Oracle® Access Manager

Patch Set Notes

Release 10.1.4 Patch Set 1 (10.1.4.2.0) **E11067-01**

December 2007

This document accompanies Oracle Access Manager and supersedes earlier documentation. This document describes patch set installation, enhancements, fixed bugs, and known issues.

This patch set is for Oracle Access Manager 10*g* (10.1.4.0.1) only.

This document contains the following sections:

- Section 1, "About This Patch Set"
- Section 2, "Enhancements in This Patch Set"
- Section 3, "Patch Set Documentation"
- Section 4, "Patch Set Requirements"
- Section 5, "Patch Set Preparation, Application, and Removal"
- Section 6, "Restoring XSL Customizations After the Upgrade"
- Section 7, "Updates to Base Component and Third-Party Support"
- Section 8, "Known Issues and Workarounds"
- Section 9, "Bugs Fixed in This Release"
- Section 10, "Documentation Accessibility"

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

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

1 About This Patch Set

Patch sets are a mechanism for delivering fully tested and integrated product fixes. Patch sets include all files that were rebuilt to implement bug fixes. All of the fixes in the patch set were tested and are certified to work with one another.

This patch set is cumulative and includes all fixes from previous patch sets for Oracle Access Manager 10*g* (10.1.4.0.1) *and* PSE Hot Fixes, through 10.1.4.0.1.

This rest of this section discusses the following topics:

- What Happens When You Apply the Patch Set

- Oracle Access Manager Releases Supported by This Patch Set

> **See Also:** To download free installation documentation, release notes, white papers, or other collateral, go to Oracle Technology Network (OTN). You must register online before using OTN. 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 documentation section of the OTN Web site at the following URL:
>
> `http://www.oracle.com/technology/documentation`

1.1 What Happens When You Apply the Patch Set

When you apply the patch set to an Oracle Access Manager installation, the patch program updates specific software and configuration files contained in the selected Oracle Access Manager component installation directory. In this document, this is referred to as *component_install_dir*. Replace this variable with the full path of the installed Oracle Access Manager component instance.

This patch set updates the software for base Oracle Access Manager components.

1.2 Oracle Access Manager Releases Supported by This Patch Set

You can only apply this patch set to Oracle Access Manager 10*g* (10.1.4.0.1).

The base product, language packs, third-party packages, and readme files that describe the download CD contents for Oracle Access Manager 10*g* (10.1.4.0.1) are at the following URL:

`http://www.oracle.com/technology/software/products/ias/htdocs/101401.html`

You should read the Oracle Access Manager 10*g* (10.1.4.0.1) release notes. The following procedure describes how to download these release notes.

To access the Oracle Access Manager 10*g* (10.1.4.0.1) release notes

1. Go to the following URL:

   `http://download.oracle.com/docs/cd/B28196_01/index.htm`

2. Click the **Getting Started** tab.

   In the section of this page labeled **Oracle Application Server Release Notes**, click the **PDF** or **HTML** link.

3. In the release notes document, click the bookmark for **Oracle Access Manager.**

2 Enhancements in This Patch Set

Oracle Access Manager 10*g* (10.1.4.0.1) was a significant new release. For a complete list of product enhancements in Oracle Access Manager 10*g* (10.1.4.0.1), see the *Oracle Access Manager Introduction*.

Oracle Access Manager Release 10.1.4 Patch Set 1 (10.1.4.2.0) updates specific software and configuration files contained in your existing 10*g* (10.1.4.0.1) installation. The result is improvements to the reliability and performance of the software. In addition, this patch set enhances several key features, as described in the following sections:

- General Enhancements
- Identity System Enhancements
- Access System Enhancements
- SDK and Third-Party Integration Enhancements
- Documentation Enhancements

2.1 General Enhancements

The following table describes general enhancements in this patch release.

Topic	Description of General Enhancement
Platform support	Novell eDirectory v8.8 is certified for Oracle Access Manager Release 10.1.4 Patch Set 1 (10.1.4.2.0). However, Release 10.1.4 Patch Set 1 (10.1.4.2.0) must be applied to an existing installation and cannot be used for a fresh installation. Novell eDirectory v8.8 is not certified for 10.1.4.0.1. For new Oracle Access Manager installations where you want to use Novell eDirectory v8.8, 10.1.4.0.1 can be used in the set up and configuration operations against Novell eDirectory v8.8 and then 10.1.4 Patch Set 1 (10.1.4.2.0) applied as described in "Patch Set Preparation, Application, and Removal" on page 14.
XSL files	Specific xsl files were upgraded to support a JavaScript-related fix and fixes related to the handling of large groups. If you have customized these files, note that you need to restore your customizations after applying this patch. See "Restoring XSL Customizations After the Upgrade" for details.
Upgrades	You can now perform an upgrade without shutting down service to your Oracle Access Manager customers. The zero downtime upgrade method is an alternative to the standard in-place component upgrade. The *Oracle Access Manager Upgrade Guide* includes a chapter that describes how you can perform a zero downtime upgrade. A new parameter in the globalparams.xml file, `MigrateUserDataTo1014`, is used by the Identity Server and Access Server during a zero downtime upgrade. The value of `MigrateUserDataTo1014` halts automatic user data migration when a user first logs in after upgrading. Only the multiple challenge and response attributes for Lost Password Management are affected. See the zero downtime upgrade details in the *Oracle Access Manager Upgrade Guide*.

Topic	Description of General Enhancement
Diagnostics	To diagnose a problem, you often need to configure a fine-grained threshold for logging, for example, Debug or Trace. However, you may not want to generate detailed logs for every component function. For example, to diagnose slow response times for an Identity Server's LDAP directory, you might want to generate detailed logs only for LDAP operations. In this release, you can configure different log threshold levels for different modules or functions of a component. When you configure multiple threshold levels, Oracle Access Manager generates detailed logs for specific component areas, while maintaining concise logs for the other areas, as specified in the logging configuration file. For example, you can generate Debug logs for LDAP operations performed by the Identity Server and Error logs for all other Identity Server functions. See the *Oracle Access Manager Identity and Common Administration Guide* for details.
LDAP bind password	You may need to periodically update the LDAP bind password for the directory servers that communicate with Oracle Access Manager components. For example, you may want to update the LDAP bind password to comply with government regulations. Functionality for updating the LDAP bind password has been added in this release. The `ModifyLDAPBindPassword` command enables you to reset the LDAP bind password in the Oracle Access Manager configuration files. You can reset the LDAP bind password without restarting any servers or re-running setup. In previous releases, after updating the LDAP bind password, it was necessary to re-run setup. In this release, it is no longer necessary to rerun setup. See the chapter on reconfiguring the system in the *Oracle Access Manager Deployment Guide* for details.
Logging the time taken for different types of calls	You can now generate logs that show details about the time consumed by different types of calls to external components. This information can help you determine if requests to specific components are taking longer than expected. For more information, see the *Oracle Access Manager Identity and Common Administration Guide*.
Auditing	Oracle Instant Client binaries are now shipped with the Identity Server and Access Server. This eliminates the requirement for a 10.1.0.5 *ORACLE_HOME* on the computer that hosts Identity and Access Servers when auditing to an Oracle database with an OCI connection type.
NLS libraries	Even if an environment variable is set to ORACLE_HOME or ORA_NLS10, or a third-party Web component refers to a different version of the NLS libraries and data files than the one used by Oracle Access Manager, Oracle Access Manager components choose NLS data files from the *Oracle_Access_Manager_component_install_dir.*

Topic	Description of General Enhancement
Troubleshooting	The Access Server and Identity Server have new diagnostic tools to help you work with an Oracle Technical Support representative to troubleshoot problems. The diagnostic tools enable you to do the following: ■ Obtain hard-to-locate information about component configuration and behavior. ■ Automatically capture events that immediately precede a core dump. ■ Manually capture a stack trace of any event in the Identity or Access System. See the *Oracle Access Manager Identity and Common Administration Guide* for details.
Logging operating system errors	Extended operating system error information is now included in the logs to assist with determining why calls are failing. For example, when an attempt to create a listener thread fails, the error code returned on `GetLastError()` is added to the log files. Operating system error information is logged at the DEBUG3 level.
Switching o.s. platforms	The *Oracle Access Manager Upgrade Guide* includes a new chapter that explains how you can upgrade while making a switch from a Solaris platform to a Linux platform.
Stack traces	If Oracle Access Manager experiences a core dump, it can now write a stack trace to a log file. To enable this functionality, you turn on logging at any minimal level. You can send the log file that contains the stack trace information to Oracle, along with a report of the problem. See the appendix on troubleshooting in the *Oracle Access Manager Identity and Common Administration Guide* for details.
Failover	A new parameter in globalparams.xml named `LDAPOperationTimeout` sets an amount of time that the Identity Server, Access Server, or Policy Manager waits for a response from the directory server for a single entry of a search result before the component fails over to a secondary server, if one is configured. A `heartbeat_ldap_connection_timeout_in_millis` parameter in globalparams.xml determines the time limit for establishing a connection with the directory server. If the time limit is reached, the Identity and Access Servers start establishing connections with another directory server. This parameter enables the Identity and Access Servers to proactively identify when a directory server is down, and it enables failover without requiring an incoming directory service request and a subsequent TCP timeout. See the chapter on failover in the *Oracle Access Manager Deployment Guide* and the appendix on parameter files in the *Oracle Access Manager Customization Guide* for details.

2.2 Identity System Enhancements

The following table describes Identity System enhancements in this patch release.

Topic	Description of Identity System Enhancement
IdentityXML	When using IdentityXML, the `XSLProcessor` parameter in the file globalparams.xml indicates the processor to use when generating the page. The only officially supported value, `default`, indicates that the XDK processor should be used. The values `XALAN` or `DGXT` can be used for testing. See the appendix on configuration parameters in the *Oracle Access Manager Customization Guide* for details.
Group performance	For large static groups, for example, groups with over 10,000 members, operations that involve the group can cause memory to spike. Group performance has been improved in this release. However, if you find that a large static group still affects performance, you can modify the default evaluation method for the group using the `LargeStaticGroups` parameter in globalparams.xml. There are a number of additional actions that you can take to improve the performance of large groups. See the chapter on performance tuning in the *Oracle Access Manager Deployment Guide* for details.
Identity Server polling	In a multi-process environment, many processes may poll the Identity Server. For example, if 100 processes are running, each process could result in an update to the webpass.xml file. To eliminate any possible overload, Oracle Access Manager ensures that only one process can acquire poll tracking information for a particular time. If any configuration changes are detected, the webpass.xml file is updated for the specific time. When setting up multiple Identity Servers or modifying WebPass, administrators can now configure the `PollTrackingRefreshInterval` in the webpass.xml file. This interval is configured in seconds. There are implications for configuring this parameter when setting up multiple Identity Servers or modifying a WebPass instance. See the *Oracle Access Manager Identity and Common Administration Guide* for details.

Automatic login after password change	Users can be logged in automatically after changing their password. To configure automatic login, the change password redirect URL must include `STLogin=%applySTLogin%` as a parameter.
	The following is an example of a change password redirect URL that logs the user in:
	`http://machinename:portnumber/identity/oblix/apps/lost_`
	`password_mgmt/bin/lost_password_mgmt.cgi?program=`
	`redirectforchangepwd&login=%login%%userid%&backURL=%`
	`HostTarget%%RESOURCE%&STLogin=%applySTLogin%&target=top`
	To implement this with a form-based authentication scheme, you must configure the challenge parameter `creds` by supplying the user name credential parameter as the first token, the password credential parameter as the second token, then any other credential parameters.
	See the *Oracle Access Manager Identity and Common Administration Guide* for details.

IdentityXML and localization	To support internationalization and localization, IdentityXML and SOAP interfaces accept ISO-8859-1 (Latin-1) and UTF-8. However, in previous releases, the XML response was always in UTF-8. In this release, IdentityXML responses are now sent in the same encoding format as the request. When a request uses Latin-1 encoding (encoding="ISO-8859-1"), the response uses Latin-1 encoding. When a request uses UTF-8 encoding, the response uses UTF-8 encoding.

2.3 Access System Enhancements

The following table describes Access System enhancements in this patch release.

Topic	Description of Access System Enhancement
Authentication	In a form-based authentication scheme, you can now specify a `maxpostdatabytes` challenge parameter. The value of this optional parameter is the maximum number of data bytes that an end user can post for authentication to a Web server that uses a WebGate. If the POST data exceeds the threshold set by maxpostdatabytes in the form-based authentication scheme, user receives an error and a log entry is added at the DEBUG3 log level in the oblog.log file. Example: `maxpostdatabytes:100` If you omit this parameter, the end user can post unlimited length strings for authentication to a Web server that is protected by a WebGate. Very long strings can cause the WebGate or Web server to crash, denial of service, or another fatal error.
Impersonation	In addition to configuring impersonation for resources on a computer that is protected by a WebGate, you can extend impersonation to other resources on the network. This is known as assigning a Delegate impersonation level to the client. See the chapter on Windows Impersonation in the *Oracle Access Manager Integration Guide* for details. Note that the information on impersonation has moved from the *Oracle Access Manager Access Administration Guide* to the *Oracle Access Manager Integration Guide*
Avoiding retries to a non-responsive server	A WebGate can keep retrying requests until the Access Server is shut down. A WebGate-to-Access Server timeout threshold specifies how long (in seconds) the WebGate waits for the Access Server to respond before it considers it unreachable and attempts the request on a new connection. If the Access Server takes longer to service a request than the value of the timeout threshold, the WebGate abandons the request and retries the request on a new connection. Note that the new connection that is returned from the connection pool can be to the same Access Server, depending on your connection pool settings. Additionally, other Access Servers may also take longer to process the request than the time allowed by the threshold. In these cases, the WebGate can continue to retry the request until the Access Servers are shut down. You can now configure a limit on the number of retries that the WebGate performs for a non-responsive server using the `client_request_retry_attempts` parameter. This is a user-defined parameter in the Access System. The default value for this parameter is -1. Setting the parameter value to -1 (or not setting it at all) allows an infinite number of retries. See the *Oracle Access Manager Access Administration Guide* for details.
Virtual hosting	As of Oracle Access Manager 10.1.4.0.1, the **Preferred HTTP Host** field became required. This introduced issues for environments that support virtual hosting. In this release, to support virtual hosts you set the **Preferred HTTP Host** value to **HOST_HTTP_HEADER** for most Web hosts or **SERVER_NAME** (Apache-based). Additional configuration is required for IIS. See the chapter on configuring Access Servers and AccessGates in the *Oracle Access Manager Access Administration Guide* for details.

Topic	Description of Access System Enhancement
Performance	In previous releases, it could take a long time to create a large number of policy domains and URL prefixes in the Policy Manager. In this release, searches to the directory server have been minimized for these operations, resulting in better performance for these operations. Additionally, a parameter named `ldapFilterSizeLimitInBytes` has been added to the globalparams.xml file for the Policy Manager. This parameter controls the size of the LDAP search filter. The default value is 1024 (1Kb) if you do not set the value explicitly in globalparams.xml, or if it is set to 0 or a negative number. If you set a value between 1 and 128, the value used is 128. This information will be added to the appendix on parameter files in the *Oracle Access Manager Customization Guide* in a future release. Finally, 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* will note this change.

2.4 SDK and Third-Party Integration Enhancements

The following table describes SDK and third-party integration enhancements in this patch release.

