Oracle® Access Manager

Introduction

10*g* (10.1.4.0.1)

B25342-01

July 2006

This manual provides an overview of Oracle Access Manager 10*g* (10.1.4.0.1), product globalization, system behaviors, a road map to related manuals, and a glossary of terms.

ORACLE®

Oracle Access Manager Introduction 10*g* (10.1.4.0.1)

B25342-01

Primary Author: Gail Tiberi

Contributor: Nina Wishbow, Darren Calman, Howard Bae, Bill Bathurst, Guru Sashikumar, Frank Villavicencio

Contents

5 Overview of 10*g* (10.1.4.0.1) Behaviors

6 Road Map to Manuals

Preface

This guide provides an overview of Oracle Access Manager 10*g* (10.1.4.0.1) features, components, applications, and functions. A road map to Oracle Access Manager manuals is provided, which outlines content, audiences, and prerequisites. A Glossary is included for quick reference.

> **Note:** Oracle Access Manager was previously known as "Oblix NetPoint".

This Preface covers the following topics:

Audience

This guide is intended for anyone who is interested in an introduction to Oracle Access Manager, globalization within the product, concepts, terminology, and the suite of manuals.

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.

Related Documents

For more information, see the following documents in the Oracle Access Manager Release 10*g* (10.1.4.0.1) documentation set:

- *Oracle Access Manager Introduction*—Provides an introduction to Oracle Access Manager, a road map to Oracle Access Manager manuals, and a glossary of terms.
- *Oracle Application Server Release Notes*—Read these for the latest Oracle Access Manager updates. The release notes are available with the platform-specific documentation. The most current version of the release notes is available on Oracle Technology Network at: `http://www.oracle.com/technology/documentation`.
- *Oracle Access Manager Installation Guide*—Explains how to install and configure the components.
- *Oracle Access Manager Upgrade Guide*—Explains how to upgrade earlier versions to the latest version.
- *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, for example, adding basic information about a user, providing additional information about the user, and approving the new user entry, into a chain of automatically performed steps. This book also describes administration functions that are common to the Identity and Access Systems, for example, directory profile configuration, password policy configuration, logging, and auditing.
- *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. This guide covers capacity planning, system tuning, failover, load balancing, caching, and migration planning.
- *Oracle Access Manager Customization Guide*—Explains how to change the appearance of Oracle Access Manager applications and how to control Oracle

Access Manager by making changes to operating systems, Web servers, directory servers, directory content, or by connecting CGI files or JavaScripts to Oracle Access Manager screens. This guide also describes the Access Manager API and the authorization and authentication plug-in APIs.

- *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 run with third-party products such as BEA WebLogic, the Plumtree portal, and IBM WebSphere.
- *Oracle Access Manager Schema Description*—Provides details about the Oracle Access Manager schema.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in Oracle Access Manager?

This chapter describes a listing of new features introduced with Oracle Access Manager 10*g* (10.1.4.0.1) and provides pointers to additional information in the suite of product manuals.

The following sections are included:

Product and Component Name Changes

The original product name, Oblix NetPoint (also known as Oracle COREid) has changed to Oracle Access Manager. Many component names remain the same.

However, there are several important changes that you should know about, as shown in the following table:

Item	Was	Is
Product Name	Oblix NetPoint Oracle COREid	Oracle Access Manager
Product Name	Oblix SHAREid NetPoint SAML Services	Oracle Identity Federation
Product Name	OctetString Virtual Directory Engine (VDE)	Oracle Virtual Directory
Product Release	Oracle COREid 7.0.4	Also available as part of Oracle Application Server 10g Release 2 (10.1.2).
Directory Name	COREid Data Anywhere	Data Anywhere
Component Name	COREid Server	Identity Server
Component Name	Access Manager	Policy Manager
Console Name	COREid System Console	Identity System Console
Identity System Transport Security Protocol	NetPoint Identity Protocol	Oracle Identity Protocol
Access System Transport Protocol	NetPoint Access Protocol	Oracle Access Protocol
Administrator	NetPoint Administrator COREid Administrator	Master Administrator
Directory Tree	Oblix tree	Configuration tree
Data	Oblix data	Configuration data
Software Developer Kit	Access Server SDK ASDK	Access Manager SDK
API	Access Server API Access API	Access Manager API
API	Access Management API Access Manager API	Policy Manager API
Default Policy Domains	NetPoint Identity Domain COREid Identity Domain	Identity Domain
Default Policy Domains	NetPoint Access Manager COREid Access Manager	Access Domain
Default Authentication Schemes	NetPoint None Authentication COREid None Authentication	Anonymous
Default Authentication Schemes	NetPoint Basic Over LDAP COREid Basic Over LDAP	Oracle Access and Identity Basic Over LDAP
Default Authentication Schemes	NetPoint Basic Over LDAP for AD Forest COREid Basic Over LDAP for AD Forest	Oracle Access and Identity for AD Forest Basic Over LDAP

Item	Was	Is
Access System Service	AM Service State	Policy Manager API Support Mode

All legacy references in the product or documentation should be understood to connote the new names.

User Interface and Usability Changes

- Identity System function names and user interface changes have been made to improve usability
- Access System function names and user interface changes have been made to improve usability

  See Also: This *Oracle Access Manager Introduction* provides an overview of 10*g* (10.1.4.0.1) and system behaviors.

Globalization

- Oracle Access Manager 10*g* (10.1.4.0.1) provides support for 29 languages though the use of Unicode and UTF-8 encoding.

  See Also: This *Oracle Access Manager Introduction* provides an overview of globalization.

- The Oracle National Language Support Library (NLSL) is installed automatically with each component. However, you may need to perform specific tasks before installation when you have a non-English (AMERICAN) Operating System. You can install language packs in concert with components, or independently after component installation.

  See Also: *Oracle Access Manager Installation Guide*

- Automated language processing occurs during an upgrade to Oracle Access Manager 10*g* (10.1.4.0.1). In addition, you may need to take specific actions before and after the upgrade to ensure that older plug-ins operate properly, incorporate workflows, ensure that auditing and access reporting work properly, and the like.

  See Also: *Oracle Access Manager Upgrade Guide*

- You must perform specific tasks to use multiple installed languages and display information in various supported languages.

  See Also: *Oracle Access Manager Access Administration Guide*.

- As a result of globalization and translation of messages into 29 languages, some .lst files have been transformed into .xml files

  See Also: Specific file names in all manuals in this suite of books.

- You must use form-based authentication for non-ASCII login credentials

  See Also: *Oracle Access Manager Access Administration Guide*

- Multi-byte support impacts IdentityXML functions and parameters, compatability with XML pages, SOAP/IdentityXML requests, and Identity Event Plug-in data sent to executables; compatability with the Access Manager SDK, Access Manager APIs, and custom AccessGates.

  See Also: *Oracle Access Manager Developer Guide*

- Oracle Access Manager uses a locale-based case insensitive sorting method when you click the column heading (Full Name, for example) in the search results table.

  See Also: *Oracle Access Manager Identity and Common Administration Guide*

- Multi-byte support and custom C programming language Authorization Plug-in Interfaces behavior in 10*g* (10.1.4.0.1) (and earlier releases) is discussed, as well as backward compatability with custom authorization plug-ins.

  See Also: *Oracle Access Manager Developer Guide*

- Globalization and multi-byte support impacts stylesheets and customizations.

  See Also: *Oracle Access Manager Customization Guide*

Auditing

You can now audit to an Oracle Database as well as to Microsoft SQL Server. The Crystal Reports package is no longer provided with the Oracle Access Manager package. You must obtain this product from the vendor.

See Also: *Oracle Access Manager Identity and Common Administration Guide* and "Logging" on page -xvi

Authentication Schemes

- **Disabling Authentication Schemes:** It is no longer necessary to disable an authentication scheme before you modify it.

  See Also: *Oracle Access Manager Access Administration Guide*

- **Persistent Cookies in Authentication Schemes**: You can configure an authentication scheme that allows the user to log in for a period of time rather than a single session.

  See Also: *Oracle Access Manager Access Administration Guide*

Behaviors in 10*g* (10.1.4.0.1)

- **Overview**: A brief overview of Oracle Access Manager 10*g* (10.1.4.0.1) product behaviors is outlined for quick reference.

  See Also: This *Oracle Access Manager Introduction*

- **Summary of Earlier Behaviors and New Behaviors in Upgraded Environments**: Numerous changes have been made to support globalization. In addition, a number of other changes have been made to improve usability and performance.

A brief overview of Oracle Access Manager 10*g* (10.1.4.0.1) product behaviors is outlined for quick reference.

See Also: *Oracle Access Manager Upgrade Guide*

Configuring Multiple Searchbases

- Information on configuring Oracle Access Manager for multiple directory searchbases, also called disjoint domains or realms, has been expanded.

  See Also: *Oracle Access Manager Identity and Common Administration Guide*.

Configuring Workflows

- You can dynamically assign a user to a target on a create user workflow. For example, you can define a create user workflow that enables user A to log in under `ou=users`, invoke the workflow, and create user B whose entry is automatically determined to be in the same `ou` as user A. This ability always existed in the Identity System, and is now explicitly documented in the chapter on workflows.

  See Also: *Oracle Access Manager Identity and Common Administration Guide*.

Federated Authorization

- You can authorize users by querying external authentication systems.

  When the Access System at a Service Provider site receives a request from a user in a federated environment, it may need to get additional information about the user from the user's Identity Provider. You can configure the Access System to query external Identity Providers for user authorization.

  See Also: *Oracle Access Manager Access Administration Guide*

Installation Updates

- Oracle HTTP Server (OHS) support is provided with this release for WebPass, Access Manager, and WebGate components.
- Oracle Internet Directory support is included in this release for general use.
- Updates and additions to Apache v1 and v2 chapters.
- A new chapter has been added that describes how to install the globalized product as well as describing how to prepare to install in multi-language environment.
- Following the acquisition of OctetString by Oracle, this chapter moved from the *Oracle Access Manager Integration Guide* and includes minor changes for clarification, product branding, and new information to describe graphics.

  See Also: *Oracle Access Manager Installation Guide*.

Integration Updates

All chapters in the *Oracle Access Manager Integration Guide* describe implementation details for a specific integration

- **MIIS**: The MIIS provisioning solution is deprecated in this release.
- **OracleAS Single Sign-On Server**: You can configure single sign-on between the Access System and the . An older version of this chapter previously existed in the *Oracle Access Manager Developer Guide*. It provides updated information on configuring single sign-on between Oracle Access Manager and Oracle Application Server 10g (OracleAS 10g). When you configure single sign-on you also provide identity management functionality across the Web-based applications running on Oracle Application Servers, for example, Oracle eBusiness Suite, Oracle Forms, Portals, and other Access System-protected resources. Included in this new version is information about the OHS WebGate (Apache WebGate information has been removed).

  See Also: *Oracle Access Manager Access Administration Guide*

- **SAP**: The SAP Enterprise Portal 6.0 can now be protected by the Access System.
- **RSA Securid**: Minor clarifications have been made to this chapter based on input from the field.
- **Security Connector for WebLogic SSPI**: Several clarifications have been made to this chapter.
- **Oracle Virtual Directory**: Integration with Oracle Virtual Directory (formerly known as OctetSTring Virtual Directory Engine) has been updated and moved to the *Oracle Access Manager Installation Guide* from the *Oracle Access Manager Integration Guide*.
- **WebSphere**: The integration with WebSphere Application Server (WAS) 4 is deprecated in this release. The information in this chapter has been updated for WAS 5 and 6.
- **Plumtree**: The previous integration with Plumtree Corporate Portal is supported in this release. However, that the most recent version of Plumtree Corporate Portal is now known as BEA Aqualogic Interaction.

