Oracle Access Manager

Release Notes

10*g* (10.1.4.3) for All Supported Platforms

E12496-02

October 2009

This document accompanies Oracle Access Manager 10*g* (10.1.4.3) installation packages and supersedes earlier documentation. This document contains the following sections:

The names of operating systems are shortened in this document, as follows:

Operating System	Abbreviated Name
Solaris Operating System (SPARC)	Solaris
Oracle Enterprise Linux or Red Hat Linux	Linux
Microsoft Windows	Windows

1 About This Release

Oracle Access Manager 10*g* (10.1.4.3) installation packages can be used for only a fresh installation. You cannot use 10*g* (10.1.4.3) installation packages to upgrade or patch an earlier deployment.

> **See Also:** To download free documentation, release notes, white papers, or other collateral, go to Oracle Technology Network (OTN).
>
> You must register online before downloading software. Registration is free and can be done at the following URL:
>
> `http://www.oracle.com/technology/membership`
>
> If you already have a user name and password for OTN, you can go directly to the software section of the OTN Web site at the following URL:
>
> `http://www.oracle.com/technology/software/products/ias/htdocs/idm_11g.html`

2 Documentation for this Release

The following documents are related to the Oracle Access Manager 10*g* (10.1.4.3) release.

- This document, the *Oracle Access Manager Release Notes 10g (10.1.4.3.0) For All Supported Operating Systems* provides the following information:
  - Documentation overview.
  - Known issues and workarounds for this Oracle Access Manager release.

  This document is named oamrn.htm (and oamrn.pdf).
- The following Oracle Access Manager manuals have been updated for this release:
  - *Oracle Access Manager Introduction*—Introduces Oracle Access Manager and provides a road map to Oracle Access Manager manuals and a glossary. The "What's New" chapter includes a brief introduction of all enhancements (from this document). These enhancements are combined with all enhancements for 10.1.4 in the "Overview of Behaviors" chapter.
  - *Oracle Access Manager Installation Guide*—Explains how to install and configure the 10*g* (10.1.4.3) components.
  - *Oracle Access Manager Identity and Common Administration Guide*—Explains how to configure Identity System applications to display information about users, groups, and organizations; how to assign permissions to users to view and modify the data that is displayed in the Identity System applications; and how to configure workflows that link together Identity application functions.

    This book also describes administration functions that are common to the Identity and Access Systems, for example, logging, reporting, auditing, and SNMP monitoring.
  - *Oracle Access Manager Access Administration Guide*—Describes how to protect resources by defining policy domains, authentication schemes, and authorization schemes; how to allow users to access multiple resources with a single login by configuring single- and multi-domain single sign-on; and how to design custom login forms.

    This book also describes how to set up and administer the Access System.
  - *Oracle Access Manager Deployment Guide*—Provides information for people who plan and manage the environment in which Oracle Access Manager runs.
  - *Oracle Access Manager Developer Guide*—Explains how to access Identity System functionality programmatically using IdentityXML and WSDL, how to create custom WebGates (known as AccessGates), and how to develop plug-ins.

    This guide also provides information to be aware of when creating CGI files or JavaScripts for Oracle Access Manager.
  - *Oracle Access Manager Integration Guide*—Explains how to set up Oracle Access Manager to inter-operate with other Oracle products, for example, OracleAS Web Cache.
  - *Oracle Access Manager Schema Description*—Provides details about the Oracle Access Manager LDAP schema.

3 Installation Requirements

Requirements for installation of this release are discussed in the following topics:

- Section 3.1, "Required Software and Platforms"
- Section 3.2, "Required Environment Preparation"

> **Note:** For more information, see Section 4, "Preparation, Installation, and Removal".

3.1 Required Software and Platforms

As described in the certification matrix on Oracle Technology Network (OTN), Oracle Access Manager 10*g* (10.1.4.3) server support:

- Solaris operating systems
- Linux operating systems
- Microsoft Windows operating systems

> **Note:** Oracle Access Manager Web components might also be available on other platforms.

Ensure that your environment meets the recommended system configuration requirements described in the certification matrix on Oracle Technology Network at:

`http://www.oracle.com/technology/products/id_mgmt/coreid_acc/pdf/oracle_access_manager_certification_10.1.4_r3_matrix.xls`

3.2 Required Environment Preparation

Review these instructions before installing Oracle Access Manager 10*g* (10.1.4.3):

- Review all of the information in "Installation Requirements".
- Keep Oracle Access Manager 10*g* (10.1.4.3) packages and files separate from other installation files.

4 Preparation, Installation, and Removal

The following sections describe preparing, applying, and removing Oracle Access Manager 10*g* (10.1.4.3):

- Section 4.1, "Preparing Host Computers"
- Section 4.2, "Installing Oracle Access Manager 10g (10.1.4.3)"
- Section 4.3, "Cancellation During Installation"

4.1 Preparing Host Computers

This section explains how to store platform-specific bundles in temporary directories before installation. Each platform-specific bundle contains one or more component-specific files.

Note: Oracle recommends that you create a new platform-specific directory for each bundle and store component-specific files in a separate branch (subdirectory) within the corresponding platform-specific directory tree. When your Oracle Access Manager deployment includes multiple platforms, be sure to download all appropriate platform-specific bundles.

The following procedure explains how to acquire and store 10*g* (10.1.4.3) installers from Oracle Technology Network (OTN) before you begin installation. Physical media packs and those on Oracle edelivery provide only Oracle products: Oracle HTTP Server, for example. Oracle Access Manager components for other Web servers are available on OTN.

Note: Physical Media Packs and those on Oracle edelivery provide only Oracle products.

To prepare and store installer bundles

1. Review the latest certification support matrix, as described in "Required Software and Platforms".
2. Ensure that your host computer meets all requirements.
3. Download the platform-specific bundle you need from OTN, as follows:
   a. Go to Oracle Technology Network (OTN) and log in as usual:

      `http://www.oracle.com/technology/software/products/ias/htdocs/idm_11g.html`

   b. From the **Oracle Access Manager** section of the table on OTN, click the appropriate **Readme**.

      Note: Oracle Access Manager WebGates are listed separately from core components.

   c. Print and review details in the Readme to:

      Locate the appropriate CD links in the table

      Locate the documentation library for download

   d. **Download Packages**: Locate and click the link for the package you need.
4. In the directory where you stored the downloaded bundles, extract all files to a new temporary platform-specific directory. For example:
   - oam10143_tmp_linux
   - oam10143_tmp_sparc
   - oam10143_tmp_win32x
5. In the platform-specific directory, extract the contents of each component-specific file to an individual component-specific subdirectory. For example:

   oam10143_tmp_sparc/access_server

6. Repeat the steps above for each platform-specific bundle and component that you need.
7. **Get Documentation**: Use instructions in the Readme to obtain the relevant documentation and Release Notes, including additional documents that might be available with certain components.

