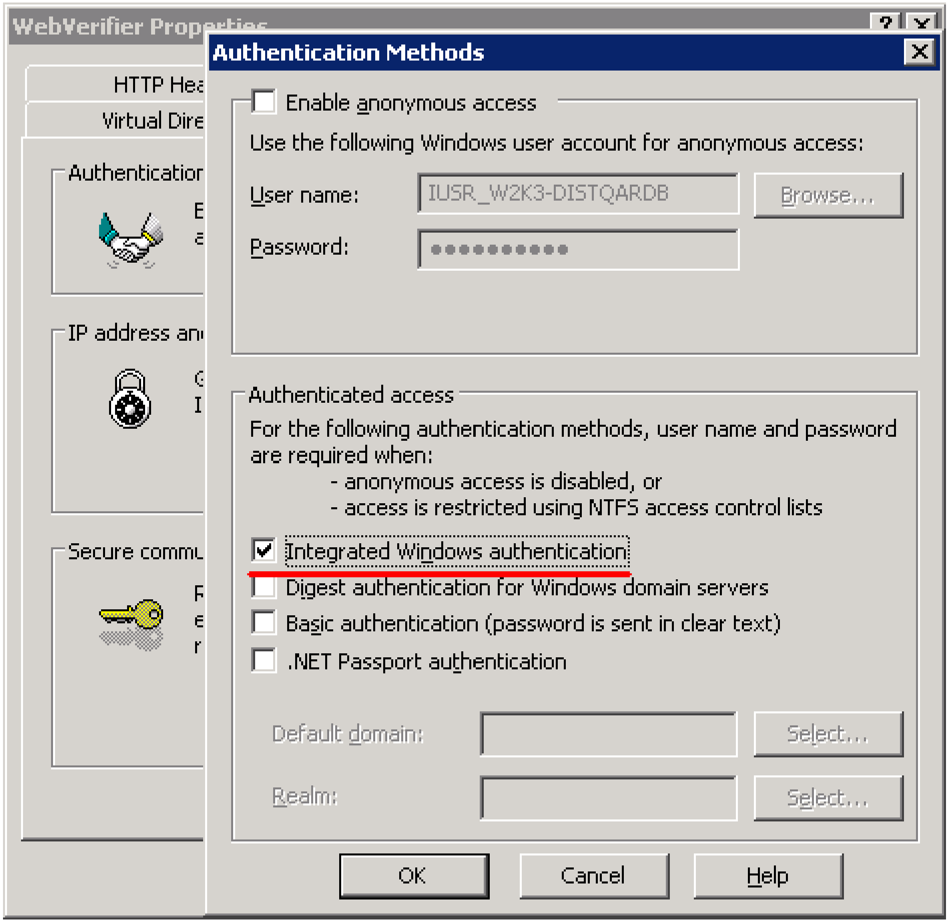
Grant or deny access to this resource using IP addresses or Internet domain names.

Secure communications

Require secure communications and enable client certificates when this resource is accessed.

Figure 6-5: Entering the Authentication and access control area

3. In the *Authentication methods* dialog, enable *Integrated Windows Authentication* and disable all other authentication methods



Authentication Methods

□ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: IUSR_W2K3-DISTQARDB

Password: ●●●●●●●●●●●

Authenticated access

For the following authentication methods, user name and password are required when:
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☑ Integrated Windows authentication

□ Digest authentication for Windows domain servers

□ Basic authentication (password is sent in clear text)

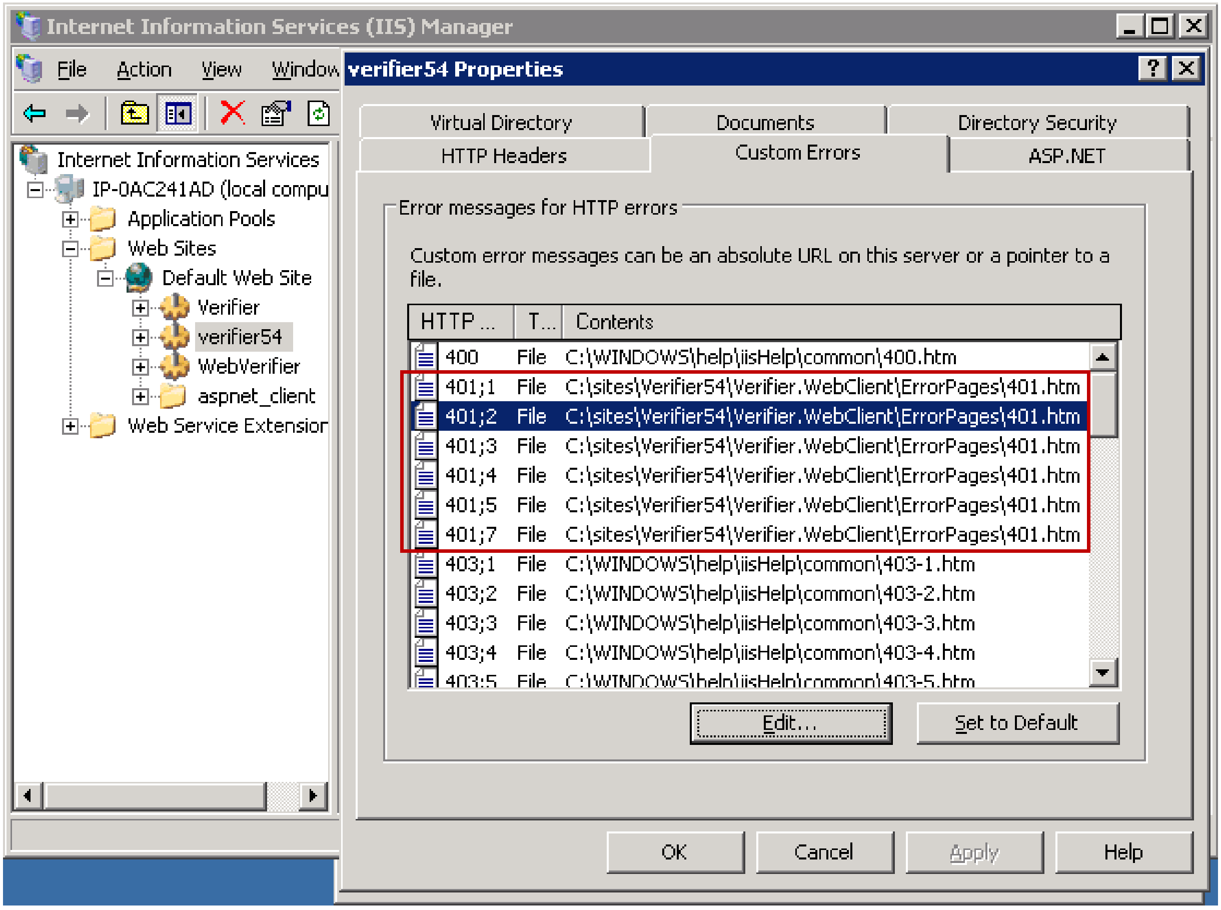
□ .NET Passport authentication

Default domain:

Realm:

Figure 6-6: Enabling/Disabling authentication methods

4. In order to enable custom error page for “Not Authorized” status, it is needed to configure IIS to redirect to <Web Verifier Installation Directory>/ErrorPages/401.htm when 401.x error is received:
   - Select WVC application properties.
   - Go to *Custom Errors* tab.
   - Select each of the 401;x error code properties one after another.
   - When one of the properties selected, press the *Edit* button.
   - In the *Edit Custom Error Properties* dialog, select *File* for *Message Type.*
   - Enter path to <Web Verifier Installation Directory>/ErrorPages/401.htm

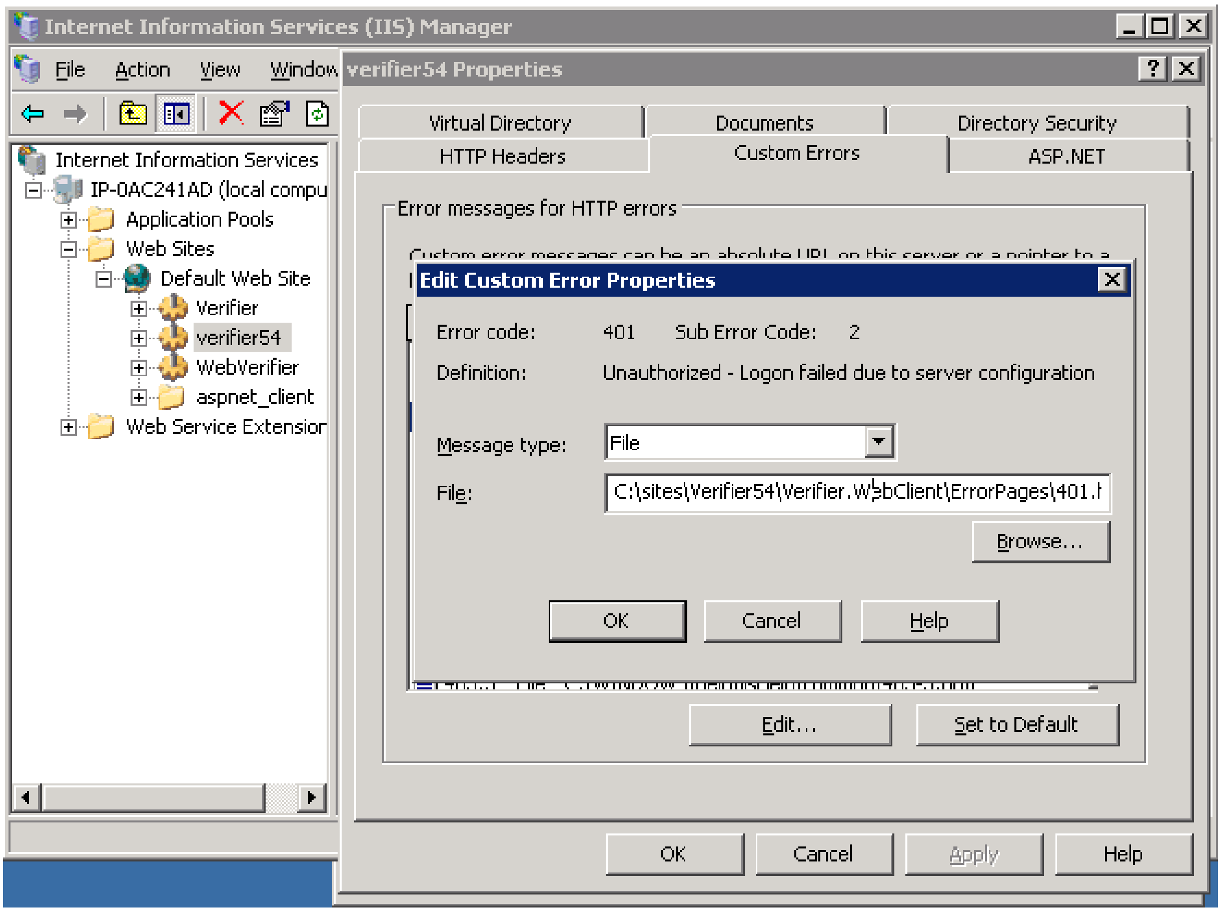


Error messages for HTTP errors

Custom error messages can be an absolute URL on this server or a pointer to a file.

