Oracle® WebCenter Interaction Identity Service for Active Directory

Installation and Upgrade Guide

10g Release 3 (10.3)

November 2008

ORACLE

Oracle WebCenter Interaction Identity Service for Active Directory Installation and Upgrade Guide, 10g Release 3 (10.3)

Contents

CHAPTER 1

Welcome to Oracle WebCenter Interaction Identity Service for Active Directory

This book describes how to install and deploy Oracle WebCenter Interaction Identity Service for Active Directory 10.3. It also provides instructions for upgrading to Oracle WebCenter Interaction Identity Service for Active Directory 10.3 from earlier versions.

Oracle WebCenter Interaction Identity Service for Active Directory allows you to import Active Directory users and groups into your portal and authenticate against repositories inside or outside of your network. Portal administrators can then create Remote Authentication Sources that access the Active Directory. This installation and upgrade guide describes the requirements for installing Oracle WebCenter Interaction Identity Service for Active Directory and briefly outlines the installation process.

Typographical Conventions

This book uses the following typographical conventions.

Table 1-1 Typographical Conventions

Convention	Typeface	Examples/Notes
• Items you need to take action on (such as files or screen elements)	**bold**	• Upload **Procedures.doc** to the portal. • To save your changes, click **Apply Changes**.
• User-defined variables • New terms • Emphasis • Object example names	*italic*	• The migration package file is located in *install_dir*\serverpackages. • *Portlets* are Web tools embedded in your portal. • The URI *must* be a unique number. • The example Knowledge Directory displayed in Figure 5 shows the *Human Resources* folder.

• Text you enter
• Computer generated text (such as error messages)
• Code samples
	`computer`	• Type `Marketing` as the name of your community.
		• This script may generate the following error: `ORA-00942 table or view does not exist`
		• Example:
		`<setting name="SSOCookieIsSecure">`
		`<value xsi:type="xsd:integer">0</value>`
		`</setting>`

• Environment variables	ALL_CAPS	• ORACLE_HOME specifies the directory where Oracle products are installed.

Oracle Documentation and Resources

This section describes the documentation and resources provided by Oracle.

Table 1-2 Oracle Documentation and Resources

Resource	Description
Configuration Worksheet	This worksheet allows you to record prerequisite information necessary for installing and configuring Oracle WebCenter Interaction Identity Service for Active Directory. It is available on the Oracle Technology Network at http://download.oracle.com/docs/cd/E13158_01/alui/integration/activedirectoryids/docs103/index.html.
Release Notes	The release notes provide information about new features, issues addressed, and known issues in the release. It is available on the Oracle Technology Network at http://download.oracle.com/docs/cd/E13158_01/alui/integration/activedirectoryids/docs103/index.html.
Online Help	The online help is written for all levels of Oracle WebCenter Interaction Identity Service for Active Directory users. It describes the user interface for Oracle WebCenter Interaction Identity Service for Active Directory and gives detailed instructions for completing tasks in Oracle WebCenter Interaction Identity Service for Active Directory. To access online help, click the help icon.
Oracle Technology Network (OTN)	The Oracle Technology Network is the world's largest community of developers, DBAs, and architects using Oracle products and industry-standard technologies. Every day, members collaborate via OTN to share real-world insight, expertise, and best practices on how to build, deploy, manage, and optimize applications. As a member of the Oracle Technology Network you will enjoy access to software downloads, discussion forums, documentation, wikis, podcasts, blogs, plus much more. Access the Oracle Technology Network at http://www.oracle.com/technology/index.html.
Oracle Support	The Oracle Support site provides access to all Oracle support resources including online support, software and patches, technical articles, and contact numbers. Access the Oracle Support site at http://www.oracle.com/support/index.html.

CHAPTER 2

Completing Pre-Installation Steps

Complete the following basic steps to prepare your network and host computers for deployment:

1. Download the most up-to-date documentation from http://download.oracle.com/docs/cd/E13158_01/alui/integration/activedirectoryids/docs103/index.html .
2. Read the product release notes for information on compatibility issues, known problems, and workarounds that might affect how you proceed with your deployment. Release notes are located at http://download.oracle.com/docs/cd/E13158_01/alui/integration/activedirectoryids/docs103/index.html .
3. Organize the information needed for the installation process by completing the *Configuration Worksheet for Oracle WebCenter Interaction Identity Service for Active Directory.*
4. Provision host computers for your deployment and install prerequisite software. For details, see "Hardware and Software Requirements" on page 2-2.
5. Ensure you have administrative access to the resources you need to complete installation and configuration tasks. For details, see "Administrative User Requirements" on page 2-2.

