

# Oracle® Distributed Document Capture

Installation Guide

Release 10gR3

E13869-01

November 2010

---

This document describes how to install Oracle Distributed Document Capture. It contains the following main sections:

- ["Installation Overview"](#) on page 1
- ["Installing Oracle Distributed Document Capture"](#) on page 4
- ["Configuring Capture"](#) on page 5
- ["Configuring the Server"](#) on page 10
- ["Copyright and Patent Notices"](#) on page 21

## 1 Installation Overview

This section covers the following topics:

- ["About Oracle Distributed Document Capture"](#) on page 1
- ["List of Components"](#) on page 2
- ["System Requirements"](#) on page 2
- ["Implementation"](#) on page 3

### 1.1 About Oracle Distributed Document Capture

Oracle Distributed Document Capture provides scanning and optional indexing at remote locations using the Internet or a corporate intranet. It is comprised of these components:

- The *client*, which is automatically downloaded and installed as soon as users connect to the server. Running entirely in the user's Web browser, it uses the industry standard TWAIN interface to capture documents from desktop scanners or other TWAIN compliant input devices.

In the client, users scan or import documents in batches, review and index them, then send them to the server. Users scan and index documents using settings administrators save in scan profiles.

- The *server*, which runs as a service and processes batches received from clients. Documents are committed (archived) so they can be accessed in the content management system. Documents are committed using settings saved in a commit profile.
- The *Capture Administration* component, which provides a centralized area for administrators to manage file cabinets, index fields, users, commit profiles, pick-lists, and database lookups.

After installing and configuring components as described in this guide, refer to the *Administrator's Guide for Oracle Distributed Document Capture* for information about Capture administration.

## 1.2 List of Components

Oracle Distributed Document Capture includes the components listed in [Table 1](#).

**Table 1 Oracle Distributed Document Capture Components**

Component Type	Component
Capture Administration	Admin
	Batch Manager
	Import/Export
Oracle Distributed Document Capture	
Commit Drivers	Oracle I/PM Commit Driver
	Oracle I/PM 11g Commit Driver
	Oracle UCM Commit Driver
	Oracle UCM 11g Commit Driver
	Text File Commit Driver
	Database Commit Driver

## 1.3 System Requirements

The following table lists the minimum operating system (O/S), processor, and memory requirements for Oracle Distributed Document Capture components:

Component	Windows O/S	Processor	Available Component Memory
Client	XP/Vista/7	Pentium 4, 1 Ghz	64 MB
Server	XP/2003/Vista/7/2008 R2	Pentium 4, 2 Ghz	256 MB

- The server workstation requires at least 500MB of free hard disk space.
- For multi-user systems, a database server is required (Oracle 10.1 or above, or Microsoft SQL Server 2000 or above). Oracle Database 11gR2 is supported.
- The Oracle Distributed Document Capture server requires Microsoft Internet Information Server (IIS) version 5.x, 6.x, or 7.x. Version 7.x is supported only on Windows Vista. In addition, the Java Runtime Environment (JRE) version 1.6 or above must be installed on any computer using Oracle Distributed Document Capture Administration.
- The client requires Microsoft Internet Explorer 6 or above (32-bit version) and a TWAIN compliant device. The client will not run in the 64-bit version of Internet Explorer. Scripting must be enabled on the client.
- The Import/Export utility requires Java 1.6 or higher. If your configuration includes Oracle Document Capture components installed on separate workstations, you must install the Import/Export utility on each workstation containing one or more Oracle Document Capture components.

- This release provides 64-bit support on the following platforms, except for the Import Server's virtual printer, which is supported on 32-bit platforms only:
  - Windows 2003
  - Windows 7
  - Windows 2008 R2

---

---

**Note:** In order to use Oracle Distributed Document Capture on a 64-bit system, a 32-bit Java Virtual Machine 1.6.0\_10 or higher must be installed. (This release does not support 64-bit JVMs.) The Oracle UCM 10g, Oracle UCM 11g, and Oracle I/PM 11g commit drivers require Java.

---

---

## 1.4 Implementation

Figure 1 displays a typical Oracle Distributed Document Capture implementation scenario.

- Capture Administration is handled in the **Document Capture** application, where administrators configure elements such as file cabinets, users, commit profiles, pick-lists, and database lookups.
- The **Distributed Document Capture Server** is administered through a Web browser, allowing administrators to centrally configure scanning profiles, which become available to clients based on their assigned file cabinets.
- **End-User Clients** capture and index documents from desktop scanners or other TWAIN-compliant devices from remote sites, or by importing from disk. After sending completed batches to the server as PAK files, receipt is verified and the batches are removed from client workstations.
- After the server processes received batches, they are typically committed (archived) directly into a content management system such as Oracle Universal Content Management (Oracle UCM) or Oracle Imaging and Process Management (Oracle I/PM). Alternately, batches may be sent to the **Oracle Document Capture Commit Server**, which performs commit processing to the content management system.