HTTP ...	T...	Contents
400	File	C:\WINDOWS\help\iisHelp\common\400.htm
401;1	File	C:\sites\Verifier54\Verifier.WebClient\ErrorPages\401.htm
401;2	File	C:\sites\Verifier54\Verifier.WebClient\ErrorPages\401.htm
401;3	File	C:\sites\Verifier54\Verifier.WebClient\ErrorPages\401.htm
401;4	File	C:\sites\Verifier54\Verifier.WebClient\ErrorPages\401.htm
401;5	File	C:\sites\Verifier54\Verifier.WebClient\ErrorPages\401.htm
401;7	File	C:\sites\Verifier54\Verifier.WebClient\ErrorPages\401.htm
403;1	File	C:\WINDOWS\help\iisHelp\common\403-1.htm
403;2	File	C:\WINDOWS\help\iisHelp\common\403-2.htm
403;3	File	C:\WINDOWS\help\iisHelp\common\403-3.htm
403;4	File	C:\WINDOWS\help\iisHelp\common\403-4.htm
403;5	File	C:\WINDOWS\help\iisHelp\common\403-5.htm

Figure 6-7: Custom Error properties for 401 errors



Error code: 401 Sub Error Code: 2

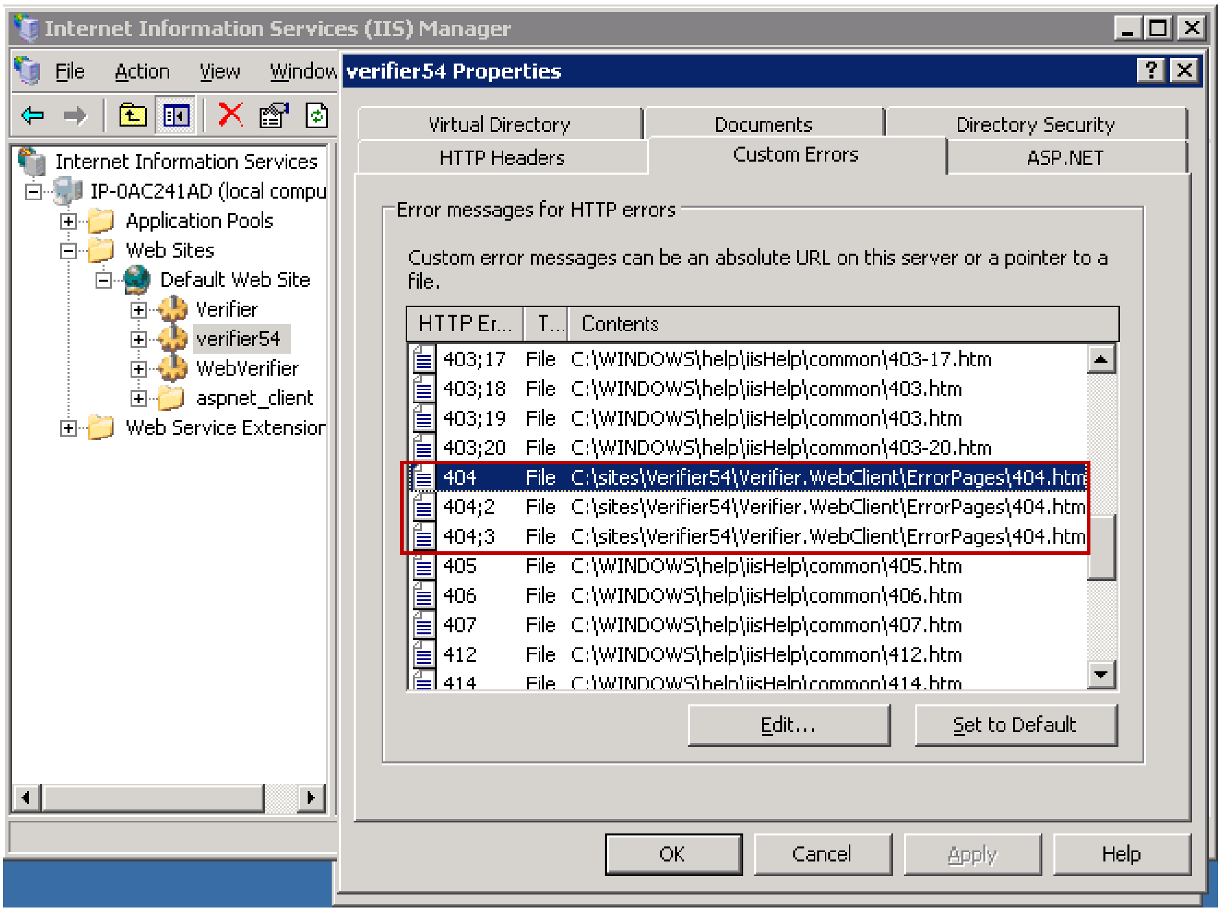
Definition: Unauthorized - Logon failed due to server configuration

Message type: File

File: C:\sites\Verifier54\Verifier.WebClient\ErrorPages\401.h

Figure 6-8: Editing Custom Error properties

5. In order to enable custom error page for “Not Found” status it is needed to configure IIS to redirect to <Web Verifier Installation Directory>/ErrorPages/**404**.htm when 404.x error is received.
   - Select WVC application properties.
   - Go to *Custom Errors* tab.
   - Change all 404;x error code properties to point to file
   <Web Verifier Installation Directory>/ErrorPages/404.htm



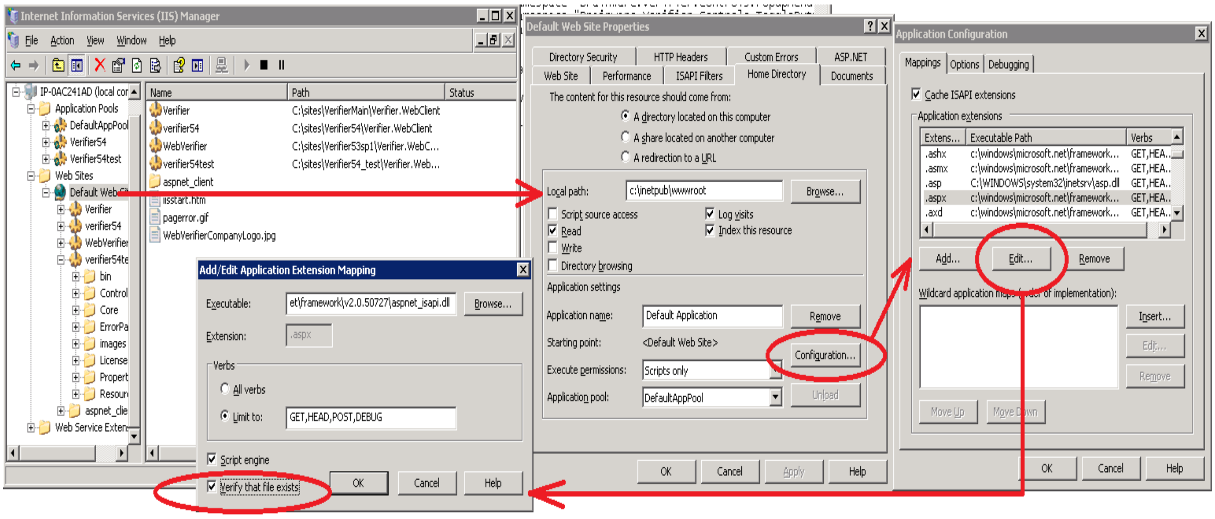
Error messages for HTTP errors

Custom error messages can be an absolute URL on this server or a pointer to a file.

HTTP Er...	T...	Contents
403;17	File	C:\WINDOWS\help\iisHelp\common\403-17.htm
403;18	File	C:\WINDOWS\help\iisHelp\common\403.htm
403;19	File	C:\WINDOWS\help\iisHelp\common\403.htm
403;20	File	C:\WINDOWS\help\iisHelp\common\403-20.htm
404	File	C:\sites\Verifier54\Verifier.WebClient\ErrorPages\404.htm
404;2	File	C:\sites\Verifier54\Verifier.WebClient\ErrorPages\404.htm
404;3	File	C:\sites\Verifier54\Verifier.WebClient\ErrorPages\404.htm
405	File	C:\WINDOWS\help\iisHelp\common\405.htm
406	File	C:\WINDOWS\help\iisHelp\common\406.htm
407	File	C:\WINDOWS\help\iisHelp\common\407.htm
412	File	C:\WINDOWS\help\iisHelp\common\412.htm
414	File	C:\WINDOWS\help\iisHelp\common\414.htm

Figure 6-9: Custom Error properties for 404 errors

6. In order to “Not Found” page being shown for invalid .aspx addresses (e.g. Batch.aspx – does not exist but would be a valid page name from IIS point of view) configure IIS the following way:
   - Go to properties of Default Web site.
   - Select the *Home Directory* tab.
   - Press the *Configuration* button.
   - Select the *Mappings* tab.
   - Select the .aspx extension option from the list.
   - Press the *Edit* button.
   - Check the *Verify that file exists* checkbox.



Name	Path	Status
Verifier	C:\sites\VerifierMain\Verifier.WebClient	
verifier54	C:\sites\Verifier54\Verifier.WebClient	
WebVerifier	C:\sites\Verifier53sp1\Verifier.WebC...	
verifier54test	C:\sites\Verifier54_test\Verifier.Web...	
aspnet_client		
iisstart.htm		
pagerror.gif		
WebVerifierCompanyLogo.jpg		

The content for this resource should come from:

● A directory located on this computer
○ A share located on another computer
○ A redirection to a URL

Local path: c:\inetpub\wwwroot

□ Script source access
☑ Read
□ Write
□ Directory browsing
☑ Log visits
☑ Index this resource

Application settings

Application name: Default Application

Starting point: <Default Web Site>

Execute permissions: Scripts only

Application pool: DefaultAppPool

☑ Cache ISAPI extensions

Application extensions

Extens...	Executable Path	Verbs
.ashx	c:\windows\microsoft.net\framework...	GET,HEA...
.asmx	c:\windows\microsoft.net\framework...	GET,HEA...
.asp	C:\WINDOWS\system32\inetsrv\asp.dll	GET,HEA...
.aspx	c:\windows\microsoft.net\framework...	GET,HEA...
.axd	c:\windows\microsoft.net\framework...	GET,HEA...