Hardware and Software Requirements

The following table summarizes the hardware, operating system, and software requirements for Oracle WebCenter Interaction Identity Service for Active Directory.

Table 2-1 Hardware and Software Requirements

Component	Requirement
Identity Service Host Computer	**Hardware** • 1.6 GHz of higher, with 2MB L2 cache • 1 GB memory • 2 GB disk space **Operating System** • Microsoft Windows 2000 SP3 Server • Microsoft Windows 2003 Server **Application Servers** • Microsoft IIS 5.0, 6.0 • .NET Framework version 1.1.4322
Portal Software	Oracle WebCenter Interaction 10.3

Administrative User Requirements

The installation and configuration of Oracle WebCenter Interaction Identity Service for Active Directory requires the following administrative user permissions.

Table 2-2 Administrative User Requirements

User	Permissions
Local Host Administrator Account	To install Oracle WebCenter Interaction Identity Service for Active Directory components, you must log in to the host computers as the local Administrator.

CHAPTER 3

Installing Oracle WebCenter Interaction Identity Service for Active Directory

This chapter describes the steps you take to install Oracle WebCenter Interaction Identity Service for Active Directory components:

1. Ensure that you have completed pre-installation steps. For details, see Chapter 2, "Completing Pre-Installation Steps."
2. Install and verify deployment of Oracle WebCenter Interaction Identity Service for Active Directory. For details, see "Installing Oracle WebCenter Interaction Identity Service for Active Directory" on page 3-1

Installing Oracle WebCenter Interaction Identity Service for Active Directory

To install Oracle WebCenter Interaction Identity Service for Active Directory:

1. Log on to the host computer as the local administrator.
2. Locate and double-click the installation file, **WebCenterInteractionIdentityServiceForActiveDirectory_10.3.0.0.0.exe**.

3. Complete the installation wizard pages as described in the following table and according to the settings you planned when you completed the *Configuration Worksheet for Oracle WebCenter Interaction Identity Service for Active Directory.*

Wizard Page	Description
Introduction	Click **Next**.
Choose Components	Choose the components that you want to install. • Choose **Identity Service for Active Directory** to install the identity service on your remote server. • Choose **Image Server Files for Windows Image Service** if your Image Server is on this machine. Click **Install**.
Choose Install Folder	Accept the default: **C:\bea\alui**. This is the location is where the component will be installed.
Specify Image Service Folder	Specify the location of your Image Service folder. **Note:** We recomend using: **\ptimages**
Fully Qualified Domain Name	Enter the **Fully Qualified Domain Name** for your host computer, for example: mycomputer.mycompany.com.
Web Protocol	The installer asks you to choose whether to use a secure HTTP protocol for the Web service (https) or a standard Web protocol (http).
Select IIS Web Site	Specify if you want to use the default Web site: • **Use Default Web Site** - Choose this option to create a virtual directory called adaws in the Web directory http://<RemoteServer>/adaws. The default Web site listens on port 80. • **Use another web site** - You will specify the web site particulars on the next page.
Specify IIS Web Site Information	If you selected to use another web site, specify the information for that site: • **IIS Web Site Name** - Enter the name of the site on which you want to deploy Oracle WebCenter Interaction Identity Service for Active Directory. • **IIS Web Site Port** - If necessary, change the port for this site. The default port is 8082. • **IIS Web Site Secure Port** - If necessary, change the secure port for this site. The default port is 9092.