---

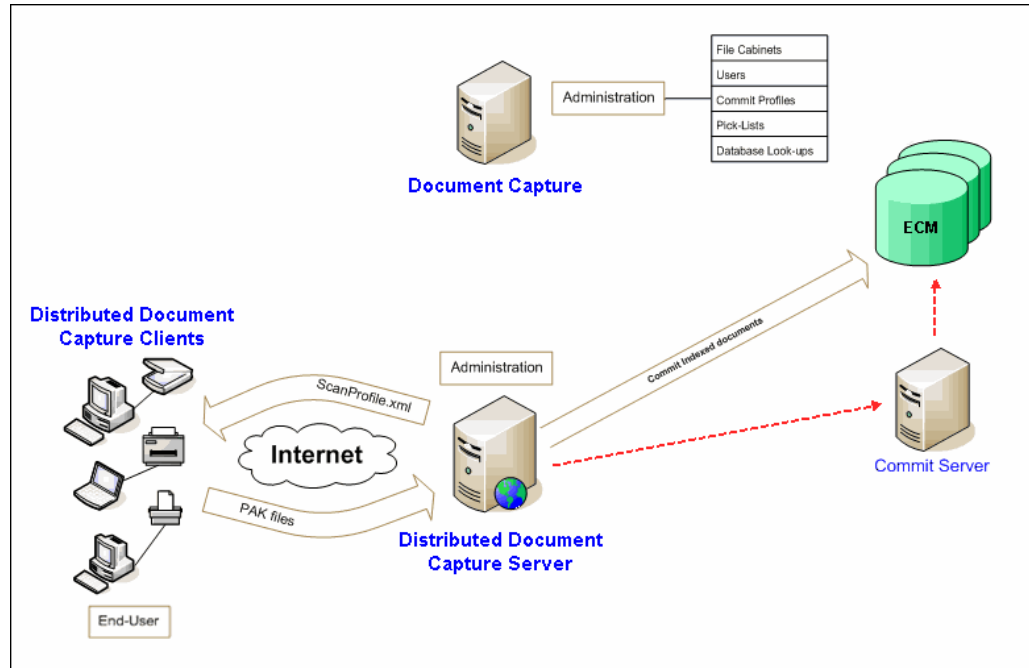
---

**Note:** The Oracle Document Capture Commit Server is recommended for production environments, particularly if committing directly to a content management system. If the content management system is unavailable, the Commit Server can automatically retry batch commits.

---

---

Figure 1 Typical Configuration of Oracle Distributed Document Capture Components



## 2 Installing Oracle Distributed Document Capture

This section covers the following topics:

- ["Installing Oracle Distributed Document Capture Components"](#) on page 4
- ["Uninstalling the Software"](#) on page 5

### 2.1 Installing Oracle Distributed Document Capture Components

Installation consists of running the installer and selecting the components appropriate for that workstation. (You can also choose the **Complete** option to install all components.) Also see ["Implementation"](#) on page 3 for a diagram illustrating a typical implementation.

---

**Note:** You must be logged in to Windows with Administrator privileges to install Capture.

---

1. Run the SETUP.EXE application for Oracle Distributed Document Capture. The Installation Wizard is displayed.
2. Click **Next**.  
When prompted, enter a username and organization and identify an installation folder. The default installation folder is C:\Program Files\Oracle\Document Capture.  
The Setup Type window is displayed.
3. Select **Complete** to install all Capture components. Select **Custom** to install certain components only. Click **Next**.

The setup application guides you through the rest of the installation process.

4. Complete the installation by rebooting the computer when prompted.

---

---

**Note:** You must restart your computer when prompted to complete the installation.

---

---

## 2.2 Uninstalling the Software

To uninstall Oracle Distributed Document Capture, follow standard Windows procedures for removing programs in the Control Panel.

## 3 Configuring Capture

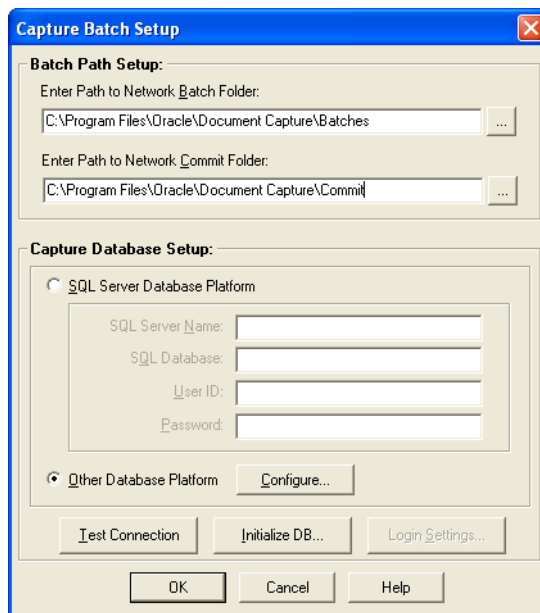
This section covers the following topics:

- "Specifying Capture Batch Folders" on page 5
- "Configuring the Capture Database" on page 6
- "Configuring Security" on page 10

### 3.1 Specifying Capture Batch Folders

To begin configuring Capture, start the application and complete settings in the screens that are displayed.

1. Start Oracle Document Capture by double-clicking its desktop icon. (You can also start the application from the list of programs on the Start menu.) The Capture Batch Setup screen is displayed.



2. In the **Enter Path to Network Batch Folder** field, enter or select the folder in which Capture batches will be stored. Capture creates the folder if it does not already exist.