Enhancement	Description of SDK and Third-Party Integration Enhancement
NLS libraries	Even if an environment variable is set to ORACLE_HOME or ORA_NLS10, or a third-party Web component refers to a different version of the NLS libraries and data files than the one used by Oracle Access Manager, Oracle Access Manager components choose NLS data files from the *Oracle_Access_Manager_component_install_dir.*
Impersonation	In addition to configuring impersonation for resources on the computer that is protected by a WebGate, you can extend impersonation to other resources on the network. This is known as assigning a Delegate impersonation level to the client. Note that the information on impersonation has moved from the *Oracle Access Manager Access Administration Guide* to the *Oracle Access Manager Integration Guide* See the chapter on configuring impersonation in the *Oracle Access Manager Integration Guide* for details.
SharePoint Office Server 2007 support	Integrating Oracle Access Manager with SharePoint Office Server 2007 is now supported. See the chapter on integrating with SharePoint in the *Oracle Access Manager Integration Guide* for details.
SAP NetWeaver support	Integrating Oracle Access Manager with SAP NetWeaver is now supported. See the chapter on integrating with SAP in the *Oracle Access Manager Integration Guide* for details.
Siebel support	Integrating Oracle Access Manager with Siebel in a multi-domain Active Directory environment is now supported. See the chapter on integrating with Siebel in the *Oracle Access Manager Integration Guide* for details.

Enhancement	Description of SDK and Third-Party Integration Enhancement
Weblogic 9.2 support	Integrating Oracle Access Manager with Weblogic 9.2 is now supported. This integration is now supported on Windows as well as previously supported platforms. See the chapter on integrating with WebLogic in the *Oracle Access Manager Integration Guide* for details.
WebSphere 6.1 support	Integrating Oracle Access Manager with WebSphere 6.1 is now supported. See the chapter on integrating with WebSphere in the *Oracle Access Manager Integration Guide* for details.

2.5 Documentation Enhancements

The following table describes documentation enhancements in this patch release.

Topic	Description of Documentation Enhancement
All enhancements in this patch set	Except where noted, the enhancements documented in these patch notes have also been added to the appropriate location in the Oracle Access Manager documentation library.
The *Oracle Access Manager Upgrade Guide*	The *Oracle Access Manager Upgrade Guide* includes the following information: ■ A new section describes a methodology to accomplish a zero-downtime upgrade. ■ A new chapter explains how you can upgrade while making a switch from a Solaris platform to a Linux platform.
The *Oracle Access Manager Deployment Guide*	The following information has been added to the *Oracle Access Manager Deployment Guide*: ■ A chapter on performance tuning describes tuning group-related features in the Identity System and Access System. This chapter describes various deployment strategies and scenarios for Oracle Access Manager. ■ A new chapter outlines various backup and recovery strategies for Oracle Access Manager installations. For details, see the chapter on backup and recovery strategies in the *Oracle Access Manager Deployment Guide*. ■ A new "Deployment Overview" chapter has been added to introduce various deployment types, environments, and categories. ■ Details have been added to the "Capacity Planning" chapter to provide methods for calculating hardware requirements in a deployment. ■ New information has been added on performance tuning, failover, load balancing, caching, and migration planning.
The *Oracle Access Manager Integration Guide*	Information about configuring global logout from a single sign-on session has been added to an appendix on logout. Information about Domino and Impersonation has been moved to this guide.
The *Oracle Access Manager Introduction*	New terms have been added to the glossary in the *Oracle Access Manager Introduction* for the Oracle Access Manager Configuration Manager.

Topic	Description of Documentation Enhancement
The *Oracle Access Manager Access Administration Guide*	New information has been added to the appendix on logout regarding removing ObSSOCookies. Information about Domino and Impersonation has been moved to the *Oracle Access Manager Integration Guide*. Information about the SSOCookie parameter has been added to the appendix on configuring form-based authentication.
The *Oracle Access Manager Identity and Common Administration Guide*	New information about the Out of Office tab has been added to the "Workflow" chapter.

3 Patch Set Documentation

The following documents are related to this Oracle Access Manager Release 10.1.4 Patch Set 1 (10.1.4.2.0) patch release.

- This document, the *Oracle Access Manager Patch Set Notes for 10g Release 3 Patch Set 1 (10.1.4.2)* provides the following information:
  - Information needed to install or de-install the patch set itself.
  - Known issues and workarounds for Oracle Access Manager.
  - Bugs fixed in this release.

  This document is named oam_101420_readme.htm (or .pdf). It is in the directory named Docs/ in the patch set distribution.
- The following Oracle Access Manager manuals have been updated in this patch set release:
  - *Oracle Access Manager Introduction*—Introduces Oracle Access Manager and provides a road map to Oracle Access Manager manuals and a glossary.
  - *Oracle Access Manager Installation Guide*—Explains how to install and configure the 10*g* (10.1.4.0.1) components.

    For details about installing the horizontal data migration tool, see the *Oracle Access Manager Configuration Manager Installation and Administration Guide*.
  - *Oracle Access Manager Upgrade Guide*—Explains how to upgrade components to 10*g* (10.1.4.0.1).
  - *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 Single Sign-On, as well as third-party products, for example, BEA WebLogic, the Plumtree portal, and IBM WebSphere.
- *Oracle Access Manager Schema Description*—Provides details about the Oracle Access Manager LDAP schema.
- *Oracle Access Manager Configuration Manager Installation and Administration Guide*—Provides information about pushing configuration data changes from one Oracle Access Manager Release 10.1.4 Patch Set 1 (10.1.4.2.0), or Oracle COREid Release 7.0.4, deployment to another.

  For example, you can push changes from a development deployment to a preproduction deployment.

4 Patch Set Requirements

Requirements for this patch set are discussed in the following topics:

- Required Software and Platforms
- Required Environment Preparation
- XSL File Requirements
- Zero Downtime Upgrade and User Data Migration Requirements
- Requirements for Subsequent Patches

Note: For more information about in-place component upgrades and zero downtime upgrades, see the *Oracle Access Manager Upgrade Guide*.

4.1 Required Software and Platforms

Ensure that your environment meets the recommended system configuration described in the *Oracle Access Manager Installation Guide* and other Oracle Access Manager manuals.

The rest of this section discusses the following topics:

- Base Oracle Access Manager Version for This Patch
- Operating System Support

4.1.1 Base Oracle Access Manager Version for This Patch

You may apply Oracle Access Manager Release 10.1.4 Patch Set 1 (10.1.4.2.0) only to Oracle Access Manager 10*g* (10.1.4.0.1) installations.

If you have an earlier release, you must upgrade to Oracle Access Manager 10*g* (10.1.4.0.1) before applying this patch set.

> **Caution:** You cannot perform a fresh installation using Oracle Access Manager Release 10.1.4 Patch Set 1 (10.1.4.2.0) packages. You cannot perform an *in-place* upgrade of earlier Oracle Access Manager components with Release 10.1.4 Patch Set 1 (10.1.4.2.0) packages.

4.1.2 Operating System Support

Oracle Access Manager Release 10.1.4 Patch Set 1 (10.1.4.2.0) is supported on the following operating systems:

- Solaris operating systems supported by Oracle Access Manager
- Linux operating systems supported by Oracle Access Manager
- Microsoft Windows operating systems supported by Oracle Access Manager

4.2 Required Environment Preparation

Review these instructions before installation of this patch set:

- Review all of the information in "Patch Set Requirements".
- Keep Oracle Access Manager 10.1.4.2.0 release files separate from your other NetPoint or COREid installation files.
- When patching or un-patching a component, use the same login credentials that you used for installation of the component.

  Using different credentials can result in unexpected behavior, for example, several error messages can be displayed.
- Keep patch set installation files for each component available so that the patch set can be removed (uninstalled) at a future date.

  You must use original patch set files when removing a patch.

> **Note:** Patch sets are not cumulative. You do not need to remove any patch sets that you may have already applied before applying the current patch set.

4.3 XSL File Requirements

When you apply the Release 10.1.4 Patch Set 1 (10.1.4.2.0), the following modified xsl files replace your existing xsl files of the same name in your identity/oblix/lang/shared directory:

- gsc_view_profile_vertical.xsl
- gsc_view_profile_horizontal.xsl
- gsc_modify_profile_vertical.xsl
- gsc_modify_profile_horizontal.xsl
- deactivateuser.xsl
- navbar.xsl

After applying the patch, you need to ensure that your customized files include the enhancements. For more information about recovering your own xsl files after applying the patch set, see Section 6, "Restoring XSL Customizations After the Upgrade".

4.4 Zero Downtime Upgrade and User Data Migration Requirements

The following are requirements for zero downtime upgrades and user data migration at first login.

Oracle Access Manager provides a file named globalparams.xml that contains a number of global parameters. With Release 10.1.4 Patch Set 1 (10.1.4.2.0), a new parameter in globalparams.xml, `MigrateUserDataTo1014`, is used by the Identity Server and Access Server during a zero downtime upgrade. Depending on the value of `MigrateUserDataTo1014`, this parameter can halt automatic user data migration when a user first logs in after upgrading. Only the multiple challenge and response attributes for Lost Password Management, introduced with Oracle Access Manager 10*g* (10.1.4.0.1), are affected. No other user data attributes are migrated during a user's first login.

There are two possible values for `MigrateUserDataTo1014`:

- `true`: This value enables the automatic migration of a user's or administrator's Lost Password Management challenge parameters during their first login.

  The value is set to `true` by default in the following situations:

  - After you install Oracle Access Manager 10*g* (10.1.4.0.1) and apply Release 10.1.4 Patch Set 1 (10.1.4.2.0).
  - After you perform an in-place component upgrade to Oracle Access Manager 10*g* (10.1.4.0.1) and apply Release 10.1.4 Patch Set 1 (10.1.4.2.0).

- `false`: This value halts the automatic migration of a user's Lost Password Management challenge parameters during their first login.

  The value is set to `false` by default only when you upgrade using the zero downtime upgrade method. During a zero downtime upgrade, you install Oracle Access Manager 10*g* (10.1.4.0.1) and then apply Release 10.1.4 Patch Set 1 (10.1.4.2.0) before finishing the upgrade. As a result, components are upgraded to Oracle Access Manager Release 10.1.4 Patch Set 1 (10.1.4.2.0).

  After finishing the zero downtime upgrade and validating that it is successful, you must change the `MigrateUserDataTo1014` parameter value to `true` in the globalparams.xml file of each Release 10.1.4 Patch Set 1 (10.1.4.2.0) Identity Server and Access Server. Automatic propagation of changes to globalparams.xml is not provided. As mentioned in the first bullet, a value of `true` starts the automatic migration of a user's Lost Password Management challenge parameters during their first login.

A globalparams.xml file is located in the following directories:

*IdentityServer_install_dir/*identity/oblix/apps/common/bin

*WebPass_install_dir/*Webcomponent/identity/oblix/apps/common/bin

*PolicyManager_install_dir/*Webcomponent/access/oblix/apps/common/bin

*AccessServer_install_dir/*access/oblix/apps/common/bin

Only the Release 10.1.4 Patch Set 1 (10.1.4.2.0) Identity Server and Access Server use the `MigrateUserDataTo1014` parameter. In general, some parameters in the globalparams.xml file are the same for all components while other parameters are specific to only few components. For more information about the content of the globalparams.xml file, see the *Oracle Access Manager Customization Guide*.

4.5 Requirements for Subsequent Patches

Oracle Access Manager 10*g* (10.1.4.0.1) is a major release, not a patch set. Oracle Access Manager Release 10.1.4 Patch Set 1 (10.1.4.2.0) is a patch set.

Be aware of the following requirements for future patch sets in regards to these releases:

- When you install Oracle Access Manager 10*g* (10.1.4.0.1) and then apply Release 10.1.4 Patch Set 1 (10.1.4.2.0), the component instances are considered to be 10*g* (10.1.4.0.1).

  In this case, you must remove Release 10.1.4 Patch Set 1 (10.1.4.2.0) before applying subsequent patch sets.

- When you upgrade earlier components to Oracle Access Manager 10*g* (10.1.4.0.1) using the standard in-place component upgrade method, and then apply Release 10.1.4 Patch Set 1 (10.1.4.2.0), the component instances are considered to be release 10*g* (10.1.4.0.1).

  In this case, you must remove Release 10.1.4 Patch Set 1 (10.1.4.2.0) before applying subsequent patch sets.

- When you upgrade earlier component instances using the zero downtime upgrade method, you must use tools available with Oracle Access Manager Release 10.1.4 Patch Set 1 (10.1.4.2.0).

  To obtain these tools, you will install a fresh instance of each Oracle Access Manager 10*g* (10.1.4.0.1) and then apply Release 10.1.4 Patch Set 1 (10.1.4.2.0) before you start the zero downtime upgrade. With the zero downtime upgrade method, upgraded component instances are considered to be release Release 10.1.4 Patch Set 1 (10.1.4.2.0). As a result, you cannot remove Release 10.1.4 Patch Set 1 (10.1.4.2.0) before you apply any subsequent patch sets.

5 Patch Set Preparation, Application, and Removal

The following sections describe preparing, applying, and removing the patch set:

5.1 Preparing Patch Set Components

This section introduces patch set bundles and their content, and explains how to store them in temporary directories so that they are organized and separate from the files within your original installation.

Oracle Access Manager patch set releases are distributed in individual platform-specific bundles (ZIP files) with file names similar to the following: p5957301 _101420_*platform*.zip. Earlier bundles for Unix platforms were delivered as tar files. Today, all top-level platform-specific bundles are delivered as ZIP files.

Table 1 lists all patch set bundles for this release.

Table 1 Oracle Access Manager Platform Bundles

Component Name	Release
p5957301_101420_MSwin2000.zip	10.1.4.2.0
p5957301_101420_Solaris-32.zip	10.1.4.2.0
p5957301_101420_Linux-32.zip	10.1.4.2.0

When your Oracle Access Manager installation includes multiple platforms, be sure to download all appropriate platform-specific bundles. Each platform-specific bundle contains one or more component-specific files.

The following procedure explains how to unzip and store Release 10.1.4.2.0 files before you begin installing the patch set.

> **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.

To prepare and store patch set bundles and components

1. Download the platform-specific ZIP bundle you need from Oracle Metalink, as follows:
   - Go to Oracle MetaLink at the site below and log in as usual:

     `http://metalink.oracle.com`

   - Click **Patches & Updates** in the list on the Oracle MetaLink page.
   - Click **Quick Links to the Latest Patchsets, Mini Packs, and Maintenance Packs**.
   - Under **Latest Oracle Server/Tools Patchsets**, click **Oracle Access Manager** from the **Patchsets for Product Bundles** area.

- Click the patch number for this Oracle Access Manager release (**5957301**).
- Select the release and platform, then click the **Download** button.

2. In the directory where you stored the downloaded zip files, unzip and extract all files to a new temporary platform-specific directory. For example:
   - v10.1.4.2.0_tmp_linux
   - v10.1.4.2.0_tmp_sparc
   - v10.1.4.2.0_tmp_win32x
3. In the platform-specific directory, locate a component-specific patch set file and complete the steps below as needed for your platform.
   - **Windows, Solaris, Linux**: Unzip and extract the contents of each component-specific patch set file to an individual component-specific subdirectory. For example:

     v10.1.4.2.0_tmp_sparc/access_server
4. Repeat the steps above for each platform-specific bundle and component that you need to patch your installation.

5.2 Applying the Oracle Access Manager 10.1.4.2.0 Patch

This section describes how to patch the Oracle Access Manager components. While individual methods and commands may differ depending on your platform, the overall procedure is the same.