4. On the Pre-Installation Summary page, review the installation settings and click **Install** to begin installation.
5. You must restart your computer before you can use Oracle WebCenter Interaction Identity Service for Active Directory. Select **Yes, restart my system**, and click **Done**.
6. Verify installation by navigating to the installation verification log file. For example: <**install_dir**>\WebCenter_Interaction_Identity_Service_for_Active_Directory_InstallLog.log

Note: After you have imported the migration package into the portal, you can also run a diagnostic utility to verify connectivity among deployment components. To verify deployment, in a Web browser open the URL for the Remote Server diagnostic utility. For example: http://<remoteserver>/adaws/install/index.html

CHAPTER 4

Post-Installation Tasks

This chapter contains information on the following post-installation tasks:

IIS Virtual Directory Settings

To edit virtual directory time-out and security settings:

1. Open **Internet Information Services**.
2. Expand the IIS hierarchy as necessary, right-click the **adaws** virtual directory, and select **Properties**.
3. In the Properties dialog box, click **Configuration**.
4. In the Application Configuration dialog box, click the **Options** tab. The ASP Script timeout can be left at the default of 90 seconds.

   The Session timeout should be set to the same value as the timeout value specified in the web.config file. See "Editing the Web.config File" on page 5-2 for more information.

   For synchronizations of large user directories, a timeout between 120 and 240 minutes is recommended.

5. Return to the Properties dialog box and click the **Directory Security** tab to edit anonymous access and authentication control. The account used for anonymous access can be either a local or domain user, but in most circumstances the local user **IUSR** is recommended.
6. When you are done, close the Properties dialog box.

Windows Installation Directory Settings

The Windows installation directory settings are located in **<install_dir>\ptadaws\10.3.0\webapp\adaws** (for example, C:\bea\alui\ptadaws\10.3.0\webapp\adaws).

The following security settings are the minimum requirements needed for Oracle WebCenter Interaction Identity Service for Active Directory and logging to work correctly:

- The local ASPNET user must have Full Control rights. Allow ASPNET and the SYSTEM group Full Control rights on the folder.
- The account used for anonymous access, described in "IIS Virtual Directory Settings" on page 4-1, must have **Read and Execute, List Folder Contents**, and **Read** rights on the folder. Whether this is a domain user or the local IUSR user, this account will be a member of the Authenticated Users group. Allow Authenticated Users these rights on the folder.
- Administrators will want to be able to view and modify the content of the folder, so allow the Administrators group Full Control rights on the folder.

Registering the Oracle WebCenter Interaction Identity Service for Active Directory in the Portal

After completing installation, you must register the Oracle WebCenter Interaction Identity Service for Active Directory in the portal. To register the Oracle WebCenter Interaction Identity Service for Active Directory in the portal, perform the following steps:

1. "Import the Active Directory Migration Package" on page 4-3.
2. "Create a Remote Authentication Source" on page 4-3.
3. "Create a Remote Profile Source" on page 4-4.

Import the Active Directory Migration Package

To import the Oracle WebCenter Interaction Identity Service for Active Directory migration package (pte) into the portal:

1. Log on to the portal as a user with administrative rights.
2. Click **Administration**.
3. In the Select Utility menu, click **Migration-Import**.
4. On the Package Settings page, leave **File Path** selected and click **Browse** to locate the pte file (for example, C:\bea\alui\ptadaws\10.3.0\serverpackages\IdentityService-ActiveDirectory.pte).
5. Click **Load Package**.
6. Click **Finish**.

New portal objects are imported into the **Active Directory** folder.

Create a Remote Authentication Source

After importing the pte file, you must create an authentication source:

1. In the Administrative Object Directory, open the **Active Directory** folder.
2. In the Create Object menu, click **Authentication Source - Remote**.
3. In the Choose Web Service dialog box, select **Active Directory** (the Web service created during import), and click **OK**.
4. On the Remote Active Directory Agent Configuration page, fill out the information specific to your Active Directory server. For more information, refer to online help.
5. Create a job to run your authentication source:
    a. Open an administrative folder.
    b. In the Create Object menu, click **Job**.
    c. Complete the Job Editor. For more information, refer to online help.

Create a Remote Profile Source

After importing the pte file and creating a remote authentication source, you must create a remote profile source:

1. In the Administrative Object Directory, open the **Active Directory** folder.
2. In the Create Object menu, click **Profile Source - Remote**.
3. In the Choose Web Service dialog box, select **Active Directory (2)** (the Web service created during import), and click **OK**.
4. On the Remote Active Directory Configuration page, fill out the information specific to your Active Directory server. For more information, refer to online help.
5. Create a job to run your profile source:
    a. Open an administrative folder.
    b. In the Create Object menu, click **Job**.
    c. Complete the Job Editor. For more information, refer to online help.