4.2 Installing Oracle Access Manager 10*g* (10.1.4.3)

This section outlines how to install Oracle Access Manager components. While individual commands might differ depending on your platform, the overall procedure is the same.

Task overview: Installing Oracle Access Manager 10*g* (10.1.4.3)

1. Review the certification matrix as described in Section 3.1, "Required Software and Platforms".
2. Complete all activities in Section 4.1, "Preparing Host Computers".
3. Locate and review the *Oracle Access Manager Deployment Guide* before you start installation.
4. Locate and review the *Oracle Access Manager Installation Guide*, chapter 1, for an introduction to the installation task, options, and methods.
5. Locate the *Oracle Access Manager Installation Guide* and review preparation tasks in chapter 2:
   - About Installation Prerequisites
   - Synchronizing System Clocks
   - Meeting Oracle Access Manager Requirements
   - Meeting Web Server Requirements
   - Meeting Directory Server Requirements
   - Installation Preparation Checklists
6. If you are installing with an Oracle-provided Language Pack or on a computer running a non-English (American) language or territory operating system, complete activities in the *Oracle Access Manager Installation Guide*, chapter 3.
7. Install and set up components in the following order, using instructions in the *Oracle Access Manager Installation Guide*:
   - First Identity Server
   - First WebPass
   - Identity System setup
   - Additional Identity System instances
   - Policy Manager installation and set up
   - Access Server preparation and installation
   - WebGate preparation and installation
8. Refer to the manuals for administration, customization, and other details as you start configuring and customizing your 10*g* (10.1.4.3) deployment.

4.3 Cancellation During Installation

During Oracle Access Manager component installation, information is saved after certain operations. Until information is saved, you can return and restate details. However, after you are informed that a component is being installed, Oracle Access Manager files are added to the file system. If you cancel the installation process after this message and before completing all procedures, you must restore the system to it's previous condition to remove Oracle Access Manager-related information.

For more information, see the chapter on removing Oracle Access Manager in the *Oracle Access Manager Installation Guide*.

5 Post-Installation Tasks for NPTL

Oracle Access Manager 10*g* (10.1.4.3) can use either Native POSIX Thread Library (NPTL) or LinuxThreads. The default mode is LinuxThreads. To support the default, the start_ois_server and start_access_server scripts start in LinuxThreads mode. In this case, the variable LD_ASSUME_KERNEL is automatically set to 2.4.19. The message "Using Linux Threading Library." appears in the console and in the server's oblog file.

To support NPTL, you can use the start_*xxx*_nptl (or restart_*xxx*_nptl) scripts. In this case, the message "Using NPTL Threading Library." appears in the console and in the server's oblog file. The NPTL-ready scripts include:

- Identity Server: start_ois_server_nptl or restart_ois_server_nptl
- Access Server: start_access_server_nptl or restart_access_server_nptl

Standard stop scripts and the following standard setup scripts operate successfully whether you use LinuxThreads or NPTL: start_setup_ois, start_setup_webpass, start_setup_access_manager, start_configureAAAServer, stop_snmp_agent.

For more information, see the topic "NPTL Requirements and Post-Installation Tasks" in the troubleshooting appendix of the Oracle Access Manager Installation Guide.

6 Known Issues and Workarounds

This section describes known issues and workarounds. The following topics are discussed:

6.1 Platform-Specific Known Issues and Workarounds

Table 1 describes any known issues and workarounds for specific platforms in Oracle Access Manager 10*g* (10.1.4.3).

Table 1 Known Issues and Workarounds for Specific Platforms

Bug	Description

7679865	During Policy Manager setup on Linux, error messages might appear in the Policy Manager log file that do not indicate an actual error. For example:
	`... "No such file or directory"`
	`... "Could not read file"`
	
	For a list of messages, see Knowledge base note number 835857.1 on My Oracle Support (formerly MetaLink) at: https://metalink.oracle.com.

7637414	On Solaris 10 systems with a patch level less than 127127-11, the Identity Server installer might fail (core dump) on exiting. This does not effect Identity Server installation and can be safely ignored.
n/a	On Linux and Solaris, if any executable installer package does not have execute permissions, you must run the following command to make the package executable: `chmod u+x package_name`

6.2 General System-Wide Known Issues

Table 2 describes any general known issues and workarounds for Oracle Access Manager 10*g* (10.1.4.3).

Table 2 General System Wide Known Issues

Bug	Description
N/A	The "AM Service State" in previous releases of the Access System was renamed to "Access Management Service". In 10.1.4 Access Server and AccessGate configuration pages, "Access Management Service" appears correctly. However, the following product areas incorrectly refer to "Policy Manager API Support" rather than "Access Management Service": ▪ Access Server Cluster configuration page ▪ Help for Access Server and AccessGate configuration pages
6413451 7690968	Oracle Access Manager 10*g* (10.1.4.3) provides fresh Language Packs; however there are no Language Pack-related changes. Messages added for minor releases (10*g* (10.1.4.2.0) and 10*g* (10.1.4.3) as a result of new functionality might not be translated and can appear in only English.
7307688	On Red Hat Linux v5, the on-demand stack trace feature might not operate with the NPTL thread library.
7136566	Oracle Access Manager 10*g* (10.1.4.3) provides installation packages for a fresh install only. Do not use 10*g* (10.1.4.3) installers to upgrade an earlier release.

Table 2 (Cont.) General System Wide Known Issues

Bug	Description
8483595	When installing Oracle Access Manager in a different language, ensure that the graphical user interface (GUI) has the correct fonts installed for the specific language. Without the appropriate character sets, characters cannot be displayed correctly for the Oracle Access Manager installer: ■ If installing Oracle Access Manager with the Oracle-provided Chinese Language Pack on a Solaris computer, ensure that the x windows server (or equivalent GUI interface application for Solaris) has the correct Chinese fonts installed (zh_CN or zh_TW). ■ If installing Oracle Access Manager with the Oracle-provided Chinese Language Pack on a Windows computer, ensure that the appropriate character set in the "Regional and Language options" has been installed and enabled.

Table 2 (Cont.) General System Wide Known Issues

Bug	Description

8556756	The validity of the Root CA certificate bundled with Oracle Access Manager installers expires JULY 5 2010. After that date, the certificate cannot verify or generate any X.509 certificate. This Root CA is required for Oracle Access Manager components communicating in Simple mode. You can use the following procedure to extend the life of the Simple mode certificate.
	