Wildcard application maps (order of implementation):

Executable: et\framework\v2.0.50727\aspnet_isapi.dll

Extension: .aspx

Verbs

○ All verbs
● Limit to: GET,HEAD,POST,DEBUG

☑ Script engine
☑ Verify that file exists

Figure 6-10: Configuring the "Not Found" page to be shown

7. After submitting, the "Inheritance Overrides" dialog will be present. Choose WebVerifier application to apply this setting.

Note: The "Not found" error page configuration is also used for standard authentication mode.

8. The web.config file needs to be modified. See Changes to Web.config File section below.
9. Close all of the running browser sessions prior to access the Web Verifier application.
10. Add the Windows user to the database. Please refer to the **Designer User Guide** for information on how to do this.

6.4.3. Changes to Web.config File

It is highly recommended to have two versions of the web.config file – one for standard authentication and one for Windows Authentication. This will simplify switching between modes.

The following list shows required steps to convert standard web.config to a web.config with Windows Authentication enabled.

The steps generally apply to both, IIS 6 and IIS 7. Exceptions are mentioned appropriately.

1. Change <authentication> section (located in the <configuration><system.web>) to the following:
   <authentication mode="Windows">
2. Remove the following line:
   <forms loginUrl="Login.aspx" defaultUrl="BatchView.aspx" />
   This is a child of the <authentication> section, and is only needed for standard authentication.
3. Change <authorization> section (located in the <configuration><system.web>) from 'deny' to 'allow':

```
<authorization>
   <allow users="?"/>
</authorization>
```

4. Add enableSessionState attribute to <pages> section (located in the <configuration><system.web>):

   ```
   <pages enableSessionState="true">
   ```

5. Remove all <location> sections (located in the <configuration> right before <appSettings>). Those sections look like the following:

   ```
   <location path="WL">
      <system.web>
         <authorization>
            <allow users="*" />
         </authorization>
      </system.web>
   </location>
   ```

6. This step only applies to IIS 6.
   For correct display of ‘Not Found’ error page add section <customErrors> after <authorization> section to be the following

   ```
   <customErrors mode="On" defaultRedirect="~/Error.aspx">
      <error statusCode ="404" redirect="~/ErrorPages/404.htm" />
   </customErrors>
   ```

   The page referenced here is the same 404.htm that was configured in IIS settings. This “Not found” error page configuration is also used for standard authentication mode.

6.4.4. Reverting Back to Standard Authentication

To switch from Windows Authentication mode back to standard authentication mode, the following adjustments to IIS are required:

IIS 7.x (Windows 7, Windows Server 2008, Windows Server 2008 R2)

Please refer to Step 2 of section 6.4.1. Disable Windows Authentication and enable both, Anonymous and Forms Authentication.

IIS 6 (Windows Server 2003)

Please refer to Step 3 of section 6.4.2. Disable Windows Authentication and enable Anonymous Authentication.

Changes to Web.config

Get the back up file which was done at the beginning of the configuration process.

6.5 Configuring SSL for Web Verifier

For information how to set up SSL on your Information Services machine please refer to:

http://support.microsoft.com/kb/299875

6.6 Configuring Additional Languages

Web Verifier supports an extended list of languages:

Chinese Simplified, Chinese Traditional, Danish, Dutch, English, French, Finnish, German, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Romanian, Russian, Spanish, Swedish, Turkish.

Note: By default, the Chinese language selection points to Traditional Chinese. In case Simplified Chinese language has to be used, the content of the Bin\Resources\cmn folder can be copied into the "zho" folder which contains the Traditional Chinese. Prior to overwriting the “zho” folder content, please ***back it up****..*

6.7 Virus Check

Please note, that the settings for the Virus Checker on the Web Server exclude the [Local Temp Folder]/CdrDbCache directory (Batch and the Common Learnset folders) from the locations which are checked for viruses. This is due to performance considerations.

6.8 Enabling New Columns for Batch View

Four additional columns are available to hold additional information on batches:

- Batch.ExternalGroupId - default display name: "User Group"

  data type: The Group ID which has been assigned to a batch is relating to security. Batches can be assigned to user group via a unique ID. For example, German invoices belong to Group 1 and English invoices belong to Group 2. When in a shared service center, you could hide all German invoice batches from English Verifiers.

- Batch.ExternalBatchId - default display name: "Batch Group"

  data type: It allows the developer to uniquely identify the batch. For example, external system ID, storage box ID, etc.

- Batch.TransactionId - default display name: "Transaction"

  data type: It allows the developer to synchronize a newly created batch of documents with another external system. It can be used to identify originators of batch of documents.

- Batch.TransactionType - default display name: "Transaction Type"

  data type: It allows the developer to synchronize a newly created batch of documents with another external system. It can used to identify the types of documents (Invoices, Claim forms etc.) in batches or source of document (Email, Scanned etc.)

These table columns are not WebCenter Forms Recognition project or application specific and therefore cannot be configured in Designer or Verifier or RTS applications.

By default, these columns will be invisible. To configure the columns’ visibility for Web Verifier, adjust the batch columns’ attributes in the batchColumnVisibility section of the web.config file appropriately (please refer to 0).

The values of the columns can only be set via the Project Script (PostimportBatch). Check the SQL scripts in the installation folder to activate the displaying of those columns. After enabling one or all of the additional columns in database, it applies to all application modules.

The additional columns can be enabled with columns customized.

For Oracle:

Syntax:

```
exec sp_SetGlobalApplicationSetting 'ColumnSettingName', 'Column Name to Display', 0|1
```

Examples:

```
exec sp_SetGlobalApplicationSetting 'SysAppBatchColumnExternalGroupId', 'User Group', 1
```

For SQL Server:

Syntax:

```
exec sp_SetGlobalApplicationSetting 'ColumnSettingName', 'Column Name to Display', Enabled Boolean
```

Examples:

```
exec sp_SetGlobalApplicationSetting 'SysAppBatchColumnExternalGroupId', 'User Group', True

exec sp_SetGlobalApplicationSetting 'SysAppBatchColumnExternalBatchId', 'Batch Group', True

exec sp_SetGlobalApplicationSetting 'SysAppBatchColumnTransactionId', 'Transaction', True

exec sp_SetGlobalApplicationSetting 'SysAppBatchColumnTransactionType', 'Transaction Type', True
```

Note: For setting up the Group ID column, due to the security control, make sure the group ID is matching with the ID created for the users.

6.9 Changing Custom Column Names

After you have enabled new custom columns following the instructions in section 6.8, Enabling New Columns for Batch View, you may want to give them more meaningful names.

6.9.1. Custom Column Names for Web Verifier

To change the custom column names for the Web Verifier application:

1. Navigate to C:\Program Files (x86)\Oracle\WebCenter Forms Recognition Web Server\Bin\Resources\eng
2. Open the file in notepad: Brainware.Verifier.WebClient.resx
3. Change the name of the four items below by adjusting the value parameter (highlighted in red in the sample below):

Example:

```
<data name="TEXT_EXTERNALBATCH_NAME" xml:space="preserve">
    <value>External Batch ID</value>
  </data>
  <data name="TEXT_EXTERNAL_GROUP_ID" xml:space="preserve">
    <value>User Group</value>
  </data>
  <data name="TEXT_TRANSACTION_ID" xml:space="preserve">
    <value>Transaction ID</value>
  </data>
  <data name="TEXT_TRANSACTION_TYPE" xml:space="preserve">
    <value>Transaction Type</value>
```

For the other application languages, repeat the steps outlined above using the appropriate Brainware.Verifier.WebClient.resx file from the appropriate folder under:

C:\Program Files (x86)\Oracle\WebCenter Forms Recognition Web Server\Bin\Resources\....

6.9.2. Custom Column Names for Thick Verifier Client

For the Thick Verifier Client, custom column names can be changed via SQL Script. Run the below mentioned script by changing the ‘Column Name to Display’ value.

Syntax:

```
exec sp_SetGlobalApplicationSetting 'ColumnSettingName', 'Column Name to Display', Enabled Boolean
```

Example:

```
exec sp_SetGlobalApplicationSetting 'SysAppBatchColumnExternalGroupId', 'User Group', True
```

6.9.2.1. Global Application Setting Configuration

This setting is taken place in the database, and it enables/disables Workflow History Reporting, disables Batch Deletion in Designer/ MMC, and enables some additional custom columns.

This feature allows user to enable/disable for Document Level, Field Level, table Level, Classification, Document Separation, Learning, etc.

Note: This feature is only available for the Database.

To execute the setting:

1. Launch the SQL Server Management Studio.
2. Point to the Database.
3. Type in the following script:

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

Setting Name is the text name of the setting to be modified for application.

Setting value is the text value to configure for it.

Status Flag contains True (Setting enabled) or False (Setting disabled). This is disabled by default in the current version of Forms Recognition.

To enable item with Document Level:

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

To enable item with Field Level:

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

To enable Batch Deletion in Designer (Default setting):

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

To disable Batch Deletion in Designer:

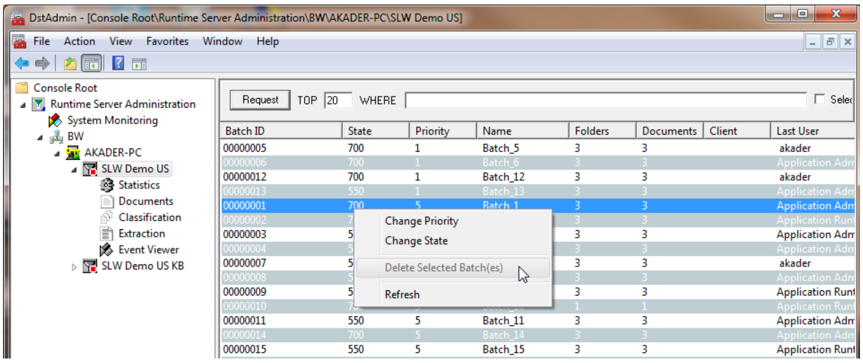
```
exec sp_SetGlobalApplicationSetting 'SysAppBatchDeletionDisabledInDesigner', 'True', True
```

To enable Batch Deletion in RTS (Default setting):

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

To disable Batch Deletion in RTS:

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



TOP 20 WHERE

□ Selec

Batch ID	State	Priority	Name	Folders	Documents	Client	Last User
00000005	700	1	Batch_5	3	3		akader
00000006	700	1	Batch_6	3	3		Application Adm
00000012	700	1	Batch_12	3	3		akader
00000013	550	1	Batch_13	3	3		Application Adm
00000001	700	5	Batch_1	3	3		Application Adm
00000002	7			3	3		Application Runt
00000003	5			3	3		Application Adm
00000004	5			3	3		Application Adm
00000007	5			3	3		akader
00000008	5			3	3		Application Adm
00000009	5			3	3		Application Runt
00000010	7			1	1		Application Runt
00000011	550	5	Batch_11	3	3		Application Adm
00000014	700	5	Batch_14	3	3		Application Adm
00000015	550	5	Batch_15	3	3		Application Runt

Figure 6-11: Delete Batch Function is disabled in RTS

It takes immediate effect right after you have configured it in the database and it applies to all users.