When applying a patch to a component, always use the same login credentials that you used when installing the component.

You can only patch one component instance at a time. For example, if you have multiple Identity Servers, repeat the following steps for each Identity Server that you want to upgrade.

> **Note:** Oracle recommends that you back up your existing Oracle Access Manager components before you apply Oracle Access Manager 10.1.4.2.0. If you choose to remove this patch set, you can restore your original environment.

To apply the patch set to 10*g* (10.1.4.0.1) on all platforms

1. Complete all activities in "Preparing Patch Set Components".
2. Stop the Oracle Access Manager component instance you are patching, for example, the Identity Server.
3. Back up your Oracle Access Manager component installation directory.
4. Move the backup directory to another location and record this so you can locate it later, if needed.
5. **IIS 5 Web Server**: Before applying the patch for any Oracle Access Manager Web component (WebPass, Policy Manager, and Webgate) running with a Microsoft IIS 5 Web server, you must stop the following IIS 5 services:
   - IIS 5 World Wide Web Publishing Service
   - IIS Admin Service

After applying the patch, restart the services.

6. Change to the temporary component-specific directory you created, and run the patchinst program for your platform, for example:

   Windows Systems: `patchinst.exe`

   All Unix Operating Systems: `./patchinst`

7. When prompted, type the name of the directory where you want to apply the new patch set.

   You must apply the new release in the same location as the component you are upgrading, for example: *installdir*\identity or *installdir*\access.

   The .exe program upgrades the component and creates a new directory that contains a backup of your earlier files. The command window displays a prompt when the patch set is complete.

8. Restart the component that you patched.

9. Repeat the steps above to patch any additional instance of the same component.

10. Repeat the steps above to patch any other Oracle Access Manager component instance.

5.3 Failure During Patch Set Application

If there is a failure during your application of the patch, your original installation is restored automatically.

You may check the window to see if you can discern the problem, then correct it and restart the patch set application. If you cannot correct the problem, send the patch installation logs to Oracle Technical Support for assistance.

5.4 Removing the Oracle Access Manager 10.1.4.2.0 Patch Set After Modifying the LDAP Bind Password

The following procedure describes how to remove this patch set and restore the system to your original installation if you modified the LDAP bind password after initially applying the patch. While individual methods and commands may differ depending on your platform, the overall procedure is the same.

Notes: This section describes removing a patch if you used the modify LDAP bind password tool after applying the 10.1.4.2 patch. The following procedure describes reverting to the base version of the configuration files after modifying the directory server password.

Review all information in this section before performing any steps.

The storage format of Oracle Access Manager metadata has changed. As a result, before you can remove the Release 10.1.4 Patch Set 1 (10.1.4.2.0) patch set, you must return component metadata to the 10*g* (10.1.4.0.1) format and update the LDAP bind password. This is a two-part task:

- Restore metadata in configuration files
- Restore metadata in the configuration directory server

To perform the task, you run the `modifyldapbindpassword` tool for each instance of the Access Server, Identity Server, and Policy Manager, in the following directory for the component:

component_install_dir/oblix/tools/modbinpasswd/

Where *component_install_dir* is the installation directory for the component for which you are updating the directory bind password, for example, *IdentityServer_install_dir*.

Steps to perform this task are outlined in the following procedure. For details about using `modifyldapbindpassword`, see the chapter on "Reconfiguring the System" in the *Oracle Access Manager Deployment Guide*.

To revert the oblix metadata to the 10.1.4 base release format you must run `modifyldapbindpassword` as if you are performing a password update. When reverting oblix metadata, however, you should give any dummy password when the tool asks for the new bind password.

You can run `modifyldapbindpassword` in interactive or non-interactive mode. The minimum parameters to run the tool in interactive mode are as follows:

modbinpasswd -i *installation_directory* -c *component* -t *file|all|ds*.

The `-c` flag is compulsory, along with the appropriate component value. The component value must be one of the following:

- `is` (Identity Server)
- `pm` (Policy Manager)
- `as` (Access Server)

> **Note:** The Identity Server provides options for target `-t` as `file`, directory server (`ds`), and so on. In the following procedure, always use `file` as the target for the Identity Server. The Policy Manager and Access Server have only `file` as the target option.

To remove a patch set from any system

1. Restoring Metadata in Configuration Files: Perform the following steps to return metadata in configuration files to the 10*g* (10.1.4.0.1) format and update the LDAP bind password for each component.

   See the chapter on "Reconfiguring the System" in the *Oracle Access Manager Deployment Guide* for details on the `modifyldapbindpassword` command.

   a. Non-interactive Mode: Generate the password file using `modifyldapbindpassword` with the option `-genpasswdfile`. Skip this step if you are running the tool in interactive mode. For example:

      ```
      modifyldapbindpassword.exe -genpasswdfile password
      ```

      The tool asks for passwords that are required during the bind password update process. *Password* is the name of a password file. An .xml extension is provided if you do not supply one, for example, *password*.xml.

   b. Use `modifyldapbindpassword` with the `-t file` option to update the LDAP bind password for configuration files.

      The following is an interactive mode example:

```
modifyldapbindpassword.exe -i IdentityServer_install_dir -c is -t
file
```

The following is a non-interactive mode example:

```
modifyldapbindpassword.exe -i IdentityServer_install_dir -c is -t
file -j password.xml [parameters]
```

Where:

File is the name of a password file. An .xml extension is provided automatically if you do not supply one.

Parameters represents additional parameters. See the chapter on "Reconfiguring the System" in the *Oracle Access Manager Deployment Guide* for details.

c. Repeat Step b for every Identity Server, Policy Manager, and Access Server instance in your environment.

d. Repeat Step b for each host name variation in your system.

For example, if you are running a host named "machine1" that resides in domain ".company.com," you can configure the host name in Oracle Access Manager as both "machine1.company.com" and "machine1." In this case, you need to run the tool twice, once for each configured host name.

Host name variations are described in detail in the *Oracle Access Manager Identity and Common Administration Guide*.

e. Repeat steps a through c using the `modifyldapbindpassword` tool to update the LDAP bind password in configuration files for all other directory servers, as follows:

```
modifyldapbindpassword.exe -genpasswdfile -t file
```

2. Restoring Metadata in the Configuration Directory Server:

a. Go to the Identity System Console and log in.

b. Click **System Configuration**, **Configure Directory Options**, then **Configure Profiles**.

c. Under the label **Configure LDAP Directory Server Profiles**, click a profile name to display the Modify Directory Server Profile page.

d. On the Modify Directory Server Profile page, click a name beside the **Database Instance** label to display the Modify Database Instance page.

e. On the Modify Database Instance page, change the **Root Password** for the instance and click **Save**.

f. Repeat the preceding steps for each directory profile.

3. Stop the component.

Also stop any application connecting to the component, if required.

If you have set up failover, you do not need to stop any application connecting to the component.

4. Back up the component installation directory.

5. Move the backup directory to another location and record this so you can locate it later, if needed.
6. Open a command window and locate the component binary parameter file, for example:

   Oracle_Access_Manager10_1_4_2_0_Patch_win32_Access_Server_binary_parameter

   This parameter file was installed with the patch set, for example, *component_install_dir*\identity\access\oblix\patch\101420*xx*.

   The following is an example of a full path to this file:

   C:\OracleAccessManager\access\oblix\patch\101420RC510\Oracle_Access_Manager10_1_4_2_0_Patch_win32_Access_Server_binary_parameter
7. Navigate to the directory that contains the binary file.
8. Enter the command for your platform as shown below, then press **Enter**:

   Windows Systems: `patchinst.exe -u`

   All Unix Operating Systems: `./patchinst -u`
9. Type the full path to the component's installation directory and press **Enter**. For example, a typical path could be:

   C:\OracleAccessManager\access

The patch set release is now uninstalled and the original installation is restored.

6 Restoring XSL Customizations After the Upgrade

When you apply Release 10.1.4 Patch Set 1 (10.1.4.2.0), some xsl files are modified to support a JavaScript-related fix and fixes related to the handling of large groups.

The modified xsl files reside in the following directory:

IdentityServer_install_dir\identity\oblix\lang\shared

The following xsl files are modified:

- gsc_view_profile_vertical.xsl
- gsc_view_profile_horizontal.xsl
- gsc_modify_profile_vertical.xsl
- gsc_modify_profile_horizontal.xsl
- deactivateuser.xsl

When you applied the patch, the original xsl files were automatically backed up to the following directory:

IdentityServer_install_dir\identity\backup-Oracle-101401RC2-binary_parameter \oblix\lang\shared

After applying the patch, you can recover any customizations to these files in one of two ways:

- Add your customizations to the patched version of these files.

- Or, modify the backup copy of your customized files to include the new information, and move the updated backup copy to the original installation location.

The following procedure describes modifying the backup copy of your customized files to include the latest fixes available with Release 10.1.4 Patch Set 1 (10.1.4.2.0).

To recover your earlier xsl files after applying the patch

1. Apply the Release 10.1.4 Patch Set 1 (10.1.4.2.0) as described in Section 5, "Patch Set Preparation, Application, and Removal".
2. Locate the backup copy of your files in the following directory:

   Identity_Server_install_dir\identity\backup-Oracle-101401RC2-binary_parameter\oblix\lang\shared
3. In your backup file gsc_view_profile_vertical.xsl, add the following information:

   Find the following lines:

   ```
   <xsl:template match="oblix:ObGroupProfile">
   <xsl:apply-templates select="oblix:ObTextMessage"/>
   ```

   Immediately after these lines, add the following information:

   ```
   <xsl:variable name="isLargeGroup"><xsl:value-of select="/oblix:Oblix/
   oblix:ObGroupProfile/oblix:ObForm/oblix:ObInput[@obname='isLargeGroup'
   ]/@obvalue"/></xsl:variable>
   <xsl:if test="$isLargeGroup='true'">
   <p>
       <font>
           <xsl:call-template name="addPageWarningAttr"/>
           <xsl:variable name="MLargeGroup">This is a large group and hence
          members for this group will not be displayed on the profile page.
           Please use "Manage Group Members" feature to search and manage
           members.
               </xsl:variable>
           <b><xsl:value-of select="$MLargeGroup"/></b>
           <br/>
       </font>
   </p>
   </xsl:if>
   ```

4. Save the file and restart the Identity Server
5. Repeat step 3 in each backup copy of your customized gsc_*.xsl files.
6. Modify your deactivateuser.xsl file as follows:

   Find the following lines:

   ```
   <xsl:template match="oblix:ObColumnInfo">
      <tr bgcolor="#006699">
          <td align="{$alignLeft}" valign="middle" class="tableheader-text"
          width="5%">
          ...
   <xsl:otherwise>
      <xsl:choose>
         <xsl:when test="/oblix:Oblix/oblix:ObDeactivateUser/oblix:ObForm
         [@obname='DeactivateSearchResults']/oblix:ObInput[@obname='sortBy']
   ```

```
      /@obvalue=@ObAttribute">
         <xsl:choose>
<xsl:when
test="/oblix:Oblix/oblix:ObDeactivateUser/oblix:ObForm[@obname='Deactivat
eSearchResults']/oblix:ObInput[@obname='sortOrder']/@obvalue='ascending'"
>
<a onmouseout="self.status=''" class="tableheader-text">
<xsl:attribute name="href">javascript:sortDeactivatedUsers('<xsl:value-of
select="@ObAttribute"/>','descending')</xsl:attribute>
```

Remove the next line:

```
<xsl:attribute name="onmouseover">self.status='<xsl:value-of
select="$MSortDec"/>'; return true</xsl:attribute>
```

Add the following two items in its place:

```
<xsl:attribute name="onMouseOver">self.status='<xsl:call-template
name="oblix:PrepForJS">

<xsl:with-param name="strToPrep" select="$MSortDec"/>
</xsl:call-template>'; return true</xsl:attribute>
```

7. Modify your deactivateuser.xsl file as follows:

Find the following lines:

```
<b>
   <xsl:value-of select="@obattrName"/>
</b>
...
<xsl:otherwise>
   <a onmouseout="self.status=''" class="tableheader-text">
      <xsl:attribute name="href">javascript:sortDeactivatedUsers('<xsl:
      value-of select="@ObAttribute"/>','ascending')</xsl:attribute>
```

Remove the following line:

```
<xsl:attribute name="onmouseover">self.status='<xsl:value-of
select="$MSortAsc"/>'; return true</xsl:attribute>
```

Add the following two items in its place:

```
<xsl:attribute name="onMouseOver">self.status='<xsl:call-template
name="oblix:PrepForJS">

<xsl:with-param name="strToPrep" select="$MSortAsc"/> </xsl:call-template
>'; return true</xsl:attribute
```

8. Modify your deactivateuser.xsl file as follows:

Find the following lines:

```
<b>
   <xsl:value-of select="@obattrName"/>
</b>
...
<xsl:otherwise>
   <a onmouseout="self.status=''" class="tableheader-text">
       <xsl:attribute name="href">javascript:sortDeactivatedUsers('<
       xsl:value-of select="@ObAttribute"/>','ascending')</xsl:attribute>
```

Remove the following line:

```
<xsl:attribute name="onmouseover">self.status='<xsl:value-of
select="$MSortAsc"/>'; return true</xsl:attribute>
```

Add the following two items in its place:

```
<xsl:attribute name="onMouseOver">self.status='<xsl:call-template
name="oblix:PrepForJS">

<xsl:with-param name="strToPrep" select="$MSortAsc"/> </xsl:call-template
>'; return true</xsl:attribute>
```

9. Save the file.
10. After performing steps 2-8 in the backup copy of your customized files, move these files to the installation directory where you applied the patch set and replace the patched versions.

7 Updates to Base Component and Third-Party Support

Oracle continuously upgrades Oracle Access Manager's support for applications, platforms and operating systems. The following sections describe how to find and download the latest supported components:

- Viewing Currently Supported Platforms and Applications
- Downloading and Patching the Latest Supported Platforms

7.1 Viewing Currently Supported Platforms and Applications

Look for the latest support information on MetaLink, as described in the following procedure.

> **Note:** Information on supported platforms has been removed from the manuals. Go to Metalink for the latest information.

To obtain the latest certification matrix from MetaLink

1. Go to Oracle MetaLink at:

   `http://metalink.oracle.com`

2. Log in to Oracle MetaLink as directed
3. Click the **Certify** tab.
4. Click **View Certifications by Product**.
5. Select the **Application Server** option and click **Submit**.
6. Choose **Oracle Identity Management** and click **Submit**.
7. Click **Oracle Identity Management Certification Information** (html) to display the Oracle Identity Management page.
8. Click the link for **Section 6, "Oracle Access Manager Certification"** to display the certification matrix.

7.2 Downloading and Patching the Latest Supported Platforms

If you find support for a component on a new platform that you want, as described in "Viewing Currently Supported Platforms and Applications" on page 23, you can download the new component. If the component is part of the base Oracle Access Manager component set, you can patch it to Release 10.1.4 Patch Set 1 (10.1.4.2.0).

> **Note:** Note that third-party integrations, for example, the BEA Weblogic Connector, are not part of the base component set. You do not patch these components.