	Note: For more information on X.509 OpenSSL, go to http://www.openssl.org/docs/apps/x509.html
	
	To extend the life of the Simple mode certificate
	
	1. Back up the Identity Server `cacert.pem` file. For example:
	
	From:
	
	IdentityServer_install_dir\oblix\tools\openssl\simpleCA\cacert.pem
	
	To:
	
	backup_oam_ois\oblix\tools\openssl\simpleCA\cacert.pem
	
	2. In the original path, rename `cacert.pem` to `cacert.org`.
	
	3. Generate a new root certificate to extend the term of cacert.pem using the following command:
	
	`openssl req -new -x509 -key cakey.pem -out cacert.pem -days 3650 -config IdentityServer_install_dir\oblix\tools\openssl\openssl.cnf`
	
	4. Respond to prompts with information that must be entered as shown here to identify the original certificate authority (Oblix)--use a period at the end of Inc. (Organization=) and leave Email= blank:
	
	`Country=US`
	`State=California`
	`Locality=Cupertino`
	`Organization=Oblix, Inc.`
	`Organizational Unit=NetPoint`
	`Common Name=NetPoint Simple Security CA - Not for General Use`
	`Email=`
	
	5. Extend the term of cacert.pem using the following command (the -text option prints the certificate in text form, including the public key, signature algorithms, issuer and subject names, serial number, any extensions present, and any trust settings):
	
	`openssl.exe x509 -in cacert.pem -text`
	
	6. Copy the new cacert.pem to all component directory paths, including other Identity Servers:
	
	IdentityServer_install_dir\oblix\tools\openssl\simpleCA\
	WebPass_install_dir\oblix\tools\openssl\simpleCA\
	PolicyManager_install_dir\oblix\tools\openssl\simpleCA\
	AccessServer_install_dir\oblix\tools\openssl\simpleCA\
	WebGate_install_dir\oblix\tools\openssl\simpleCA\
	
	7. Restart components and Web servers after adding the new file.

6.3 LDAP Directory Known Issues and Workarounds

Table 3 describes any known issues and workarounds for platform support for Oracle Access Manager 10*g* (10.1.4.3).

Table 3 LDAP Directory Known Issues and Workarounds

Bug	Description

8540031	Some group functions (expand pure dynamic group, add a member to a pure dynamic group, and the like), might not work with Oracle Internet Directory 10.1.4.3. You could see this error:
	`OID RETURNS LDAP ERROR 16 IF ATTRIBUTE TO BE REPLACED DOES NOT EXIST`
	To solve this problem, apply the Oracle Internet Directory patch 7274801.
	1. Go to My Oracle Support (formerly MetaLink) and log in as usual:
	`http://metalink.oracle.com`
	2. From the **Quick Find** list, choose **Patch Number**, in the empty field to the right, enter **7274801**, and then click **Go**.
	3. On the Patch 7274801 page, click the **Download** button.
	4. **Readme**: Click the **View Readme** button to display the Release Notes, which you can print to obtain the installation instructions.

6664581	Oracle has discovered a problem with the use of the Oracle Access Manager Fast Bind option for Microsoft Active Directory. Oracle recommends that you do not use the Fast Bind option for Microsoft Active Directory in your deployment.

Table 3 (Cont.) LDAP Directory Known Issues and Workarounds

Bug	Description
650599	For all platforms, Sun Directory Server Enterprise Edition v6.0 (DSEE 6.0) is certified for Oracle Access Manager Release 10*g* 10.1.4.0.1 but does not appear in the Oracle Access Manager installers or user interface. To use Sun Directory Server Enterprise Edition v6.0 (DSEE 6.0): 1. Install Oracle Access Manager 10*g* (10.1.4.3) as described in the Oracle Access Manager Installation Guide. 2. When asked to specify a directory server during Identity Server (or Policy Manager) installation, choose the "Sun Directory Server 5.x" option. 3. Do not automatically update the schema and data. 4. After installation, load the Oracle Access Manager schema and index files using the DSEE 6.0 Management Console, as follows: ▪ LDAP server instance hosting user data only: – *install_dir*/access|identity/oblix/data.ldap/common/iPlanet_user_schema_add.ldif – *install_dir*/access|identity/oblix/data.ldap/common/iPlanet5_user_index_add.ldif ▪ LDAP server instance hosting user data and configuration data (or configuration data and policy data, or policy data only): – *install_dir*/access|identity/oblix/data.ldap/common/iPlanet_oblix_schema_add.ldif – *install_dir*/access|identity/oblix/data.ldap/common/iPlanet5_oblix_index_add.ldif 5. Proceed to Identity Server or Policy Manager setup.

6.4 Identity Server Known Issues and Workarounds

Table 4 describes any known issues and workarounds for the Identity Server for Oracle Access Manager 10*g* (10.1.4.3).

Table 4 Known Issues and Workarounds for the Identity Server

Bug	Description
8621422	Navigating in the Identity System should be successful without producing any error message in the Web server log file. However, while navigating in the User Manager and Group Manager tabs, errors might be logged in Web server log files for denying access to some files. For example, the following can appear in the SunOne Web server (NSAPI) Web server log file (*Web_server_home*/logs/errors: `[22/Jun/2009:13:23:21] security ... : for host ... trying to GET ... denying access to ...` The applet tries to access and load several unnecessary classes and files which are no longer present. While accessing resources, the Identity System attempts to load the missing classes and files and logs errors when these resources are not present.
8617638	If you set the attribute "oboutofofficeindicator" semantic type to "Out Of Office - Indicator" and then modify the "Out Of Office - Indicator" attribute in a user's profile, the OIS-OIS (Identity Server to Identity Server) cache flush for the Out Of Office Indicator attribute should appear. However, the wrong logs (FLUSH_LPM_POLICY_CACHE) are displayed during an Identity Server to Identity Server cache flush. For example: `2009/06/20@02:58:54.265200 8631 8631 OIS_MGMT DEBUG1 ... ... MgmtKey^FLUSH_LPM_POLICY_CACHE` Aside from showing the wrong MgmtKey name in debug level logs, there is no impact to any functionality. Cache flush updates are successful to other Identity Servers.