7 Security

7.1 WebCenter Forms Recognition Security

7.1.1. Project Security

WebCenter Forms Recognition contains an internal application security model with 5 project security roles:

- **Administrator**: The Administrator's role (ADM) is to manage users, groups, and user-to-group assignments. Administrators install the system, configure applications, and manage data. They also design and maintain projects. This role is the most powerful of the roles because it is the highest role within WebCenter Forms Recognition.
- **Learnset Manager**: The Learnset Manager (LSM) role is used to define, modify, and maintain the global project Learnset. Reference WebCenter Forms Recognition Designer and Verifier documentation for additional information.
- **Supervised Learning Verifier**: The Supervised Learning Verifier (SLV) role is to collect and manage the local training data. These verifiers are subject-matter experts who can propose Learnset improvements.
- **Verifier User**: The Verifier role (VER) is to make document correction that could not be automatically processed. Typically members of this group are data correction users.
- **Setting Role**: The Verifier Settings (SET) role is used to give permission to the Verifier (VER) to alter or access the verifier configuration settings.
- **Filtering Role**: The filtering role (FLT) is to allow Verifier user to configure custom filtering of batches. By application design, FLT users would be able to use the filtering feature even if they do not have the SET role. This solution provides more flexibility and security.

Note: Additional information on adding users and groups can be found in the Designer documentation.

7.1.2. Project & Windows Authentication Security

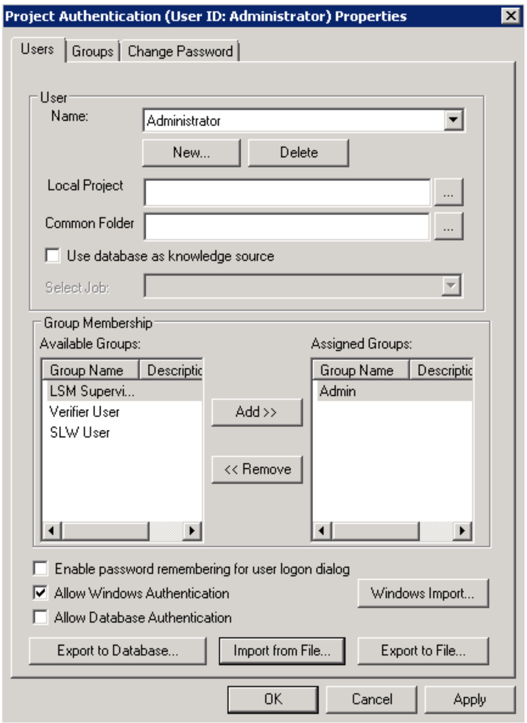
Local workstations and network Windows users can be imported into the WebCenter Forms Recognition project authentication sub-system allowing automatic project authentication with the currently logged in Windows user account for all WebCenter Forms Recognition applications.

To enable Windows based authentication in WebCenter Forms Recognition for a desired project:

1) Open the corresponding project file in the WebCenter Forms Recognition Designer application

2) Select *Options*, *Users, Groups and Accounts*… menu item

3) Enable *Allow Windows Authentication* check-box on the *Users* tab of the *Project Authentication Settings* dialog



Project Authentication (User ID: Administrator) Properties

User

Name: Administrator

Local Project

Common Folder

☐ Use database as knowledge source

Select Job:

Group Membership

Available Groups:

Group Name	Descriptic
LSM Supervi...	
Verifier User	
SLW User	

Assigned Groups:

Group Name	Descriptic
Admin	

☐ Enable password remembering for user logon dialog

☑ Allow Windows Authentication

☐ Allow Database Authentication

Figure 7-1 Forms Recognition Project Security

When using Database Authentication in Verifier, access rights have to be granted to the verifier user.

By default, this should be:

- Read and Write to all database tables

- Execute rights to stored procedures and functions.

7.2 File System Security

Although WebCenter Forms Recognition does provide application-level security, the product relies on integrated Windows file system security built into the underlying operating system for file system access.

WebCenter Forms Recognition uses operating system files (.sdp, .dat, .wdc, .sdb, etc.) to store all application and project data. A combination of shared and NTFS permissions are used to protect application data.

NTFS file and folder permissions are used to control the type of access that a user, group, or application has to folders and files. This includes everything from reading the contents of a folder or a file to modifying a folder's contents and/or executing individual files. There are five basic NTFS file and six folder permissions:

File Permission	Access Granted
Read	Allows the user or group to read the file and view its attributes, ownership, and the permissions set.
Write	Allows the user or group to overwrite the file, change its attributes, view its ownership, and view the permissions set.
Read and Execute	Allows the user or group to run and execute the application. In addition, the user can perform all duties allowed by the Read permission.

File Permission	Access Granted
Modify (CHANGE)	Allows the user or group to modify and delete a file including performing all of the actions permitted by the Read, Write, and Read and Execute NTFS file permissions.
Full Control	Allows the user or group to change the permission set on a file, take ownership of the file, and perform actions permitted by all of the other NTFS file permissions.

Table 7-1: NTFS File Permissions

Folder Permission	Access Granted
Read	Allows the user or group to view the files, folders, and subfolders of the parent folder. It also allows the viewing of 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 contained within the folder.
Read and Execute	Allows the user or group to navigate through all files and subfolders, and to perform all actions allowed by the Read and List Folder Contents permissions.
Modify (CHANGE)	Allows the user to delete the folder and perform all activities included in the Write and Read & Execute NTFS folder permissions.
Full Control	Allows the user or group to change permissions on the folder, take ownership of it, and perform all activities included in all other permissions.

Table 7-2: NTFS Folder Permissions

The difference between NTFS file and folder permissions is the “List Folder Contents NTFS” folder permission. NTFS folder permissions enable system administrators to limit a user’s ability to browse through a tree of folders and files. This is useful for securing a specific directory such as an application directory. A user must know the name and location of a file to read or execute it when this permission is applied to its parent folder. However, in a WebCenter Forms Recognition environment, client applications in the product suite, instead of Windows Explorer, are used to process project data. The intent of file and folder permissions is to minimize the probability of accidental or malicious data destruction.

Shared permissions serve for purposes similar to NTFS permissions: They help protect files from unauthorized access. If you are a member of the Administrators or Power Users group, you can share folders on a local computer so that users on other computers can access those folders over the network. By assigning shared folder permissions to any shared folder, you can restrict or allow access to those folders over the network. Use NTFS folder permissions if the shared folder is located on a NTFS drive. NTFS permissions are effective on the local computer and over the network.

For more information regarding folder permissions, reference Appendix B.

7.3 Access to Project Data

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

All WebCenter Forms Recognition components (including services, applications, and users) need appropriate access rights to the project directory and all of its subfolders.

See section 7.2 File System Security for details on how to enable access to project data.

Once WebCenter Forms Recognition has been installed, configured, and prepared for production, appropriate file access security should be applied to the project directory before releasing the implementation to the general user community. A correct application of file access security can prevent unauthorized access to project data while granting access to authorized users.

To apply file access security to the WebCenter Forms Recognition project directory:

2) Launch Windows Explorer on the WebCenter Forms Recognition server (or the server containing the project directory).
3) Locate the project folder, right click the folder name, and select *Properties*.
4) In the *Properties* dialog box, go to *Sharing* tab.
5) Click *Share this folder*.
6) In the *Share* name field, type a name for the share.
7) Click *Permissions*. In the *Share Permissions* dialog box, do the following tasks, and then click *OK*:

- Add the local WebCenter Forms Recognition group with *Full Control* permission
- Add the local WebCenter Forms Recognition Users group with *Change* permission
- Add the local Administrators group with *Full Control* permission
- Remove the *Everyone* group

8) Go to *Security* tab.
9) Do the following tasks and click *OK* when finished:

- Add the local WebCenter Forms Recognition group with *Full Control* permission
- Add the local WebCenter Forms Recognition Users group with *Change* permission
- Add the local Administrators group with *Full Control* permission
- Remove the *Everyone* group

Note: The WebCenter Forms Recognition and WebCenter Forms Recognition Users groups are local groups. The WebCenter Forms Recognition local group should be created on all WebCenter Forms Recognition servers and RemoteAdmin machines; the WebCenter Forms Recognition Users local group is only required on the WebCenter Forms Recognition server storing the project data. For an explanation of these groups, see next section.

7.4 Accounts and File Access Security

Access to project data in a WebCenter Forms Recognition implementation should be granted using a combination of Discretionary Access Control (DAC) and Role-based Access Control (RBAC).

The Discretionary Access Control model allows the owner of objects or resources (in this context, a System Administrator) to control who accesses them and what operations they can perform. For example, a System Administrator who creates a share called “Projects” to hold data pertaining to a particular WebCenter Forms Recognition project can control and dictate (per the organization’s security policy and business rules) who can access the items within the share.

The Role-Based Access Control model, also referred to as a non-discretionary model, makes access decisions based on the rights and permissions granted to a role or groups, instead of an individual. In this model, System Administrators create roles (or groups), and then assign rights and permissions to the role (or group) instead of directly to a user; users are then placed into a role (or group) and inherit the rights and permissions assigned to the role (or group).

The following table lists the recommended groups and accounts that should be created for each implementation of WebCenter Forms Recognition:

Group/Account Name	Purpose
Forms Recognition ProjectUsers	Global group containing all users designated as a Forms Recognition project designer and/or data verifier within an organization.
Forms Recognition Admin	Global group containing all users designated as a Forms Recognition System Administrator within an organization. This group should be added to the local Forms Recognition group on all RTS servers and RTS Remote Admin workstations.
Forms Recognition	Local group used to grant access to local Forms Recognition resources; the Forms Recognition Admin global group should be added to its membership. Create this group on all Forms Recognition Server and RemoteAdmin machines
Forms Recognition Users	Local group used to grant access to the project directory. Add the global group Forms Recognition ProjectUsers to its membership. Create this group on the Forms Recognition server housing the project directory.
Forms Recognition RTSsvc	Service account used to start the Forms Recognition Service Manager. This user should be a member of the Forms Recognition Admin global group and the local Administrators group on all Forms Recognition servers and Remote administration machines.

Table 7-3: Recommended Group/Account Names for Forms Recognition.

The following table lists the groups and accounts, assigned permissions, and the folders/objects on which the permissions should be applied for each implementation of WebCenter Forms Recognition:

Group/Account Name	Permission Type: Shared	Permission Type: NTFS	Folder/Objects Assigned On
Forms Recognition	Full Control	Full Control	C:\Program Files\ [company]\ [ProjectName]
Forms RecognitionUsers	Change	Modify	C:\Program Files\ [company]\ [ProjectName]

Table 7-4: Group/Account and Permissions.

For a comprehensive list of security settings and options, see Appendix B.