To download and patch the latest supported platform

1. Review the supported platforms described in "Viewing Currently Supported Platforms and Applications".
2. If you require support for an application or platform not supported by the base distribution, go to the following URL:

   ```
   http://www.oracle.com/technology/software/products/ias/ht
   docs/101401.html
   ```

   This download page contains readmes to help you determine what CD contains the component that you want. Note that WebGates are often listed in the "third-party integration" CDs, although WebGates are base components that you can patch.
3. Download the component of interest.
4. Apply the Release 10.1.4 Patch Set 1 (10.1.4.2.0) patch, as described in this document.

8 Known Issues and Workarounds

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

- Platform Support Known Issues and Workarounds
- Identity Server Known Issues and Workarounds
- WebPass Known Issues and Workarounds
- Policy Manager Known Issues and Workarounds
- WebGate Known Issues and Workarounds
- Performance Issues and Workarounds
- Software Developer Kit (SDK), API, and Third-Party Known Issues and Workarounds
- Documentation Known Issues

8.1 Platform Support Known Issues and Workarounds

Table 2 describes any known issues and workarounds for platform support in this patch set release.

Table 2 Known Issues and Workarounds for Platform Support

Bug	Description
6413451	Oracle Access Manager Release 10.1.4 Patch Set 1 (10.1.4.2.0) does not include any language pack-related changes. There is no translation support for the SNMP agent InstallShield wizard.
6505991	Sun Directory Server Enterprise Edition v6.0 (DSEE 6.0) is certified for Oracle Access Manager Release 10.1.4 Patch Set 1 (10.1.4.2.0). However, Release 10.1.4 Patch Set 1 (10.1.4.2.0) must be applied to an existing installation and cannot be used for a fresh installation. Sun Directory Server Enterprise Edition v6.0 (DSEE 6.0) is not certified for 10.1.4.0.1 and does not appear in the Oracle Access Manager installers or user interface. For new Oracle Access Manager installations if you want to use Sun Directory Server Enterprise Edition v6.0 (DSEE 6.0), do the following: **1.** Install Oracle Access Manager 10.1.4.0.1 as described in the *Oracle Access Manager Installation Guide.* **2.** During Oracle Access Manager installation, choose the "Sun Directory Server 5.x" option. **3.** Do not automatically update the schema and data. **4.** 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.** Apply Release 10.1.4 Patch Set 1 (10.1.4.2.0) as described in Section 5, "Patch Set Preparation, Application, and Removal".

8.2 Identity Server Known Issues and Workarounds

Table 3 describes any known issues and workarounds for the Identity Server in this patch set release.

Table 3 Known Issues and Workarounds for the Identity Server

Bug	Description
6346413	This patch release updates all of the WSDL files. These files are bundled with the WebPass in the following directory: *WebPass_install_dir*/identity/oblix/WebServices The following files are updated: ■ WSDL/common_asynchResumeWorkflowProcess_interface.wsdl ■ WSDL/om_workflowSelfRegistrationSave_interface.wsdl ■ WSDL/om_delete_interface.wsdl ■ WSDL/um_workflowSelfRegistrationSave_interface.wsdl ■ XMLSchema/usc_workflowDeactivateUserSave.xsd ■ XMLSchema/component_workflowTicket.xsd ■ XMLSchema/gsc_view_members_with_searchbar.xsd ■ XMLSchema/usc_workflowReactivateUserSave.xsd ■ XMLSchema/gsc_profile.xsd ■ samples/WSDL/java_axis/testwsdl_search_deactivated_users.java If you have customized any of these files, note that they are overwritten when you apply the patch. You must re-apply the customizations. The patch tool backs up the original files to the following directory: *WebPass_install_dir*/identity/backup-Oracle-101401RC21-binary_ parameter/oblix/WebService

6342010	When implementing customized XSL on Solaris, the Identity Server can crash if you use a backward slash ("\") instead of a forward slash ("/") in the href attribute of an `xsl:include` or `xsl:import` element. On Windows and Linux systems, this problem returns an error page.
	For example, suppose that you use the following snippet in a customized XSL:
	`<xsl:include href="..\..\shared\MyBasic.xsl"/>`
	If the backward slash is used, the Identity Server can crash. If you use a forward slash instead of the backward slash, as follows, an error page appears and the server crash is avoided:
	`<xsl:include href="../../shared/MyBasic.xsl"/>`

6168189	The tab name in the Org Manager is always **Select Tab** instead of the name of the tab that the user selected. This has been fixed in the current release. However, applying this patch overwrites any customizations that you have made to navbar.xsl. If you have customized this file, additional modifications are required to preserve your modifications. See "Bug Fix Details for the Identity Server" on page 46 for details.

6143913	When configuring WSDL for an IdentityXML function, the `setApplication` function does not work properly.
	This is a known issue in this release.
	To direct WSDL to the appropriate application, you must change the line in the WSDL file where you specify the host and port for the application. The following example points to the URL for processing Group Manager functions:
	`<soap:address`
	`location="http://130.35.50.153:8080/identity/oblix/apps/groupservc`
	`enter/bin/groupservcenter.cgi"/>`

Table 3 (Cont.) Known Issues and Workarounds for the Identity Server

Bug	Description
6076283	In the Identity System Console, you can set an Identity Server Timeout Threshold. The Identity Server Timeout Threshold field specifies how long (in seconds) the WebPass attempts to contact a non-responsive Identity Server before it considers it unreachable and attempts to contact another. Oracle recommends a timeout value of -1, which indicates that there is no timeout. If you set this value to a low number, you run a risk of the socket connection closing before a reply from the Identity Server is received.
6063327	In an environment that uses Oracle Internet Directory, you cannot use special characters in the name of a Lost Password Management Policy. This issue applies if you do the following: 1. From the Identity System Console, click the **System Configuration** sub-tab, then click **Lost Password Policy**. 2. In the Lost Password Policy page, click **Add**. 3. In the **Lost Password Policy Name** field, enter a name. If you use Oracle Internet Directory, do not use special characters in the name.
6055167	When Identity Server operations occur at a high volume, the server can exhibit a memory leak. The workaround for this problem is to restart the Identity Server when it reaches approximately 1 GB of virtual memory.
5901108, 5524369	When using the Group Manager to manage large static groups, response time can be very slow for many operations. For example, searching the groups can take longer than expected. When working with large sets of users, dynamic groups are a good alternative for static groups. Note that this patch release also provides improved performance for the Manage Group Members search operation when working with very large static groups.
5888497	When configuring a large group using the Query Builder or the Selector, you can receive an error if the group contains more than 2,500 static members and the group panel contains the group member attribute. The following is an example of the actions leading to this error: 1. Log in as a Master Administrator. 2. From the Group Manager, search for a group with more than 2,500 static members. 3. View the group profile page. 4. Click the **Modify** button. 5. Click **Query Builder** and modify the dynamic filter for the group. There are two workarounds for this problem: ■ If a group has more than 2,500 static members, do not display group members on the profile page. To implement this workaround, do not add the group member attribute to the group panel. ■ If you must display group members, do not use the Query Builder or the Selector to modify the group. Instead, use WSDL requests to modify dynamic filters, group members, group owners, and so on.

Table 3 (Cont.) Known Issues and Workarounds for the Identity Server

Bug	Description
5569442	To implement automatic login after password change with a form-based authentication scheme, you must configure the change password redirect URL must include `STLogin=%applySTLogin%` as a parameter, as in the following example: `http://`*`machinename`*`:`*`portnumber`*`/identity/oblix/apps/lost_password_mgmt/bin/lost_password_mgmt.cgi?program=redirectforchangepwd&login=%login%%userid%&backURL=%HostTarget%%RESOURCE%&STLogin=%applySTLogin%&target=top` To implement this with a form-based authentication scheme, you must configure the challenge parameter `creds` by supplying the user name credential parameter as the first token, the password credential parameter as the second token, then any other credential parameters. See the information on password change redirect URLs in the *Oracle Access Manager Identity and Common Administration Guide* for details.

8.3 WebPass Known Issues and Workarounds

Table 4 describes any known issues for the WebPass in this patch set release.

Table 4 Known Issues and Workarounds for WebPass

Bug	Description
n.a.	If you deploy a WebPass on an IIS 6.0 Web server, the Web server may show an increase in memory (virtual bytes). If this happens, Oracle recommends that you configure multiple worker process in IIS. You should also enable the recycling of worker processes after consuming 1000 MB of virtual memory.
6204811, 6204769	Before applying this patch to any Oracle Access Manager Web component (WebPass, Policy Manager, and Webgate) running with a Microsoft IIS 5 Web server, you must shut down the component and stop the following IIS 5 services: ■ IIS 5 World Wide Web Publishing Service ■ IIS Admin Service After applying the patch, you can restart the component and the services.

8.4 Access Server Known Issues and Workarounds

Table 5 describes any known issues and workarounds for the Policy Manager in this patch set release.

Table 5 Known Issues and Workarounds for the Access Server

Bug	Description
5880426	As of Oracle Access Manager 10.1.4.0.1, the **Preferred HTTP Host** field became required. This introduced issues for environments that support virtual hosting. To work around these issues, you must configure new parameters along with the **Preferred HTTP Host** setting. See "Access System Enhancements" on page 7 for details.

8.5 Policy Manager Known Issues and Workarounds

Table 6 describes any known issues and workarounds for the Policy Manager in this patch set release.

Table 6 Known Issues and Workarounds for the Policy Manager

Bug	Description
5722931	IIS Policy Manager installation fails on non-English Windows platform. A workaround is required for this bug. For details, see the Troubleshooting chapter of the *Oracle Access Manager Installation Guide*.
6204811, 6204769	Before applying the patch for any Oracle Access Manager Web component (WebPass, Policy Manager, and Webgate) running with a Microsoft IIS 5 Web server, you must shut down the component and stop the following IIS 5 services: ■ IIS 5 World Wide Web Publishing Service ■ IIS Admin Service After applying the patch, restart the component and the services.

8.6 WebGate Known Issues and Workarounds

Table 7 describes known issues and workarounds for the WebGate in this patch set release.

Table 7 Known Issues and Workarounds for WebGates

Bug	Description
n.a.	If you deploy a WebGate on an IIS 6.0 Web server, the Web server may show an increase in memory (virtual bytes). If this happens, Oracle recommends that you configure multiple worker process in IIS. You should also enable the recycling of worker processes after consuming 1000 MB of virtual memory.
6629755	After you apply this patch to a WebGate that runs on a Windows Apache 1 Web server and restart the server, the first request to this Web server can produce a pop-up message regarding a memory reference error. You can safely click **OK** and and ignore this error message.
6524438	A Web server issues a 302 response when a user attempts to access a resource that is protectedusing based-authentication. This problem arises when a challenge redirect is used or if a reverse proxy server is used to hide a WebGate host. To work around this issue, you can upgrade the Apache or Oracle HTTP Server from version 1.3.x to a higher version, for example, 2.x.x. Alternatively you can configure your browser to use the HTTP 1.0 protocol. This solution requires placing an HTTP server as a forward proxy in front of Oracle Identity Federation WebGates. However, this solution can cause problems in some browsers, for example, Firefox because content can be removed when it is sent to the browser.

Table 7 (Cont.) Known Issues and Workarounds for WebGates

Bug	Description
6360356	An issue can occur with password reset after basic authentication, form-based authentication, or a challenge redirect on a standalone Web server. If a challenge and response has not yet been configured for a user and the user's password is reset, the user may be challenged twice to present credentials. For example, instead of the following typical procedure, the user is prompted for a second authentication after step 5: **1.** The user attempts to access a protected resource. **2.** The authentication WebGate presents a login form. **3.** The user is redirected to a Change Password page, enters credentials, and clicks **Save**. **4.** The user clicks **Back**, as prompted. **5.** The user supplies new authentication credentials. **6.** The user is redirected to a Challenge and Response configuration page, provides input, and clicks **Save**. **7.** The user is served the requested resource. Instead of moving from step 5 to step 6, a second WebGate authentication dialog appears. To avoid this problem, be sure that the Host Name variation in `ObWebPassPrefixURL` in the authentication scheme and the configured Preferred HTTP Host are the same. For example, do not enter *host*:*port* as the Preferred HTTP host and *host*:*domain*:*port* in ObWebPassPrefixURL, as this produces the duplicate authentication. Note that you should always use the fully qualified domain name for multi-domain environments.
6359813	As noted in the chapter on authentication in the *Oracle Access Manager Access Administration Guide*, you can configure an authentication scheme that allows the user to log in for a period of time rather than a single session by adding the challenge parameter `ssoCookie:max-age` in the authentication scheme. The released version of this document mentions that this feature works only with the Mozilla. However, this feature works with Internet Explorer as well as Mozilla-based browsers.

Table 7 (Cont.) Known Issues and Workarounds for WebGates

Bug	Description
6316619	After a user resets a password, if the new password is the same as the old password, the WebGate does not prompt the user for new credentials when using the Basic Over LDAP authentication scheme if no value has been supplied in the optional Password History field of the password policy definition. If the user specifies the old password as the value of the new password, step 5 below is omitted, and the user is given access to a requested resource without re-authentication: 1. The user accesses a protected resource. This user's password has expired and a challenge and response has been configured for this user. The authenticating WebGate provides a login dialog. 2. The user logs in and clicks **OK**. The user is redirected to a Change Password page. 3. The user enters password reset information. A password reset confirmation appears. 4. The user clicks **Back** to return to the requested resource. 5. The user re-authenticates in the WebGate login dialog box. 6. The user accesses the requested resource.
6204811, 6204769	Before applying this patch to any Oracle Access Manager Web component (WebPass, Policy Manager, and Webgate) running with a Microsoft IIS 5 Web server, you must stop the following IIS 5 services: ■ IIS 5 World Wide Web Publishing Service ■ IIS Admin Service After applying the patch, restart the services.

6195755	After migrating a WebGate, you may see errors similar to the following in the oblog.log file:
	`2007/07/05@21:06:55.971096      14453   16384   INIT    ERROR`
	`0x000003B6`
	`../oblistrwutil.cpp:180 "Could not read file"`
	`filename^/export/home/zdtm_704/wg_ap2_`
	`6767/access/oblix/apps/common/bin/globalparams.xml`
	`2007/07/05@21:06:55.981324      14453   16384   INIT    ERROR`
	`0x000003B6`
	`../oblistrwutil.cpp:180 "Could not read file"`
	`filename^/export/home/zdtm_704/wg_ap2_`
	`6767/access/oblix/config/oblog_config.xml`
	`2007/07/05@21:06:56.013475      14453   16384   INIT    ERROR`
	`0x000003B6`
	`../oblistrwutil.cpp:180 "Could not read file"`
	`filename^/export/home/zdtm_704/wg_ap2_`
	`6767/access/oblix/lang/en-us/netlibmsg.xml`
	These errors are generated because the xml files are not present in the named locations. However, the WebGates do not use these files, so these messages can be ignored.

Table 7 (Cont.) Known Issues and Workarounds for WebGates

Bug	Description
6124736	Rather than rely on the default TCP/IP timeout, you can specify the **Access Server Timeout Threshold** in the **Access System Console**, **Access System Configuration**, **AccessGate Configuration**. The default value of -1 means the default network TCP/IP timeout is used. A typical value for this parameter is between 30 and 60 seconds. However, if this parameter is set to a very low value, the socket connection can be closed before a reply from the Access Server is received, resulting in an error. This is a known configuration issue. However, in this patch release the WebGate will not crash.
5463350	Access clients that are configured for the X.509 certificate authentication challenge method may fail authentication after you upgrade to version 7.0.4.3 or higher. In the newer releases, stricter criteria is imposed for how a certificate is formed. This challenge method requires making all certificate attributes, for example, Distinguished Name, CN, Serial Number, and so on, available to subsequent plug-ins for credential mapping.