Logging

- Changes to logging parameters take effect within one minute, rather than requiring you to restart the server where the changes were made.

  See Also: *Oracle Access Manager Identity and Common Administration Guide*.

Object Classes and Attributes

There have been several schema changes in this release to support password policy enhancements and lost password management.

- The following oblixPersonPwdPolicy attributes have been added: obAnsweredChallenges, obYetToBeAnsweredChallenges, obLastSuccessfulLoginTime, obLastFailedLoginTime.
- A new object class named oblixLPMPolicy has been added.

This object class stores information about new lost password management policies, including the challenges and responses that have been configured and how challenge phrases are presented to users.

- The following attributes have been added to oblixDBInstance: obDatabaseName, obDSNName
- The following attributes have been added to oblixAAAEngineConfig: obSessionTokenCache, obMaxSessionTokenCacheElements
- The definition of obCompoundData has been updated throughout the *Oracle Access Manager Schema Description*.

See Also: *Oracle Access Manager Schema Description*

Parameters for Complex Stylesheets

- If you use complex stylesheets, you may want to increase the value of the StringStack parameter in globalparams.xml.

See Also: *Oracle Access Manager Customization Guide* for stylesheet and parameter references.

Password Policies and Lost Password Management

- You can configure the minimum and maximum number of characters users can specify in a password. For lost password management, you can set multiple challenge-response pairs, create multiple stylesheets, and configure other aspects of the user's lost password management experience. You can also redirect users back to the originally requested page after resetting a password.

See Also: *Oracle Access Manager Identity and Common Administration Guide*.

Sample Code

- Web Services code samples has been added to illustrate how to use Identity XML Web Services to make calls to a WebPass. Two samples have been added, to show how to create a Web service call when a WebPass is protected by a WebGate and when a WebPass is not protected by a WebGate.
- Additional IdentityXML samples have been added to the book.
- Many samples are provided in the \unsupported directory.

See Also: *Oracle Access Manager Developer Guide*.

Triggering Authentication Actions After the ObSSOCookie Is Set

You can cause authentication actions to be executed after the ObSSOCookie is set.

Typically, authentication actions are triggered after authentication has been processed and before the ObSSOCookie is set. However, in a complex environment, the ObSSOCookie may be set before a user is redirected to a page containing a resource. In this case, you can configure an authentication scheme to trigger these events.

See Also: *Oracle Access Manager Access Administration Guide*

Tuning the Directory

- To optimize performance, you should ensure that your directory performance is optimal.

  See Also: *Oracle Access Manager Deployment Guide*.

Tuning Workflows

- There are best practices for optimizing workflow performance.

  To minimize the impact that workflows have on server performance, you can tune various parameters in workflowdbparams.xml. You can also tune various workflow search parameters to enhance performance.

  See Also: *Oracle Access Manager Deployment Guide*.

Tuning Your Network

- There are best practices for optimizing network and Oracle Access Manager performance.

  See Also: *Oracle Access Manager Deployment Guide*.

Upgrade Paths, Requirements, Tips

- You can get a quick look at the upgrade paths from various starting releases, as well as the upgrade process.
- There has been a change in the release numbering, which you should be aware of.
- Review the summary of 10*g* (10.1.4.0.1) behaviors as compared with behaviors in previous releases
- Find out what is preserved and what manual processes are needed after the upgrade.

  See Also: *Oracle Access Manager Upgrade Guide*

WebGate Updates

- WebGates have been updated to use the same code as the Access System, and WebGate configuration parameters that once existed in WebGateStatic.lst have been moved to the Access System Console. The WebGateStatic.lst file no longer exists.

  After installing new WebGates or upgrading to 10*g* (10.1.4.0.1) WebGates, you can now configure such parameters as `IPValidation` and `IPValidationExceptions` from the Access System Console, Access System Configuration tab.

  See Also: *Oracle Access Manager Access Administration Guide*

  Oracle Access Manager Customization Guide

- When you have older WebGates and new 10*g* (10.1.4.0.1) Access Servers, you must set the `isBackwardCompatible` flag to "`true`" in new 10*g* (10.1.4.0.1) Access Server globalparams.xml file.

See Also: This *Oracle Access Manager Introduction*

Oracle Access Manager Upgrade Guide

Oracle Access Manager Customization Guide

- Check for new details about customizing to allow auto-login.

  See Also: *Oracle Access Manager Customization Guide*

- Look for new information about denying access to unprotected resources automatically.

  See Also: *Oracle Access Manager Customization Guide*

- A new lazyload method has been added to the ObUserSession constructor in the Access Manager API as a result of the WebGate rewrite.

  See Also: *Oracle Access Manager Developer Guide*

- New diagnostics have been added as a result of the WebGate rewrite.

  See Also: *Oracle Access Manager Developer Guide*

- New status codes have been added as a result of the WebGate rewrite.

  See Also: *Oracle Access Manager Developer Guide*

1

Introducing Oracle Access Manager

This chapter provides an overview of Oracle Access Manager 10*g* (10.1.4.0.1) and includes the following topics:

About Oracle Access Manager

Oracle Access Manager (formerly known as Oblix NetPoint and Oracle COREid) provides a full range of identity administration and security functions, that include Web single sign-on; user self-service and self-registration; sophisticated workflow functionality; auditing and access reporting; policy management; dynamic group management; and delegated administration.

Oracle Access Manager offers a DMZ-type three-tier architecture to provide a highly secure deployment with maximum protection of data and applications that includes the following:

- **Identity System**: The industry's first and most mature enterprise identity management system. The Identity System (formerly known as NetPoint COREid) provides user management and self service, dynamic group management and organization management, privacy enforcement, delegated administration, and powerful workflow to secure additions and changes to any of these. The Identity System is used to manage hundreds of thousands to millions of users in some of the world's largest extranets and portals.
- **Access System**: The access-control system (formerly known as the NetPoint Access System). The Access System, Network Computing's 2003 Product of the Year, provides single sign-on across any Web application. It supports a variety of access policies, and is fully integrated with the Identity System so that changes in user profiles are instantly reflected in the Access System's policy enforcement.
- **Integration Services**: Extends Oracle Access Manager capabilities to all your applications. By providing integration points with systems and applications from other vendors, Oracle Access Manager enables out-of-the box integrations with most leading application servers, Web servers, directories, portal servers, system management products, and packaged applications.

Oracle Access Manager Feature Overview

Oracle Access Manager includes a Web-based interface that provides a single point of entry. The Web-based System Console enables administrators to assign and delegate administrative responsibilities and to manage the appearance and behavior of Access and Identity components and applications.

10*g* (10.1.4.0.1) enables you to present static data such as error messages and display names for tabs, panels, and attributes to users in their native language. Unicode UTF-8 encoding enables data transmission and storage in a universal format, as described in Chapter 4, "About Globalization and Multibyte Support". English is the default language and is always installed.

Oracle Access Manager Identity System—Provides delegated administration, user self-service, and real-time change management. For example, you can create, manage, and delete groups in the directory server. You can define a subscription policy for a group, including self-service with no approval needed, subscription with approvals, rule-based subscription, and no subscription allowed.

Administrators can build password management and other functions on top of the Oracle Access Manager identity management system. You can integrate other applications with the primary Identity System components using a single identity management system so that access cards, computer accounts, and payroll functions can all be modified from one identity change function when an employee leaves an organization. Customization and XML-based integration features are included.

End users can search for and view other users and groups, depending on the rights granted to them by an administrator; modify personal information such as phone numbers and passwords; and display organizational information such as floor plans and asset lists.

For details about Identity System components, applications, features, and functions, see Chapter 2, "About the Identity System".

Oracle Access Manager Access System—Stores information about configuration settings and security policies that control access to resources in a directory server that uses Oracle Access Manager-specific object classes. You can use the same directory to store the Access System configuration settings, access policy data, and user data, or you can store this data on separate directory servers.

Administrators can use the Access System to protect Web resources and enterprise resources such as J2EE applications, servlets, Enterprise Java Beans (EJBs), and legacy systems. The Access System also supports both Web (HTTP) and similar types of data in non-Web (non-HTTP) resources. Using the Access System for security administration enforces your company's access security policies for Web applications and content; provides common security measures across multiple Web servers and applications; combines centralized policy creation with decentralized management and enforcement; and enables granular control over security across heterogeneous applications and systems.

For more information about Access System components, features, and functions, see Chapter 3, "About the Access System"

Oracle Access Manager **Integration Services**—Oracle Access Manager integrations exist across multiple operating systems and third-party products to support the heterogeneous nature of most large-enterprise IT environments. The following is only a short list of the integration options Oracle offers:

- Single sign-on integrations
- Portal integrations

- Application server integrations
- Third-party authentication integrations

For more information, see the *Oracle Access Manager Integration Guide*.

In addition, you may also perform the following integrations:

- Real-time integration of multiple directories and user repositories through a single LDAP service using Oracle Access Manager combined with Oracle Virtual Directory. For details, see the *Oracle Access Manager Installation Guide*.
- Integration with an optional Simple Network Management Protocol (SNMP) Agent. This provides data that can be used by SNMP and a Network Management System (NMS) to monitor the status and activity of the Identity and Access Servers resident on the same server host where the agent was installed. To install SNMP, see the *Oracle Access Manager Installation Guide*. For monitoring details, see the *Oracle Access Manager Identity and Common Administration Guide*.

Examples of Oracle Access Manager Use

Oracle Access Manager enables you to change from a perimeter defense model in which you unilaterally block outside access to your resources to a security model based on business rules. You can securely provide business systems and data to employees, customers, and suppliers.

Automated bank tellers (ATMs) provide a useful analogy for the Oracle Access Manager solution. At one time, people had to conduct bank transactions in person. With the advent of ATM technology, banks could move to a self-service model for most transactions. Similarly, Oracle Access Manager enables you to move away from a centralized administration model to a distributed model where you provide data and applications securely over the Internet.

Oracle Access Manager helps your enterprise facilitate delivery of corporate functions to extended groups of employees, customers, partners, and suppliers; maintain a high level of security across applications; enable users and business partners to access the information they need.

For example, suppose that your internal users, your suppliers, and your customers require access to unique data sets. In addition, suppose that you also have common data that everyone should see. Using Oracle Access Manager, your identity-based policies can provide the right levels of access to each group while ensuring that everyone can securely access only the data that they need and that they have the right to access.

Using Oracle Access Manager, it is possible to manage a corporate portal that is open to external business partners. For instance, for a portal that allows customers to order manufacturing materials and equipment, all applications exposed through the portal are protected with one platform (Oracle Access Manager) which grants access rights. Administration of the access policies protecting these resources can be delegated throughout the corporation so that business units, rather than the IT department, make decisions about the customers, suppliers, and partners who are to be given access rights. This is possible even for companies with billions of dollars of revenue and tens of thousands of employees.

Using Oracle Access Manager, it is also possible to grant different types of privileges to different classes of users. For instance, a health-care organization can manage its data so that different groups can view different kinds of data, as follows:

- Health-care plan members can view their health-care information.

- Companies providing health-care services to their employees can manage their health-care plans.
- Doctors and hospitals can view patient information.

An organization can use Oracle Access Manager to aggregate application accounts. For example, financial institutions can configure self-service portals to allow their customers to access different accounts from a single login, including online banking, mortgage information, and insurance.