7.5 Configuring the Service Account for WebCenter Forms Recognition

7.5.1. Running WebCenter Forms Recognition on a Domain Network

WebCenter Forms Recognition Runtime Server Service utilizes a Windows service that runs in the Server background. This service manages the operation of Runtime Server Instances, and processing of documents automatically.

When running WebCenter Forms Recognition on multiple servers located on a Domain Network, it is recommended that the WebCenter Forms Recognition Runtime Server Service is assigned a Domain user against the Windows Service. This will allow WebCenter Forms Recognition to communicate with all servers running the service across the Domain.

The Service Account used in WebCenter Forms Recognition is also given permission to any file/folder shares across the servers to allow the Runtime Server service access to all project related files.

7.5.2. System Monitoring

The System Monitoring service is used to send email notification to selected users to notify of any errors, or warnings, that any Runtime Server instance may raise during its operation.

The Service User Account used for System Monitoring should have sufficient rights to be able to send emails on the server and Domain.

7.5.3. Email Importing and Service User Accounts

WebCenter Forms Recognition provides the ability to perform email importing, automatically downloading emails from a Mail Box account and importing it into the system. The Runtime Server Service must have sufficient access rights to be able to access the mailbox in order to download emails for process.

8 Configuring Runtime Components

Once you install WebCenter Forms Recognition you must configure the Runtime Service Manager before you can use the application.

8.1 Configuring the Runtime Service Manager

Below are the steps required for configuring the Runtime Service Manager. Administrator rights are needed to do these steps:

1) Click *Start* on the lower left of your screen.
2) Click Run.
3) At the command window, type “services.msc” and press Enter.
4) In the Scope panel, double click the WebCenter Forms Recognition Runtime Service Manager.
5) On the *General* tab, under *Startup type*, select *Automatic* from the drop down list.
6) Go to *Log On* tab.
7) Under *Log on as*, select *This account*.
8) Click *Browse…*
9) Find and add the domain user with appropriate and sufficient for WebCenter Forms Recognition processing network access rights (e.g. WebCenter Forms Recognition RTSsvc), and then click *OK*.
10) Type the domain password for the user in the fields provided.
11) Click *Apply* and *OK,* and then close the Computer Management MMC.

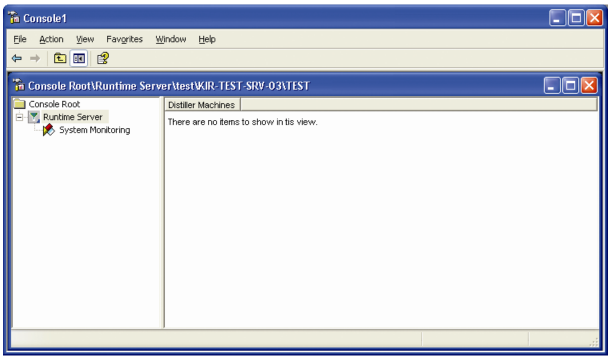
8.2 Configuring the RTS RemoteAdmin MMC Snap-in

The installation of WebCenter Forms Recognition creates a default console, called WebCenter Forms Recognition Service Manager that you can use to configure the RTS RemoteAdmin MMC snap-in.

Very Important!

Before configuring the RemoteAdmin MMC snap-in, make sure that the steps outlined in section 8.1 have been performed and the Runtime Service Manager is started. Unless the service has been started, the MMC will not connect to the machine.

1) Launch the WebCenter Forms Recognition Service Manager MMC snap-in by selecting *Start>Programs>*Oracle>WebCenter Forms Recognition>Forms Recognition *Runtime Service > Management Console* on the desktop of the target machine. The WebCenter Forms Recognition Service Manager MMC console appears.



Console Root\Runtime Server\test\KIR-TEST-SRV-03\TEST

Console Root
Runtime Server
System Monitoring

Distiller Machines

There are no items to show in tis view.

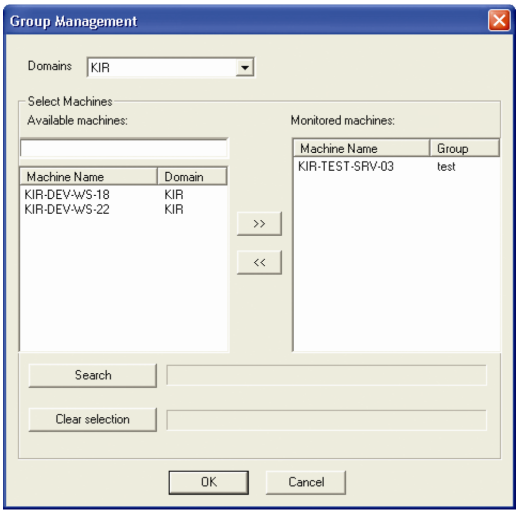
Figure 8-1: The administration console

2) Right click the WebCenter Forms Recognition Runtime Server node and select *New RTS Group* from the context menu.

3) On the *New Group* dialog, type a group name and click *OK*.

4) Expand the WebCenter Forms Recognition Runtime Server node, right click the group you created, and then select *New Machine*.

5) In the Domains dropdown, select the domain where the machine being configured locates.



Domains: KIR

Available machines:

Machine Name	Domain
KIR-DEV-WS-18	KIR
KIR-DEV-WS-22	KIR

Monitored machines:

Machine Name	Group
KIR-TEST-SRV-03	test

Figure 8-2: Group management of runtime service

6) On the *Group Management* dialog box, type the name of the WebCenter Forms Recognition server and click *OK*.

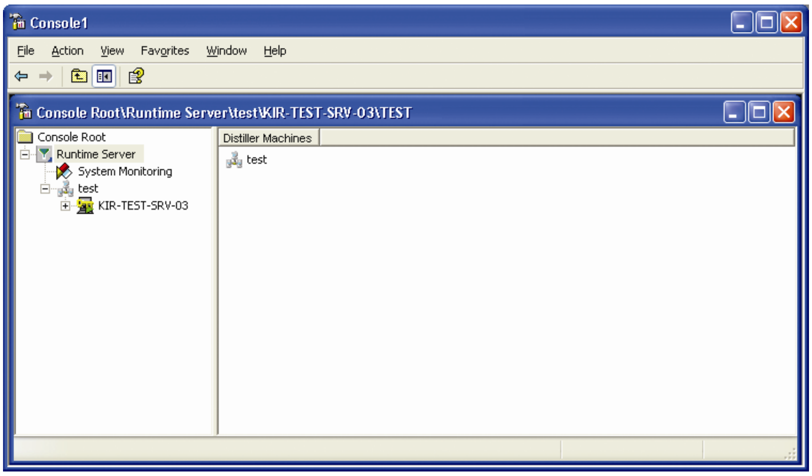
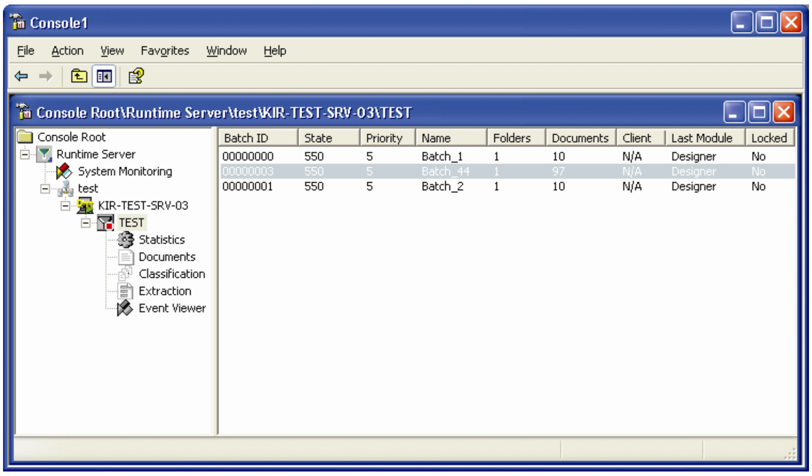


Figure 8-3: Administration console with added machine

7) Right click on the machine name. Select *License*, and set the license path.

8) Right click on the machine name and select *New>RTS Instance*

9) On the New RTS Instance dialog, type the instance name and then click *OK*. The configuration for RTS RemoteAdmin MMC snap-in should look like the example in Figure 8-4.



Batch ID	State	Priority	Name	Folders	Documents	Client	Last Module	Locked
00000000	550	5	Batch_1	1	10	N/A	Designer	No
00000003	550	5	Batch_44	1	97	N/A	Designer	No
00000001	550	5	Batch_2	1	10	N/A	Designer	No

Figure 8-4: Administration console with instance

See Also

For information on how to configure project settings for a WebCenter Forms Recognition instance, see the WebCenter Forms Recognition Runtime Server User’s Guide.

8.3 Advanced Logging

The standard Runtime Server Log includes System Level Resource information and, in the event of a system crash or failure, special error logs.

8.3.1. System Resource Logging

In the WebCenter Forms Recognition\bin\Log folder, the log files for the different WebCenter Forms Recognition components can be found as following:

- V_ log file for Verifier messages, e.g. any custom script errors would be logged there.
- H_ log file for Runtime Server messages.
- VA_ log file for Advanced Verifier messages.
- L_ log file for Learnset Manager messages, e.g. when the user triggers document learning, or when a backup of the Learnset is taken, etc.
- D_log file for Designer messages (including scripting errors).
- U_log file for Unknown/External application messages.
- S_log file for Standard Service Manager messages.
- The I_ log files are component log files for all applications and are written to by the application during the normal running.

Examples for file name syntax, e.g. for the Runtime Server log file:

> [Application directory]\bin\Log\H_<instance name>_yyyymmdd.log
> For example:
> C:\Program files\Oracle\WebCenter Forms Recognition\bin\Log\H_Test_20100203.log

Standard Service Manager log file:

> [Application directory]\bin\Log\S_yyyymmdd.log
> For example:
> C:\Program files\Oracle\WebCenter Forms Recognition\bin\Log\S_20100203.log

The following System Resource information has been added to the log files:

- Available physical memory (in kb).

- Used physical memory (in kb).
- Available virtual memory (in kb).
- Used virtual memory (in kb).
- Virtual memory used by this RTS host instance process (in kb).
- Physical memory used by this RTS host instance process (in kb).
- Handles used by the process (in number of handles).
- GDI resources used by the process (in number of handles).
- User Objects used by the Process (in number of Objects).

Using the following format:

Entry Nr.	Entry Description
1	Type of message (info, warning, error, etc)
2	Severity of message
3	Time logged
4	Process ID (PID)
5	Overall used/available physical memory
6	Overall used/available virtual memory
7	Used physical/virtual memory by this Runtime Manager
8	Process handles used by this Runtime Manager
9	GDI resources/UserObjects used by this Runtime Manager
10	Message Description

Table 8-1: Log files format

S_log example:

```
[Info]   |30| 00:35:26.146 |  2628 | 2663792k/14110392k | 2983264k/24429476k | 51660k/18932k |
154 | 4/14 | Sent '13' to Host '5.2FullSetup-RTS' Conn: 1
```

H_log example

```
[Info]   |20| 01:00:57.656 |  5584 | 1005944k/15768240k | 1097012k/26315728k | 8276k/7004k |
84 | 4/5 | Username: SYSTEM, Computername: WIN-RSL5FCPK7A4
```

8.3.2. Crash / Failure Logging

In the case of a System or Application Crash or Failure an additional error log file will be created with a format:

```
C_<Process ID>_yyyymmdd.log
```

This will log crashes under the following circumstances.