After batches are sent to the server bundled as PAK files and extracted, the Capture batches created are stored in this location before commit processing.

If the path is on a network, we recommend using a UNC (Universal Naming Convention) Path. However, you can also use a mapped driver letter.

3. In the **Enter Path to Network Commit Folder** field, enter or select the folder to which Capture batches will be committed. Capture creates the folder if it does not already exist.

This folder specifies the default commit folder for the Commit Text File driver. It is possible to change this path on a per commit profile basis. For more information about committing batches, see the section on commit profiles in the *Oracle Distributed Document Capture Administrator Guide*.

---

---

**Important:** The Batch and Commit folders you specify in these steps should not be scanned by anti-virus programs. Anti-virus programs lock files, which makes them inaccessible to Capture processes.

---

---

## 3.2 Configuring the Capture Database

The Capture database stores batch, image, and audit information. It must be properly configured before Capture can be used.

- For *single* user systems, you can configure Capture to use a Microsoft Access database, as described in "[Configuring a Microsoft Access Database](#)" on page 8.
- For *multiple* user systems, it is recommended that you configure the Capture database on a client/server database server platform such as Oracle (see "[Configuring an Oracle Database](#)" on page 6) or Microsoft SQL (see "[Configuring a Microsoft SQL Server Database](#)" on page 9).

Here are the main steps for configuring the Capture database, described in the sections that follow.

1. Select and configure an OLE Database Provider to connect to the Capture database.
2. Initialize the database to create the Capture database schema.
3. Identify the database script. Refer to the following table to determine the script file to use.

Database Platform	Database Version	Capture Script File
Oracle	10.1 or later	Capture_Oracle.sql
Microsoft SQL Server	2000 or later	Capture_SQL.sql
Microsoft Access	2000 or later	Capture_SQL.sql

4. Set up the security model you want used. The Windows Domain and Capture security models are described in "[Configuring Security](#)" on page 10.

### 3.2.1 Configuring an Oracle Database

Follow these steps to configure Capture with an Oracle database. You will need to identify an Oracle data source.

Typically, you create a new Oracle Document Capture user/schema on the Oracle database with database administration rights. In the steps below, you identify this user in the data source and use it to initialize and create the database schema and tables. A full install of the Oracle Database client on the Oracle Document Capture server is recommended, installing the same version or greater than the Oracle database.

---

---

**Note:** These instructions assume that you have installed and configured the Oracle Database client to connect to the database in order to use it with Oracle Distributed Document Capture.

---

---

1. In the Capture Batch Setup screen, select **Other Database Platform** under Capture Database Setup options.
2. Click **Configure**.  
The Configure Database Connection screen is displayed.
3. Click **Configure DB Connection**.  
The Data Link Properties screen is displayed.
4. Select the Oracle Provider for OLE DB. Click **Next**.
5. In the **Data Source** field, enter an Oracle data source.
6. Enter a valid user name and password to the Oracle database server.
7. Click the **Test Connection** button to verify that Capture can access the Oracle database server.
8. Click **OK** to save the Database Connection settings.
9. Click **OK** to return to the Capture Batch Setup screen.
10. Click the **Initialize DB** button to create the table schema within the database.  
A message warns that this operation will erase all information in the database.

---

---

**Caution:** If the Capture database already exists and you are configuring a new Capture workstation only, do NOT click the **Initialize DB** button, since it will destroy all data and recreate the database schema.

---

---

---

---

**Note:** Whenever you initialize the database, you must delete any existing batch folders to prevent potential conflicts.

---

---

11. Click **Yes** to proceed. The Security Model screen is displayed, prompting you to select a security model.
12. Select a security model. See "[Configuring Security](#)" on page 10. You are prompted to select a database script file.
13. Select the Capture\_Oracle.SQL file in the Oracle Document Capture installation folder.

### 3.2.2 Configuring a Microsoft Access Database

---

---

**Note:** Microsoft Access database use is supported in a standalone environment only. If you do choose to share a Microsoft Access database on a network, it is highly recommended that you install the NetBEUI network protocol on all workstations that will access the database, including the file server.

---

---

After installing Capture, a blank database called Capture.mdb is placed into your installation folder (e.g., C:\Program Files\Oracle\Document Capture). Use this database when configuring Capture for use with a Microsoft Access database.

Follow these steps to configure Capture with a Microsoft Access database.

1. In the Capture Batch Setup screen, select **Other Database Platform** under Capture Database Setup options.
2. Click **Configure**.  
The Configure Database Connection screen is displayed.
3. Click **Configure DB Connection**.  
The Data Link Properties screen is displayed.
4. Select the Microsoft Jet 4.0 OLE DB Provider. Click **Next**.
5. On the Connection tab, click **Browse** under step 1. Select the Capture.mdb database file from the folder into which you installed Oracle Distributed Document Capture.  
The Capture.mdb file provided does NOT require a user name or password.
6. Click the **Test Connection** button to verify that Capture can access the database file. Click **OK**.
7. Click **OK** to save the Database Connection settings.
8. Click **OK** to return to the Batch Setup screen.
9. Click the **Initialize DB** button to create the table schema within the database.  
A message warns that this operation will erase all information in the database.