About Installation

The Oracle Access Manager applications that access sensitive data reside within the firewall. The directory server is isolated so it is not exposed. The only server outside the firewall (or in the DMZ) is a Web server with a WebGate or WebPass installed.

The installation and setup sequence is outlined next and described in detail the *Oracle Access Manager Installation Guide*.

Task overview: Installing Oracle Access Manager

1. Prepare the host machine
2. Install the Identity Server and update the schema with Oracle Access Manager configuration data
3. Install a WebPass
4. Set up the Identity System
5. Install the Policy Manager and policy data, then set up the Policy Manager
6. Install the Access Server
7. Install the WebGate

Non-Production/Test Environments—Oracle Access Manager components may be installed on a single machine. In this case, the machine must be hosting a Web server when you perform installation and setup tasks. Do not install the WebPass in the same directory as the Identity Server. Do install the Policy Manager at the same directory level as a WebPass.

Production Environments—In a production environment, Oracle Access Manager components are usually installed on different machines in your network. For example, a simple deployment may include:

- The Identity Server and Access Server can be installed on separate machines, protected by the firewall. For better performance, the Identity and Access Servers should reside on different hosts.
- The Web servers, WebPass, WebGate, and Policy Manager can reside in the DMZ.

See also the *Oracle Access Manager Installation Guide* and *Oracle Access Manager Deployment Guide*.

Installation Directories for Language-Specific Files

All Oracle Access Manager installations include a directory named \lang, which contains a named subdirectory for each installed language. For example, \lang\en-us contains English-language-specific subdirectories and files and is provided with each installation automatically. When you install a Language Pack (for French or Arabic, for instance), additional language-specific directories are included. For example:

IdentityServer_install_dir\identity\oblix\lang\en-us
IdentityServer_install_dir\identity\oblix\lang\fr-fr
IdentityServer_install_dir\identity\oblix\lang\ar-ar

Your installation will be English only unless one or more Oracle-provided Language Packs are installed. For more information about directories, see Chapter 4, "About Globalization and Multibyte Support".

Looking Ahead

Other chapters in this guide provide a more in depth look at Oracle Access Manager components, applications, functions, features, manuals, and terminology:

- Chapter 2, "About the Identity System", which includes the diagram of a simple installation
- Chapter 3, "About the Access System", which includes the diagram of a simple installation
- Chapter 4, "About Globalization and Multibyte Support"
- Chapter 5, "Overview of 10g (10.1.4.0.1) Behaviors"
- Chapter 6, "Road Map to Manuals"
- Glossary

2

About the Identity System

Identity administration governs how digital identities, groups and organizations are created, maintained, and leveraged throughout an organization. The Oracle Access Manager Identity System provides a full range of identity administration applications and functions that provide a simple, controlled means to change user, role, group, and organization information that dynamically affects access privileges. It is the roles and relationships used by the policies that determine what on-line systems and applications a person can access.

This chapter provides a more in depth look at:

- Key Identity System Features
- Identity System Components, Applications, and Functions
- Identity System Customization

Key Identity System Features

Table 2–1 outlines Identity System administration features. Descriptions follow the table.

Table 2–1 Features and Benefits of the Identity System

Features
■ Centralized user management ■ Group management ■ Organizational entity management ■ Dynamic role-based identity administration ■ Workflow for automating requests and approvals relating to identity data ■ Multi-level delegation of identity administration ■ Self-registration and Self-service for maintaining identity data ■ Data management layer ■ Password management ■ User interface customization ■ Extensive APIs for identity integration ■ Auditing and reporting to provide proof of compliance

The items in the table above are described in greater detail below:

- **Centralized User, Group, and Organization (object) Management**—Enables you to provide different access policies for different people and groups and to manage

organizational entities, such as assets and maps. Information in the Oracle Access Manager Identity System can then be leveraged by the Oracle Access Manager Access System to manage access privileges based on user attributes, group membership, or association with an organizational entity.

- **Dynamic Role-Based Identity Administration**—Provides security that is guided by user identity-based access privileges. For example, a role may include all users or all managers or direct-reports only, and so on.
- **A Customizable Multi-Step Identity Workflow Engine**—Enables you to map and automate business processes, policies, and approvals relating to identity data. For example, you can model your business processes in the Identity System using workflows to:
  - Create, delete, and modify users, groups, and organizations
  - Implement self-registration of users and organizations
  - Subscribe and unsubscribe to groups
- **Multi-Level Delegation of Identity Administration**—Enables you to scale up to millions of users by delegating identity administration activities. Administrators can delegate all or some of the rights they have been granted, and they can choose whether or not to allow their delegates to pass these rights on to others. The tasks that are delegated are specific to the right, the target, and the tree path.
- **Self-Service**—Enables you to implement a secure self-service model for organizational functions such as password change. Users with self-service permissions can manage their own information without the use of a workflow.
- **Self-Registration**—Provides limited access to your system through the initiation and processing of a self-registration workflow.

  For example, you can set up a self-registration workflow such that when a user self-registers, the registration request is forwarded to appropriate people for approval. Upon approval, the user is immediately and automatically granted access to all appropriate resources based on his or her identity attributes.
- **Data Management Layer**—Supports multiple LDAP environments, RDBMS databases, and split-directory profiles. This feature is also known as Data Anywhere and is available with Oracle Virtual Directory. Data Anywhere aggregates and consolidates data from RDBMS and LDAP directories into a virtual LDAP tree. The tree can be managed by the Oracle Access Manager Identity System and used to support authentication and authorization with the Oracle Access Manager Access System. For complete details, see the *Oracle Access Manager Identity and Common Administration Guide*.
- **Password Management Services**—Enables you to specify multiple password policies, constraints on password composition, a configurable password validity period and notification, forced password change, lost password management setup, and password creation/change rules.
- **User Interface Customization**—Provides several methods you can use to change the appearance of Oracle Access Manager applications and control operations, and connect CGI files or JavaScripts to Oracle Access Manager screens. For details, see the *Oracle Access Manager Customization Guide*.
- **Extensive APIs for Identity Integration**—Enables you to gain access and interact with Oracle Access Manager without using a browser, and implement functions and executables triggered by events within Oracle Access Manager. For details, see the *Oracle Access Manager Customization Guide*.

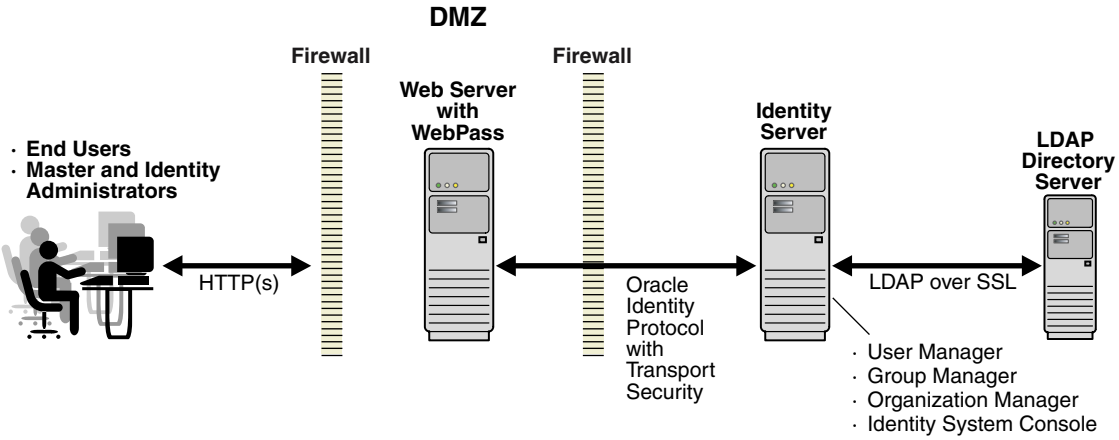
Unless otherwise indicated, you can find more information about these features and how to configure them in the *Oracle Access Manager Identity and Common Administration Guide*. For a simple installation diagram, see the next discussion: "Identity System Components, Applications, and Functions".

Identity System Components, Applications, and Functions

The Oracle Access Manager Identity System provides the infrastructure needed for other applications and systems to leverage user identity and policy information across the enterprise. This eliminates the need to create and manage separate user identity repositories for each application.

Figure 2–1 illustrates the basic Identity System components in a simple environment, as well as transport security between components over the Oracle Identity Protocol (formerly known as the NetPoint or COREid Identity Protocol). The end users and Administrators are separated from components by a firewall. The Web server with WebPass installed resides in the DMZ. The Identity Server and directory server reside behind the second firewall.

Figure 2–1 Components in a Simple Environment



The Oracle Identity Protocol facilitates communication between Identity Servers and associated WebPass instances. Transport security between Oracle Access Manager Web clients (WebPass and Identity Server) may be specified as Open, Simple (Oracle-provided), or Cert (third-party CA). In both Simple and Cert mode, Oracle Access Manager components use X.509 digital certificates only. Transport security between Identity Servers and the directory server may be either open or SSL-enabled.

During Identity System installation and setup, the LDAP directory server is updated to include the Oracle Access Manager schema with object classes and attributes for the entire system. Oracle Access Manager enables you to store various types of data on the same directory server type, or separate directory server types. Data types include:

- **User Data**—User directory entries managed by Oracle Access Manager.
- **Configuration Data**—Oracle Access Manager configuration details stored in the directory and managed by the Identity System.
- **Policy Data**—Access policy definitions defined in the Policy Manager are stored in the directory server.

For more information, see the *Oracle Access Manager Installation Guide*.

Also during Identity System installation and setup, the Master Oracle Access Manager Administrator (Master Administrator) is assigned. The Master Administrator is a super user who is empowered to configure the deployment and assign administrative tasks. Using the System Console, the Master Administrator can create additional Master Administrators, as well as Master Identity Administrators and Master Access Administrators. For example, a Master Identity Administrator can delegate authority to other administrators, which enables management of millions of users.

In addition to managing identity information, you can use the Identity System to manage access privileges for a user based on a specific user attribute, membership in a group, or association with an organization. Administrators can link privileges together into a workflow so that, for example, when a user self-registers, the registration request is forwarded to appropriate people for signoff.

The Identity System is required in all Oracle Access Manager installations and consists of:

- The Identity Server and Identity Applications
- WebPass

The Identity Server and Identity Applications

Your Oracle Access Manager installation must include at least one Identity Server. You use the Identity Server to manage identity information about users, groups, organizations, and other objects. Your installation may include one or more Identity Server instances. The Identity Server performs three main functions:

- Reads and writes to your LDAP directory server across a network connection
- Stores user information on a directory server and keeps the directory current
- Processes all requests related to user, group, and organization identification

Each instance of the Identity Server communicates with a Web server through a WebPass plug-in, as discussed in "WebPass" on page 2-6.

The Identity Server provides the following Identity applications, which are accessed through a Web-based interface. All have a reporting capability:

- **User Manager**—Enables complete management of all identity information related to individual network users.

  The User Manager enables administrators to add, modify, deactivate, and delete user identities. In addition, the User Manager enables administrators to provide users with access privileges based on their directory profiles (and substitute rights), as well as view and monitor requests.

  Typically, end users can view other users and modify their own identity information. The users that a person can view and the identity information that someone can modify depends on the privileges granted by the Master Administrator.

- **Group Manager**—Enables authorized personnel to create, manage and delete static, dynamic, or nested groups or to delegate group administration.

  Administrators can create or delete groups, and enable users to subscribe or unsubscribe from groups.

  End users can view groups and subscribe to membership in a group. The groups that a person can view, and subscription rights, are granted by a Master Administrator.