- Import Crashes - The log file will have stack information specific to the status of the system when the crash/failure occurred.
- OCR Engine Crashes - The log file will have a "ReadZone" entry for the specific OCR engine for which the crash occurred and stack information specific to the status of the system when the crash/failure occurred.
- Classification Engine Crashes - The log file will have a "Classify" entry for the specific Classification engine for which the crash occurred, the specific Class name where the crash occurs, and stack information specific to the status of the system when the crash/failure occurred.
- Extraction Engine Crashes - The log file will have an "EvalZone" entry for the specific Extraction engine for which the crash occurred, the field where the crash occurs, and stack information specific to the status of the system when the crash/failure occurred.
- Export crashes - The log file will have a "StepExport" and stack information specific to the status of the system when the crash/failure occurred.
- Clean-up crashes - The log file will have a "ProcessDocumentsCleanUp" and stack information specific to the status of the system when the crash/ failure occurred.
- Script Events - The name of the script event, which could be project level or a certain class. For script events on field level, the field name will be added to the crash/failure log.

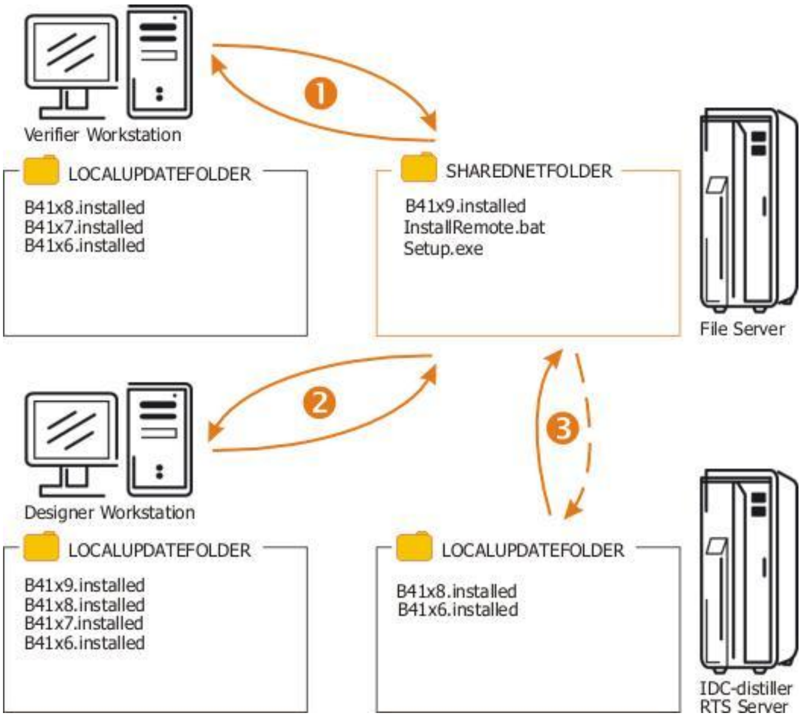
9 Auto-Update

9.1 Description

9.1.1. How the Automatic Update Works

The auto update feature allows the Administrator to update automatically WebCenter Forms Recognition software versions with latest available service updates on different workstations where WebCenter Forms Recognition applications are running. For this purpose, it is required to set up a “Shared Network Folder” where the new service updates are to be placed.

The workstations must have sufficient file access permissions to access this shared directory.



Furthermore, a Local Update Folder has to exist for each workstation, where automatic updates are to be configured. Through this directory, the system will check which software builds have already been installed.

There are three files to be copied to the Shared Network Folder to enable automatic updates:

- One system file (called “Build Level” file for further reference) identifies the build level of the service update to deploy automatically (for example, “B4117.installed“).
- The service update to deploy automatically. (It is recommended to define a unique name associated with execution of service update installations, for example “Setup.exe“.)
- One batch file for execution of the service update in Silent Mode ("InstallRemote.bat“).

When starting the Verifier (or Designer/RTS applications) the batch file will check whether the same “Build Level” file located in the “Shared Network Folder is already available in the Local Update Folder.

1. If this is not the case, the "InstallRemote.bat" is going to be invoked. After completion of the silent installation, the “Build Level” file from the Shared Network Folder is going to be copied to the Local Update Folder directory and the Verifier (or the other desired application) is going to be started.

2. In case the same “Build Level” file is already available in the Local Update Folder, the silent update step is going to be skipped and only the launching of the application is going to take place.
3. In order to auto-update the Runtime Server (RTS) software version, the RTS service has to be stopped first. It is recommended to apply this operation when the RTS is not loaded with the document processing activities. For this purpose the Windows "Winat" function can be used, which can be configured to:

- Stop the RTS service at the specific desired time (e.g., via usage of the "Stop RTS running as NT Service.bat" from the application directory of Forms Recognition).
- Start the auto-update feature (the file "AutoInstall.bat" from the Forms Recognition application directory contains all required instructions).
  Note: The enclosed file paths have to be adjusted manually.
- Start the RTS service at the desired time (e.g., via usage of the "Start RTS as NT Service.bat" from the application directory of Forms Recognition).

The used batch files are going to be created during the full setup installation of WebCenter Forms Recognition. In case the Auto Update feature was not configured during the installation, the used file paths have to be entered/adjusted in the following batch files (after the installation): “StartIfNotInstalled.bat“, “AutoInstall.bat“. In order to enable the auto update feature for the Verifier and Designer applications, they have to be started via the corresponding “DstVer_AutoUpdate.bat” (or “DstDsr_AutoUpdate.bat") from the WebCenter Forms Recognition application directory.

9.1.2. Manual Configuration of the Auto Update Function

9.1.2.1. Editing the “AutoInstall.bat” Batch File

The path Shared Network Folder has to be entered in the “AutoInstall.bat“. For this purpose, edit the “AutoInstall.bat“ batch file using, e.g., Windows Notepad application (right click on the “AutoInstall.bat“ file in Windows Explorer, select *Edit* menu item).

```
@echo off

REM
====================================================================================================
=====

REM This Batch file checks the Shared Network Install folder ("SHAREDNETFOLDER" variable) for
available

REM software service updates.

REM Please adjust the "SHAREDNETFOLDER" variable with your network path, where new service updates
are

REM going to be placed for automatic installation by Verifier and/or Runtime Service workstations.

REM

REM Example: \Your File ServerYour Forms Recognition Service Update Share

REM

REM "ACTIVEDIR" variable: Location of this batch file (generated automatically by the Forms
Recognition setup).

REM

REM (c) 2008 Oracle Corporation

REM
====================================================================================================
=====

SET SHAREDNETFOLDER ="\\YourNetworkInstallServerName\YourInstallShareName"

SET ACTIVEDIR ="C:\Programme\Oracle\Forms Recognition"
```

```
IF EXIST %SHAREDNETFOLDER %\*.installed GOTO NEW_SU

echo no.updates.available.root

GOTO END

:NEW_SU

CD %SHAREDNETFOLDER %

for %%1 in (*.installed) do Call %ACTIVEDIR %\StartIfNotInstalled %%1 %SHAREDNETFOLDER % %ACTIVEDIR
%

CD %ACTIVEDIR %

:END
```

Change the content of the variable “SHAREDNETWORKFOLDER” to the network location of the new service updates that is going to be used as the master location of the software setups for Auto Update feature.

9.1.2.2. Change Shortcuts

The shortcuts used to start Designer and/or Verifier applications (Available in Windows Start menu and/or on the desktop) invoke the corresponding programs directly, in case the Auto Update function was not configured during the setup.

In order to adjust this, replace the target file “DstDsr.exe“ (or “DstVer.exe“ for the Verifier application’s shortcut) with the batch file DstDsr_AutoUpdate.bat“ (or “DstVer_AutoUpdate.bat“) in the *Properties* of the corresponding application’s shortcut (Right click on the shortcut and select the *Properties* menu item).

9.2 Usage

The Auto Update feature can be used for automation of the WebCenter Forms Recognition installation process and can save time in administration efforts to deploy future software update on, e.g., 100 different production developments, and testing workstations and servers where WebCenter Forms Recognition is running.

10 Enabling Additional OCR Engine Languages

WebCenter Forms Recognition supports many OCR engine languages. The main languages, English, French, German, Spanish, and Italian are enabled by default, but for some OCR engines you can request additional recognition languages at Oracle.

Oracle will confirm that the requested language is effectively supported by the desired OCR engine and will deliver special custom language files in this case.

10.1 To Enable a Language for an OCR Engine

A language can only be processed by WebCenter Forms Recognition if it is installed on the server machine, and if it is present in the FineReader directory:

1. Exit all Forms Recognition applications.
2. On the WebCenter Forms Recognition servers, stop the WebCenter Forms Recognition Runtime Server services.
3. Copy the custom language file(s) received from Oracle to the .\Langfile sub-folder on your local system.
4. Copy the language file to the appropriate FineReader folder:

   for instance: .\ Oracle\Components\Cairo\Finereader8 on all configured WebCenter Forms Recognition machines.
5. Restart the WebCenter Forms Recognition Runtime Server services.
6. Restart the client application.

Note: If not already done, you first have to enable the support of double byte and extended ASCII character sets, (Greek, Russian, Hebrew) for your system. The steps depend on your operating system:

10.2 To add Input Language for Windows 7

1. Select *Start* → *Control Panel* → *Clock, Language, and Region* → *Region and Language.*
2. Click the *Keyboards and Languages* tab.
3. Click *Change keyboards*.
4. Under *Installed services*, click *Add*.
5. Double-click the language you want to add, double-click *Keyboard*.
6. Select the text services options you want to add.
7. Click *OK* to confirm.

10.3 To add Input Language for Windows XP

1. Select *Start* → *Control Panel* → *Language and Regional Options*.
2. Select the *Languages* tab.
3. Check the two check boxes for *Supplemental language support.*
4. Click *Apply*.
5. Reboot the machine.

10.4 To add Input Language for Windows Vista

1. Select *Start* → *Control Panel* → *Clock, Language, and Region* → *Regional and Language Options.*

2. Click the *Keyboards and Languages* tab.
3. Click *Change keyboards*.
4. Under *Installed services*, click *Add*.
5. Double-click the language you want to add, double-click the text services you want to add.
6. Select the text services options you want to add.
7. Click *OK* to confirm.