CHAPTER 5

Advanced Configuration

This chapter describes the following advanced configuration options for Oracle WebCenter Interaction Identity Service for Active Directory:

Editing the Web.config File

There are several configurable settings in the **Web.config** file that help you avoid some common error cases and define logging parameters. If you want to edit the **Web.config** file, it can be found in the following location: <**install_dir**>\ptadaws\10.3.0\webapp\adaws (for example, C:\bea\alui\ptadaws\10.3.0\webapp\adaws\Web.config).

Logging Settings

Within the **Web.config** file, locate the **log4net** section. The default settings for the parameters in this section should be sufficient in most cases, but there are several settings that you can change.

The log files created by **log4net.dll** are self-cleaning based on the following parameters:

- **MaximumFileSize**- Specifies the maximum size a log file can be before it is rolled over into a new file if RollingStyle is set to Size.
- **MaxSizeRollBackups**- Sets the number of rolled-over files that are saved.

Additional log4net- Settings are based on these parameters:

- **AppendToFile**- Determines whether writes to the log file will be appended to the end of the file, or if the file will be overwritten. This should be set to true.
- **RollingStyle**- Can be set to Size or Date.
- **StaticLogFileName**- When set to true means that the active file name will always be **ADAWSLog.txt**. Rollover files will be renamed with .1, .2, .3, and so on extensions. This should be set to true.

With the default settings, the most disk space that will ever be used by logging is 100MB.

The log level can be set to INFO, ERROR, or FATAL. The default setting of INFO provides information that describes when the web service is called and what parameters are provided, as well as logging any failures and their causes. The ERROR setting logs only failures. A setting of FATAL runs silently.

Even with the log level set to INFO, the logging for a single synchronization run never exceeds 10MB.

Note: The **log4net.dll** handles all log file creation and deletion. Deleting rollover files that were created by log4net while it is still running causes log4net to fail, and furthermore causes the Oracle WebCenter Interaction Identity Service for Active Directory to fail. Because of this, rollover files should not be deleted manually. If they are, restart IIS to ensure that

log4net continues to run properly. The rollover files can be viewed and copied without any adverse affect.

Logging Best Practices

When setting the logging practices, you should not delete or modify the rollover files. You should let log4net handle log file manipulation. The following three sections indicate the best settings for your environment.

Choosing An Appropriate Rolling Style

If several synchronization jobs are run a day, you may wish to set the **RollingStyle** to **Size**, so that the individual log files do not grow too large. If synchronization jobs are only run once a day or less, you may chose to set the **RollingStyle** to **Date**. The log files do not grow too large because they contain one run and the log for a single run never splits between two files (unless the job runs past midnight). If you choose to rollover based on **Date**, the **MaximumFileSize** setting does not take affect.

If synchronization jobs are run past midnight, using **Date** causes the log for a single synchronization job to be split into two files (due to the rollover at midnight). It is therefore recommended to use **Size** and to set the **MaximumFileSize** based upon the typical log size for a single run.

Recommendation for the Number of Rollover Files

The number of rollover files you set for the **MaxSizeRollBackups** value depends on how much disk space you choose to devote to log files. If **RollingStyle** is set to **Size** then it is easy to calculate the amount of space used. It is the **MaximumFileSize** you set multiplied by the **MaxSizeRollBackups** value. If you rollover based on **Date** then you must look at the average size of the log created by a single synchronization run to determine what the total disk space is. If synchronizations are run once a week, then setting **MaxSizeRollBackups** to 10 provides approximately two months of job histories. If synchronizations are run on a daily basis then you may wish to increase the number of rollover files to keep a history that exceeds ten days.

Archiving Log Files

You may wish to keep a permanent archive of all the logs on another machine, or simply wish to keep a larger history than the one determined by the **MaxSizeRollBackups** setting. You can manually copy the files before the rollover limit is reached and they are overwritten. You could

also set up a recurring task that copies files to another location. The frequency of this task is determined by the frequency of your synchronization runs, and your logging settings.

Note: Do not delete or move the rollover files without restarting IIS.