- **Organization Manager**—Helps you manage system rules, access privileges, and workflows to manage ongoing changes for entire organizations.

  Administrators can create and delete organizations and other objects (such as floor plans and assets) that do not belong in the User Manager or Group Manager.

  End users can view organizational entities. The organizational entities that a person can view depend upon the rights granted by a Master Administrator.

- **Identity System Console**—Provides Web-based administration and configuration that is used to create administrators and assign the right to delegate administrative tasks. Look for the following tabs in the Identity System Console to gain access to specific identity administration functions:

  – ***System Configuration Tab***—Permits you to configure and manage the following functions:

    * Password Policy: For the Oracle Access Manager Identity System
    * Lost Password Policy: For Oracle Access Manager
    * Directory Profiles: Configure separate directory server profiles that each contain information for different parts of the DIT (for directory server partitioning).
    * Identity Servers: Display, add, remove, and modify Identity Server configurations, including audit and logging details
    * WebPass: Display, add, remove, and modify WebPass configurations
    * Server Settings: View and change various Identity Server configuration parameters, including: session timeout, email destinations, mail server settings, and URL prefix cache, and multi-language settings
    * Diagnostics: Select an Identity Server on which to run diagnostics to verify the state of the Identity Servers and their connectivity to the Directory Server.
    * Administrators: View and modify Master Administrators and Master Identity Administrators
    * Styles: Create and deploy a customized style for the user interface
    * Photos: Import custom photograph images for your User Manager User Profiles after assigning the Photo semantic type to any attribute in the gensiteorgperson object class.

  – ***User Manager Configuration Tab***—Enables you to manage and customize Oracle Access Manager User Manager appearance and behavior, including tabs, reports, and auditing policies.

  – ***Group Manager Configuration Tab***—Permits you to manage and customize Oracle Access Manager Group Manager appearance and behavior, and provides the following functions:

    * Tabs
    * Reports
    * Group types
    * Group Manager Options
    * Auditing policies
    * Group cache

- ***Organization Manager Configuration Tab***—Enables you to manage and customize Organization Manager appearance and behavior, including tabs, reports, and auditing policies.
- ***Common Configuration Tab***—Enables you to configure functionality common to Identity applications, including object classes, workflow panels, master audit policy, and global auditing policies.
- ***System Management*** Tab—Eliminated in 10*g* (10.1.4.0.1). In earlier releases this tab provided the Diagnostics function, which now appears on the System Configuration tab.

Administrators access the Identity System Console by entering the following URL in a browser, where *hostname* refers to the machine that hosts the WebPass Web server; *port* refers to the HTTP port number of the WebPass Web server instance; /identity/oblix connects to the Identity System landing page:

http://*hostname:port*/identity/oblix

WebPass

A WebPass is an Oracle Access Manager Web server plug-in that passes information back and forth between a Web server and the Identity Server. Depending upon its configuration, the Identity Server processes the request either as an XML or HTML file.

A WebPass can communicate with multiple Identity Servers. Each Web server instance that communicates with the Identity Server must be configured with a WebPass. In a Oracle Access Manager installation:

- At least one WebPass must be installed on a Web server and configured to communicate with at least one Identity Server.
- A WebPass is required on each machine hosting an Oracle Access Manager Policy Manager.

After installing an Identity Server and a WebPass, you must complete an initial Identity System setup process so the Identity Server and WebPass can communicate.

Process overview: WebPass functions

1. The WebPass receives the user request and maps the URL to a message format.
2. The WebPass forwards the request to an Identity Server.
3. The WebPass receives information from the Identity Server and returns it to the user's browser.

Identity System Customization

Various components and methods are provided to help you customize the Identity System. See also:

- Identity Event Plug-Ins and API
- IdentityXML
- Portal Inserts
- PresentationXML

Identity Event Plug-Ins and API

The Identity Event Plug-in API is a standard component installed with the Identity Server. It is a subset of the Oracle Access Manager Software Developer Kit (also known as the Access Manager SDK). The Identity Event Plug-in API enables you to extend base Identity System functionality by developing your own small applications (called actions) to perform custom business logic and integrate with external systems. The Identity System makes certain data available to the actions, which are then allowed to modify the data and influence the outcome of the event.

For example, when defining a workflow for user creation, you may want to call out to a Human Resources Management System, which in turn creates an account for a user. The new user ID can then be returned to the Identity System.

More information is provided in the *Oracle Access Manager Developer Guide*.

IdentityXML

IdentityXML enables you to access Identity System functionality without a browser. Through IdentityXML, external applications can initiate remote procedure calls that pass arguments to the Identity System.

For example, an external application can initiate batch processing of new users in the Identity System without going through the Identity System browser interface. IdentityXML allows for cross-firewall integration without exposing the directory.

More information on IdentityXML is provided in the *Oracle Access Manager Developer Guide*.

Portal Inserts

Portal inserts are embeddable pieces of Oracle Access Manager Identity System functionality that are available as URLs. You can place a portal insert anywhere on your site or portal to insert content generated by the Identity System into other applications, without programming.

You can, for instance, use the Identity System's searching capabilities to add a company directory search feature to your site or embed a page from the Group Manager into your extranet portal. Users can access this functionality directly from the portal without viewing the standard Identity System interface.

More information about portal inserts is available in the *Oracle Access Manager Customization Guide*.

PresentationXML

PresentationXML enables you to tailor the Identity System user interface. For example, you can:

- Apply your organization's look and feel to the user pages, including color schemes, fonts, button images, and logos.
- Add, modify, or remove functions on a page.
- Create hidden information on a page for the Identity Event API to use.
- Create new pages and functionality.

More information on PresentationXML is provided in the *Oracle Access Manager Customization Guide*.

Looking Ahead

Other chapters in this guide provide a more in depth look at other Oracle Access Manager components, applications, functions, features, behaviors, and terminology. For example:

- Chapter 3, "About the Access System" includes the diagram of a simple Access System installation
- Chapter 4, "About Globalization and Multibyte Support"
- Chapter 5, "Overview of 10g (10.1.4.0.1) Behaviors"
- Chapter 6, "Road Map to Manuals"
- Glossary

3

About the Access System

The Oracle Access Manager Access System is an optional companion to the Oracle Access Manager Identity System. The Access System provides centralized authentication, authorization, and auditing to enable single sign-on and secure access control across enterprise resources. Resources include Web content, applications, services, objects in applications on the Web, and similar types of data in non-Web (non-HTTP) resources.

This chapter provides a more in depth look at:

Key Access System Features

Table 3–1 outlines key access-control features. Details follow the table.

Table 3–1 Access System Features

Features
■ Authentication ■ Authorization ■ Auditing ■ Personalization ■ Single sign-on ■ Delegated access administration

Primary Access System features include authentication, authorization, and auditing (sometimes known as AAA). These features help enforce your company's access security policies for Web applications and content as described in more detail below:

- **Authentication Services**—Provide a generalized means to authenticate users and systems attempting to access resources protected by Oracle Access Manager. Authentication services support both the basic username and password authentication method as well as stronger methods such as digital certificates or SecurID cards.

You can either use standard authentication plug-ins or create your own custom plug-ins using the Authentication Plug-In API. Each custom plug-in implements the authentication interface to pass relevant information between the Access Server and the plug-in. Methods within the interface parse the data. See also "Access System Customization" on page 3-8 and "External Authentication" on page 3-9.

Once a user is authenticated, Oracle Access Manager creates a single-sign-on (SSO) session for the client that frees the user from having to sign on again to access other resources or applications.

- **Authorization Services**—Deliver consistent, centralized management of policies across applications, while providing users granular access to Web-based content and resources. You can secure sensitive information while helping ensure that users and systems have the easy access they need.

  Authorization is governed by a policy domain that includes an authorization expression among a set of default rules that specify how resources for this domain are protected. You can use the authorization scheme provided by the Access System or configure one or more custom schemes that include custom plug-ins created using the Authorization Plug-In API. For details about APIs, see the *Oracle Access Manager Developer Guide*.

  Once authorization is confirmed, the user is granted access to the resource.

- **Auditing Services**—Provide flexible and detailed reporting, auditing, and logging of events in Oracle Access Manager with out-of-the-box reports for Crystal Reports. The auditing and log files enable you to perform threat and intrusion detection, security monitoring, and business-level reporting by integrating with third-party products. Auditing services are global and can be used for Identity System functions as well. For more information about auditing, see the *Oracle Access Manager Identity and Common Administration Guide*.

- **Personalization Services**—Enable personalization for other applications through HTTP header variables and redirection URLs. When Oracle Access Manager authenticates or authorizes user requests, the URL it returns can contain HTTP header variables which in turn can contain any user data stored under the authenticated user's ID in the directory.

  The downstream application can decode this information and use it to personalize the user experience. You can include a redirection URL with the URL returned by Oracle Access Manager, which may take the user to another Web page tailored to the identity of the user.

- **Single Sign-On**—Enables users and groups of users to access multiple applications after a single login and authentication. This improves the user experience by eliminating multiple logins. During a session, a cookie is generated and stored on the user's computer. This cookie eliminates the need for additional logins when users need access to single-domain servers for subsequent requests to the Web site. Users needing access to multi-domain servers have a cookie generated by a central Web login server; this occurs transparently for each accessed server within the associated Web system.

- **Delegated Access Administration**—Enables distribution of administrative tasks. When the responsibility for managing the Access System falls on a few people, you may want these people to appoint others to share the work. For example, you can delegate the ability to modify the revoked user list and to add, modify, or delete configuration details and schemes.

The next discussion provides a sample Access System installation.