10.5 To add Input Language for Windows 2008

1. Select *Start* → *Control Panel* → *Regional and Language Options.*
2. Click the *Keyboards and Languages* tab.
3. Click *Change keyboards*.
4. Under *Installed services*, click *Add*.
5. Double-click the language you want to add, double-click the text services you want to add.
6. Select the text services options you want to add.
7. Click *OK* to confirm.

10.6 To add Input Language for Windows 2003

1. Select *Start* → *Control Panel* → *Regional and Language Options.*
2. Select the *Languages* tab.
3. Under *Supplemental language support*, check the two check boxes.
4. Click *OK* or *Apply*.
5. Reboot the machine.

11 Workarounds

11.1 Running Multiple Web Verifier and RTS instances

Problem Description

When running more than approx. 12 concurrent Web Verifier user sessions or more than approx. 14 Runtime Service instances, the system may start experiencing lack of Windows desktop heap resources and the extra user sessions / RTS instances can be failing with different internal memory allocation errors.

Problem Cause

The default Windows OS setting of desktop heap size for the non-interactive Windows station often appears to be too low to host multiple simultaneously running Web Verifier or Runtime Service instances with extensive script engine utilization.

Steps to Resolve / Recommended Configuration Changes

1. Open Windows Registry Editor.
2. Browse to the key "[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems\Windows]".
3. Check / modify the third argument of the "SharedSection" parameter:

   SharedSection=1024,3072,512

   512 (KB) is exactly the default value that causes the issue as described in the "Problem Description" section above.

   Note that for some OS versions, this default setting can be different. The table below gives the recommended values for this setting:

# of RTS and/or WVC instances	DH Size in KB
1 – 10	512
11 – 24	1024
25 – 36	1536
37 – 48	2048
49 – 60	2560
61 – 72	3072

   Legend:

   DH Size: Desktop heap size for non-interactive window station

   # of RTS and/or WVC: Cumulative number of simultaneously running Runtime Service instances PLUS number of concurrent Web Verifier users running on the same physical server.

4. After modifying this parameter reboot the server.

Appendix A Web.Config Options

The table below contains some items which can be modified in the Web.Config with regards to enabling/disabling/customizing certain features.

Option	Default Value	Description
ADOCommandExecutionTimeOut	Web Verifier	Optional attribute. Timeout in seconds for database stored procedures execution. If not specified timeout from database connection string is used. `<client ADOCommandExecutionTimeOut=10></client>`
AllowAccessToDocumentsToIndexOnly	false	This option controls whether navigation is enabled only for documents for indexing (those with states from enabled workflow input states). This option only takes effect when "Disable navigation to valid documents" is set to *True* in settings. When set to *False* (or not included in web.config) WVC works as before allowing navigation to out-of-workflow documents.

assembly		*Note: This attribute is not configurable.*
		Required attribute. Assembly contains custom user provider class.
		`<user.controller>`
		`<userProvider.assembly="Brainware.Verifier.WebClient" ...`
		`</user.controller>`
		Required attribute. Assembly containts custom logger provider class.
		`<system.logger>`
		`<userProvider.assembly="Brainware.System.Logger" ...`
		`</system.logger>`

batchColumnVisibility	Web Verifier	Configuration of additional columns in the Batch View:
		Setting this attribute to true will display the External Group ID batch column in WVC
		`externalGroupIdColumn visible="true"/`
		Setting this attribute to true will display the External Batch Name column in WVC
		`externalBatchNameColumn visible="true"/`
		Setting this attribute to true will display the Transaction ID batch column in WVC
		`transactionIdColumn visible="true"/`
		Setting this attribute to true will display the Transaction Type batch column in WVC
		`transactionTypeColumn visible="true"/`

Option	Default Value	Description
BatchViewPageSize	20	The number of batches to display on Web Verifier in the batch list. Any batches exceeding that count are divided into other navigation pages. The default value is 20, allowing for up to 20 batches to be shown in the Web Verifier batch list. Example `<add key="BatchViewPageSize" value="20"/>`
cacheSize	5	An optional parameter in the web.config that allows users to specify the number of documents to cache when working on a batch of documents. The cache size is associated with the loading data issue. It can avoid inaccessibility of the workstation when loading a huge amount of batches at once. Within the web.config file, set the value for the cacheSize property within the <system.controllers>/<document.controller>/<document> section. The default value is 5, which means the minimum number of document cache is 5. Changing the value to 1 will disable document caching.

class		Required attribute. Custom user provider.
		`<user.controller>`
		`<userProvider.class="Brainware.Verifier.WebClient.Core.WebUserProvider" ...`
		`</user.controller>`
		Required attribute. Custom logger provider.
		`<system.logger>`
		`<userProvider.assembly="Brainware.System.Logger.LoggerFactory" ...`
		`</system.logger>`

connectionStrings		Configuration connects to database.
		`<connectionStrings>`
		`<add name="Entities" connectionString="…” providerName="System.Data.EntityClient" />`
		`</connectionStrings>`

DocumentViewPageSize	4	The number of folders to display in the Document Tree view, when selecting *Show Selected Batch*. The default value, 4, denotes 4 folders to display in *Show Selected Batch* view; any additional batches are shown in subsequent navigation panels.

Option	Default Value	Description
		Example `<add key="DocumentViewPageSize" value="4"/>`

formEvents		Required attribute. Enable/disable focus changed event on fields on the Verification view.
		`<focusChanged enabled=”true|false”/>`
		Controls firing of FocusChanged event on Enter key press in a field. Defaults to true, if web.config does not have this setting, it is considered to be turned on. This setting has no effect on FocusChanged event in case <mouseClicked> is set to true.
		Required attribute. Enable/disable mouse click event on fields and table on the Verification view in Indexing mode.
		`<mouseClicked enabled="true"/>`
		Required attribute. Enable/disable tabPressed event on fields and table on the Verification view in Indexing mode.
		`<tabPressed enabled=”true”/>`
		Required attribute. Enable/disable itemCopied event.
		`<itemCopied enabled=”true”/>`
		Required attribute. Enable/disable table cell select event.
		`<tableCellSelected enabled=”true”/>`

inactiveUserTimeout		Required attribute. It is not used to control user session timeout. The user session timeout is controlled by the <sessionState Timeout. parameter.

inspectionServerTimeout		Required attribute. Time of the periodical ping the IIS server by the process in separate mode.
		`<system.project>`
		`<project. inspectionServerTimeout ="00:00:20" ...`
		`</system.project>`

inspectionTimeOut		Required attribute. It is not used to control user session timeout. The user session timeout is controlled by the <sessionState Timeout. parameter..
instanceName	Web Verifier	The name of the Web module that will be shown to have access the batch list. Example `<client instanceName="Web Verifier"></client>`
licensePath	“C:\My Shared License\Runtime.lic”	The location of the shared license file, reference documentation regarding configuration. This should point to the License Share file.

Option	Default Value	Description
		Example `<project licensePath="C:\My Shared License\Runtime.lic"   mpdDistance="19" mpdThreshold="60"/>`
loadInSeparateProcess	True	Required attribute. Read only. The value is 'True' only.
pathToProjectExe	"Oracle \ WebCenter Forms Recognition \ bin\"	The location of the WebCenter Forms Recognition Designer module (DstDsr.exe). Example `pathToProjectExe="C:\Program Files\Oracle\WebCenter Forms Recognition\bin\"`
priority	ERROR	Set this attribute to identify tracing level. Options are, - DEBUG: Full tracing of information and errors. - ERROR: Errors only. Example `<priority value="ERROR"/>`
reinitScript	True	By default, this attribute is always set to true. This will recover the script engine whenever a script error occurs in Web Verifier application.
remoteObjectRenewalTimeout	60	Optional attribute. Remote object references are renewed at this time period (in seconds). Defaults to 60. Minimum accepted value is 30. The lower the number the faster unused objects free memory but this can lead to errors for long running commands. One can increase this value if some actions (i.e. field validation) take a while to finish with remoting error. *Note that this value should be set in both web application config file and Brainware.System.Project.exe config file* `<client remoteObjectRenewalTimeout =45></client>`
ShowExtendedErrorMessages	True	Set this attribute to true to enable stack trace information in the error messages appearing in Web Verifier. Messages are written to the Trace Log file. Allowable values are True and False. Example `<add key="ShowExtendedErrorMessages" value="true"/>`

Web.Config Options

Option	Default Value	Description
slogan	*Empty*	A text message that can be displayed on the Web Verifier browser header with corporate messages / announcements / Corporate Slogan.

Trace log/ debug file 1		It keeps the debug/ trace log file under X size. Once the X size is reached, the log is recycled/ deleted and a new log is created.
		For example, below its set to 100kb, as soon as the trace.log file went over 100kb the log file size changed to 0kb and new log messages were written.
		`<appender name="RollingFile" type="log4net.Appender.RollingFileAppender,log4net">`
		`<layout type="log4net.Layout.PatternLayout,log4net">`

Trace log/ debug file 2		When the file reaches X size, it is archived as trace.log.1 and a new trace.log will be created. When the trace.log exceeds size once more, trace.log.1 becomes trace.log.2 and the existing trace.log becomes trace.log.1, again a new trace.log will be created.
		trace.log.1
		config
		`<appender name="RollingFile" type="log4net.Appender.RollingFileAppender,log4net">`
		`<layout type="log4net.Layout.PatternLayout,log4net">`

sessionState Timeout	20	The <sessionState Timeout parameter controls the timeout for a user session. The value represents the number of minutes that a user is allowed to be inactive before the session is ended.
usePath		Required attribute. Enable/disable using pathToProjectExe parameter. Set this attribute to false to set pathToProjectExe parameter is current directory.
waitLoadTimeOut		Required attribute. Timeout for initial loading of project.exe. This parameter is used with enable option: loadInSeparateProcess = true

Table 11-1: Options for "web.config”

Appendix B File Permission Matrix

The table below displays the various file permissions that are used within WebCenter Forms Recognition.

Role/Group	Description
Administrators	Administrator user with full access rights to all application modules and features.
Developers	The groups of users that develop, maintain, and enhance projects.
Learnset Manager	Typically one user in the organization responsible for maintaining the project Learnsets.
Advanced Verifiers	Several users responsible for identifying documents for improvements to the project Learnset.
Standard Verifiers	Data entry clerks 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.