7147350	Identity Server oblog.log file lists unexplained error messages indicating that Identity Server is trying to read files that do not exist in the Identity Server installation directory. However, these do not indicate an actual error. For example:
	`"Could not read file "`
	`... OIS_Install_Dir/../data/common/ldapaccessdbparams.xml`
	`... OIS_Install_Dir/../data/common/accessdbparams.xml`
	
	For a list of messages, see Knowledge base note number 835857.1 on My Oracle Support (formerly MetaLink) at: https://metalink.oracle.com.

7275401	You can write a stack trace to a log file if Oracle Access Manager experiences a core dump on the Access Server and the Identity Server. However, writing the stack trace might prevent the core dump from being written. You might need to disable the `StackDumpEnabled` parameter in globalparams.xml when pursuing diagnostic issues or when instructed by Oracle Support to re-create a core dump scenario.Here are the values: See the troubleshooting appendix of the *Oracle Access Manager Identity and Common Administration Guide* for details and steps to you must perform to enable or disable the stack trace when pursuing diagnostic issues or recreating crashes.

Table 4 (Cont.) Known Issues and Workarounds for the Identity Server

Bug	Description
8449425	The Identity Server fails to start when the ORACLE_HOME environment variable is set with a trailing slash character, /. Incorrect: ORACLE_HOME=/opt/OHS11g_oracle/product/11.1.1/as_1/ or ORACLE_HOME=D:\oracle\product\11.1.1\as_1\ Correct: ORACLE_HOME to "/opt/OHS11g_oracle/product/11.1.1/as_1 or ORACLE_HOME=D:\oracle\product\11.1.1\as_1 Confirm there is no trailing slash in your ORACLE_HOME environment variable.
8613400	Although there is no loss of functionality, the following JavaScript error might appear in a pop-up box when navigating in the Identity System Console: "A Runtime Error has occurred. Do you wish to Debug? Line47 Error: Object expected" With Internet Explorer, when the "Disable Script Debugging" option is is disabled (Tools, Internet Options, Advanced Settings), the pop up does not appear; however, the error is seen in the bottom-left corner at the Status bar.

6.5 WebPass Known Issues and Workarounds

Table 5 describes any known issues for the WebPass for Oracle Access Manager 10*g* (10.1.4.3).

Table 5 Known Issues and Workarounds for WebPass

Bug	Description
8628901	When creating a User or Group, valid symbols are visible and searchable. However, in 10*g* (10.1.4.3), Oracle encodes the following characters and recommends that you do not use these special characters in User or Group names: & (ampersand) " (double quote) < (less than) > (greater than) ' (single quote) \ (backslash) If User or Group names contain any of these special characters, the characters are converted (for example, "&" becomes "&") and searches might return the following error: "No profile is associated with this Group"

Table 5 (Cont.) Known Issues and Workarounds for WebPass

Bug	Description
7421435	A response to a dynamic request sent to WebPass from IIS 6 has the 'Connection' header set to the value 'Close'. As a result, you might see TCP port exhaustion at the Web server end. This in turn limits the number of concurrent connections from the client (browsers or IDXML clients) to the Web server. **Note**: The other Web servers (for example, IPlanet (Sun Web server)), use chunked encoding on the response. As a result, the 'Connection' header is not set to 'Close'. **Solution**: By adding the parameter, 'SetContentLengthHeader' in the WebPass globalparams.xml file and setting it to true, the 'Content-length' header would be set in the response coming from the WebPass to the Web server. Because of this, the Web server would not send the 'Connection' header with the value 'Close' in its response to the browser. For more information, see the *Oracle Access Manager Customization Guide*.

6.6 Policy Manager Known Issues and Workarounds

Table 6 describes any known issues and workarounds for the Policy Manager for Oracle Access Manager 10*g* (10.1.4.3).

Table 6 Known Issues and Workarounds for the Policy Manager

Bug	Description

7679865	During Policy Manager setup on Linux, error messages might appear in the Policy Manager log file that do not indicate an actual error. For example:
	
	`... "No such file or directory"`
	`... "Could not read file"`
	
	For a list of messages, see Knowledge base note number 835857.1 on My Oracle Support (formerly MetaLink) at: https://metalink.oracle.com.

6882112	An unresolved issue that causes the Access Server and Policy Manager to become unresponsive and require a restart. This occurs when SSL is enabled for LDAP servers used by the Access Server and Policy Manager while performing Add and Update operations to Host Identifiers from two or more browsers simultaneously. Until a fix is identified, Oracle recommends that changes to Host Identifiers be made only from one browser instance at a time.

6.7 Access Server Known Issues and Workarounds

Table 7 describes any known issues and workarounds for the Access Server for Oracle Access Manager 10*g* (10.1.4.3).

Table 7 Known Issues and Workarounds for the Access Server

Bug	Description
5885660	Oracle Access Manager 10*g* (10.1.4.3) provides encoding for ob_url in Access Server audit records. This guards against spoofing attacks that could lead to spoofed entries being added to Audit Logs. You can revert Access Server audit record encoding by adding a new parameter (`EncodeURLBeforeAuditing`) with a value to `false` to the Access Server globalparams.xml file. Oracle strongly recommends that encoding behavior not be changed using this parameter. **Caution**: Oracle strongly recommends that encoding behavior not be changed using this parameter. The `EncodeURLBeforeAuditing` parameter applies to only Access Server globalparams.xml.
8449425	The Access Server fails to start when the ORACLE_HOME environment variable is set with a trailing slash character, /. Incorrect: ORACLE_HOME=/opt/OHS11g_oracle/product/11.1.1/as_1/ or ORACLE_HOME=D:\oracle\product\11.1.1\as_1\ Correct: ORACLE_HOME to "/opt/OHS11g_oracle/product/11.1.1/as_1 or ORACLE_HOME=D:\oracle\product\11.1.1\as_1 Confirm there is no trailing slash in your ORACLE_HOME environment variable.
6882112	An unresolved issue that causes the Access Server and Policy Manager to become unresponsive and require a restart. This occurs when SSL is enabled for LDAP servers used by the Access Server and Policy Manager while performing Add and Update operations to Host Identifiers from two or more browsers simultaneously. Until a fix is identified, Oracle recommends that changes to Host Identifiers be made only from one browser instance at a time.
7275401	You can write a stack trace to a log file if Oracle Access Manager experiences a core dump on the Access Server and the Identity Server. However, writing the stack trace might prevent the core dump from being written. You might need to disable the `StackDumpEnabled` parameter in globalparams.xml when pursuing diagnostic issues or when instructed by Oracle Support to re-create a core dump scenario. See the troubleshooting appendix of the *Oracle Access Manager Identity and Common Administration Guide* for details and steps you must perform to enable or disable the stack trace when pursuing diagnostic issues or recreating crashes.