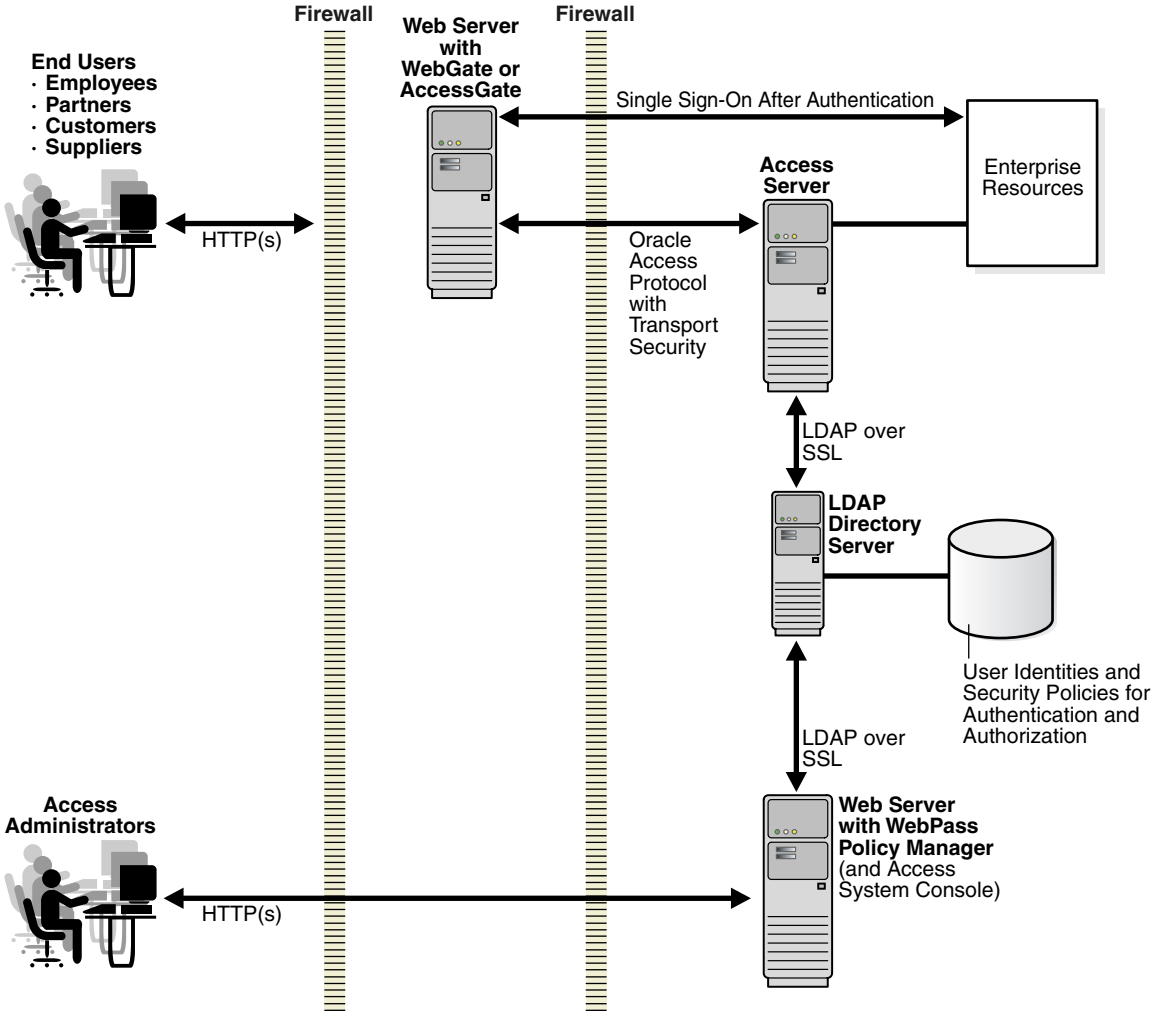
Access System Components and Functions

The Oracle Access Manager Access System enables you to centralize access policy creation while decentralizing policy management and enforcement. The following types of resources can be protected using the Access System:

- HTTP resources including directories, pages, Web-based applications, query strings, and so forth
- J2EE application server resources, including Java server pages (JSPs), servlets, and enterprise Java beans (EJBs)
- Other resources, including standalone programs (Java, C, C++), ERP applications, CRM applications, and the like

Figure 3–1 shows the basic components of the Access System. The WebGate communicates with the Access Server; the Access Server communicates with the directory server; the Policy Manager communicates with the directory server through a WebPass.

Figure 3–1 Basic Access System Installation



The Oracle Access Protocol (formerly known as the NetPoint or COREid Access Protocol) enables communication between Access System components during user

authentication and authorization. Transport security between Oracle Access Manager Web clients (Policy Manager and WebPass; Access Server and WebGate) can be Open, Simple (Oracle-provided), or Cert (third-party CA). In both Simple and Cert mode, Oracle Access Manager components use X.509 digital certificates only.

Transport security between Access Servers and the directory server (and Policy Managers and directory server) may be either open or SSL-enabled. The same mode must be used between all Policy Managers and the directory server.

During Policy Manager installation and setup, the LDAP directory server is updated to include policy data (access policy data). All access policy definitions defined in the Policy Manager are stored in the directory server.

Access System components and operations are discussed in greater detail in the discussions:

- Policy Manager and Access System Console
- The Access Server
- WebGates and AccessGates
- Access System Operation

Policy Manager and Access System Console

This discussion introduces the Policy Manager, Access System Console, and functions available with each.

Policy Manager—Provides a Web-based interface where administrators can create and manage access policies. The Policy Manager also communicates with the directory server to write policy data, and communicates with the Access Server over the OAP to update the Access Server when certain policy modifications are made.

Master Access Administrators and Delegated Access Administrators use the Policy Manager to:

- Create and manage policy domains that consist of:
  - Resource types to protect
  - Authentication, authorization, and audit rules
  - Policies (exceptions)
  - Administrative rights
- Add resources to policy domains
- Test access policy enforcement

The Policy Manager must be installed on a machine hosting a Web server instance with a WebPass (installed at the same directory level as the Policy Manager). Oracle recommends that you install multiple Policy Managers for fault tolerance. For details about installing and setting up the Policy Manager, see the *Oracle Access Manager Installation Guide*.

Access System Console—Included with the Policy Manager installation. The Web-based Access System Console provides a login interface to the tabs and functions that allow any Master Administrator, Master Access Administrator, and Delegated Access Administrator to perform specific operations, including:

- **System Configuration Tab**—Enables a Master Administrator to assign one or more users to be a Master Access Administrator, as well as add or remove Delegated Access Administrators and their rights. Responsibilities of a Master

Access Administrator include defining resource types, policy domains, and authentication and authorization schemes.

From the System Configuration tab, administrators can also view and change server settings. For example, specify email addresses for bug reports, user feedback, and the company Web master.; change the default logout URL for single sign-on; configure directory server settings; view cache settings.

- **System Management Tab**—Enables a Master Administrator to manage:
  - Diagnostics—Show Access Server details, including connection information.
  - Manage Reports—Create, view, or modify user access privilege reports.
  - Manage Sync Records—Archive or purge synchronization records generated by the Policy Manager before a given date. To help manage the space these records consume on the directory server, it is a good idea to periodically archive or purge all the records before a specified date.
- **Access System Configuration Tab**—Enables a Master Access Administrator or Delegated Access Administrator to complete the following tasks:
  - View, add, modify, and delete AccessGates, Access Servers, Access Server clusters, Host Identifiers
  - View and modify authentication and authorization parameters; Web resource user rights; and common information
  - Configure common information, including:

    Shared Secret: Generate a cryptographic key that encrypts cookies to a browser.

    Master Audit Rule: Create the default Master Audit Rule for this installation.

    Resource Type Definitions: Define and manage resource types.

    Flush Password Policy Cache: Select a password policy and flush all associated caches or select a Lost Password Management policy and flush all associated caches.

    Duplicate Actions: Select a policy for handling Duplicate Action Headers

Administrators access the Policy Manager and Access System Console by entering the following URL in a browser, where *hostname* refers to the machine that hosts the WebPass and Web server; *port* refers to the HTTP port number of the WebPass Web server instance; and /access/oblix connects to the targeted Access System.

```
http://hostname:port/access/oblix
```

The Access Server

The Oracle Access Manager Access Server plays a key role in authentication and authorization:

- Authentication involves determining what authentication method is required for a resource and gathering credentials from the directory server, then returning an HTTP response based on the results of credential validation to the access client (WebGate or AccessGate).
- Authorization involves gathering access information and granting access based on a policy domain stored in the directory and the identity established during authentication.

To perform these operations, you may have one or more standalone Access Server instances that communicate with both the directory server and WebGate. Before you can install an Access Server instance, you must define it in the Access System Console.

> **Note:** Oracle recommends that you install multiple Access Servers for failover and load balancing.

Process overview: The Access Server

1. Receives requests from an Oracle Access Manager access client (WebGate or AccessGate)
2. Queries authentication, authorization, and auditing rules in the directory server to determine whether:
   a. The resource is protected (and if so, how)
   b. The user is already authenticated (if the user is not yet authenticated, a challenge is provided)
   c. The user credentials are valid
   d. The user is authorized for the requested resource, and under what conditions
3. Responds to the access client as follows:
   a. Sends the authentication scheme
   b. Validates credentials
   c. Authorizes the user
   d. Audits
4. Manages the session, by:
   a. Helping the WebGate terminate user sessions
   b. Re-authenticating when there is a time out
   c. Tracking user activity during a session
   d. Setting session timeouts for users

WebGates and AccessGates

Throughout Oracle Access Manager manuals, the terms AccessGate and WebGate may be used interchangeably. However, there are differences worth noting:

- A WebGate is a Web server plug-in access client that intercepts HTTP requests for Web resources and forwards them to the Access Server for authentication and authorization. A WebGate is shipped out-of-the-box with Oracle Access Manager.
- An AccessGate is a custom access client that is specifically developed using the Software Developer Kit (SDK) and Oracle Access Manager APIs, either by you or by Oracle. An AccessGate is a form of access client that processes requests for Web and non-Web resources (non-HTTP) from users or applications. For more information, see "Custom Access Clients" on page 3-8.

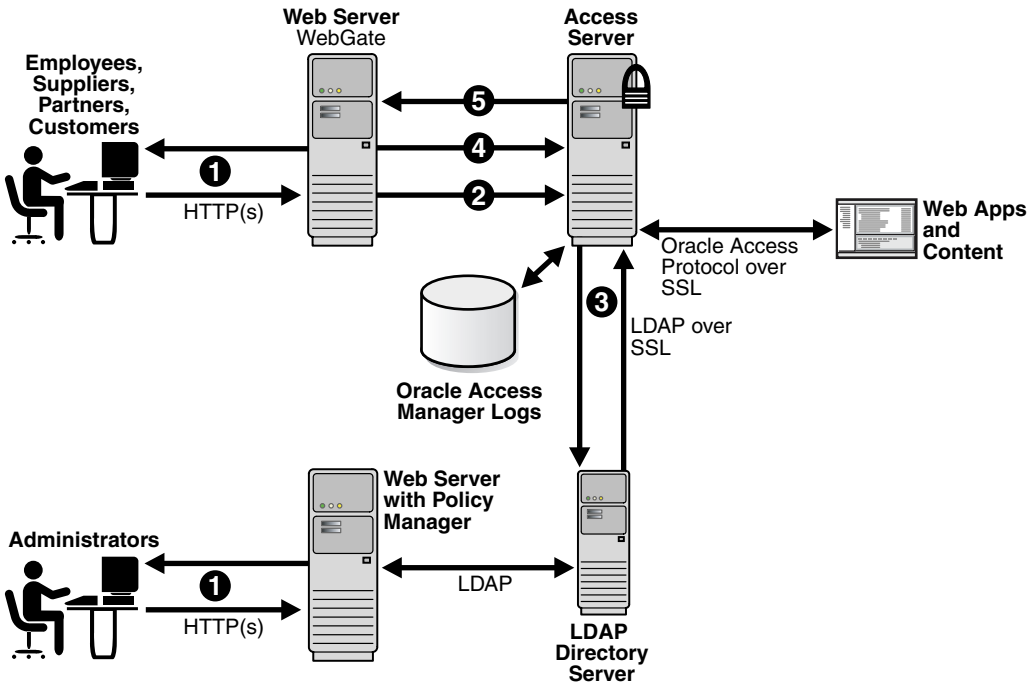
A WebGate intercepts requests for resources from users or applications and forwards requests to the Access Server for authentication and authorization. See "Access System Operation" on page 3-7 for more information.

Before you can install a WebGate, you must define it in the Access System Console and associate it with an Access Server or cluster of Access Servers. For details, see *Oracle Access Manager Installation Guide*.

Access System Operation

Figure 3–2 illustrates how Access System components work in concert during authentication and authorization. A description follows the figure.

Figure 3–2 Basic Access System Operations



Process overview: When a user requests access

1. The WebGate intercepts the request.

   Servers that can be protected include Web servers, application servers, and FTP servers (using the Oracle Access Manager SDK), among others.

2. The WebGate forwards the request to the Access Server to determine whether the resource is protected, how, and if the user is authenticated (if not, there is a challenge).

3. The Access Server checks the directory server for credentials such as a user ID and password, sends the information back to WebGate, and generates an encrypted cookie to authenticate the user.