Directory	Groups	NTFS Permissions						
		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**	☑	☑	☑	☑	☑	☑	□
Root Batch Folder	**Administrators** **Developers** **Learnset Manager** **Advanced Verifiers** **Standard Verifiers** **RTS Service User**	☑	☑	☑	☑	☑	☑	□
Common Folder	**Administrators** **Developers** **Learnset Manager** **Advanced Verifiers**	☑	☑	☑	☑	☑	☑	□
	Standard Verifiers **RTS Service User**	□	□	□	□	□	□	☑
Global Project	**Administrators** **Developers** **Learnset Manager** **RTS Service User**	☑	☑	☑	☑	☑	☑	□
	Advanced Verifiers **Standard Verifiers**	□	□	☑	☑	☑	□	□
Local Project	**Administrators** **Developers**	☑	☑	☑	☑	☑	☑	□

Directory	Groups	NTFS Permissions						
		Full Control	Modify	Read & Execute	List Folder Content	Read	Write	No Access
	Learnset Manager RTS Service User Standard Verifiers	□	□	□	□	□	□	☑
	Advanced Verifiers	☑	☑	☑	☑	☑	☑	□
Local Learnset	Administrators Developers	☑	☑	☑	☑	☑	☑	□
	Learnset Manager RTS Service User Standard Verifiers	□	□	□	□	□	□	☑
	Advanced Verifiers	☑	☑	☑	☑	☑	☑	□
Global Learnset	Administrators Developers Learnset Manager RTS Service User	☑	☑	☑	☑	☑	☑	□
	Advanced Verifiers Standard Verifiers	□	□	☑	☑	☑	□	□
ASE Pool	Administrators Developers RTS Service User	☑	☑	☑	☑	☑	☑	□
	Learnset Manager Advanced Verifiers Standard Verifiers	□	□	☑	☑	☑	□	□
ASSA CSV File	Administrators Developers RTS Service User	☑	☑	☑	☑	☑	☑	□
	Learnset Manager Advanced Verifiers Standard Verifiers	□	□	□	□	□	□	☑

Appendix C Registry Options

The table below contains some items which can be modified in the Registry with regards to enabling/disabling/customizing certain features.

Option	Default Value	Description
DumpProjectScriptCode	N/A	This key is available to allow Support/Certified System Administrator / Professional Services to carry out advanced troubleshooting on any issues with script running on the Web Verifier. To create the registry key to provide script dumps, follow the instructions outlined below: 1. Launch Windows Registry Editor 2. Navigate to HKEY_LOCAL_MACHINE, SOFTWARE, Oracle (or HKEY_LOCAL_MACHINE, SOFTWARE, Wow6432Node, Oracle for 64 bit systems), and Cedar location. 3. Create a new REG_DWORD (DWORD Value key) and call it DumpProjectScriptCode 4. Modify the new key created and enter the one of the following values: 3 – to enable this feature for script page export. 0 – to disable this feature. With the feature enabled the scripting engine files can be used to review any compilation problems, this is an advanced feature and requires advanced knowledge of the product.

Option	Default Value	Description
ErrorTraceDir	N/A	The ErrorTraceDir registry key is available for those customers who wish to place the component tracing logs in a different location than the default WebCenter Forms Recognition\bin\log folder. The registry key allows the administrator to place the logs in a specific folder location separate from the core product logs. The registry setting is only applicable for the component logs, not for the core product logs. To configure a new location for Component Logs, follow the instructions outlines below: 1. Launch Windows Registry Editor 2. Navigate to HKEY_LOCAL_MACHINE, SOFTWARE, Oracle (or HKEY_LOCAL_MACHINE, SOFTWARE, Wow6432Node, Oracle for 64 bit systems), and ErrorTrace location. 3. Create a new REG_SZ (String Value key) and call it ErrorTraceDir 4. Modify the new key created and enter the filepath location for component logs to be entered. Verify that the path entered exists and the service account/user has sufficient permissions to write to that location. For the change to take place, exit all WebCenter Forms Recognition application, and stop any services running on the machine related to WebCenter Forms Recognition, then launch the application and all new component logs will be written in the desired location.
LanguageSupportWork-flowSettingsVisible	N/A	This registry key is used within WebCenter Forms Recognition to allow the developer to utilize advanced Language Support configuration and setting. This additional feature can be enabled via the Registry using the steps outlined below: 1. On the server/machine where Designer is installed and used, launch the Windows Registry Editor. 2. Navigate to HKEY_LOCAL_MACHINE, SOFTWARE, Oracle (or HKEY_LOCAL_MACHINE, SOFTWARE, Wow6432Node, Oracle for 64 bit systems), and Cedar location. 3. Create a new REG_DWORD (DWORD Value key) and call it LanguageSupportWorkflowSettingsVisible 4. Modify the new key created and enter the one of the following values: a. 1 – to enable this feature to allow the developer to configure advanced options for language conversion. b. 0 – to disable this feature. For the change to take place, exit all WebCenter Forms Recognition application, and stop any services running on the machine related to WebCenter Forms Recognition, then launch the application and all new component logs will be written in the desired

Option	Default Value	Description
		location. To view the advanced options in WebCenter Forms Recognition Designer, 1. Launch Designer application 2. From the Options Menu select Settings 3. Navigate to the Definition tab and new settings will display. With the settings showing, the developer can utilize additional language features which will allow them to convert words/etc to extended ASCII character set.
ASEnginePoolAllowed **CharDifference**	*N/A*	In certain instances some duplicates in the ASE/ASSA search may not be returned from the vendor/customer search. In these cases it may be that the ASSA engine perceives these as duplicates of existing entries. There is a configuration step that can be undertaken which can return the suspected duplicates as well. This may slightly increase the results of the ASE pool, but also return potential items which were not returned in the original search. To configure the ASE pool to return additional likely results: - Launch Registry Editor - Navigate to HKLM\Software \Oracle\Cedar (or HKLM\Software\Wow6432Node\Oracle\Cedar for 64 bit systems) - Create a new DWORD registry variable for ASEnginePoolAllowedCharDifference - Close the Registry Editor Reanalyze the document once more and any missing entries should now appear.
HideBatchReleaseDialog	*0*	This key allows Support/ Certified System Administrator/ professional Services to disable the Batch Release dialog box within the Verifier, where the business does not require prompting users on next task. The registry value can be used to determine the next action carried out by users. The default action of the Batch Release dialog box is to verify the next invalid batch. When the dialog is suppressed, 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. To create the registry key to suppress the Batch Release confirmation screen, follow the instructions below: – Launch Windows Registry Editor – Navigate to HKEY_LOCAL_MACHINE\SOFTWARE \Oracle\Cedar (or HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Oracle\Cedar for 64 bit systems) – Create a new REG_DWORD (DWORD Value key) and call it

Option	Default Value	Description
		HidebatchReleaseDialog – Modify the new key created and enter the one of the following values: • 0- to enable the confirmation screen (default) • 1- to disable/ hide the confirmation screen For the change to take place, exit all WebCenter Forms Recognition application, and then launch the application again. To view that the change has been implemented, – Launch Verifier – Verify the batch to completion – no dialog box should appear This setting is available from version 5.3.
All	1	The ErrorTrace registry Key was introduced into core product logs to provide additional trace information on any errors or warnings in the system. The default value after installation is to record errors only related details. Modify the registry values to set the value from 0 to either 1, 2, or 3 1-Only Errors 2-Errors & Warnings 3-Errors & Warnings&Information To configure ErrorTrace All value: - Launch Registry Editor - Navigate to HKEY_LOCAL_MACHINE\SOFTWARE \Oracle\ErrorTrace (or HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Oracle\ErrorTrace for 64 bit systems) - Create a new DWORD registry variable for All, set to the appropriate value of either 0, 1, 2, or 3. - Close the Registry Editor
MaximumDiskspace-UsageMB	N/A	This registry value controls the amount of disk space allocated for component level logs on this server / workstation in MB. Setting this value to “0” has the same effect as if the value is not created at all, which is “deactivated”. To configure the ASE pool to return additional likely results: - Launch Registry Editor - Navigate to HKEY_LOCAL_MACHINE\SOFTWARE \Oracle\ErrorTrace (or HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Oracle\ErrorTrace for 64 bit systems) - Create a new DWORD registry variable for MaximumDiskspaceUsageMB, set to the appropriate value in Mb. - Close the Registry Editor

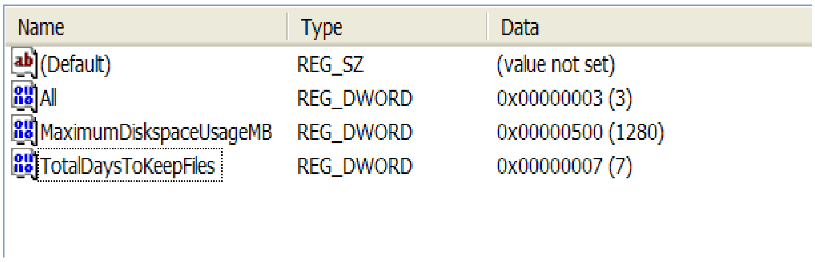
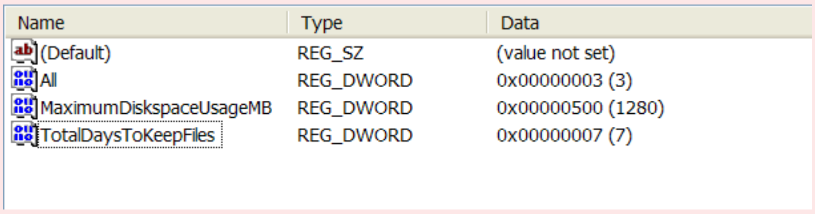
<table>
<tr><th>Option</th><th>Default Value</th><th>Description</th></tr>
<tr><td></td><td></td><td><table><tr><th>Name</th><th>Type</th><th>Data</th></tr><tr><td>(Default)</td><td>REG_SZ</td><td>(value not set)</td></tr><tr><td>All</td><td>REG_DWORD</td><td>0x00000003 (3)</td></tr><tr><td>MaximumDiskspaceUsageMB</td><td>REG_DWORD</td><td>0x00000500 (1280)</td></tr><tr><td>TotalDaysToKeepFiles</td><td>REG_DWORD</td><td>0x00000007 (7)</td></tr></table></td></tr>
<tr><td><b>TotalDaysToKeepFiles</b></td><td>N/A</td><td>This registry value maintains the number of days the old component level logs are kept by the WebCenter Forms Recognition server. Setting this value to “0” has the same effect as if the value is not created at all, which is “deactivated”.
To configure the ASE pool to return additional likely results:
- Launch Registry Editor
- Navigate to HKEY_LOCAL_MACHINE\SOFTWARE \Oracle\ErrorTrace (or HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Oracle\ErrorTrace for 64 bit systems)
- Create a new DWORD registry variable for TotalDaysToKeepFiles, set to the appropriate value in numeric (total days to maintain logs – the screenshot below shows 7 days).
- Close the Registry Editor
<table><tr><th>Name</th><th>Type</th><th>Data</th></tr><tr><td>(Default)</td><td>REG_SZ</td><td>(value not set)</td></tr><tr><td>All</td><td>REG_DWORD</td><td>0x00000003 (3)</td></tr><tr><td>MaximumDiskspaceUsageMB</td><td>REG_DWORD</td><td>0x00000500 (1280)</td></tr><tr><td>TotalDaysToKeepFiles</td><td>REG_DWORD</td><td>0x00000007 (7)</td></tr></table></td></tr>
</table>

Table 11-2: Registry Options