6.8 WebGate Known Issues and Workarounds

Table 8 describes known issues and workarounds for the WebGate for Oracle Access Manager 10*g* (10.1.4.3).

Table 8 Known Issues and Workarounds for WebGates

Bug	Description

8636800	Oracle recommends using the following as broad guidelines when tuning httpd.conf directives for Oracle HTTP Server 11g with Oracle Access Manager 10*g* (10.1.4.3):
	`Timeout 500`
	`MaxKeepAliveRequests 500`
	`KeepAliveTimeout 10`
	
	`<IfModule mpm_worker_module>`
	`ServerLimit 25`
	`StartServers 2`
	`MaxClients 500`
	`MinSpareThreads 25`
	`MaxSpareThreads 75`
	`ThreadsPerChild 25`
	`MaxRequestsPerChild 0`
	`AcceptMutex fcntl`
	`LockFile`
	`"${ORACLE_INSTANCE}/diagnostics/logs/${COMPONENT_`
	`TYPE}/${COMPONENT_NAME}/http_lock"`
	`</IfModule>`

7540597	WebGate oblog.log file lists unexplained error messages indicating that WebGate is trying to read files that do not exist in the WebGate installation directory. However, these do not indicate an actual error. For example:
	`"Could not read file "`
	`... WG_Install_Dir/../apps/common/bin/globalparams.xml`
	`... WG_Install_Dir/../data/common/config/oblog_config.xml`
	`... WG_Install_Dir/../lang/en-us/netlibmsg.xml`
	
	For a list of messages, see Knowledge base note number 835857.1 on My Oracle Support (formerly MetaLink) at: `https://metalink.oracle.com`.

8279704	The *Oracle Access Manager Access Administration Guide* section "Securing the ObSSOCookie in an Authentication Scheme" instructs you to specify a challenge parameter `ssoCookie:httponly`. However, the functionality (`ssoCookie:httponly`) is enabled by default in Oracle Access Manager 10*g* (10.1.4.3) to ensure that the ObSSOCookie is not accessible to client side scripts such as JavaScript. To disable this functionality, which produces a less secure environment, specify `ssoCookie:disablehttponly` in the authentication scheme. See Also: Bug 8279704 in "Documentation Known Issues" on page -21.
8596762	When using the `ssoCookie:httponly` challenge parameter (the default) in an Authentication scheme, you can prevent JavaScript running in the browser from accessing the ObSSOCookie. This provides a more secure environment. However, browser support for the `ssoCookie:httponly` challenge parameter is inconsistent and can cause applets to not run correctly. This parameter can be disabled if needed. However, disabling this challenge parameter does result in a less secure environment: Specify `ssoCookie:disablehttponly` in the authentication scheme challenge parameter.

6.9 Performance Issues and Workarounds

As explained in the chapter on caching in the *Oracle Access Manager Deployment Guide*, you can ensure that the Access Server is automatically informed of changes in the Identity System by configuring the Identity Server to notify the Access Server of each change to user and group information. The Access Server caches are then automatically flushed and replaced with the latest information. This is a best practice to ensure that all components have up-to-date information.

However, even though automatic cache flush is a best practice, it can cause performance issues if you have multiple Access Servers that use a secure communication mode. The performance issues occur as follows:

- There are frequent cache flush requests as a result of the Identity System performing IdentityXML operations to modify a profile.
- There is an SSL handshake for each request to each Access Server that is configured in Simple or Cert transport security mode.

  The SSL handshakes that are required in a secure multi-server environment can impede performance.

Oracle Access Manager 10*g* (10.1.4.3) provides a better way to implement mixed-mode communication for cache flush operations. For more information, see the *Oracle Access Manager Deployment Guide*.

Table 9

Bug	Description
7280995	When plug-in parameters differ between the "Basic Over LDAP" Authentication scheme versus "Oracle Access and Identity Basic over LDAP" Authentication scheme, performance degradation can be noticeable. For example, 1000 requests for resources protected by the same policy domain can be up to 50% slower when "Oracle Access and Identity Basic Over LDAP" plug-in parameters and values do not match Basic Over LDAP plug-in parameters and values. **Workarounds** 1. **Tune Oracle Internet Directory**: If this is your directory server, be sure to perform relevant tasks in the section on "Tuning for Oracle Internet Directory" in the *Oracle Access Manager Installation Guide*. 2. **Modify Plug-in Parameters**: a. In the Policy Manager, ensure that the Oracle Access and Identity Basic Over LDAP Authentication scheme is not included in the authentication rules of any active policy domains. b. From the Access System Console, click Access System Configuration, then click Authentication Management. c. On the Authentication Management: List All Authentication Schemes page, click the Basic Over LDAP authentication scheme. d. On the Details for Authentication Scheme page, click Modify. e. On the Modifying Authentication Scheme page, click the Plugins tab, copy information for use in the Oracle Access and Identity Basic Over LDAP Authentication scheme, and then click Back. f. On the Authentication Management: List All Authentication Schemes page, click Oracle Access and Identity Basic Over LDAP. g. On the Details for Authentication Scheme page, click Modify. h. On the Modifying Authentication Scheme page, click the Plugins tab, click Modify, modify information to match the use in the plug-ins used in the Basic Over LDAP Authentication scheme, and then click Save. i. In the Policy Manager, enable policy domains containing the Oracle Access and Identity Basic Over LDAP Authentication scheme. For more information, see the *Oracle Access Manager Access Administration Guide*.

6.10 Software Developer Kit (SDK), API, and Third-Party Known Issues and Workarounds

Table 10 describes any known issues and workarounds for SDKs and third-party integrations for Oracle Access Manager 10*g* (10.1.4.3).

Table 10 Known Issues and Workarounds for SDKs, Third-Party Integrations

Bug	Description

8602649	The Access Manager Software Developer Kit (SDK) access/oblix/tools/lang_tools directory might be missing (or files within this directory might be missing). There is a possible loss of language functionality when non-English Oracle-provided Language Packs are installed with the SDK.
	
	As explained in the *Oracle Access Manager Installation Guide*, the obnls.xml configuration file should be automatically updated for each component in *component_install_dir*\identity|access\oblix\config\obnls.xml. Installed languages and entries in obnls.xml must match for each component.
	