---

---

**Caution:** If the Capture database already exists and you are configuring a new Capture workstation only, do NOT click the **Initialize DB** button, since it will destroy all data and recreate the database schema.

---

---

---

---

**Note:** Whenever you initialize the database, you must delete any existing batch folders to prevent potential conflicts.

---

---

10. Click **Yes** to proceed. The Security Model screen is displayed, prompting you to select a security model.
11. Select a security model. See "[Configuring Security](#)" on page 10. You are prompted to select a database script file.



12. Select the Capture\_SQL.SQL file in the Oracle Document Capture installation folder.

### 3.2.3 Configuring a Microsoft SQL Server Database

Follow these steps to configure Capture with a Microsoft SQL Server database.

1. Contact your database administrator to create a new (blank) database on the SQL database server. The database should be at least 100MB and configured to grow dynamically to accommodate the size of the ecAudit table, which will continue to increase in size.

---

---

**Note:** The database should be at least 100MB.

---

---

2. In the Capture Batch Setup screen, select **SQL Server Database Platform** under Capture Database Setup options.
3. In the **SQL Server Name** field, enter the computer name of the SQL Server.
4. In the **SQL Database** field, enter the name of the SQL database that the administrator created.
5. In the **User ID** and **Password** fields, enter a valid user ID and password to communicate to the database server.

---

---

**Note:** It is the database administrator's responsibility to configure the users that can access the Capture database.

---

---

6. Click the **Test DSN** button.  
You do this to verify communication to the SQL Server and Capture database.
7. Click the **Initialize DB** button to create the table schema within the database.  
A message warns that this operation will erase all information in the database.

---

---

**Caution:** If the Capture database already exists and you are configuring a new Capture workstation only, do NOT click the **Initialize DB** button, because it will destroy all data and recreate the database schema.

---

---

---

---

**Caution:** Whenever you initialize the database, you must delete any existing batch folders to prevent potential conflicts.

---

---

8. Click **Yes** to proceed. The Security Model screen is displayed, prompting you to select a security model.
9. Select a security model. See "[Configuring Security](#)" on page 10. You are prompted to select a database script file.
10. Select the Capture\_SQL.SQL file in the Oracle Document Capture installation folder.

### 3.3 Configuring Security

Capture offers two security models:

- **Windows Domain:** This model determines Capture rights based on the current user's domain information. An advantage of this model is that users are not required to log in each time they activate Capture.
- **Capture:** This model is for use by systems that do not log in to a Windows Domain or do not want to use domain security. Each time a user activates Capture, a login screen is displayed, requiring the user to enter a user name and password; these values are then used to determine the rights within Capture.

---

---

**Note:** You can change the security model used, by initializing the database. However, doing so erases all data in the database and recreates the database schema.

---

---

Follow these steps to select a security model.

---

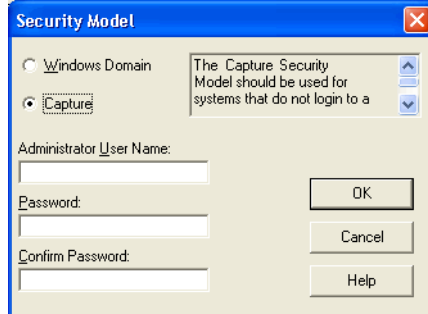
---

**Note:** The selected authenticated method also affects whether users log in and how they are authenticated. See "[Understanding Authentication](#)" on page 12.

---

---

1. After initializing the database (as described in "[Configuring the Capture Database](#)" on page 6), specify a security model in the Security Model screen that is displayed. Select **Windows Domain** or **Capture**.



The screenshot shows a dialog box titled "Security Model". It has two radio buttons: "Windows Domain" (unselected) and "Capture" (selected). To the right of the radio buttons is a text box containing the text: "The Capture Security Model should be used for systems that do not login to a". Below the radio buttons are three text input fields: "Administrator User Name:", "Password:", and "Confirm Password:". To the right of these fields are three buttons: "OK", "Cancel", and "Help".

2. If you selected Capture security, complete the **Administrator User Name** and **Password** fields.
3. Add users using Capture Administration options.  
For more information, see the section on managing Capture users in the *Administrator's Guide for Oracle Distributed Document Capture*.

## 4 Configuring the Server

This section covers the following topics:

- "[Main Configuration Steps](#)" on page 11
- "[Understanding Authentication](#)" on page 12
- "[Configuring the Virtual Directory \(Windows XP\)](#)" on page 12

- ["Configuring the Virtual Directory \(Windows 2003\)"](#) on page 14
- ["Configuring the Web Site \(Windows Vista, Windows 7, and Windows Server 2008 R2\)"](#) on page 16
- ["Configuring for Capture Security"](#) on page 18
- ["Configuring Server Settings"](#) on page 18
- ["Configuring Optional Parameters"](#) on page 20

## 4.1 Main Configuration Steps

Perform the following main steps to configure the server.

1. If needed, install the Java Runtime Environment.

Java Runtime Environment (JRE) version 1.6.0 or above must be installed on any computer using Oracle Distributed Document Capture Administration.