8.7 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. You do this 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.

The rest of this section discusses enabling automatic cache flush and secure communications while preserving system performance.

The rest of this section discusses the following topics:

- About Preventing Bottlenecks with Cache Flush Requests
- Caveats When Using Mixed Security Mode
- Configuring Mixed Transport Security Mode

8.7.1 About Preventing Bottlenecks with Cache Flush Requests

When you install and configure an Identity Server, you also automatically deploy the Access Manager SDK. This SDK is responsible for sending cache flush requests to the Access Server after IdentityXML modifies a profile.

To enhance performance, you can designate a single Access Server to handle all cache flush requests and propagate the requests to all other Access Servers in your environment. This simplifies the routing of requests among components.

You can also ensure that Open mode communication is used when the dedicated Access Server sends cache flush requests. Cache flush requests do not contain sensitive data. During cache flush operations, only the LDAP configuration is read. This enables Open mode to be appropriate for these types of requests.

Additionally, you can retain Simple or Cert mode for requests other than cache flush requests. Despite changing the security mode to Open for cache flush reqeusts, as long as you initially configure the Access Servers in Simple or Cert mode, the Access Manager SDK or WebGate will still communicate with the Access Servers in Simple or Cert mode. This enables you to preserve security for most operations.

The ability to configure an Access Server to use Open mode for some operations and a secure mode for other operations is known as a *mixed security mode*.

The following task overview describes how to configure your environment to handle cache flush requests using Open mode while retaining secure communication for other types of requests.

Task overview: To maximize performance for cache flush requests while maintaining security

1. Install all new Access Servers and configure all existing ones to use Simple or Cert mode.
2. Designate an Access Server or a cluster of Access Servers to handle all cache flush requests.
3. Configure WebGates and AccessGates to communicate with their respective Access Servers using Simple or Cert mode.
4. Convert all of the Access Servers to mixed transportation security mode.

   See "To configure Access Servers to use mixed security mode" on page 34 for details.

8.7.2 Caveats When Using Mixed Security Mode

If you configure mixed security mode, when you view a list of associated Access Servers for a particular WebGate, you may receive the following message:

"Not Responding Transport security mismatch".

You can safely ignore this message.

After configuring mixed security mode, you must follow a specific process when making any future modifications to your configuration. See "To modify an AccessGate or WebGate when using mixed transport security mode" on page 34 for details.

Warning: After configuring mixed security mode, you can encounter a bug if you modify an AccessGate or WebGate. Specifically, when you modify one of these components, all previous **Preferred HTTP Host** settings are removed.

There is a workaround for this bug. See "To modify an AccessGate or WebGate when using mixed transport security mode" on page 34 for details.

8.7.3 Configuring Mixed Transport Security Mode

The following procedures describe how to configure Access Servers so that they use Open transport security for cache flush requests, and SSL or Cert transport security for all other requests. This is useful when you have implemented automatic cache flush in an environment that primarily uses secure communication. See the chapter on caching in the *Oracle Access Manager Deployment Guide* for details.

To configure Access Servers to use mixed security mode

1. Install or configure each Access Server to communicate in Simple or Cert mode.

   Ensure that all of these servers use a secure mode.

2. Run the `configurewebgate` or `configureaccessgate` tool to configure all WebGates or AccessGates to communicate with the Access Servers in Simple or Cert mode.

   Ensure that all WebGates and AccessGates are configured to use a secure mode.

3. In the Access System Console, change the mode of every Access Server to Open from Simple or Cert.

4. Restart the Access Servers.

   After the restart, the Access Servers retain the certificates required for secure communications, and they continue to send and receive most information using SSL or Cert mode. However, these servers use Open mode for cache flush requests.

To modify an AccessGate or WebGate when using mixed transport security mode

1. Before modifying the AccessGate or WebGate, in the Access System Console, restore Simple or Cert mode to all Access Servers.

2. Modify the AccessGate or WebGate.

3. In the Access System Console, restore Open mode communication for the Access Servers.

4. Restart the Access Servers.

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

Table 8 describes any known issues and workarounds for SDKs and third-party integrations in this patch set release.

Table 8 Known Issues and Workarounds for SDKs, Third-Party Integrations

Bug	Description
n.a.	In the *Oracle Access Manager Integration Guide*, Oracle Access Manager support is shown for smart card authentication with Active Directory and IIS Web servers using ActivCard Cryptographic Service Provider (CSP) for Windows 2000. Note, however, that the process of integrating Oracle Access Manager with smart cards is the same for all supported types of smart cards, directory servers, and operating systems.

6340556	The authn_api.h header indicates that you should use credentials as the first parameter in the `SetActionFn()` function, as follows:
	`ObAnASStatus_t SetActionFn(`
	`ObAnPluginSVData_t Creds,`
	`const char* pName,`
	`const char* pValue`
	`ObAnActionType pActionType);`
	However, if you do this, the Access Server can crash. The correct first parameter is `ActionInfo`, as is correctly shown for the `GetActionFn()` function, as follows:
	`const char *AnGetAction(`
	`ObAnPluginSVData_t pActionInfo,`
	`const char* pName,`
	`ObAnActionType_t pActionType);`

6053497	When integrating Oracle Access Manager with RSA SecurId, if you provide an at-sign ("@") in the login attribute value, you must also remove the `-w` switch from the first line of the securid.pl script. This is a known issue with SecurID.
5984895	Users can receive errors when using the Weblogic Application Server Version 9.2 with the Oracle Access Manager 10.1.4 SSPI Connector. Specifically, users can receive a "not authorized" error when accessing pages that they should be able to according to the policies configured in Oracle Access Manager. When you deploy an application on Weblogic 9.2, be sure that you deploy it with the appropriate deployment descriptors for Web applications. The deployment descriptors for Web applications are web.xml and weblogic.xml. Also be sure to deploy the application with deployment descriptors for EJB applications. The files ejb-jar.xml and weblogic-ejb-jar.xml are the deployment descriptors for EJB applications.
5956583	For Weblogic and WebSphere connectors running in Simple mode, when you migrate from 7.0.4 to 10.1.4.x, the password.xml file is not migrated. For example, if you do the following, you are prompted for the NetPoint Transport Password in addition to a user name and password when starting the Weblogic server. **1.** Install the 7.0.4 Weblogic SSPI Connector in simple mode. **2.** Start migration from 7.0.4 to 10.1.4.0.1 and also migrate the Access Server SDK. **3.** After receiving the message that migration completed successfully, copy the file NetPointProvidersConfig.properties and mbean jar from the migrated 10.1.4 area to the Weblogic Portal Domain. **4.** Restart WebLogic. The workaround is to add the following to the asdk_base_files.lst file in the destination installation area (10.1.4.0.1) before running the migration tool: `file:/oblix/config/password.lst`

Table 8 (Cont.) Known Issues and Workarounds for SDKs, Third-Party Integrations

Bug	Description
5716192	After configuring an integration with WebLogic 9.2, if you attempt to add a group in WebLogic that already exists in the Oracle Access Manager Identity System, no error is displayed in WebLogic. This is a known issue to be addressed by BEA. Contact BEA support and reference Case #693143 for details.
n.a.	If you use the BEA Weblogic SSPI and you plan to use BEA Realm behavior, perform the following steps before updating the BEA Weblogic SSPI package from 10.1.4.1 to 10.1.4.2.0: **1.** Configure a New Default Authorization Provider in the following location: Go to **NetPointRealm**, then to **Providers**, then to **Authorization**. **2.** Configure a New Default Adjudication Provider in the following location: Go to **NetPointRealm**, then to **Providers**, then to **Adjudication**. **3.** Restart the Weblogic server.

8.9 Documentation Known Issues

Table 9 describes any known issues in the documentation for this patch set release.

Table 9 Known Issues and Workarounds for Documentation

Bug	Description
n.a.	There is a typo in the *Oracle Access Manager Deployment Guide*, in the chapter on performance. In the section, "Differences Between Configured and Actual Connection Pool Size", the following sentence appears: "In this scenario, if you set the maximum number of connections to 27, the number of connections to the directory will range from 19 to 27." The maximum number of connections is stated incorrectly and introduces a clarity issue in this section. The correct statement is as follows: "In this scenario, if you set the maximum number of connections to 2, the number of connections to the directory will range from 19 to 27."
n.a.	In the *Oracle Access Manager Developer Guide*, the chapter on the Authorization Plug-in API, a number of code listings incorrectly include "plug-in" instead of "Plugin". The following are a few examples: ■ `ObAzplug-insetData_t` should be `ObAzPluginSetData_t` ■ `ObAzplug-instatus_t` should be `ObAzPluginStatus_t` ■ `ObAzplug-instatusContinue` should be `ObAzPluginStatusContinue` This is a known issue and will be fixed in the next release of the documentation.
n.a.	When viewing an HTML version of the *Oracle Access Manager Integration Guide*, the chapter on integrating with Peoplesoft contains some garbled characters in the sample code. This problem will be fixed in the next release of the documentation. In the meantime, the PDF version of this document displays the sample code correctly.

Table 9 (Cont.) Known Issues and Workarounds for Documentation

Bug	Description
n.a.	In the chapter on integrating with SAP in the *Oracle Access Manager Integration Guide*, step 3 of the section, "Setting Up Oracle Access Manager for Integration with SAP" provides the following information: The following example maps uid to the SAPUID: `HeaderVar HTTP_SAPUIDuid` Note that there should be a space between `SAPUID` and `uid`. This problem will be fixed in the next release of the documentation.
n.a.	In the chapter on integrating with PeopleSoft in the *Oracle Access Manager Integration Guide*, in step 7 of the procedure titled, "To set up Oracle Access Manager for the PeopleSoft integration", the screen shot shows the PS_SSO_UID with a Return Value of uid. However, uid is an attribute. Instead of Return Value, this screen shot should show the label Return Attribute.
n.a.	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 will return the cached credential following a timeout. A new challenge parameter `"realmunique:yes"` corrects the problem. See Also: Oracle Metalink Note: 443493.1
n.a.	The description of the Environment URL in the chapter on migrating configuration data changes in the *Oracle Access Manager Configuration Manager Installation and Administration Guide* is incorrect. The book describes the Environment URL field on the Add Environment and View Environment pages as a place where you enter the URL to the LDAP directory. However, the Environment URL field on the Add Environment and View Environment pages is an optional field for the relevant Oracle Access Manager deployment for this environment. A future release of the *Oracle Access Manager Configuration Manager Installation and Administration Guide* will note the change in text and procedures. For example: **Environment URL**: The URL to the relevant Oracle Access Manager deployment for this environment. For example: *`http://141.144.74.35:3333/access/oblix/`*

Table 9 (Cont.) Known Issues and Workarounds for Documentation

Bug	Description
6660499	The *Oracle Access Manager Installation Guide* does not mention that before running Oracle Access Manager command-line tools on Linux platforms, you must set the LD_ASSUME_KERNEL environment variable to a value of 2.4.19. A future release of the *Oracle Access Manager Installation Guide* "Troubleshooting" chapter will rename and expand the topic "Identity System Components May Crash" to include the following additional information: **Oracle Access Manager Components and Tools Might Crash** **Symptom**: Oracle Access Manager command-line tools on Linux platforms crash. **Solution**: To run Oracle Access Manager command-line tools on Linux platforms, the `LD_ASSUME_KERNEL` environment variable must be set to a value of `=2.4.19` at runtime because the older Linux threading model is supported (not the native posix thread library (NPTL)). If you are running a bash shell, the exact specification is as follows: `# export LD_ASSUME_KERNEL=2.4.19` The exact command might differ if you are using a different shell.
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* will note this change.
6454109	There are appendices that provide background on XML in the *Oracle Access Manager Customization Guide* and *Oracle Access Manager Developer Guide*. In both these appendices, there is information on client-side transformation of xml style sheets. Note that in these sections, the URL for the registration tool for msxml has changed. This can be obtained from Microsoft at the following URL: `http://www.microsoft.com/downloads/details.aspx?familyid=1e6185d7-e4e4-43b1-8056-0e5ecd15a88a&displaylang=en`
6443025	The following information is missing from the 10.1.4.2 *Oracle Access Manager Access Administration Guide.* It will be added to the next version: In a form-based authentication scheme, you can now specify a `maxpostdatabytes` challenge parameter. The value of this optional parameter is the maximum number of data bytes that an end user can post for authentication to a Web server that uses a WebGate. If the POST data exceeds the threshold set by maxpostdatabytes in the form-based authentication scheme, user receives an error and a log entry is added at the DEBUG3 log level in the oblog.log file. Example: `maxpostdatabytes:100` If you omit this parameter, the end user can post unlimited length strings for authentication to a Web server that is protected by a WebGate. Very long strings can cause the WebGate or Web server to crash, denial of service, or another fatal error, because WebGates run in the context of the Web server's process.

Table 9 (Cont.) Known Issues and Workarounds for Documentation

Bug	Description
6438480	In the *Oracle Access Manager Access Administration Guide*, Chapter 3, "Configuring WebGates and Access Servers," there is a typo in the name of the user-defined parameter name. The name "InactiveReconfigPeriods" should be "InactiveReconfigPeriod." This problem will be fixed in the next release of the documentation.
6330281	Appendix B, "Configuring for ADSI" in the *Oracle Access Manager Identity and Common Administration Guide* describes requirements and procedures when you are running Oracle Access Manager with Active Directory forests and the Active Directory Services Interface (ADSI). However, special considerations are required for IIS when ADSI is configured. See "Configuring Oracle Access Manager with ADSI on IIS", immediately below this table. This information will be added to the documentation in a future release.
6359813	As noted in the chapter on authentication in the *Oracle Access Manager Access Administration Guide*, you can configure an authentication scheme that allows the user to log in for a period of time rather than a single session by adding the challenge parameter `ssoCookie:max-age` in the authentication scheme. The released version of this document mentions that this feature works only with the Mozilla. However, this feature works with Internet Explorer as well as Mozilla-based browsers.
6165044	The *Oracle Access Manager Upgrade Guide*, zero downtime upgrade section, chapter on upgrading the schema, data, and clone system, discusses extra directory profiles in a split directory configuration. In this case, extra profiles containing the old configuration DN might be created when reconfiguring the COREid Server to use the new branch in the directory. Step 8 of the procedure to set up the cloned COREid System with the new branch presents sub steps to remove extra directory profiles. However, sub step c includes an incorrect statement. **Incorrect**: 8. **Extra Directory Profiles in a Split Directory Server Configuration**: ... c. On the Configure Directory Server profiles page, check the box beside the name of any new directory profile that was created during this reconfiguration. **Corrected**: Sub step c has been corrected. A future version of *Oracle Access Manager Upgrade Guide* will contain the following correction: 8. **Extra Directory Profiles in a Split Directory Server Configuration**: ... c. On the Configure Directory Server profiles page, check the box beside the name of any old directory profile that is present with the old configuration DN.
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*

8.9.1 Configuring Oracle Access Manager with ADSI on IIS

If you have configured Oracle Access Manager with ADSI in an environment that uses an IIS 5.0 Web server, the following settings are required.

To configure IIS 5.0 for use with Oracle Access Manager and ADSI

1. Change the account used for anonymous access by the Web Server, as follows:

   a. In the IIS console, right-click the node for the computer that you want to configure, then click **Properties**, then click **Edit WWW Service Master Properties**.

   b. Click the **Directory Security** tab, then click **Anonymous Access**, then click **Authentication Control**, then click **Edit**.

   c. Enter the domain administrator account user name and password.