IIS Session Timeouts

During large synchronizations the portal must create database objects for all the users and groups returned by Oracle WebCenter Interaction Identity Service for Active Directory. This can cause IIS session timeouts between the calls to **GetGroups**, **GetUsers**, and **GetMembers**.

This timeout error can be avoided by increasing the timeout value for the **sessionState** object. To avoid this large timeout from applying to both authentication calls and synchronization calls, create two directories for Oracle WebCenter Interaction Identity Service for Active Directory. Make a copy of the directory and give it a different name.

In one of the files, set the timeout to a very large minute value for synchronization. In the other file, leave it at the default or decrease it to 5 minutes for authentication.

Create two virtual directories. One directory should point to the physical directory with the large timeout value. This directory is used for the synchronization URL. The other virtual directory points to the physical directory that contains the smaller timeout value. This virtual directory is used for the authentication URL.

For a complete discussion of IIS sessions, refer to the Release Notes.

Note: The timeout setting in the **Web.config** should match the session timeout for the virtual directory. See "IIS Virtual Directory Settings" on page 4-1 for details on setting this timeout value.

Active Directory Server Query Timeouts

There is the potential for an Active Directory server timeout during synchronizations of especially large query bases or difficult query filters. A Microsoft DirectoryServices.dll bug causes this timeout to occur. The effect of this bug is that no exception is thrown, and instead a partial list is returned. Refer to the Release Notes for a full discussion of the consequences. The Microsoft (MS hotfix number Q833789) patch is included in the Oracle WebCenter Interaction Identity Service for Active Directory release package.

Once the patch is installed, **DirectoryServices.dll** correctly passes on the timeout exception to the **Web.config** file.

At the top, in the **configSections**, you must uncomment the line with section name = **“system.directoryservices”**. This line also contains a **PublicKeyToken** value that must be set. This is the public key for your **System.DirectoryServices.dll**. To find this key, use the strong name tool **sn.exe -T system.directoryservices.dll.**

You must also uncomment the system.directoryservices section in the web.config file, and set **waitForPagedSearchData** to true. Remember that if you do this, Oracle WebCenter Interaction Identity Service for Active Directory waits and blocks until all results are returned from the Active Directory server.

Active Directory Errors During GetMembers

Occasionally, Active Directory reports an error when it tries to get the members of a specific group. This error is a result of the server not having access to specific groups from other domains, being temporarily unavailable, or a specific group having a bad membership attribute. Normally these Active Directory errors are caught and passed on by Oracle WebCenter Interaction Identity Service for Active Directory. When the synchronization job encounters this error, it reports a failure and ends.

If you prefer that groups that cause an Active Directory error during **GetMembers** are simply skipped and allow the job to continue processing other groups, then set the **GetMembersActionOnError** key to Skip instead of Fail in the **Web.config** file.

Copying Help Files to the Image Service

During installation, the following file will be copied to the install directory: <**install_dir**>\ptadaws\10.3.0\images\imageserver.tgz (for example, C:\bea\alui\ptadaws\10.3.0\images\imageserver.tgz).

To copy Oracle WebCenter Interaction Identity Service for Active Directory help files to the Image Service, open the imageserver.tgz file and extract the files to the **\ptimages** directory on your Image Service, making sure to use folder names.

CHAPTER 6

Upgrading Oracle WebCenter Interaction Identity Service for Active Directory

Oracle WebCenter Interaction Identity Service for Active Directory 10.3 continues to use the GUID as the unique name for users and groups. This simplifies the migration process and does not require any database scripts.

No work is needed to upgrade from versions 5.0.2 or 6.x.x to version 10.3. After running the 10.3 installer, the virtual directory **adaws** will have been updated to point to the 10.3.0 directory. To uninstall the previous version, simply delete the physical directory associated with that installation. Do not delete the virtual directory **adaws**.

When you install version 10.3, a new **Web.config** is installed. If you have previously edited the **sessionstate timeout** value, you will need to edit it again.

Upgrading the Active Directory AWS 1.0 or 5.0.1 Authentication Source to Oracle WebCenter Interaction Identity Service for Active Directory 10.3

1. If you are going to install Oracle WebCenter Interaction Identity Service for Active Directory 10.3 on the same remote server as the previous version, remove the previous installation:

   a. Run the uninstall executable that came with the install.

   b. If the previous installation was version 1.0, you should delete the virtual directory **ActiveDirectoryAWS**. If the previous version was 5.0.1, the installation of 10.3 will have updated the virtual directory **adaws** to point to the 10.3.0 directory. Do not delete this virtual directory.