	In this case, however, languages and entries in the SDK obnls.xml file are not updated automatically. The following error appears in installation logs within /tmp/Access Server SDK.log:
	
	`OAM_10143/asdk/AccessServerSDK/oblix/tools/lang_tools/defaultLangu age.l st (No such file or directory)"; ...`
	
	`WizardException: (error code = 200; message=OAM_10143/asdk/AccessServerSDK/oblix/tools/lang_tools/ defaultLanguage.lst (No such file or directory)"; severity = 0; exception ...`
	`...`
	`java.io.IOException: OAM_10143/asdk/AccessServerSDK/oblix/tools/lang_tools/start_ obupdate`
	
	Workaround:
	1. Perform SDK installation without any Language Packs.
	2. Copy an existing access/oblix/tools/lang_tools directory from another Oracle Access Manager Access System component directory path into the SDK installation path. For example:
	From: *AccessServer_install_dir*\accesss\oblix\tools\lang_tools
	To: *SDK_install_dir*\access\oblix\tools\lang_tools
	3. Install desired Oracle-provided Language Packs.

Table 10 (Cont.) Known Issues and Workarounds for SDKs, Third-Party Integrations

Bug	Description
5752513	Locations of the following sample code have changed in the *AccessServer_install_dir*/ path: ▪ **authn_api.h**: This file contains definitions of the set of utilities that the Access Server provides to all authentication plug-ins and definitions of the API data and functions. From: `oblix/sdk/authentication/samples/authn_api/include` To: `oblix/sdk/authn_api/` ▪ **as_plugin_utils.h**: This file defines a set of utilities that the Access Server provides to all authorization plug-ins. authz_plugin_api.h defines the API data and functions, and includes the other header file From (UNIX): `oblix/sdk/authorization/samples/authz_api/include` From (Windows): `oblix/sdk/authorization/samples/include` To (Both Platforms): `oblix/sdk/authz_api/` ▪ **authz_plugin_api.h**: This file defines the API data and functions, and includes the other header file. From (UNIX): `oblix/sdk/authorization/samples/authz_api/include` From (Windows): `oblix/sdk/authorization/samples/include` To (Both Platforms): `oblix/sdk/authz_api/`
8315442	**Problem**: Oracle Access Manager Client Certificate authentication exhibits issues if used directly from an OracleAS Web Cache site. Oracle Access Manager Client certificate authentication is not supported without loading special Oracle HTTP Server headers and parameters. Also, does not comply with non-Oracle HTTP Server Web servers. **Cause**: Oracle Access Manager Client Certificate authentication support through OracleAS Web Cache requires that mod_certheaders.so is loaded in the back-end Oracle HTTP Server-based Web server. An OracleAS Web Cache site sets special header variables when using client certificate authentication, which must be handled by the back-end Web server. If Oracle HTTP Server does not load the mod_certheaders.so, client certificate authentication cannot work for Oracle Access Manager through OracleAS Web Cache. Also, OracleAS Web Cache only supports client certificate authentication with Oracle HTTP Server-based Web servers because it is able to load the needed certheaders. **Solution**: See "Solution for Bug 8315442" on page 20.

Solution for Bug 8315442

Oracle HTTP Server should load mod_certheaders with the special parameter value of SSL_CLIENT_CERT for supporting Oracle Access Manager Client Certificate authentication. Add the following two lines in the httpd.conf of the back-end Oracle HTTP Server Web server and restart it to get Oracle Access Manager Client Certificate authentication working,

---

Note: Upon loading the mod_certheaders.so, native Oracle Access Manager does not receive the client certificates if requested directly through the Oracle HTTP Server Web server (that is, not through the configured OracleAS Web Cache site). Hence, this is not supported behavior.

The mod_certheaders.so is especially loaded so that OracleAS Web Cache communicates with Oracle Access Manager for the client certificates. Hence, the same OracleAS Web Cache site and corresponding back-end Oracle HTTP Server site cannot be used for client certificate authentication at the same time.

Oracle HTTP Server documentation explaining Client Certificate authentication is available at:
http://iasdocs.us.oracle.com/iasdl/101202fulldoc/web.1012/b14007/confmods.htm#HSADM015

To configure Client Certificate authentication for Oracle Access Manager and OracleAS Web Cache

1. Add the following two lines in the httpd.conf of the back-end Oracle HTTP Server, and then restart the Web server.

   Oracle HTTP Server v1

   ```
   LoadModule certheaders_module libexec/mod_certheaders.so
   AddCertHeader SSL_CLIENT_CERT
   ```

   Oracle HTTP Server v2

   ```
   LoadModule certheaders_module modules/mod_certheaders.so
   AddCertHeader SSL_CLIENT_CERT
   ```

2. Verify that the following selection is done in the Web Cache Administration Console to support client certificate authentication:

   a. Select "Required" for Client certificate Support in the Ports Tab for the corresponding port chosen for the OracleAS Web Cache site.

   b. Check the box on the Site's Advanced Tab for the corresponding OracleAS Web Cache site, stating that this site will support client certificate authentication.

   Note: Upon loading the mod_certheaders.so, native Oracle Access Manager does not receive the client certificates if requested directly through the Oracle HTTP Server Web server (that is, not through the configured OracleAS Web Cache site).

6.11 Documentation Known Issues

Table 11 describes any known issues in the documentation for this release.

Table 11 Known Issues and Workarounds for Documentation

Bug	Description
8636800	The *Oracle Access Manager Installation Guide* chapter on troubleshooting provides broad guidelines for tuning httpd.conf directives for Oracle HTTP Server 11g or Apache v2 with Oracle Access Manager 10g (10.1.4.3). For Oracle HTTP Server 11g specifics, see bug 8636800 in Table 8, " Known Issues and Workarounds for WebGates".