   This is the administrator of the domain that was created when Active Directory was installed. When installing Oracle Access Manager, you must log in to this computer as this administrative user. For example, you could log in as *AccessManager*\Administrator where *AccessManager* is the new domain.

2. In the same window, deselect all listed authenticated access methods.

   By default, Windows Integrated Authentication is selected. This causes issues when accessing a protected resource by calling integrated authentication.

3. In the IIS console, right-click the node for the computer that you are configuring, then click **Properties**, then click **Edit WWW Service Master Properties**.

4. Select the **Home Directory** tab, and in the drop-down list for **Execute** permissions select **Scripts and Executables**.

5. In the **Home Directory** tab, also select the **Read** checkbox to provide read access to the scripts.

9 Bugs Fixed in This Release

The following sections discuss the bugs fixed in this release

- General Resolved Issues
- Identity Server Resolved Issues
- WebPass Resolved Issues
- Access Server Resolved Issues
- Policy Manager Resolved Issues
- WebGate Resolved Issues
- Software Developer Kit (SDK), API, and Integrations Resolved Issues
- Performance Resolved Issues
- Documentation Resolved Issues

9.1 General Resolved Issues

Table 10 shows bugs that are common to all components that were fixed in this release.

Table 10 Resolved General Issues

Bug	Description
6320295	The Access Server, Identity Server, WebPass, WebGate, Access Manager, and ASDK .log and .lck file permissions are always set to -rw-rw-rw. This problem has been fixed in the current release. You can modify permissions for these files.

9.2 Identity Server Resolved Issues

Table 11 shows Identity Server bugs that were fixed in this release.

Table 11 Resolved Issues for the Identity Server

Bug	Description
6523234	The Master Identity Administrator may not be able to view all of the pages and content that he or she has permission to view. This issue can arise due to flushing the local Identity Server policy cache. This problem has been fixed in the current release. Flushing of the local cache is now similar to flushing the remote cache.
6508852	After applying a hot fix, delegated administrators cannot search for newly-added users. This problem has been fixed in the current release.
6486834	The Identity Servers can become unresponsive if one of the servers experiences a heavy CPU load. Rediscovery Information: OIS server becomes unresponsive while doing some admin operations. This problem has been fixed in the current release.
6312487	An Identity Server-to-Identity Server asynchronous cache flush can cause one of the servers to become unresponsive. This problem has been fixed in the current release. Identity Server-to-Identity Server asynchronous cache flushes work correctly.
6245556	Some users are unable to log in after upgrading. This problem occurs when lost password management is enabled, and the first object class listed on the Employee tab is not the structural object class for the tab. If the user entry does not contain the object class, authentication can fail. This problem has been fixed in this release. Users can authenticate even if their entries do not contain all of the auxiliary object classes configured on the Employee (or equivalent) tab.
6220734	When using IdentityXML and WSDL to create an asynchronous workflow, ADD operations are evaluated as REPLACE_ALL operations. This problem has been fixed in the current release. In an asynchronous workflow request, ADD operations add data but do not overwrite existing data.
6168189	The tab name in the Org Manager is always **Select Tab** instead of the name of the tab that the user selected. This has been fixed in the current release. However, applying this patch overwrites any customizations that you have made to navbar.xsl. If you have customized this file, additional modifications are required to preserve the customizations. See "Bug Fix Details for the Identity Server" on page 46 for details.

Table 11 (Cont.) Resolved Issues for the Identity Server

Bug	Description
6138106	Administrators cannot log into the Access System because the shared secret entry in the directory has changed. The user is continuously redirected to the login form. As a workaround, you could restore the shared secret value from directory server back-ups. However, this problem has been resolved in the code in this release. Also in this release, there is instrumentation regarding handling the shared secret in the Identity Server. Comprehensive logging for reads and writes of the shared secret value have been added to a new log module named SHARED_SECRET. See the information on per-module logging in "Enhancements in This Patch Set" on page 2 for details.
6132814	Several issues can occur when configuring a Create Group or Create User workflow using multiple target domains, as follows: ■ If you provide the Selector in the initiate step of a workflow with multiple target domains, when the user invokes the Selector, the target domain is reset to the default domain. The default domain is the first target domain. The user can only select the default domain if the Selector is provided in the initiate step. ■ If you defined multiple workflows that use the Selector in the initiate step, when a user invokes the selector in anything other than the default workflow, the type of workflow is reset to the default workflow. ■ When using a workflow with multiple target domains, if a user switches between the target domains, any previously entered values are lost. Issues with selecting multiple target domains have been fixed in the current release. The introduction of multiple challenge and response phrases in 10.1.4.0.1 was partially responsible for these issues.
6129796	After enabling auditing to a file on the Identity Server and auditing some events, if you set the **Audit to File** flag to **OFF**, audit events continue to be generated. You enable or disable auditing to a file as follows: **1.** In the Identity System Console, click **System Configuration**, then select **Identity Servers**. **2.** Select an Identity Server link. **3.** Modify the **Audit to File Flag** setting. This problem has been fixed in the current release. To turn off auditing to a file, change the **Audit to File Flag** value to **OFF** from **ON** and restart the Identity Server.
6067984	To optimize operations on groups in the Identity System, you should configure the value of the `UidInfoCache` parameter in globalparams.xml to accommodate approximately double the total number of user entries in the directory server instance, by the customer. The default value for this parameter is 50 (kbyte). Information on this topic has been added to the *Oracle Access Manager Deployment Guide* chapter on performance tuning and the *Oracle Access Manager Customization Guide* appendix on parameter files.
6066000	If you search for group members using attribute-based constraints (for example, "Full Name" "=" "user123"), all attributes for the entry are returned from the directory server. This problem has been fixed in the current release. Searches for group members only return attributes that you specified in the query. For example, in a query that requests the cn, only the cn is returned from the directory server.

Table 11 (Cont.) Resolved Issues for the Identity Server

Bug	Description
6063350	If Oracle Internet Directory goes down, the Access Server crashes. This problem has been fixed in the current release.
6040673	When checking for a nested group member, the member was not found if the group that the member belonged to was itself a nested member of another group. This problem has been fixed in the current release.
5949904	If you configure a create group workflow that uses multiple target domains, changing the targets from the drop-down menu produces an "insufficient access rights" error. For example, if you do the following, you get this error: **1.** Click **Create Group**. **2.** Select the **Create group - Basic workflow** template. **3.** Select a group from the **Domain** pull-down menu. This problem has been fixed in the current release. You can configure groups with multi-domain targets in a workflow.
5903430, 5903425, 5734669	Very long literal strings in XSL files can cause an Identity Server exception. This problem is caused by the handling of XSL code in XML transformations. This problem has been fixed in the current release. The parsing of long literal strings in XML files no longer affects XSL stylesheet processing.

5893175	On Windows, if the Identity Server causes high memory utilization, the system can crash.
	Fixed in the current release. The Identity Server can now use 3 GB of virtual memory, if 2 GB addressing is already enabled in the boot.ini file. The /3GB switch allocates 3 GB of virtual address space to an Identity Server that uses IMAGE_FILE_LARGE_ADDRESS_AWARE in the process header. This switch allows applications to address 1 GB of additional virtual address space above 2 GB.
	The virtual address space of Identity Server is limited to 2 GB, unless the /3GB switch is used in the Boot.ini file. The following example shows how to add the /3GB parameter in the Boot.ini file to enable Identity Server memory tuning:
	`[boot loader]`
	`timeout=30`
	`default=multi(0)disk(0)rdisk(0)partition(2)\WINNT`
	`[operating systems]`
	`multi(0)disk(0)rdisk(0)partition(2)\WINNT="????" /3GB`
	See the following URL for more information:
	`http://www.microsoft.com/whdc/system/platform/server/PAE/PAEmem.mspx`

5891100	A stylesheet that contains very long literal strings can cause the Identity server to crash during XSL parsing. This problem has been fixed in the current release. String length no longer affects the XSL parser.

Table 11 (Cont.) Resolved Issues for the Identity Server

Bug	Description
5888938	When an Identity System user belongs to one or more large groups, user profile operations can take a long time to complete. For example, if the logged-in user attempts to view their profile in the User Manager, it can take a long time to display the profile. During this time, the memory utilization of the Identity Server spikes. This problem has been fixed in the current release.
5869336, 5720055, 5483337	The Identity Server cannot terminate CLOSE_WAIT connections. This problem has been fixed in the current release.
5863956	If you add a user who is already a member of a group, this action is not logged. This problem has been fixed in the current release. Attempts to add users who already belong to a group are logged at the Error level.
5862209	In the Identity System, the functionality for setting attribute access controls is not evaluated if you have not also configured a role. For example, if you define an attribute access control with an LDAP filter, but no role, the policy is not evaluated. This problem has been fixed in the current release. Identity System access controls do not require role information.
5857854	After processing for an extended amount of time, the Identity Server runs out of memory. This problem occurs when groups are repeatedly loaded into memory during evaluation of access control policies. This problem has been fixed in the current release. The whole group is no longer loaded during a search or when displaying the My Groups page. See "Identity System Enhancements" on page 5 for details.
5842946	When you create large static groups in the Identity System, for example, groups with over 10,000 members, adding and removing members from the group takes a long time. This problem has been fixed in the current release. Group performance overall has been enhanced. See "Identity System Enhancements" on page 5 for details.
5842145	If you enable simultaneous database and file auditing, the file auditing does not work. This problem has been fixed in the current release. You can enable database and file auditing to run concurrently.
5764838	Asynchronous caching does not work between Identity Servers. Identity Servers communicate with one another primarily for cache flush requests. When a cache is updated on one server, that server tells the other servers to update their caches. The timeout for asynchronous cache flush requests is configured in the `oisClientTimeoutThreshold` parameter in the following file: *identity_server_installdir*/oblix/apps/common/bin/globalparams.xml The default value for this parameter is 60 seconds. Absence of this parameter or a value of -1 indicates synchronous cache flushing.

Table 11 (Cont.) Resolved Issues for the Identity Server

Bug	Description
5741093	If the Identity Server encountered errors while processing requests from WebPass, the associated socket was not closed when the connection was cleaned up. This caused the connection to remain in CLOSE_WAIT status indefinitely. Also, if the Identity Server was low on resources, it could not create the reader thread required to process requests from Webpass. The associated socket was not closed, causing the connection to remain in CLOSE_WAIT status indefinitely. This problem has been fixed in the current release.
5750544	When you create large static groups, for example, groups with over 10,000 members in the Identity System, the performance of the Group Search and Group Profile pages is affected. This problem has been fixed in the current release. Group performance overall has been enhanced. See "Identity System Enhancements" on page 5 for details.
5672229	In Active Directory environments that use SSL transport security, password change operations were failing. For example, user creation workflows would fail after a user password was supplied. The failure occurred because Oracle Access Manager was not enclosing the password with double quotes. This issue has been fixed in the current patch.
5663757	If you configured a date attribute in the directory but only provided a space as a value for the attribute, the Identity Server automatically set the value of the attribute to the current date. A similar problem occurred if you used the Identity System Console to configure a data type attribute with a date display type, but the attribute value in the directory only contained a space. In this patch, values are not set automatically for empty date attributes.
5551213	After using the Selector to select ten or more objects, if you use the Selector again to add more objects, the selection page is not populated with the already-selected objects. This makes it hard to keep track of already-chosen objects. For example, when setting attribute access controls for users, it is hard to see the users who are already assigned the controls. This problem has been fixed in the current release. Previously selected users are displayed in the Selector page.
5510063	An incorrect source DN value appears in the assume rights audit record. This problem has been fixed in the current release. For example, suppose user A logs in to the Identity Server and then assumes the rights of user B. In this case, the source DN of the user assuming the rights is now audited with a new keyword (`kProxyEnactSource`) in the corresponding audit record for substitute rights application. Previously, only the target user DN (the user DN whose rights are being assumed) was audited with the keyword `k/ProxyEnactdn`.

Table 11 (Cont.) Resolved Issues for the Identity Server

Bug	Description
5396371	Special characters were not returned correctly when using IdentityXML. Special characters were represented as question marks ("?") in text strings that were returned in an IdentityXML response. According to RFC 3023 (http://www.ietf.org/rfc/rfc3023.txt) and RFC 2046, an HTTP header must specify what character set to use. If a character set is omitted, Web clients must use US-ASCII. In the case of this bug, since the character set was omitted in the response, the client defaulted to US-ASCII. The client had no way of knowing the character set that was being returned. This has been fixed in the current patch set. The correct client character set is configured in globalparams.xml and is read in for the purpose of page generation.
5286765	The Access Server, Policy Manager, and Identity Server experienced memory growth. In this release the default value for the `ldapMaxSessionTimeInMins` parameter in appdbparams.xml has been set to 600 minutes. After this time, the connection between the Oracle Access Manager component and the directory server is recycled.
5263075	CPU utilization reaches 100% on host computers that run the WebPass and WebGate plugins. Utilization stays at 100% until the Web server is restarted. This problem is due to a Netscape library function `netbuf_getc()` causing infinite looping during a POST request. This is a known issue. See Sun Problem 4728951: Error encountered while using POST request to upload zipped files. An Oracle Access Manager library function `GetFormDataChar()` uses the function `netbuf_getc()` to receive the data from NS library. This release implements the workaround "Use netbuf_getbytes()" suggested by Sun.
5192906	If the Oracle Access Manager configuration directory is down and the Identity Server is started, an error message states that the server could not be initialized. However, a subsequent message states that more details can be found in a file that does not exist (*InstallDir*/identity/oblix/logs/errors). The errors are actually logged in oblog.log, and the message now reflects this.

9.2.1 Bug Fix Details for the Identity Server

The following paragraphs provide details on selected fixes for the Identity Server.

9.2.1.1 Bug 6168198: Org Manager Tab Name Is Always Set to "Select Tab" As of this release, when you click a tab in the Org Manager, the correct tab name is displayed. Previously, the label **Select Tab** appeared even if you selected a particular tab. To implement this fix, changes were made to the following file:

Identity_Server_installdir\oblix\lang\shared\navbar.xsl

If you were using a customized version of this file, these changes are overwritten when you apply this patch. There are two ways to merge the new file with your customizations:

- Modify your original navbar.xsl file using the changes described in the following paragraphs, and overwrite the file that was installed with this patch.

The original file is located in the following directory:

Identity_Server_installdir\identity\backup-Oracle-101401RC2-binary_parameter\oblix\lang\shared

- Identify your customizations, and add them to the 10.1.4.2 navbar.xsl file.