   The Access Server authenticates the user with a customer-specified authentication method to determine the identity, leveraging information stored in the directory server. Oracle Access Manager authentication supports any third-party authentication method as well as different authentication levels. Resources with varying degrees of sensitivity can be protected by requiring higher levels of authentication that correspond to more stringent authentication methods.

4. Following authentication, the WebGate prompts the Access Server to look up the appropriate security policies, compare them to the user's identity, and determine the user's level of authorization.
   - If the access policy is valid, the user is allowed to access the desired content or applications.
   - If the policy is false, the user is denied access and redirected to another URL determined by the organization's administrator.

As mentioned earlier, the Policy Manager communicates with the directory server to write policy data, and communicates with the Access Server over the OAP to update the Access Server when you make certain policy modifications. The WebPass intercepts and forwards administrator requests for the Policy Manager.

Access System Customization

Various components and methods are provided to help you customize the Oracle Access Manager Access System, including:

- Custom Access Clients
- Custom Authentication and Authorization Plug-ins
- Access Manager API
- Policy Manager API
- Software Developer Kit

Custom Access Clients

AccessGates are custom-built Access Server clients (or agents) that process user requests for access to resources within the LDAP domain protected by Oracle Access Manager. The code for processing user requests can be embedded in a plug-in or written as a standalone application.

An AccessGate uses an Access Server to control attempts to access a Web site. AccessGates allow you to extend authorization and authentication rules to other resources in addition to URLs and to control user interaction with applications outside of Oracle Access Manager. This provides you with centralized policy information that applies to Web and non-Web resources.

For more information about AccessGates, see the *Oracle Access Manager Developer Guide*. See also "Access Manager API" on page 3-9.

Custom Authentication and Authorization Plug-ins

You can either use the standard authentication and authorization plug-ins that are installed with the product, or create your own custom plug-ins using the Oracle Access Manager Authentication Plug-In API and Authorization Plug-In API. Each custom plug-in implements the appropriate interface (authentication or authorization). Depending on the plug-in, the interface is activated to pass relevant information between the Access Server and the plug-in. Methods within the interface parse the data.

Custom plug-ins can be developed using the C language and C# (.NET managed code) Authentication Plug-In API and Authorization Plug-In API.

Access Manager API

The Access Manager API is a subset of the Software Developer Kit. You can use the Access Manager API to write custom access client code in any of the four supported development languages to integrate with Java, C and C++, and C# (.NET) applications. The four implementations are functionally equivalent even though each takes advantage of platform-specific features to implement the API.

For more information, see "Custom Access Clients" on page 3-8.

Policy Manager API

You can use the Policy Manager API (a subset of the Access Manager SDK) to create and manage policy domains and their contents and to allow custom applications to access the authentication, authorization, and auditing services of the Access Server. For example, you can write applications that use the programmatic interface instead of the GUI to create, modify, delete, and retrieve policy domains and their contents.

To better understand the functions provided by the Policy Manager (and Policy Manager API), explore the Policy Manager GUI and see information in the *Oracle Access Manager Access Administration Guide*.

The Policy Manager API provides Java, C, and managed code bindings for classes which you can use to instantiate specific objects. For more information, see *Oracle Access Manager Developer Guide*.

Software Developer Kit

The Oracle Access Manager Software Developer Kit is an optional component that must be installed independently. It provides libraries, build instructions, examples and resources for Access System APIs for each of the supported development platforms. Using the APIs, you can construct interfaces that can be built into commercially available application servers such as IBM WebSphere, Sun, or another application that can access the Access Server for authentication and authorization.

Individual Access System APIs are introduced in this chapter. For details about the Software Developer Kit and all APIs, see the *Oracle Access Manager Developer Guide*.

External Authentication

Oracle Access Manager external authentication enables you to integrate multiple security systems across corporate boundaries through trust and technology relationships.

After installation, Oracle Access Manager must be configured to trust an external SSO solution for authentication. During authentication runtime, identity information provided by the third-party authentication mechanism is accepted and mapped to the appropriate user being authorized by Oracle Access Manager.

For details about external authentication mechanisms, see the *Oracle Access Manager Access Administration Guide* and the *Oracle Access Manager Integration Guide*.

Federated Authentication

The term *federation* is derived from the Latin word for trust. When used in the context of security management, federation essentially means integrating multiple security systems together through trust and technology relationships. Federated authentication enables you to integrate multiple security systems across corporate boundaries.

For details about external authentication mechanisms supported by Oracle Identity Federation, see the *Oracle Identity Federation Administrator's Guide*.

Looking Ahead

Other chapters in this guide provide a more in depth look at concepts, behaviors, manuals, and terminology:

- Chapter 4, "About Globalization and Multibyte Support"
- Chapter 5, "Overview of 10g (10.1.4.0.1) Behaviors"
- Chapter 6, "Road Map to Manuals"
- "Glossary"

4

About Globalization and Multibyte Support

This chapter introduces Oracle Access Manager 10*g* (10.1.4.0.1) globalization, localization for international languages, and multibyte support through the use of Unicode to enable processing of internationalized data. The following topics are included:

Oracle Access Manager Globalization and Localization

Oracle Access Manager 10*g* (10.1.4.0.1) has undergone a globalization process. Globalization means providing multi-lingual applications and software products that can be accessed and run anywhere simultaneously, without modification, while rendering content in the native user's language and locale preferences.

A locale is the linguistic and cultural environment in which a system or program is running; data associated with a locale provides support for formatting and parsing of dates, times, numbers, currencies, and the like based on the linguistic and cultural requirements that corresponds to a given language and country.

Oracle product globalization is a two part process that includes internationalization and localization. *Internationalization* (sometimes shortened to "I18N", meaning "I - eighteen letters -N") requires that software products and applications must be usable on a machine running any supported operating system (in any supported language), with non-US keyboards or other country-specific hardware. Oracle applications do not have hard-coded dependencies on language strings, and inter-operate with non-US versions of other products. Oracle applications can handle multibyte characters and differences in a distributed environment, as well as being able to detect the user's desired locale. Oracle Access Manager10*g* (10.1.4.0.1) meets these requirements and conforms to Unicode Standard 4.0 discussed in "Oracle Access Manager and the Unicode Standard" on page 4-3.

Localization includes translation of separated file text. In Oracle products, including Oracle Access Manager, information is presented in a manner that is consistent with the user's local cultural conventions, including data formatting, collation, currency, date, time, and directionality of text (right-to-left or left-to-right), as discussed next.

Languages For Localized Messages in Oracle Access Manager

Translatable information can be categorized into two types: end-user information (accessible to all users) and administrative information (for users with administrator privileges). When you install Oracle Access Manager 10*g* (10.1.4.0.1) without a Language Pack, English is the default language for Administrators and end users. When you install 10*g* (10.1.4.0.1) with Oracle-provided Language Packs, you can choose the language to be used as the default for Administrative activities. Regardless of the default Administrator language you choose during installation, English is always installed.

For end-users, Oracle Access Manager10*g* (10.1.4.0.1) enables the display of static application data such as error messages, and display names for tabs, panels, and attributes in the End Users languages identified in Table 4–1. Administrative information can be displayed in only the Administrators languages listed in Table 4–1. If administrative pages are requested in any other language (by the browser setting), the language that was selected as the default during product installation is used to display the pages.

Table 4–1 Languages for Localized Messages in Oracle Access Manager

Language Tag for Installation Directory	End User Information	Administrators
en-us	English	English
ar-ar	Arabic	
pt-br	Brazilian Portuguese	Brazilian Portuguese
fr-ca	Canadian French	Canadian French
cs-cs	Czech	
da-dk	Danish	
nl-nl	Dutch	
fi-fi	Finnish	
fr-fr	French	French
de-de	German	German
el-gr	Greek	
he-il	Hebrew	
hu-hu	Hungarian	
it-it	Italian	Italian
ja-jp	Japanese	Japanese
ko-kr	Korean	Korean
es-mx	Latin American Spanish	Latin American Spanish
no-no	Norwegian	
pl-pl	Polish	
pt-pt	Portuguese	
ro-ro	Romanian	
ru-ru	Russian	
zh-cn	Simplified Chinese	Simplified Chinese
sk-sk	Slovak	

Table 4–1 (Cont.) Languages for Localized Messages in Oracle Access Manager

Language Tag for Installation Directory	End User Information	Administrators
es-es	Spanish/Spain	Spanish
sv-sv	Swedish	
th-th	Thai	
zh-tw	Traditional Chinese	Traditional Chinese
tr-tr	Turkish	

Bi-directional Language Support

Most Western languages are written left to right (LTR), from the top of the page to the bottom. East Asian languages are usually written top to bottom, from the right side of the page to the left (RTL)—although exceptions are frequently made for technical books translated from Western languages.

Some languages, such as Hebrew and Arabic, are written and read predominantly from right to left. Numbers reverse direction in Arabic and Hebrew. While the text is written right to left, numbers within the sentence are written left to right with the most significant digit on the left, as in European and other LTR languages.

When LTR languages are mixed in with RTL languages, the complete document or content is considered *bi-directional*. Oracle Access Manager can support bi-directional languages. If the browser on the host machine is configured to use any bi-directional language, then Oracle Access Manager will handle it properly.

Note: No administrative languages require bi-directional support.

To provide support for multiple languages and bi-directional languages, Oracle Access Manager 10*g* (10.1.4.0.1) supports the Unicode standard for encoding.

Note: Writing direction does not affect the encoding of a character. Regardless of the writing direction, Oracle stores data in logical order—the order used by someone typing a language—rather than the order in which it is presented on the screen.

Oracle Access Manager and the Unicode Standard

Oracle Access Manager 10*g* (10.1.4.0.1) supports the Unicode standard, which has been adopted by many software and hardware vendors. Many operating systems and browsers now support Unicode, and Unicode is required by modern standards such as XML, Java, JavaScript, LDAP, CORBA 3.0, WML, Windows XP, and others. The Unicode standard is also synchronized with the ISO/IEC 10646 standard.

Computers represent all characters as numbers. A character set is the mapping of individual characters to binary values. This mapping is also known as an encoding scheme. There are dozens of different encoding schemes for characters.

Unicode is a universal encoding scheme that defines codes for characters that are used in every major contemporary language written today. Unicode enables information from any language to be stored using a single character set. The Unicode standard assigns a distinct numeric value, called a codepoint, to each character and organizes

characters into blocks of related characters. Unicode codepoints are commonly expressed in hexadecimal form. Unicode provides a unique code value for every character whatever the platform, program, or language.

The Unicode standard primarily encodes scripts rather than languages. A script is a collection of symbols used in one or more related languages. When more than one language shares a set of symbols that have an historically-related derivation, the set of symbols of each such language is unified into a single collection identified as a single script. For example, the Cyrillic script is a superset of all the characters used by the different Cyrillic alphabets.

As with many technologies, Unicode has more than one implementation standard: fixed-width UCS-2 form (or its superset UTF16) and the reasonably compact, variable-width UTF-8 form used by Oracle.

Note: The canonical UCS-2 form (used internally in Windows NT, for example), uses 2 bytes for each character (including ASCII characters).

UTF-8 Encoding

Oracle products, including Oracle Access Manager 10*g* (10.1.4.0.1), support UTF-8 encoding. Incoming data uses UTF-8 encoding. Outgoing text, such as the HTML pages and information from Oracle Access Manager, use UTF-8 encoding. This means that outgoing characters are displayed in the appropriate language (LTR, RTL, or bi-directional), as needed.