2. Configure the virtual directory or Web site on the Microsoft Internet Information Server.

For instructions, choose the operating system used:

- ["Configuring the Virtual Directory \(Windows XP\)"](#) on page 12
- ["Configuring the Virtual Directory \(Windows 2003\)"](#) on page 14
- ["Configuring the Web Site \(Windows Vista, Windows 7, and Windows Server 2008 R2\)"](#) on page 16

3. If using Capture security, set up Oracle Distributed Document Capture for Capture security.

See ["Configuring Security"](#) on page 10 and ["Configuring for Capture Security"](#) on page 18. (Skip this step if using Windows Domain security.)

4. Select settings in the Distributed Document Capture Server Configuration application.

Open this application by selecting it from the Oracle Distributed Document Capture Start menu options. See ["Configuring Server Settings"](#) on page 18 for more information.

On the System Settings tab of this application, configure the method by which users will be authenticated. See ["Understanding Authentication"](#) on page 12.

5. Assign rights to client users.

Users must have full control to the Program Files\Oracle\Document Capture folder. How you do this depends on your selected authentication method (see ["Understanding Authentication"](#) on page 12):

- For **Oracle Distributed Document Capture Prompted Login** access, assign these rights to the anonymous user.
- For **Web Server Authenticated Access**, assign access to the groups to which your users belong.

6. On Windows 2003 or XP systems, configure the virtual directory to use Low (IIS Process) Application Protection. (This setting is recommended.)

7. Set the Oracle Distributed Document Capture service to start automatically, and start the service.

## 4.2 Understanding Authentication

Oracle Distributed Document Capture provides two methods of authenticating users, set in the Distributed Document Capture Server Configuration application, as described in "[Configuring Server Settings](#)" on page 18.

### 4.2.1 Anonymous Access (Oracle Distributed Document Capture Prompted Login)

- Users are authenticated by IIS via the anonymous account. Anonymous access to the virtual directory or Web site (Vista) is required.
- Works with either Windows Domain or Capture Security.
- The client login screen always displays, requiring users to log in.

---

---

**Note:** You can prevent caching of Oracle Distributed Document Capture user names and passwords through LoadClient.js file configuration, as described in "[ALLOWLOGINCACHE Parameter](#)" on page 21.

---

---

### 4.2.2 Authenticated Access (Web Server Authenticated Access)

- Anonymous access to the virtual directory or Web site (Vista) must be disabled. Basic authentication options must be configured.
- Works with either Windows Domain or Capture security. If Capture security is selected, only client users who match domain users are automatically logged on. For example,

Domain user	[domain]\userA
Capture user	userA must exist

- No client login screen displays. Users do not log in.

## 4.3 Configuring the Virtual Directory (Windows XP)

Follow these steps to configure the virtual directory on an IIS server running Windows XP.

1. From the Control Panel, choose **Administrative Tools**, and then start the Internet Information Services (IIS) applet.
2. Browse to your default Web site.
3. Right-click and select **New Virtual Directory**.

This virtual directory is used by remote sites to access the client. The Creation Wizard starts. Specify an Alias name of *Capture*.

4. In the Directory field, specify the correct content directory.

The default directory is  
c:\Program Files\Oracle\Document Capture\WebPages.

5. Under Access Permissions, check the **Read** and **Run scripts** permissions.
6. Click **Next**, then select **Finish** to complete creating the virtual directory.

7. From the same Internet Information Services applet, right-click the newly created Capture folder and select **Properties**. Capture Properties are displayed.
8. Specify virtual directory settings.
  - Check **Read**.
  - Select **Low (IIS Process)** under Application Protection (recommended).
9. Click the Directory Security tab.
10. Click **Edit** in the Anonymous access and authentication control section.
11. Complete settings in the Authentication Methods screen.
  - If you chose **Anonymous access** for authentication (Oracle Distributed Document Capture Prompted Login, as described in "[Understanding Authentication](#)" on page 12), select the **Anonymous access** field and complete anonymous access settings. Note that the default username is the IUSR account. If using Capture security, specify the IUSR account here.
  - If you chose **Authenticated access** for authentication (Web Server Authenticated Access, as described in "[Understanding Authentication](#)" on page 12), complete the Authenticated access settings. Select the **Basic authentication** field and enter a default domain and realm.

---

---

**Note:** When you select Basic authentication, a message box reminds you that usernames and passwords will be sent in clear text. If this is a concern, users can set up IIS to run in HTTPS.

---

---

---

---

**Note:** Select the **Integrated Windows Authentication** field if appropriate for your authentication scenario. When checked, network credentials are used to access the Web site instead of via a login prompt, as provided by the Basic Authentication field. For example, if some users access the Web site from within your organization and others access it through the public Internet, you might activate both Basic Authentication and Integrated Windows Authentication options.

---

---

---

---

**Note:** If you do not select Integrated Windows authentication or if IIS cannot determine who the user is, an IIS-generated login message box displays when users start the client.

---

---

---

---

**Note:** A conflict involving Integrated Windows Authentication may occur in a certain scenario, in which remote client users cannot access database lookups or database pick-lists. This can occur when the IIS and SQL server are set to use Integrated Windows Authentication. To work around this limitation, either deselect Integrated Windows Authentication on the IIS or create a user on the SQL server to access the database lookup or pick-list.