Table 11 (Cont.) Known Issues and Workarounds for Documentation

Bug	Description
5752513	The *Oracle Access Manager Developer Guide* incorrectly states the locations of several samples, as follows: ■ **authn_api.h**: This file contains definitions of the set of utilities that the Access Server provides to all authentication plug-ins and definitions of the API data and functions. From: `oblix/sdk/authentication/samples/authn_api/include` To: `oblix/sdk/authn_api/` ■ **as_plugin_utils.h**: This file defines a set of utilities that the Access Server provides to all authorization plug-ins. authz_plugin_api.h defines the API data and functions, and includes the other header file From (UNIX): `oblix/sdk/authorization/samples/authz_api/include` From (Windows): `oblix/sdk/authorization/samples/include` To (Both Platforms): `oblix/sdk/authz_api/` ■ **authz_plugin_api.h**: This file defines the API data and functions, and includes the other header file. From (UNIX): `oblix/sdk/authorization/samples/authz_api/include` From (Windows): `oblix/sdk/authorization/samples/include` To (Both Platforms): `oblix/sdk/authz_api/`
8279704	The *Oracle Access Manager Access Administration Guide* section "Securing the ObSSOCookie in an Authentication Scheme" instructs you to specify a challenge parameter: `ssoCookie:httponly`. However, `ssoCookie:httponly` and `ssoCookie:secure` might have been misstated in the guide. **Note**: Together, `ssoCookie:httponly` and `ssoCookie:secure` in the challenge parameter of the Authentication scheme secure the ObSSOCookie. The challenge parameter is case-sensitive. Be sure to enter an uppercase C in ssoCookie. ■ `ssoCookie:httponly` is enabled by default to ensure that the ObSSOCookie is not accessible to client side scripts such as JavaScript. This parameter can be disabled by specifying `ssoCookie:disablehttponly` in the authentication scheme. ■ `ssoCookie:Secure` must be added to the challenge parameter of an Authentication scheme to ensure that an ObSSOCookie is not set when a resource is accessed using HTTP under a secure network. The cookie is set only when the resource is accessed through HTTPS. **Note**: Be sure to enter an uppercase S in Secure. The ssoCookie: challenge parameter can contain multiple values separated by a semicolon (;). For example, to send the ObSSOCookie over an SSL connection while allowing access to the ObSSOCookie through client side scripts, you can set `ssoCookie:Secure;disablehttponly` as the challenge parameter. **Note**: `ssoCookie:max-age` is another general cookie attribute supported by Oracle Access Manager. This attribute creates a persistent cookie in some browsers (Internet Explorer and Mozilla), rather than a cookie that lasts for a single session. In the challenge parameter for the Authentication scheme, add the following information based on the needs of your environment: `ssoCookie:max-age=`*`time-in seconds`* For more information, see "Retaining the ObSSOCookie Over Multiple Sessions" in the Oracle Access Manager Access Administration Guide.

Table 11 (Cont.) Known Issues and Workarounds for Documentation

Bug	Description
8443139	**Setup**: An Apache-based Web server is configured as a Reverse Proxy, and a proxy for Web server root "/" is added in the httpd.conf. You can access all the resource Web server URLS through the Reverse Proxy host-port details. If the Lost Password Management (LPM) setting is enabled on the Reverse Proxy WebGate environment, the flow behaves through Reverse Proxy access. If a user's password has been reset, the user is asked to change the password. During the flow, the backURL is picked up by the WebGate of the back-end resource WebGate. Also, upon completing the change password or set challenge responses flow, the user is sent to the backURL (of the resource WebGate). **Problem**: The backURL is fetching the value of the back-end resource WebGate. Also, upon successful completion of the change password or set challenge/response flow for lost password management (LPM), the user is sent to the backURL of the resource WebGate. **Required Configuration**: In a Reverse proxy environment, the backURL should not be set to the actual resource Web source because this can lead to the disclosure of back-end WebGate details. See "Required Configuration for Bug 8443139" on page 26.
7667220	The *Oracle Access Manager Installation Guide* chapter "Configuring Apache v1.3-based Web Servers for Oracle Access Manager" contains incorrect information in Step 5 of the procedure "To tune Oracle HTTP Server for Oracle Access Manager Web components". **Incorrect**: 5. In httpd.conf file on the Policy Manager, comment-out the following lines: #LoadModule perl_module modules/mod_perl.so #LoadModule php4_module modules/mod_php4.so **Correct**: 5. In httpd.conf file on the Policy Manager, comment-out the following lines: #LoadModule perl_module libexec/libperl.so #LoadModule php4_module modules/libphp4.so
8437838	The *Oracle Access Manager Identity and Common Administration Guide* information on password policy qualification is not explicit with regard to the role of filters. **Incorrect**: A user can qualify under more than one policy in a domain. In this situation, password policies are evaluated in a bottom-to-top order. The first policy that applies to the user is selected, as illustrated in Figure 7-1. **Problem**: The example used assumes that no filters are used in the password policies. **Correct**: Additional language should be added to address the use of password policies that have filters. For details, see "Guidelines for Bug 8437838" on page 27.

Table 11 (Cont.) Known Issues and Workarounds for Documentation

Bug	Description
4447307	A new feature was introduced in Oracle COREid 7.0.4.2, that is not described in recent manuals. When using "`Basic over LDAP`" authentication, the browser returns the cached credential following a timeout. A new challenge parameter `"realmunique:yes"` enables a basic authentication mode that causes realm parameters sent by WebGate to be unique (by appending a date/time string to the realm string). As a result, the browser never encounters the same realm twice, thus never sends cached credentials to WebGate.
6596842	In previous releases, the start page for the Policy Manager was the **My Policy Domains** page. If there were many policies on this page, it would take a long time to appear. In this release, the start page for the Policy Manager is now a search page instead of the **My Policy Domains** page. A future release of the *Oracle Access Manager Access Administration Guide* should note this change.
6160534	The help topic on defining organization workflows refers to the *COREid Access and Identity Administration Guide*. The correct document name is *Oracle Access Manager Identity and Common Administration Guide*
n/a	Certain manuals reference this release note document with an incorrect file name: Incorrect:oam_10143_readme_doc.pdf Correct: This document is named oamrn.htm (and oamrn.pdf).

n/a	Two files are required when configuring SSO for Oracle Fusion Middleware, as described in the *Oracle Fusion Middleware Security Guide*:
	
	▪ oamAuthnProvider.jar
	
	`ORACLE_INSTANCE/modules/oracle.oamprovider_11.1.1/oamAuthnProvider.jar`
	
	▪ oamcfgtool.jar
	
	`ORACLE_INSTANCE/modules/oracle.oamprovider_11.1.1/oamcfgtool.jar`
	
	Both files are available in the Oracle Web Tier. However, if you configure SSO with a stand alone Oracle WebLogic Server, you can locate the Oracle Access Manager files on Oracle Technology Network (OTN) as follows:
	
	`http://www.oracle.com/technology/software/products/ias/htdocs/idm_11g.html`
	
	▪ oamauthnprovider_<*version*>.zip: oamauthnprovider_10_1_4_3_0.zip
	
	Oracle Access Manager 10g Core Components (10.1.4.3.0) DVD
	
	▪ oamcfgtool_<*version*>.zip: oamcfgtool_10_1_4_3_0.zip
	
	Oracle Access Manager 10g WebGates (10.1.4.3.0) DVD

Table 11 (Cont.) Known Issues and Workarounds for Documentation

Bug	Description
n/a	In the *Oracle Access Manager Access Administration Guide*, the section "Configuring User-Defined AccessGate Parameters" states: **Incorrect**: .n earlier versions of Oracle Access Manager, a file named WebGateStatic.lst was used to configure various settings for a WebGate... have moved to the AccessGate configuration page...as user-defined parameters. ....To implement user-defined parameters, ...and contact Oracle for a patch for the WebGate. **Correct**: The reference to "... contact Oracle for a patch for the WebGate" is not relevant for 10*g* (10.1.4.3) and can be ignored.