2. Ensure that you have completed pre-installation steps. For details, see Chapter 2, "Completing Pre-Installation Steps."

3. Install the 10.3 version as outlined in "Installing Oracle WebCenter Interaction Identity Service for Active Directory" on page 3-1.

4. Open the authentication source you have been using for Active Directory AWS 1.0 or 5.0.1. On the Remote Active Directory Agent Configuration page you must make these changes:

   a. Active Directory AWS 1.0 does not let you set the User Authentication Attribute. It uses **distinguishedName**. Active Directory AWS 5.0.1 does let you set this attribute, but defaults to **distinguishedName**. For 10.3, it is recommended you enter **userPrincipalName**. See product release notes for more information.

   b. Set the URL for authentication service to: **http://<RemoteServer>/adaws/AuthProviderSoapBindingRpc.asmx**.

   c. Set the URL for synchronization to: **http://<RemoteServer>/adaws/SyncProviderSoapBindingRpc.asmx**.

   d. You will also need to re-enter the authentication password. Each installation of Oracle WebCenter Interaction Identity Service for Active Directory encrypts this password using a different key.

5. Run the synchronization job associated with this authentication source.

Note: The first time you run the job, the job log will report that every user's name appears to have changed because **userPrincipalName** is being used instead of the distinguishedName for authentication. This attribute is changed for every user. However,

this value is hidden from the user and is only used behind the scenes. Users should continue to log in with the same name they have been. No users are deleted during this process.

Migrating Users from a Native Active Directory Authentication Source to a Remote Active Directory Authentication Source

For each native Active Directory authentication source in use in your portal, perform the following steps:

1. Create a remote Active Directory authentication source to replace your native Active Directory authentication source:
   - Set the SOAP timeout to a high number of seconds, at least 540.
   - Set the Authentication Source Prefix to a temporary category/prefix that is not otherwise used in any other authentication source in the system.
   - Set all Active Directory LDAP parameters identically to the corresponding native Active Directory authentication source.
   - Set the synchronization settings to Full Synchronization.
2. Run the remote authentication source. This should synchronize the same users and groups as the native authentication source. If your native authentication source uses partial synchronization, the remote authentication source may have additional users and groups. However, the native authentication source should never include users and groups that are not included in the remote authentication source.
3. Make sure that you can log in to the portal as a user imported from the remote authentication source.
4. Back up the portal database.
5. Edit both upgrade SQL script templates (located in **<install_dir>/ptadaws/10.3.0/usermigration/sql/<mssql or oracle>/**) by inserting the appropriate object ID numbers on the lines “DEF oldid” and “DEF newid”.
6. Run **<install_dir>/ptadaws/10.3.0/usermigration/sql/<mssql or oracle>/adaws.sql** against the portal database.

7. If the script output indicates that there are native authentication source users or groups that are not in the remote authentication source, verify that the remote authentication source parameters are correct and identical to the native authentication source parameters. If they are not, correct the problems and run the remote authentication source job again. If they are correct and identical, either manually delete the excess users and groups from the native authentication source or run the native authentication source job to drop the excess users and groups.
8. Run **<install_dir>/ptadaws/10.3.0/usermigration/sql/<mssql or oracle>/adaws2.sql** against the portal database.
9. Make sure that you can log in to the portal as with the original user account information.
10. Verify that the authentication source prefix of the remote authentication source has been changed (by the scripts) from the temporary prefix to the same prefix as the native authentication source.
11. Delete the temporary users and groups imported through the remote authentication source. These users and groups have the temporary prefix and are in the temporary category that was created when you first synchronized the remote authentication source.
12. Delete the native authentication source from the portal.

APPENDIX A

Uninstalling Oracle WebCenter Interaction Identity Service for Active Directory

To uninstall Oracle WebCenter Interaction Identity Service for Active Directory use the Windows Control Panel **Add/Remove Programs** utility to launch the Oracle WebCenter Interaction Identity Service for Active Directory uninstall wizard.