---

---

12. Assign the appropriate rights to the ClientAccess folder, giving users access to copy .pak files to the server.

From the Internet Information Services applet, choose **Properties** on the ClientAccess folder within the Capture virtual directory. On the Directory tab, add Write access and click **OK** to save changes.

13. Configure the virtual directory to use Application Protection of Low (IIS Process). It is recommended that you specify low application protection.

#### 4.4 Configuring the Virtual Directory (Windows 2003)

Follow these steps to configure the virtual directory on an IIS server running Windows 2003.

1. From the Control Panel, choose **Administrative Tools**, then select the Internet Information Services (IIS) applet.
2. Browse to the default Web site.
3. Right-click and select **New Virtual Directory**.

The virtual directory will be used by remote sites to access the client. The Creation Wizard starts. Specify an Alias for your virtual directory (for example, Capture).

4. Click **Next**.
5. In the Directory field, specify the correct content directory.

The default directory is  
c:\Program Files\Oracle\DocumentCapture\WebPages.

6. Under Access Permissions, select the Read and Run scripts permissions.
7. Click **Next**, then **Finish** to complete creating the virtual directory.
8. From the same Internet Information Services applet, right-click the newly created Capture folder and select **Properties**.
9. Click the Directory Security tab.
10. Click **Edit** in the Authentication and Access control section.
11. Complete settings on the Authentication Methods screen.

- If you chose **Anonymous access** for authentication (Oracle Distributed Document Capture Prompted Login, as described in "[Understanding Authentication](#)" on page 12), select the **Enable anonymous access** field and complete anonymous access settings. Note that the default user name is the IUSR account. If using Capture security, specify the IUSR account here.

---

---

**Note:** It is acceptable to use the local IUSR account for the Anonymous access. (This user needs to be an administrator.) For increased security measures, it is recommended that you use a local user account created specifically for accessing this virtual directory. This account should be a member of the Local Administrator group. As an alternate security measure if using Windows domain security, you may want to specify a user that is in the domain and is also a Capture administrator.

---

---

- If you chose **Authenticated access** for authentication (Web Server Authenticated Access, as described in "[Understanding Authentication](#)" on

page 12), complete the Authenticated access settings. Select the Basic authentication field and enter a default domain and realm.

---

---

**Note:** When you select **Basic Authentication**, a message reminds you that usernames and passwords will be sent in clear text. If this is a concern, users can set up IIS to run in HTTPS.

---

---

---

---

**Note:** If you do not check Integrated Windows authentication or if IIS cannot determine who the user is, an IIS-generated login message will appear when users start the client.

---

---

---

---

**Note:** Select the **Integrated Windows Authentication** field if appropriate for your authentication scenario. When checked, network credentials are used to access the Web site instead of via a login prompt, as provided by the Basic Authentication field. For example, if some users access the Web site from within your organization and others access it through the public Internet, you might activate both Basic Authentication and Integrated Windows Authentication options.

---

---

---

---

**Note:** A conflict involving Integrated Windows Authentication may occur in a certain scenario, in which remote client users cannot access database lookups or database pick-lists. This can occur when the IIS and SQL server are set to use Integrated Windows Authentication. To work around this limitation, either deselect Integrated Windows Authentication on the IIS or create a user on the SQL server to access the database lookup or pick-list.

---

---

12. Expand the virtual directory.
13. Right-click the ClientAccess folder and select **Properties**.
14. On the Directory tab, add Write access and click **OK** to save the change.

This action will give the user the proper virtual directory permissions to copy.
15. Give the appropriate rights to the ClientAccess folder, giving users access to copy .pak files to the server by granting write privileges.
16. Configure the virtual directory to use Application Protection of Low (IIS Process).

It is recommended that you specify low application protection.
17. In Internet Information Services, right-click the Web Sites folder.
18. Select **Properties** from the dropdown menu.
19. Click the Service tab.
20. Select the **Run WWW service in IIS 5.0 isolation mode** field.
21. Click the Apply button, then click **OK**.
22. Within the Internet Information Services applet, select the Web Server Extensions folder.

23. Select the Active Server Pages extension in the right pane, and click the Allow button.  
This will permit you to load the WebCapture.asp and WebCaptureAdmin.html pages.
24. Select the WebDAV extension in the right pane, and click the Allow button.  
This will permit you to send batches from the client to the server.
25. Right-click the computer name within the Internet Information Server applet.
26. From the menu, select **All Tasks**, then select **Restart IIS**.
27. In the confirmation box, select **Restart Internet Services** on MACHINENAME, where MACHINENAME is the name of your computer, and click **OK**.

## 4.5 Configuring the Web Site (Windows Vista, Windows 7, and Windows Server 2008 R2)

Configuring a server running IIS 7 and Windows Vista, 7 or 2008 R2 involves the following steps:

- ["Configure IIS 7 for ASP Applications"](#) on page 16
- ["Create an Application Pool"](#) on page 17
- ["Create the Client Web Site"](#) on page 17

### 4.5.1 Configure IIS 7 for ASP Applications

Oracle Distributed Document Capture requires that IIS 7 be configured to host Classic ASP applications, which is not the standard default configuration. Follow these steps to enable classic ASP support on IIS.

#### For Windows Vista or Windows 7

---

---

**Note:** You only need to perform these steps once if configuring multiple Oracle Distributed Document Capture Web sites on a single server.