Note: Earlier releases of Oracle Access Manager supported only the Latin-1 encoding standard, as discussed in "Oracle Access Manager and Latin-1 Encoding" on page 4-5. With 10*g* (10.1.4.0.1), Unicode is provided in new installations while backward compatibility is provided for customizations in older installations that have been upgraded to 10*g* (10.1.4.0.1). For more information, see Chapter 5, "Overview of 10g (10.1.4.0.1) Behaviors".

Most modern character encodings have an historical grounding in ASCII, which is the most common format for text files in computers and on the Internet. In an ASCII file, each alphabetic, numeric, or special character is represented with a 7-bit binary number. Unix and DOS-based operating systems use ASCII for text files. Windows NT, 2000, and XP use Unicode.

UTF-8 is the Unicode 8-bit encoding standard, which is a strict superset of 7-bit ASCII. This means that each 7-bit ASCII character is available in UTF-8 with the same corresponding codepoint value. While each 7-bit ASCII character occupies 1 byte, each UTF-8 codepoint value generates a bit pattern that is distributed over one to four bytes. This means that in UTF-8 encoding, a single Unicode character can be 1 byte, 2 bytes, 3 bytes, or 4 bytes.

In the UTF-8 form of Unicode supported by Oracle, accented Latin characters as well as Greek, Cyrillic, Arabic, and Hebrew characters occupy 2 bytes each. All other characters, including Chinese, Japanese, Korean, Indian, occupy 3 bytes each. Supplementary characters occupy 4 bytes each.

Oracle Unicode Character Sets

Historically vendors have defined different character sets for their hardware and software, primarily because there were no official standards. Different character sets support different character inventories (known as repertoires). When character sets were first developed, they had limited repertoires. For example the ASCII 7-bit character set provided only 128 symbols and the Unix ROMAN8 8-bit character set provided only 256 symbols. UTF8 an older multibyte character set developed by Oracle is based on an older Unicode standard.

Unicode (UTF-8) is a multibyte character set with the capability to define over a million characters. Because character sets are typically based on a particular writing script, one character set can support more than one language.

The Oracle equivalent for the Unicode UTF-8 standard is the AL32UTF8 character set. The code used to process this character set resides within the libraries bundled with each Oracle Access Manager component and installed automatically with the product.

Oracle Access Manager 10*g* (10.1.4.0.1) uses the AL32UTF8 character set to process all data. Data coming in to Oracle Access Manager is UTF-8 encoded. Outgoing data is UTF-8 encoded.

Background on Oracle AL32UTF8 and Other Oracle Character Sets

The following information is provided for information only:

- Oracle AL32UTF8 and UTF8 Character Sets
- Older Oracle Unicode Character Sets

Oracle AL32UTF8 and UTF8 Character Sets

With Oracle9*i* Oracle introduced the Unicode character set, AL32UTF8 with enhancements based on Unicode standard 3.0. Starting with the Oracle 10*g* Release 2 (10.1.2) AL32UTF8 maps to the latest version of the Unicode Standard (Unicode 4.0) and provides support for newly defined supplementary characters. All supplementary characters are stored as 4 bytes. As the UTF-8 standard evolves, so too will the AL32UTF8 character set.

With Oracle8 and 8*i*, Oracle introduced UTF8 as the UTF-8 encoded character set (based on Unicode version 2.1). Oracle9*i* included an updated version of the Oracle UTF8 character set to support Unicode standard 3.0. To maintain compatibility with existing installations, the UTF8 character set will remain at Unicode version 3.0.

Older Oracle Unicode Character Sets

Oracle began supporting Unicode as a database character set starting with Oracle database version 7. AL24UTFFSS was the first Unicode character set supported by Oracle. AL24UTFFSS is an acronym for the multibyte Unicode character encoding scheme UTF-FSS. The naming convention <Language><bit size><encoding> was used, where AL24UTFFSS represents *All Languages 24 bits size UTFFSS* encoding. AL24UTFFSS was based on Unicode standard 1.1, which is now obsolete. AL24UTFFSS support was dropped as of Oracle9*i*.

Oracle Access Manager and Latin-1 Encoding

Earlier releases of Oracle Access Manager supported only Latin-1 encoding, which allowed the product to process a subset of European languages.

Latin-1 encoding was developed jointly by the International Organization for Standardization (ISO, which is not an acronym) and the International Electrotechnical Commission (IEC). This 8-bit character encoding standard for computers is known formally as ISO/IEC 8859 and informally as ISO 8859. The standard is divided into numbered parts; each part is published separately. Part 1 (also known as ISO 8859-1) is the most widely used and encompasses Latin-1 encodings.

ISO 8859-1 (Latin-1) encodings can be represented in a single byte (8-bits) in computer memory and enable support for various Western European languages, such as English, French, German (and some other Western European languages), Eastern European languages (Albanian), as well as Afrikaans and Swahili.

ISO-8859-1 is the default encoding used for legacy HTML documents and for documents transmitted through MIME messages, such as HTTP responses when the document's media type is "text" (for example, "text/html").

The eight-bit ISO-8859 standard was developed as a true extension of ASCII. ISO 8859-1 Latin-1 leaves the original ASCII character-mapping intact and adds additional values greater than the 7-bit range. ISO/IEC 8859-1 and the original 7-bit ASCII remain the most common character encodings in use today.

Backward compatibility is automatic in upgraded environments and Latin-1 encoding remains the default in older installations that you upgrade to 10*g* (10.1.4.0.1).

Note: When you add a 10*g* (10.1.4.0.1) Identity or Access Server to an upgraded environment, you must manually set flags to enable backward compatibility. For details, see Chapter 5, "Overview of 10g (10.1.4.0.1) Behaviors".

Looking Ahead

Other chapters in this guide provide a more in depth look at concepts, behaviors, manuals, and terminology:

- Chapter 5, "Overview of 10g (10.1.4.0.1) Behaviors"
- Chapter 6, "Road Map to Manuals"
- Glossary

5

Overview of 10*g* (10.1.4.0.1) Behaviors

This chapter provides a brief summary of Oracle Access Manager 10*g* (10.1.4.0.1) behaviors and mentions earlier behaviors (if those were different).

> **Note:** 10*g* (10.1.4.0.1) refers to any Oracle Access Manager release in the 10.1.4 series (for example, 10.1.4.0.1 and 10.1.4.0.2 when that becomes available).

Topics include:

- General Behavior Summary
- Identity System Behavior Summary
- Access System Behavior Summary

> **Note:** Complete details of all features are presented throughout the suite of Oracle Access Manager manuals. For a list of new functions in 10*g* (10.1.4.0.1), see "What's New in Oracle Access Manager?" on page -xi. Also, see "Product and Component Name Changes" on page -xi.

General Behavior Summary

A number of earlier product behaviors have changed to support product globalization. In addition, new features have been added and changes have been made to improve product usability and performance.

If you have upgraded an earlier installation to Oracle Access Manager 10*g* (10.1.4.0.1), some backward compatibility is enabled during the upgrade and some manual processing must occur. For more information about upgrading, see the *Oracle Access Manager Upgrade Guide*, which includes details about components and third-party products that are no longer supported.

To ensure that you always have the most up to date information, support details are not presented in manuals. For the latest platform and support information, be sure to see the Certify tab at `https://metalink.oracle.com`.

To use Metalink

1. Navigate to `http://metalink.oracle.com`.
2. Log in to 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 Application Server and click Submit.

Whether you install the Identity System alone or include the Access System, Table 5–1 briefly summarizes overall Oracle Access Manager 10*g* (10.1.4.0.1) behaviors.

Table 5–1 General Oracle Access Manager Behavior Summary

Function	Behavior
Acquiring and Using Multiple Languages	Early product releases provided messages for end users and administrators in only the English language. Starting with release 6.5, support for translatable messages was provided through Language Packs for certain Latin-1 languages (French and German). Oracle Access Manager 10*g* (10.1.4.0.1) provides support for nearly a dozen Administrator languages and over two dozen end-user languages, as described in Chapter 4, "About Globalization and Multibyte Support". When you install the product without a Language Pack, only English is available. Administrative information can be displayed in the Administrators languages listed in Table 4–1 only. When installing components with Oracle-provided Language Packs, you can choose the language (locale) to be used as the default for administrative tasks. If administrative pages are requested in any other language (based on browser settings), the language that was selected as the default during product installation is used to display the pages. See the *Oracle Access Manager Installation Guide* for installation details. After installing Oracle Access Manager with Oracle-provided Language Packs, you must enable all languages to be used, then configure Oracle Access Manager to use the installed languages by entering display names for attributes, tabs, and panels as described in the *Oracle Access Manager Identity and Common Administration Guide*. Messages in Oracle Access Manager stylesheets depend upon a language. Beginning with release 6.5, messages have been brought out of the stylesheets and defined separately as variables in msgctlg.xsl (and msgctlg.js for JavaScript files). In addition, each stylesheet has a corresponding language-specific thin wrapper stored in *IdentityServer_install_dir*\identity\oblix\lang\langTag\style0 to segregate the main functionality of the stylesheet template from language-specific messages in the stylesheets. For more information, see the *Oracle Access Manager Customization Guide*.
Auditing and Access Reporting	To support all available languages, definitions of oblix_audit_events, oblix_rpt_as_reports, oblix_rpt_as_resources, and oblix_rpt_as_users tables have changed. For details, see the *Oracle Access Manager Identity and Common Administration Guide*. The Crystal Reports package is no longer provided with the Oracle Access Manager package. You must obtain this product from the vendor. You can now audit to an Oracle Database as well as to Microsoft SQL Server. Support for MySQL is deprecated in this release. When configuring Audit Policies in the Identity System Console, you can specify a list of profile attributes for every audit record. Profile attributes (Full Name, Employee Number, Department Number, and the like) are specific to the user performing the action/event being audited (Search or View Profile or Modify Profile, for example). The purpose of profile attributes is to help you identify the user performing the action/event. **Warning**: To avoid exposing a challenge phrase or response attribute, Oracle recommends that you do not select these as profile attributes for auditing. If you add a challenge phrase or response as a profile attribute, it is audited in proprietary encoded format. Before auditing in an environment you upgraded to 10*g* (10.1.4.0.1), you must retain the original database and data, create a new database instance for use with 10*g* (10.1.4.0.1), generate new tables, and import earlier data before you start auditing (this last item is a must only if you want to query/generate reports using both old and new data), as described in the *Oracle Access Manager Upgrade Guide*.
Automatic Schema Update Support for ADAM	Removed due to an ldifde.exe tool licensing issue. For ADAM, the schema must be updated manually, as described in the *Oracle Access Manager Installation Guide*.
C++ Programs	When upgrading from releases earlier than 7.0, you may need to recompile C++ programs created with the Software Developer Kit and APIs after the upgrade. See other topics in this chapter for an overview of the impact on Identity System event plug-ins; Access Manager SDK, Access Manager API, and custom AccessGates; and custom authentication and authorization plug-ins and interfaces. See also, the *Oracle Access Manager Developer Guide*.