In this patch, the lines shown in bold have been added to navbar.xsl:

```
<xsl:template match="oblix:ObApps/oblix:ObApplication/oblix:ObTabs">
  <font face="Arial, Helvetica, sans-serif" size="2" color="#000000">
    <xsl:variable name="urlContainingSelectedTab"><xsl:value-of
select="/oblix:Oblix/oblix:ObNavbar/oblix:ObMisc/oblix:ObButton[@obaction='T1
about']/@obhref"/></xsl:variable>
       <select id="applist" name="applist" size="1"
onchange="self.location.href = this.options[this.selectedIndex].value; return
true;">
          <option><xsl:value-of select="$MSelTab"/></option>
              <xsl:for-each select="oblix:ObButton">
                  <xsl:if test="@obanchorText">
                     <xsl:variable name="thisTab"><xsl:value-of
select="@obaction"/></xsl:variable>
                        <option value="{@obhref}">
                            <xsl:if test="contains($urlContainingSelectedTab,
$thisTab)"><xsl:attribute name="selected">true</xsl:attribute></xsl:if>
                            <xsl:call-template name="oblix:PrepForJS">
                                <xsl:with-param name="strToPrep"
select="@obanchorText"/>
                            </xsl:call-template>
                        </option>
                    </xsl:if>
                </xsl:for-each>
            </select>
        </font>
    </xsl:template>
```

In this patch, the line shown in bold has been deleted from navbar.xsl:

```
<xsl:template match="oblix:ObApps/oblix:ObApplication/oblix:ObTabs">
        <font face="Arial, Helvetica, sans-serif" size="2" color="#000000">
. . .
                <option><xsl:value-of select="$MSelTab"/></option>
                <xsl:for-each select="oblix:ObButton">
                    <xsl:if test="@obanchorText">
. . .
```

9.3 WebPass Resolved Issues

Table 12 describes WebPass bugs that were fixed in this release.

Table 12 Resolved Issues for WebPass

Bug	Description
5856408	After you install a WebPass, you can configure the maximum number of connections that this WebPass can establish with the Identity Server. However, on a multi-process Web server, the WebPass opens more connections to the Identity Server than you specify in the WebPass configuration. This problem has been fixed in the current release. WebPasses that run on multi-process Web servers only open the configured number of connections to the Identity Server.
5844594	When calling a Web service from an IdentityXML client, the tag `<Soap:Header>` causes the following IdentityXML error: `XML request contains unknown element Header.` The WebPass does not accept requests that contain the `<Soap:Header>` tag. This problem has been fixed in the current release. The WebPass and Identity Server can now accept the header tag in a SOAP request. However, child nodes of the header node are not processed for any actions.
5840844	Client requests that are sent to the Identity Server are processed even if the client abandons the request. This problem has been fixed in the current release. The Identity Server now checks if the connection is still open before processing a queued request.
5840834	The WebPass can retry its connections to the Identity Server indefinitely. When configuring a WebPass, the **Identity Server Timeout Threshold** field specifies how long (in seconds) the WebPass attempts to contact the Identity Server before it considers it unreachable and attempts to contact another. However, if the Identity Server takes longer to service a request than the value of the timeout threshold, the WebPass abandons the request and retries the request on a new connection. Note that the new connection that is returned from the connection pool can be to the same Identity Server, depending on your connection pool settings. Also, other Identity Servers may also take longer to process the request than the time specified on the threshold. In these cases, the WebPass can continue to retry the request until the Identity Servers are shut down. This problem has been fixed in the current release. You can now configure a limit on the number of retries that the WebPass performs for a non-responsive server using the `client_request_retry_attempts` parameter in globalparams.xml. The default value for this parameter is -1, which retains the WebPass behaviors in 10.1.4.01. The value can be set to any finite integer to change the behavior. See the *Oracle Access Manager Customization Guide* for details.
5756236	Extended operating system error information was not captured in the logs. This problem has been fixed in the current release. To assist with determining why calls are failing, extensive operating system error information is logged at the DEBUG3 level.
5467723	When using the following configuration between an Identity Server and a WebPass, performance becomes very slow: ■ The components communicate in Cert mode ■ The **Identity Server Timeout Threshold** field in the WebPass configuration page is set to a value higher than 0 (no timeout). This problem has been fixed in the current release.

Table 12 (Cont.) Resolved Issues for WebPass

Bug	Description
5400749	WebPass performs a core dump when the maximum requests per client is set to a low number. This problem has been fixed in this release.

9.4 Access Server Resolved Issues

Table 13 describes Access Server bugs that were fixed in this release.

Table 13 Resolved Issues for the Access Server

Bug	Description
6325082	The Access Server can crash when a user accesses a protected resource after changing a password. This problem occurs if a lost password policy has been set, but the user has not created a password challenge and response. This problem has been fixed in the current release.
6201694	An issue occurs when using a Basic Over LDAP authentication scheme with a Lost Password Management policy that includes a challenge redirect. After the user resets the password, he or she is redirected to the authenticating WebGate instead of being served the originally requested resource. This problem has been fixed in the current release. After resetting the password, the user is served the requested resource.
6158232	An issue can occur when a user accesses a protected URL, is redirected to a WebGate for authentication, authenticates, and is redirected back to the target URL. If the original request URL contains a query string, the query string is truncated after the redirection to the WebGate. For example, if the user enters the following http://myapp.oracle.com:81/doc/test.html?test=test1 After authenticating, the redirection URL is truncated to the following: http://myapp.oracle.com:81/doc/test.html This problem has been fixed in the current release.
6152030	After changing a password, a user is prompted to re-authenticate using the default authentication scheme instead of the scheme defined in the policy. You can configure a policy that uses an authentication scheme other than the default. For example, the policy can protect resources based on a variation of the query string for the resource protected by the policy domain. However, when a user password is reset using the Lost Password Management functionality, after being redirected to the protected resource, the user is prompted to re-authenticate using the default authentication scheme instead of the authentication scheme for the policy. This problem applies to policies for URLs that have query strings. The query string is modified in the redirect URL generated by the change password page. This problem has been fixed in the current release.

Table 13 (Cont.) Resolved Issues for the Access Server

Bug	Description
6143692	The Access Server crashes if the Oracle Access Manager-specific data (OSD) cache is disabled. For example, the following steps reproduce this problem: **1.** Set up Oracle Access Manager, and during Policy Manager setup, create a policy to protect the /identity and /access domains. **2.** In the Policy Manager, select **My Policy Domains**, then **Identity Domains**, then **Default Rules**, then **Authorization Expression**. The authorization expression should be set to **Default Authorization rule**. **3.** In the Policy Manager, select **My Policy Domain**s, then **Identity Domains**, then **Authorization Rules**, then the default authorization rule, then **Allow Access**. Allow one person, for example, the Master Administrator and one group. Do **not** allow the Anyone role. **4.** Edit the Access Server installation file access/oblix/data/common/appdbparams.xml and change value of `disablecache` from `no` to `yes`. **5.** Restart all the Identity and Access Servers to clear the cache. **6.** From a new browser, log into the Identity System as a user from the group selected in Step 3, and invoke the User Manager (a protected resource). This problem has been fixed in the current release.

6111325	When running the configureAAAserver tool, you may receive a message that references an obsolete file, similar to the following:
	`For Silent mode installation, use these additional options:`
	`-S -f <aaa_input.lst file>`
	In messages like this one, the file name should be aaa_input.xml.
	This problem has been fixed in the current release.

6082856	On Linux systems, before you run the ConfigureWebGate tool, you must set the environment variable `LD_ASSUME_KERNEL` is to value 2.4.19. If this environment variable is not set, intermittent crashes can occur. This problem has been fixed in the current release. It is no longer required to configure the `LD_ASSUME_KERNEL` environment variable.
6075501	The Access Server crashes when a blank space is provided in the Escape Character field in a master audit policy, as follows: **1.** From the Access System Console, click the **Access System Configuration** tab, then click **Common Information Configuration** in the left navigation pane. **2.** Click the **Master Audit Rule** sub-tab. Click **Add**. This problem has been fixed in the current release.
6032747	You can configure form-based authentication along with a password reset policy that uses challenge response policies. However, the user may not be redirected to the originally requested resource after responding to the challenges and resetting the password. Instead of being redirected to the form-based login page's action URL, an error appears. This problem has been fixed in the current release.

Table 13 (Cont.) Resolved Issues for the Access Server

Bug	Description
6020577	A problem occurs when a Lost Password Management policy is configured for users whose passwords have been reset. Users whose passwords are reset are not redirected to a challenge-and-response page when they access protected resources. This problem has been fixed in the current release. Redirection to the challenge-and-responses page occurs as expected.
5971014	After you upgrade from Oracle Access Manager 7.0.4 to version 10.1.4.0.1, any authentication scheme that contains multiple challenge parameter rows are truncated. Only the first challenge parameter row remains. The others are deleted. This problem has been fixed in the current release. After upgrading to 10.1.4.2.0, all challenge parameters are preserved.
5969074	After configuring Fatal-level log messages for an environment that uses a language other than English, the log messages appear in English instead of in the local language. This problem has been fixed in the current release
5912931	Users who have authenticated with a low-level authentication scheme must re-authenticate if they subsequently attempt to access a resource that is protected by a higher authentication level. However, the user can be caught in an infinite loop during this process. This problem has been fixed in the current release. Users are no longer caught in a loop when moving from a lower level of authentication to a higher level.

5893183	On Windows systems the Access Server cannot process requests that require an address space greater than 2 GB. This causes high memory consumption and outages.
	Fixed in the current release. The Access Server can now use 3 GB of virtual memory, if 2 GB addressing is already enabled in the boot.ini file. The /3GB switch allocates 3 GB of virtual address space to an Identity Server that uses IMAGE_FILE_LARGE_ADDRESS_AWARE in the process header. This switch allows applications to address 1 GB of additional virtual address space above 2 GB.
	The virtual address space of Access Server is limited to 2 GB, unless the /3GB switch is used in the Boot.ini file. The following example shows how to add the /3GB parameter in the Boot.ini file to enable Access Server memory tuning:
	`[boot loader]`
	`timeout=30`
	`default=multi(0)disk(0)rdisk(0)partition(2)\WINNT`
	`[operating systems]`
	`multi(0)disk(0)rdisk(0)partition(2)\WINNT="????" /3GB`
	See the following URL for more information:
	`http://www.microsoft.com/whdc/system/platform/server/PAE/PAEmem.mspx`

5880426	As of Oracle Access Manager 10.1.4.0.1, the **Preferred HTTP Host** field became required. This introduced issues for environments that support virtual hosting. These issues have been resolved in the current release. See "Access System Enhancements" on page 7 for details.

Table 13 (Cont.) Resolved Issues for the Access Server

Bug	Description
5852510, 5601019	When the WebGate connects to the Access Server, the Access Server creates connections with a status of CLOSE_WAIT. When WebGate closes the connection with the Access Server, it is not closed properly. Over time this leads to many connections with a CLOSE_WAIT status and, eventually, an Access Server crash. This problem has been fixed in the current release.
5845258	Access Servers process requests without checking if the connection to the client that made the request is still open. This processing is unnecessary if the client has already abandoned the request. Access Server performance can be optimized by checking if the client is still waiting for the request before picking up the request for processing from the request queue. This problem has been fixed in the current release. The Access Server now checks if the client that issued the request has closed the connection and abandoned the request.

5765203	When you configure an authentication scheme that uses HTTP headers in the `creds` list, users receive errors when they access resources, even if they should be allowed access according to the scheme.
	For example, if you set the following challenge parameters, using Accept-Language as the HTTP request header, when the user accesses a resource that is protected with this scheme, the login form is not presented, and the user receives an error:
	`form: /login.html`
	`creds:login password Accept-Language`
	This problem has been fixed in the current release. If all of the `creds` object variables are found, the value of the creds parameter is set to `true`.

5741096	If the Access Server encountered specific errors while processing requests from WebGate, the associated socket was not closed when the connection was cleaned up. This caused the connection to remain in CLOSE_WAIT status indefinitely. Also, if the Access Server was low on resources, it could not create the reader thread required to process requests from WebGate. The associated socket was not closed, causing the connection to remain in CLOSE_WAIT status indefinitely. This problem has been fixed in the current release.
5713151	A problem can occur when you configure several plug-ins for an IIS server, for example, a WebGate plug-in and an iisWASPlugin that front-ends WebSphere, and you also set the **UseIISBuiltinAuthentication** parameter to **true** from the **AccessGate Configuration** tab in the Access System Console. In this situation, the WebGate may fail to include query strings for target applications in the ObFormLoginCookie. The problem manifests if a user enters a URL to access a resource and is prompted for a form-based login. When this occurs, the target application can break if the WebGate omits the URL's query string when redirecting to the originally requested URL. This problem has been fixed in the current release. Query strings are preserved in the target application URL.
5390041	The Access Server treated cache flush requests in a case-sensitive manner. This has been fixed in the current release. Case is no longer considered when processing cache flush requests.

Table 13 (Cont.) Resolved Issues for the Access Server

Bug	Description

5390029	The Access Server uses request queues to create a sequence of incoming requests that are processed by worker threads. The number of queues in operation would not change if you issued the `Q` parameter on the `aaa_server` command from the command line.
	This problem has been fixed in this release. To implement the fix, you must add the `numQs` parameter in globalparams.xml, as follows:
	`<SimpleList>`
	`<NameValPair`
	`ParamName="numQs" Value="4">`
	`</NameValPair>`
	`</SimpleList>`
	See the *Oracle Access Manager Deployment Guide* for details on the `Q` parameter and the *Oracle Access Manager Customization Guide* for details on globalparams.xml.

5286765	The Access Server, Policy Manager, and Identity Server experienced memory growth. This problem has been fixed in the current release. In this release, the default value for the `ldapMaxSessionTimeInMins` parameter in appdbparams.xml has been set to 600 minutes. After this time, the connection to the Oracle Access Manager component is recycled.
4468422	When a user authenticates to Oracle Access Manager using an X.509 certificate, and the certificate contains more than one instance of the same attribute, user authentication fails. This problem has been fixed in the current release. If there are multiple instances of the same attribute in the user's certificate, the correct instance of the attribute is used in the user's credentials. For example, if the certificate contains "cn=Jean Smith,cn=users", the value "Jean Smith" is inserted in the user's credentials.

9.5 Policy Manager Resolved Issues

Table 14 summarizes Policy Manager bugs that were fixed in this release.

Table 14 Resolved Issues for the Policy Manager

Bug	Description
6522582	When viewing a long list of Host Identifiers, it can be hard to find the host identifier of interest because the list is not sorted. This problem has been fixed in the current release. The list of Host Identifiers is now sorted.
5962458	After you upgrade from 7.0.4 to 10.1.4, the password.lst file is not converted to a password.xml file. The required password.xml file is missing from the Access Manager SDK and the Policy Manager. This applies to installations running in Simple mode. This problem has been fixed in the current release. Upgrading to 10.1.4.2.0 produces the correct password.xml file.

Table 14 (Cont.) Resolved Issues for the Policy Manager

Bug	Description

5654052	In the Linux Policy Manager on Apache 2, the instruction file config.htm contains information on manually updating the Apache2 http.conf file for hosting the Policy Manager.
	The following entry in this file causes the Web server to fail:
	`<IfModule !mod_ssl.c>`
	`        LoadModule OBCommonModuleLoader`
	`"/home/oracle/OAM1014/identity/webcomponent/access/oblix/apps/modu`
	`le_loader/bin/obmodule_loader.so"`
	`</IfModule>`
	This problem has been fixed in the current release.

5399401	When defining a resource, entering a URL prefix that contains a question mark ("?") causes the resource to be truncated. The question mark delimits a URL. It defines the limit of the URL and the beginning of a query string. For example, if you did the following, the URL that is saved is truncated to `/test`: **1.** In a policy domain, add an HTTP resource similar to the following: `/test?st=tty` **2.** Save the resource. In this release, if you provide a "?" character in a URL, a warning message is displayed stating that only the information before the delimiter will be stored.
5384106	The Policy Manager did not permit you to retrieve user access reports. This problem only occurred when operating in ADSI mode. For example, if you did the following, the expected report did not appear: **1.** From the Access System Console, select **System Management**, then select **Manager Reports**. **2.** Click **Add**. **3.** Provide the report details. **4.** Click **Save**. This problem has been fixed in the current release.
5286765	The Access Server, Policy Manager, and Identity Server experienced memory growth. In this release the default value for the `ldapMaxSessionTimeInMins` parameter in appdbparams.xml has been set to 600 minutes. After this time, the connection to the Oracle Access Manager component is recycled.