---

---

1. In the Control Panel, open the Programs and Features applet.
2. In the side pane, select the **Turn Windows features on or off** option.
3. In the tree, expand the Internet Information Services node, then the World Wide Web Services node, then the Application Development Features node.
4. Select the following fields:
  - ASP
  - ISAPIExtensions
  - ISAPIFilters
5. Click **OK**. Windows configures IIS.

#### For Windows Server 2008 R2

1. Open the Server Manager and click **Features**.



2. Ensure that the server is configured as an IIS server.
3. Select your Web View server. Under **Role Services**, verify that the following options are displayed, adding them if needed.
  - ASP
  - ISAPIExtensions
  - ISAPIFilters

#### 4.5.2 Create an Application Pool

Follow these steps to create an application pool to host the Oracle Distributed Document Capture application.

---

---

**Note:** If configuring multiple Oracle Distributed Document Capture Web sites on a single server, you only need to perform these steps once.

---

---

---

---

**Note:** You may need to configure the application pool to use the credentials of a user with rights to the Document Capture folder (C:\Program Files\Oracle\Document Capture).

---

---

1. Display the IIS Manager or IIS Server Manager.
  - For Windows Vista or Windows 7, open the IIS Manager applet from the Control Panel.
  - For Server 2008, open the Server Manager, and select **Roles**. Expand Web Server (IIS), and choose Internet Information Services (IIS).
2. Select the Application Pools node. Right-click and choose **Add Application Pool**.
3. In the configuration screen, enter a name for the application pool, such as *ODDC*.
4. In the .NET Framework Version field, select **No Managed Code**.
5. In the Managed Pipeline Mode field, select **Classic**.
6. Select the **Start application pool immediately** field.
7. Click **OK** to create and start the application pool.

---

---

**Note:** If configuring Oracle Distributed Document Capture on a 64-bit system, set the **Enable 32-Bit Applications** field to True under Advanced Settings.

---

---

#### 4.5.3 Create the Client Web Site

Follow these steps to create the Oracle Distributed Document Capture Web site.

1. From the tree in the side pane, click the Websites node and choose **Add Website**.
2. Click the **Select** button by the application pool setting. Select the application pool you previously created, as described in "[Create an Application Pool](#)" on page 17.
3. Select the path to the ODDC webpages directory.

4. To use a port other than 80, which is used by the default Web site, change the port.

---

---

**Note:** If using a port other than 80, specify the port number in the URL (for example, `http://hostname:port number`).

---

---

5. Select the new Web site in the side pane's tree. The right-most pane displays a list of options.
6. Double-click the modules item to open it. From the list of installed modules, select **IsapiFilterModule** and **IsapiModule**, and click **OK**.

---

---

**Note:** If the IsapiFilterModule or IsapiModule modules are not listed, click **Add Native Module** from the Actions pane and add them. If they still do not appear, IIS 7 may not be configured properly; repeat the steps described in "[Configure IIS 7 for ASP Applications](#)" on page 16.

---

---

7. Open the client application.

## 4.6 Configuring for Capture Security

---

---

**Note:** No changes are needed for the Oracle Distributed Document Capture Service when using Capture security.

---

---

Follow these steps to set up Oracle Distributed Document Capture when using Capture security.

1. Configure the Capture Batch Setup to use Capture security.
2. Give the IUSR account full rights to the C:\Program Files\Oracle\Document Capture folder.

IUSR is an Internet Guest Account that is automatically created by the operating system when choosing to install Internet Information Services. The IUSR account **MUST** have full rights to the Capture folder, not just the WebPages folder.

From Windows Explorer, select the c:\Program Files\Oracle\Document Capture folder. Then, right-click and select **Properties**.

Select the Security tab, add the IUSR account, and assign full control.

---

---

**Note:** When implementing Oracle Distributed Document Capture with an Oracle database server, the IUSR account must have read/execute/write rights to the entire Oracle folder (for example, c:\Oracle). Choose the Inherit Properties option so that all child folders are updated.

---

---

## 4.7 Configuring Server Settings

Use the Server Configuration application to select server settings.

1. From the Start menu, select **Oracle Distributed Document Capture**, then **Distributed Document Capture Server Configuration**.

The Server Configuration application displays, with the Server Settings tab selected.

2. In the **Error Batch Location** field, specify the folder in which you want error batches stored.

If an error is encountered in server processing, the entire .pak file is transferred into this folder for analysis.

3. In the **Log File Location** field, specify the folder in which you want log files stored.

4. In the **Days to Keep Log** field, enter the number of days you want log files retained.

5. In the **Client Batches Folder** field, specify where user batches are temporarily stored before being sent to the server and whether client users can view and change this location.

You can choose:

- **Allow users to change batch path** (default): Creates and stores documents in a Batches folder on the hard drive containing the most space (typically C:\Batches). This folder appears to client users in their Settings options, where they can designate a different folder, including a shared network folder.

---

---

**Note:** When users are allowed to change the batch path, they can change the batch folder to a network folder and share batches with a group of users. In this scenario, each time a user opens a batch, it is temporarily locked, preventing other users from opening the same batch.