Table 11 (Cont.) Known Issues and Workarounds for Documentation

Bug	Description

n/a	A new parameter, `EnableTraceback`, has been added to the Identity Server and Policy Manager globalparams.xml files following release of the *Oracle Access Manager Customization Guide*. The following information is missing from the manual:
	
	In Oracle Access Manager 10*g* (10.1.4.3), Traceback reporting in the Bug Report Form and Stylesheet Error Report Form is disabled by default. These pages display only the message "Traceback is unavailable." in the Traceback field. However, oblogs reflect the entire Traceback.
	
	Note: Oracle recommends that traceback functionality remains disabled. This should be enabled only if there is a problem that is causing Bug Report Form and Stylesheet Error Report Form events, where additional information is needed to determine the cause of the issue.
	
	To enable Traceback display on Bug Report Form and Stylesheet Error Report Form
	
	1. Locate the Identity Server globalparams.xml file in the following path:
	`IdentityServer_install_dir\identity\oblix\apps\common\bin\globalparams.xml`
	
	2. Add the `EnableTraceback` parameter with the value set to `true`, and save the file.
	`<SimpleList>`
	`  <NameValPair`
	`  ParamName="EnableTraceback"`
	`  Value="true"></NameValPair>`
	`</SimpleList>`
	
	3. Restart the Identity Server.
	4. Repeat steps 1 through 3 for each Identity Server in your deployment.
	5. Locate the Policy Manager globalparams.xml file in the following path:
	`PolicyMsanager_install_dir\access\oblix\apps\common\bin\globalparams.xml`
	
	6. Add the `EnableTraceback` parameter with the value set to `true`, and save the file.
	`<SimpleList>`
	`  <NameValPair`
	`  ParamName="EnableTraceback"`
	`  Value="true"></NameValPair>`
	`</SimpleList>`
	
	7. Restart the Policy Manager Web server.
	8. Repeat steps 5 through 7 for each Policy Manager in your deployment.

Required Configuration for Bug 8443139

Oracle recommends the following settings in an Apache-based Reverse Proxy environment to preserve host details:

Preserve Host Details: In the Validate_password plug-in for the authentication scheme used in the policy domain that protects resources, include the `ObWebPassURLPrefix` parameter and settings for your own Reverse Proxy URL. For example:

`Validate_password: ObWebPassURLPrefix=http://ps5678.yourco.co.uk:8999`

Apache v2: Set the `ProxyPreseveHost` parameter to `ON`. This parameter is supported only by Apache v2 Web Servers.

Sample Scenarios and Settings

1. **Reverse Proxy for Basic Authentication**: Make an entry of the resource hosted on the resource WebGate.

   `ProxyPass /test.html http://ps1234.yourco.co.uk:7676/test.html`

2. **Reverse Proxy for Form Authentication**: Make an entry of the resource hosted on the resource WebGate.

   a. Make an entry of the resource hosted on the resource WebGate. For example:

      `ProxyPass /test.html http://ps1234.yourco.co.uk:7676/test.html`

   b. Make an entry of the login form hosted on the resource WebGate. For example:

      `ProxyPass /login.html http://ps1234.yourco.co.uk:7676/login.html`

   c. Make an entry of the action parameter configured in the login form and the authentication scheme. For example:

      `ProxyPass /access/dummy http://ps1234.yourco.co.uk:7676/access/dummy`

3. **Reverse Proxy for Basic Authentication with Challenge Redirect**: Make an entry of the resource hosted on the resource WebGate.

   a. Perform Steps a through c of the previous example (item 2 in this list).

   b. Make an entry for obrar.cgi hosted on the resource WebGate. For example:

      `ProxyPass /obrar.cgi http://ps1234.yourco.co.uk:7676/obrar.cgi`

4. **Reverse Proxy for Form Authentication with Challenge Redirect**: Make an entry of the resource hosted on the resource WebGate.

   a. Perform Steps a through d of the previous example (item 3 in this list).

   b. Make an entry for obrareq.cgi hosted on the resource WebGate. For example:

      `ProxyPass /obrareq.cgi http://ps1234.yourco.co.uk:7676/obrareq.cgi`

   c. Make an entry for Reverse Proxy URL details in the Challenge Redirect field of the authentication scheme. For example:

      `Challenge Redirect http://ps5678.yourco.co.uk:8999`

Guidelines for Bug 8437838

Multiple password policies can be defined at the same domain-level with different Filter fields. These policies are considered grouped together at their shared domain level and are evaluated in an arbitrary order. The first of these filtered policies to match the user is selected for the user's password policy. When using such policy definitions there are two guidelines that help avoid unexpected policy results:

Guidelines

1. Avoid filters that match overlapping sets of users. For example:

   Policy 1 is defined with Domain: `ou=accounting, o=company, c=us` and `Filter:(cn="John*")`

Policy 2 is defined with Domain: `ou=accounting, o=company, c=us` and `Filter:(cn="*Doe")`

In this example, a user with `cn="John Doe"`, both of the policy domains would match and it could not be reliably predicted which would be chosen by Oracle Access Manager.

2. Avoid mixing policies that have filters with policies that do not have filters in the same domain-level. For example:

   Policy 1 is defined with Domain: `ou=accounting, o=company, c=us` and `Filter:(cn="John*")`

   Policy 2 is defined with Domain: `ou=accounting, o=company, c=us` with no filter.

   In this example, Policy 2 might be evaluated before Policy 1 and Policy 2 might be chosen as the password policy for a user with `cn="John Doe"`.

   Alternative: Create default policies at a higher domain-level with a filter that matches the lower domain level. For example:

   Policy 2 redefined as Domain: `ou=company, c=us` and `Filter:ou=accounting`

   Using this alternative, Policy 1 is definitely evaluated before Policy 2. Policy 1 is enforced for user `cn="John Doe,ou=accounting, o=company, c=us`. Policy 2 is enforced for user `cn=Jane Doe,ou=accounting, o=company, c=us`, and for user `cn=John Doe, ou=legal, o=company, c=us`.

7 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.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request

process. Information about TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of phone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html.

Oracle Access Manager Release Notes 10g (10.1.4.3.0) For All Supported Operating Systems
E12496-02