9.6 WebGate Resolved Issues

Table 15 describes WebGate bugs that were fixed in this release.

Table 15 Resolved Issues for WebGate

Bug	Description
6443025	A user can enter a POST request that contains a very long password (4 GB, which is the POST request limit). The request can also contain binary shell code. This problem has been fixedin the current release. In a form-based authentication scheme, you can now specify a `maxpostdatabytes` challenge parameter. The value of this optional parameter is the maximum number of data bytes that an end user can post for authentication to a Web server that uses a WebGate. If the POST data exceeds the threshold set by maxpostdatabytes in the form-based authentication scheme, user receives an error and a log entry is added at the DEBUG3 log level in the oblog.log file. Example: `maxpostdatabytes:100` If you omit this parameter, the end user can post unlimited length strings for authentication to a Web server that is protected by a WebGate. Very long strings can cause the WebGate or Web server to crash, denial of service, or another fatal error.
6359813	As noted in the chapter on authentication in the *Oracle Access Manager Access Administration Guide*, you can configure an authentication scheme that allows the user to log in for a period of time rather than a single session by adding the challenge parameter `ssoCookie:max-age` in the authentication scheme. The released version of this document mentions that this feature works only with the Mozilla. However, this feature works with Internet Explorer as well as Mozilla-based browsers.
6357953	A looping error occurs when a policy domain protects the top-level directory ("/") of a Web server, and a form that resides below this directory is protected with an anonymous authentication scheme. This problem has been fixed in the current release. If you now protect a resource using anonymous authentication, the resource is always treated as a "not protected" resource.
6311786	When accessing a resource that is protected with a form-based authentication scheme, the user is redirected back to the login page after authenticating instead of being served the resource. In particular, this problem arises when the login form is protected with an anonymous authentication scheme and the form-based authentication scheme. This problem has been fixed in the current release.
6167735	A WebGate can hang when recovering from a failover event. Typically, this issue occurs when more than one connection is used for the primary and secondary servers. For example, suppose that you configure a WebGate, a primary Access Server, and a secondary Access Server, and configure two connections for each Access Server. After several users access a protected resource, the primary server fails over. Several more users access a protected resource using the secondary server. When the primary server comes back up, and additional users access additional resources, the WebGate can start spinning. This issue has been fixed in the current release.

Table 15 (Cont.) Resolved Issues for WebGate

Bug	Description
6158232	When a user accesses a protected resource, he or she is redirected to a WebGate for authentication. After authenticating, the user is supposed to be redirected to the originally requested resource. However, the query string on the original URL is truncated. For example, http://my.url.com/mydocument.html?myquery.string is truncated to eliminate "?myquery.string". This problem has been fixed in the current release. Query strings are preserved in redirection URLs.
6157298	If you configure form-based authentication and implement it along with IWA authentication, the WebGate issues an error, stating that the authentication form itself requires authentication. This issue has been fixed in the current release.
6127597	A WebGate that is running on an iPlanet server enters an infinite loop or crashes under the following conditions: ▪ Incomplete POST data is submitted during authentication. ▪ An authentication request contains an image map URL. These problems have been fixed in the current release.
6066323	The Web server can crash when a WebGate is installed on an Oracle HTTP Server version 2 (10.1.3.1.0) running Linux. This problem has been fixed in the current release.
6063120	The Web server can crash if you turn on debug mode for a WebGate that is running on an Oracle HTTP Server version 10.1.3.1 SOA, as follows: **1.** 1. From the Access System Console, select **Access Gate Configuration**. **2.** Click **Go**. **3.** Click the entry for the Oracle HTTP Server WebGate. **4.** Click **Modify** at the bottom of the page. **5.** In the Debug field, select **On** to print the debug messages. This problem has been fixed in the current release
6054889, 6001674, 5909418	Users who authenticated with a low-level authentication scheme are caught in an infinite loop when accessing a resource protected by a higher-level authentication scheme. That is, they are continuously prompted to re-authenticate. This problem has been fixed in the current release. Users are no longer caught in an infinite loop when moving from a lower level of authentication to a higher level.
6051252	A problem can occur when you configure a WebGate to protect the /identity URL and you configure a lost password management challenge redirect to this URL. After a user authenticates, a query parameter is missing on redirection. As a result, the browser is redirected to the following: /identity/oblix/.../userservcenter.cgi The browser should be directed instead to this URL: /identity/oblix/.../userservcenter.cgi?program= redirectcac This problem has been fixed in the current release. The query parameter is now appended to the redirection URL.

Table 15 (Cont.) Resolved Issues for WebGate

Bug	Description
6021640	Usually, if you go to the **AccessGate Configuration** tab in the Access System Console and set I**P Validation** to **true**, the IP address stored in the ObSSOCookie must match the client's IP address, otherwise, the user must re-authenticate. However, IP validation does not work as expected for a Domino WebGate in Oracle Access Manager 10.1.4.0.1. After IP validation is turned on, users can receive an error instead of being prompted for credentials when accessing a resource. This issue only exists if the resources are accessed using a fully qualified domain name. This problem has been fixed in the current release.
5978345	After you configure Lost Password Management, new users are not presented with the challenge-and-response page when accessing a protected resource. This problem occurs when a WebGate and a WebPass are installed on different servers. This problem has been fixed in the current release. You can specify a new validate_password plug-in parameter named `obWebPassURLprefix` to work with Lost Password Management. The value of this plug-in is as follows: http://*webpasshost*:*webpassport* The validate_password plug-in is described in the chapter on authentication in the *Oracle Access Manager Access Administration Guide*. Lost Password Management is described in the section on configuring password policies in the *Oracle Access Manager Identity and Common Administration Guide*.
5892276, 5858088	If a third-party component expects a different version of an NLS library than the one deployed with Oracle Access Manager, the Oracle Access Manager components can crash. This problem has been fixed in the current release.
5891893	For a form-based authentication scheme, if you configure a server or cgi variable using uppercase letters in the `creds` list, the variable is not recognized by the Netscape Server. This problem has been fixed in the current release.
5886637	A WebGate can keep retrying requests until the Access Server is shut down. If the Access Server takes longer to service a request than the value of the configured timeout threshold, the WebGate abandons the request and retries the request on a new connection. However, the new connection can be to the same Access Server, depending on your connection pool settings. Also, other Access Servers may also take longer to process the request than the time specified on the threshold. In these cases, the WebGate can continue to retry the request until all these Access Servers are shut down. This problem has been fixed in the current release. You can now set a limit on the number of retries using a `client_request_retry_attempts` parameter. The default value for this parameter is -1, which retains the WebGate behaviors in 10.1.4.01. The value can be set to any finite integer to change the behavior. See the section, "Configuring User-Defined Parameters" in the *Oracle Access Manager Access Administration Guide* for details.

Table 15 (Cont.) Resolved Issues for WebGate

Bug	Description
5868410	The query strings in a URL for a requested resource are not passed when using form-based authentication. For example if you do the following, in the second level redirection, the query string was missing from the returned URL: **1.** Got to a protected resource, for example, the following URL: http://test.us.mycompany.com/test1/test1.html?uid=1?afds=123 You are redirected to a login page. **2.** Fill in the fields on the login page. The form-based authentication scheme redirects you back to http://test.us.mycompany.com/test1/test1.html, but the query strings are missing. This problem has been fixed in the current release.
5852993	After you install a WebGate, you can configure the maximum number of connections that this WebGate can establish with the Access Server. However, on a multi-process Web server, the WebGate opens more connections to the Access Server than you specify in the WebGate configuration. This problem has been fixed in the current release. WebGates that run on multi-process Web servers only open the configured number of connections to the Access Server.

9.7 Software Developer Kit (SDK), API, and Integrations Resolved Issues

Table 16 summarizes bugs related to the Access Server SDK, APIs, and integrations with Oracle and third-party products that were fixed in this release.

Table 16 Resolved Issues for Access Server SDK, APIs, Integrations

Bug	Description
6457125, 6396922	When older versions of the Access Manager SDK generate ObSSOCookies that do not contain a value for idle session timeout, a 10.1.4.0.1 Access Manager SDK and WebGate may reject these cookies. The single sign-on token is treated as if it has a value of zero for the idle session timeout. This problem has been fixed in the current release. If the idle session timeout is missing from the ObSSOCookie, the SDK enforces its own idle session timeout. If the SDK detects a a non-zero value, it uses the lesser of the two idle timeout values.

6084780	If you have configured the Oracle Access Manager Security Provider for Weblogic, the Policy Deployer does not delete authorization rules. For example, if you configure NetPointWeblogicTools.properties as follows and run the Policy Deployer, any configured authorization rules are not deleted:
	`# Initial Setup`
	`ObWLTools.SetupInitialNetpointSSPIPolicies=false`
	`#`
	`# Deploy Policy`
	`ObWLTools.DeployPolicy=false`
	`ObWLTools.UnDeployPolicy=true`
	This problem has been fixed in the current release.

Table 16 (Cont.) Resolved Issues for Access Server SDK, APIs, Integrations

Bug	Description
6082856	On Linux systems, before you run the ConfigureAccessGate tool, you must set the environment variable `LD_ASSUME_KERNEL` is to value 2.4.19. If this environment variable is not set, intermittent crashes can occur. This problem has been fixed in the current release. It is no longer required to configure the `LD_ASSUME_KERNEL` environment variable.
6072614	After configuring an integration with the Weblogic Application Server version 9.2, if an application is deployed on Weblogic, role-based policies are created for this application in Oracle Access Manager. However, the policy deployer tool cannot delete these policies. This problem has been fixed in the current release.
5645476	If you configure the SSPI Connector on WebLogic 9.2, then log in as an non-administrative user, you are unable to use the Deploy link to deploy an application. Administrative users are not affected by this issue. This is a known issue to be addressed by BEA. For more information, contact BEA support and reference case number 685777.
5134098	An issue can occur when integrating with RSA SecurID if replication and next tokencode mode are enabled. In this situation, if the user waits for 140 or more seconds between entering the first and next tokencode, subsequent requests are routed to a different ACE server. This problem has been fixed in the current release. Waiting to enter the next tokencode does not lead to failover.
5962458	After you upgrade from 7.0.4 to 10.1.4, the password.lst file is not converted to a password.xml file. The required password.xml file is missing from the Access Manager SDK and the Policy Manager. This applies to installations running in Simple mode. This problem has been fixed in the current release. Upgrading to 10.1.4.2.0 produces the correct password.xml file.
5954326	A file that is required to run the registry tester is not available with IBM WebSphere Application Server 6.1. The missing file has been added in this release. See the Troubleshooting section of the chapter on "Integrating with IBM WebSphere" in the *Oracle Access Manager Integration Guide* for details.
5939157	If you configure an external authentication scheme, for example, Integrated Windows Authentication (IWA), a problem can occur when a user's session expires. After refreshing the browser, instead of being served the resource again, with re-authentication taking place in the background, an error message appears. Refreshing the page once more correctly authenticates the user and presents the resource. This problem has been fixed in the current release.
5623970	Users experience performance issues when configuring policy domains using the Policy Manager SDK. The Java API `getPolicyDomains()` would read the entire list of host IDs in the directory, once each for every policy domain object in the list. This was an expensive operation. This problem has been fixed in the current release.

Table 16 (Cont.) Resolved Issues for Access Server SDK, APIs, Integrations

Bug	Description
5574546	For the Oracle Access Manager SSPI provider for Weblogic, the role provider for Web and EJB applications takes too much network bandwidth because it retrieves all groups or roles that the user belongs to. In this release, the role provider returns a dummy role. Network bandwidth is saved because the Authorization Provider retrieves only applicable roles at a later stage. Role retrieval is postponed until authorization decision time. Also, the Authorization Provider has changed in this release. It is the responsibility of the Authorization Provider to retrieve the roles to which a user belongs.

9.8 Performance Resolved Issues

Table 17 lists bugs relating to performance issues that were resolved in this release.

Table 17 Resolved Performance Issues

Bug	Description
6144036	Performance was affected due to performing cache flushes of the LDAP policy cache for the Person object class. This problem has been fixed in the current release. The cache flush now occurs only for a Generic object class.
5901108, 5524369	Large groups can slow down performance. Enhancements have been made to the performance of groups. See "Identity System Enhancements" on page 5 for details.
4468428	Large numbers of policy domains can slow down performance. Enhancements have been made to performance when defining policy domains. See "Access System Enhancements" on page 7 for details.

9.9 Documentation Resolved Issues

The bugs relating to documentation issues have been resolved as described in Table 18.

Table 18 Resolved Documentation Issues

Bug	Description
n.a.	New information about configuring global logout from a single sign-on session has been added to an appendix on logout in the *Oracle Access Manager Access Administration Guide* and the *Oracle Access Manager Integration Guide*.

Table 18 (Cont.) Resolved Documentation Issues

Bug	Description
6156900	Previous versions of the *Oracle Access Manager Identity and Common Administration Guide* were unclear regarding the configuration of stylesheets for lost password and password change forms. The files lpm_cr.xsl and lpm_changepwd.xsl are the original stylesheets. You can copy these stylesheets, customize them, and place the files in the currently active style folder. You also modify the relevant password policy to indicate the relative path of the XSL file in the active style folder. In the Lost Password Redirect stylesheet or the Password Change Redirect stylesheet, you can optionally enter a relative path to an XSL stylesheet. For example, if the stylesheet file is located in *Identity_Server_installdir* /identity/oblix/lang/en-us/style0/myStyleSheet.xsl, you would enter /myStyleSheet.xsl. See the *Oracle Access Manager Customization Guide* for details on stylesheet configuration. See the section on lost password management in the chapter "Configuring Global Settings" in the *Oracle Access Manager Identity and Common Administration Guide* for details on lost password redirection.
5840022	In the *Oracle Access Manager Integration Guide* chapter on WebLogic, the section "Debug Log Files" states that you can configure the log level from the WebLogic administration console. This statement is incorrect and has been removed.
5673856	In the *Oracle Access Manager Installation Guide*, Chapter 20, the name of the Unix program is stated incorrectly. The program name is now stated correctly as follows: "On Unix systems, use uninstaller.bin."
5645064	In the *Oracle Access Manager Installation Guide*, Chapter 4, the syntax in "Tuning Oracle Internet Directory" is misleading. The problem has been fixed in this release and a note added: "Be sure to include a space after the attribute `orclinmemfiltprocess:` and at the start of each continuation line of the attribute value."
5250394	Information was missing on how to work with groups that do not accept subscriptions. A section on "Configuring a Group to Accept Subscriptions" has been added to the chapter on configuring the Identity System Applications in the *Oracle Access Manager Identity and Common Administration Guide*.
4468243	The `obtype` and `obnamespace` parameters were not documented for managed code. The *Oracle Access Manager Access Administration Guide* now mentions that a managed code authentication plug-in must include these parameters. A similar note was added to the *Oracle Access Manager Developers Guide*, in the section on writing plug-ins for authentication.

10 Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. 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.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Oracle Access Manager Patch Set Notes, Release 10.1.4 Patch Set 1 (10.1.4.2.0) for All Supported Platforms