---

---

- **Batches restricted to current workstation user:** Stores batches under the current user (creates a Documents and Settings\User Data\Application Data\WebCapture\Batches folder; this folder is often hidden.) Client users cannot see or change the location under Settings options.
  - **Batches available to all workstation users:** Stores batches under all users (creates an All Users\Application Data\WebCapture\Batches folder; this folder is often hidden.) Client users cannot see or change the location under Settings options.
6. Click the **Set Client Access Folders** and specify one or more folders.

Specify the folder in which scan profiles are stored and in which batches are temporarily stored when users send them from the client. (You can configure more than one client access folder if configuring multiple Capture systems.) The client access folder you specify must refer to the subfolder beneath WebPages. This folder must be accessible by your Internet/Intranet users (i.e., within an IIS virtual directory).

---

---

**Note:** You can configure multiple batch folders if needed. Organizations such as service providers or bureaus often configure multiple virtual directories (for example, web farm), and need .pak files to be uploaded and processed from each virtual directory. If using multiple batch folders, copy the contents of the web pages folder to each batch folder, as described previously.

---

---

The client access folder you specify here is a temporary holding place for scanned batches. When a user sends a batch, all of its images and associated information are packaged into a .pak file. The server checks for the existence of \*.pak files. Each time it receives a .pak file, the server processes it.

---

---

**Notes:** As a general guideline, it is recommended that you allocate enough disk space on the server to handle a day's worth of Oracle Distributed Document Capture activity.

The Client Access folder(s) you specify in this step should not be scanned by anti-virus programs. Anti-virus programs lock files, which makes them inaccessible to Capture processes.

---

---

7. On the System Settings tab, identify the username and password of a Capture administrator. Specify a domain if using Windows Domain security.

This enables the Oracle Distributed Document Capture service to log in to Capture.

---

---

**Note:** Leave the Domain field blank if using Capture security.

---

---

8. From the Authentication Methods option, specify how you want client users authenticated.

See "[Understanding Authentication](#)" on page 12.

9. If configuring for Vista, click the **Batch Setup** button and specify Capture Batch Setup settings, as described in "[Specifying Capture Batch Folders](#)" on page 5 and "[Configuring the Capture Database](#)" on page 6.

10. On the Email Settings tab, specify who should receive an email if the server encounters an error while performing processing.

The subject of the error email is *Notification of Server Error*; it identifies the batch being processed when the error occurred and describes the error.

## 4.8 Configuring Optional Parameters

These optional parameters are provided in the LoadClient.js file to customize batch processing.

- [LOCALSENDPATH](#) Parameter
- [SuppressSendComplete](#) Parameter
- [ALLOWLOGINCACHE](#) Parameter

To edit the LoadClient.js file, open it using a text editor from the WebPages folder.

#### 4.8.1 LOCALSENDPATH Parameter

Configure this parameter to copy PAK files to a specified local folder rather than send them to the Oracle Distributed Document Capture server for processing. For example, an organization might use this parameter to hold batches locally, then move the files to the web server later in the day to avoid network performance issues.

By default, the LOCALSENDPATH property is set to null and commented out, as shown below:

```
/* document.write('    <PARAM NAME="LOCALSENDPATH" VALUE="c:\\temp">');    */
```

In the example below, PAK files are set to be copied to a local folder. (If the copy is successful, the batch is considered sent.)

```
document.write('    <PARAM NAME="LOCALSENDPATH" VALUE="c:\\PAK_files">');
```

#### 4.8.2 SuppressSendComplete Parameter

Set this parameter to prevent the following standard send batch screens from displaying to end-users when they click Send in the Oracle Distributed Document Capture client:

- Confirmation screen asking users if they are sure they want to send the batch.
- Batch results screen indicating if the batch send was successful or an error occurred.

By default, the SuppressSendComplete property is commented out and the screens are displayed, as shown below:

```
/* document.write('<PARAM NAME="SuppressSendComplete" VALUE="1">');    */
```

To suppress the screens, uncomment the parameter.

#### 4.8.3 ALLOWLOGINCACHE Parameter

Set this parameter to prevent caching of Oracle Distributed Document Capture user names and passwords.

By default, the ALLOWLOGINCACHE parameter is set to 1, as shown below:

```
document.write('    <PARAM NAME="ALLOWLOGINCACHE" VALUE="1">');
```

To prevent caching, change the parameter value to 0, and the **Remember my User Name and Password on this computer** field will display dimmed to client users at login.

## 5 Copyright and Patent Notices

This product uses WinWrap® Basic, Copyright 1993-2010, Polar Engineering and Consulting, <http://www.winwrap.com>.

U.S. Patent Nos. 6,094,505, 5,768,416, 5,625,465, 5,369,508 and 5,258,855.

## 6 Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to

facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at <http://www.oracle.com/accessibility/>.

### **Accessibility of Code Examples in Documentation**

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

### **Accessibility of Links to External Web Sites in Documentation**

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

### **Access to Oracle Support**

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/support/contact.html> or visit <http://www.oracle.com/accessibility/support.html> if you are hearing impaired.

---

Installation Guide for Oracle Distributed Document Capture, Release 10gR3  
E13869-01

Copyright © 1998, 2010, Oracle and/or its affiliates. All rights reserved.

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

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

If this 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.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

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.