Table 5–1 (Cont.) General Oracle Access Manager Behavior Summary

Function	Behavior
Cache Flush	A 10*g* (10.1.4.0.1) Identity Server cannot flush the cache of an earlier Access Server, which impacts environments that you upgrade. To eliminate problems, you must upgrade the Access Server to 10*g* (10.1.4.0.1). If you install a new Access Server, ensure that it is backward compatible. See information on the Access Server in Table 5–3.
Certificate Store and Localized Certificates	You can request and add localized certificates containing non-ASCII text in all fields except Email and Country (per x509 standards). Starting with release 7.0 and continuing with 10*g* (10.1.4.0.1), the default certificate store format and name has changed to cert8.db. When you upgrade to 10*g* (10.1.4.0.1), the old certificate store is used. 10*g* (10.1.4.0.1) works with both the cert7.db (upgraded environments) and cert8.db (new installations) certificate store. Generating a new certificate store occurs transparently whenever you add, modify, or delete certificates using configureAAAServer, setup_ois, or setup_accessmanager utilities. For more information, see the *Oracle Access Manager Identity and Common Administration Guide*.
Compilers for Plug-ins	Starting with release 7.0, components on Solaris and Linux are compiled using the GCC v3.3.2 C++ compiler to address multi-threading issues encountered with earlier compiler releases. After upgrading to 10*g* (10.1.4.0.1), you must recompile custom plug-ins from release 5.x or 6.x using the GCC v3.3.2 C++ compiler available from your vendor. This includes Identity Event plug-ins and custom authentication and authorization plug-ins. For details, see the *Oracle Access Manager Upgrade Guide*.
Configuration Files	Earlier releases of Oracle Access Manager managed certain information (including but not limited to directory connection information and WebGate parameters) solely through XML and LST configuration files. Release 10*g* (10.1.4.0.1) provides the ability to manage this information through the Identity System Console and Access System Console. See also "Directory Server Connection Details" (in this table) and "WebGates" (in Table 5–3, " Access System Behavior Summary").
Connection Pool Details	Starting with release 7.0, connection pooling was consolidated to support failover across the entire system. The directory connection pool does not depend on directory type. There is some impact when upgrading (depending on the configuration of your earlier installation to each directory server that is configured). See the topic on directory server failover in this table. For more information, see the *Oracle Access Manager Upgrade Guide* and *Oracle Access Manager Deployment Guide*.
Console-based Command-Line Interfaces	Oracle Access Manager command-line tools have been modified to automatically detect the server locale and use it for processing. To override the server locale you may set either the COREID_NLS_LANG or NLS_LANG environment variables to toggle auto-detection off and take precedence over the server locale. For details, see the *Oracle Access Manager Installation Guide*. When set, NLS_LANG takes precedence over LANG and COREID_NLS_LANG takes precedence over NLS_LANG.
Customized Styles	Product functionality depends, in part, on stylesheet files in the latest \style0 and \shared directories. Starting with Oracle Access Manager release 6.5, to support multiple languages the location of JavaScript, stylesheets, and images changed. The directory structure introduced with release 6.5 continues with 10*g* (10.1.4.0.1). For general information about stylesheets and customization, see the *Oracle Access Manager Customization Guide*. Customized .XSL style files, images, and JavaScript files are not migrated during an upgrade. If files in your earlier Oracle Access Manager \style0 directory were customized, you must manually edit the newer version files in \style0 and \shared directories after the upgrade. For more information, see the discussion on incorporating custom items in the *Oracle Access Manager Upgrade Guide*.

Table 5–1 (Cont.) General Oracle Access Manager Behavior Summary

Function	Behavior
Database Input and Output	Oracle Access Manager 10*g* (10.1.4.0.1) supports the Unicode character set. In new installations, Oracle recommends that you choose a Unicode character set for your database. For more information, see Chapter 4, "About Globalization and Multibyte Support". Earlier Oracle Access Manager releases used the Latin-1 character set. As a result the varchar type for the columns of audit and reporting related tables was sufficient. 10*g* (10.1.4.0.1) supports an internationalized character set. As a result, the audit record may contain data with non Latin-1 characters (Chinese, Japanese, Arabic, and the like). For more information, see details about auditing and access reporting in this table.
Date and Time Formats	In the 10*g* (10.1.4.0.1) Identity System, the date format remains the same as in the last release and is not internationalized (on the Diagnostics page and Ticket Information page for example). However, month names taken from Identity System message catalogs are displayed in the locale specified by the browser. As in earlier releases, date order formats (MM/DD/YYYY versus DD/MM/YYYY and the like) can be configured by modifying object class attributes in the Identity System Console as described in the *Oracle Access Manager Identity and Common Administration Guide*. On the Ticket Information page, the date is displayed in the format specified in the `obDateType` parameter in the globalparams.xml file. Weekday names do not appear anywhere within the Identity System. In the Access System, month names, the date-order format (MM/DD/YYYY versus DD/MM/YYYY), and weekday names are displayed according to the locale specified for the browser. In the Access System, month and weekday names are not taken from message catalog files.
Default Product Page	As in earlier releases, there can be only one static HTML page at the address /identity/oblix/index.html and one static HTML page at the address /access/oblix/index.html. These static product pages always use the default Administrator language selected during Identity Server and Policy Manager installation at this location. Starting with release 6.5, the product supported multiple Latin-1 languages (French, German). The default product page behavior remains the same as in earlier releases. See also information about HTML pages later within this table.
Directory Profiles and Database Instance Profiles	In earlier releases, the Identity System included directory profiles and database instance profiles. A directory profile (also known as a directory server profile) contains the connection information for one or more directory servers that share the same namespace and operational requirements for Read, Write, Search, and so on. The connection information includes a name, a domain or namespace to which it applies, a directory type, and a set of operations. Starting with release 6.5, the Access System began partially using directory profiles and database instance profiles for accessing user data. Also, these directory profiles replace the UserDB.lst, GroupDB.lst, UserDBFailover.lst, and GroupDBFailover.lst configuration files that were used in earlier Access System releases. In 10*g* (10.1.4.0.1), a directory profile is created automatically each time you install an Identity Server, Policy Manager, or Access Server and specify new directory server connection information. You can create additional directory server profiles for load balancing and failover after installation. When you upgrade an earlier Policy Manager or Access Server, a message appears during the incremental upgrade to release 6.5. The message "DB Profiles created" refers to the directory server profile that is created. See also information on connection pools, earlier in this table.
Directory Server Connection Details vs. XML Files	Earlier releases managed directory connection information solely through XML configuration files. Recently, Oracle Access Manager provided the ability to manage this information through the interface using the Directory Profile page in the Identity System Console and the Access System Console. However, some configuration and policy data is still managed through XML files.

Table 5–1 (Cont.) General Oracle Access Manager Behavior Summary

Function	Behavior
Directory Server Failover	Your earlier implementation may include failover between an Oracle Access Manager server and the directory server. Following data upgrades, the Access Server handles multiple directory servers using directory profiles that are automatically created during the upgrade between release 6.1.0 and 6.5. After upgrading, it is a good idea to verify that the failover configuration you had in the earlier release operates as expected as described in the *Oracle Access Manager Deployment Guide*. See also information on connection pool details mentioned earlier in this table, and information about message and parameter .lst files that are transformed into .xml files.
Directory Server Interface	The 10*g* (10.1.4.0.1) directory server interface reads, processes, and stores data using UTF-8 encoding.
Directory Structure	When you install 10*g* (10.1.4.0.1) components, you can name the top-level directory as you like. With each installed component, Oracle Access Manager appends an identifier to the directory name you assign. For example: *IdentityServer_install_dir*\identity *AccessServer_install_dir*\access In each case, a directory named \oblix\oracle\nlstrl is created after the automatic installation of the Oracle National Language Support Library (not available in earlier releases). For more information, see the *Oracle Access Manager Installation Guide*.
Domain Names, URIs, and URLs	10*g* (10.1.4.0.1) supports ASCII characters only for domain names, URIs, and URLs. This is the same as in earlier releases. There is no support for internationalized characters.
Encryption Schemes	Cookies are encrypted using a configurable encryption key known as a shared secret. In release 5.x, the RC4 encryption scheme was recommended for shared secret keys. In release 6.x, the RC6 encryption scheme was recommended. Starting with release 7.0, AES became the default Access System encryption scheme. For more information, see shared secret details later in Table 5–3 and the *Oracle Access Manager Access Administration Guide*. The Identity System continues to use RC6 encryption for Lost Password Management responses.
Failover and Failback	Release 7 introduced a heartbeat polling mechanism to facilitate immediate failover to a secondary directory server when the number of connections in the connection pool falls below the specified threshold level. Additionally, a failback mechanism facilitates switching from the secondary directory server back to the primary server as soon as the preferred connection has been recovered. The heartbeat feature polls the primary directory server connections periodically to verify the availability of the directory service (and by implication, the network). When the host cannot be reached, further attempts to connect to that host are blocked for the specified Sleep For interval, rather than for the TCP timeout used previously. If the directory service is not available, the heartbeat mechanism immediately initiates failover to the secondary directory server. Thus, failover can take place without being triggered by an incoming directory service request and a subsequent TCP timeout. A new parameter in globalparams.xml determines the timeout interval for establishing a connection. In situations where the enterprise network performance is poor, the heartbeat feature can trigger false alarms and tear down already-established connections. Therefore, the `heartbeat_enabled` parameter in the globalparams.xml enables you to activate or deactivate the heartbeat mechanism in response to current network conditions. By default the heartbeat feature is activated. For more information, see the*Oracle Access Manager Deployment Guide*.
File and Path Names	With 10*g* (10.1.4.0.1) only ASCII characters are supported in file and path names. This is the same as in earlier releases.
Graphical User Interface	A number of changes have been made to improve and clarify the Web-based graphical user interface. The user interface is introduced in the this guide and described throughout the suite of manuals.

Table 5–1 (Cont.) General Oracle Access Manager Behavior Summary

Function	Behavior
HTML Pages	In 10*g* (10.1.4.0.1), all HTML pages generated by Oracle Access Manager use UTF-8 encoding. This encoding is communicated to Web browsers using the Content-Type HTTP header and META tags. See also information about default product pages mentioned earlier in this table.
Message and Parameter Catalogs	Release 10*g* (10.1.4.0.1) includes .XML parameter and message catalog files. The exception to this rule includes files that are used during an upgrade. In 10*g* (10.1.4.0.1), message files reside in specific directories for each installed language. For example: *IdentityServer_install_dir*/identity/oblix/lang/*langTag* /oblixbasemsg.xml. For more information, see the *Oracle Access Manager Customization Guide*.
Minimum Number of Search Characters	In earlier releases, you needed to enter at least three characters when performing a search in Identity System applications. In 10*g* (10.1.4.0.1) there is no minimum number of characters required. As in earlier releases, you can control the minimum number of characters that users must enter in the search field as described in *Oracle Access Manager Customization Guide*.
Names Assigned by Administrators and Product Names	Some product and component names have changed. Certain function names have been made consistent between the Access and Identity Systems as noun phrases. During an upgrade, earlier names are changed to the new name. For more information, see "Product and Component Name Changes" on page -xiii. However, any service names assigned by an administrator during installation or configuration are not changed during an upgrade. Therefore if you have a service named "COREid Server" or "NetPoint Server", these names remain intact after the upgrade. Also, earlier authentication scheme names and policy domain names assigned by an administrator remain unchanged after an upgrade.
Namespaces for Policy Data and User Data Stored Separately	Before release 6.5, the namespaces for policy data and user data stored in two separate directories had to be unique. During an upgrade to 10*g* (10.1.4.0.1) you need to confirm this uniqueness to ensure that multi-language capability can be enabled. For more information, see the *Oracle Access Manager Upgrade Guide*.
Object Classes and Attributes	There have been several schema changes in 10*g* (10.1.4.0.1). for more information, see *Oracle Access Manager Schema Description*.
Password Policies and Lost Password Management	This release contains password policy and password management enhancements. You can configure the minimum and maximum number of characters users can specify in a password. For lost password management, you can set multiple challenge-response pairs, create multiple style sheets, and configure other aspects of the user's lost password management experience. You can also redirect users back to the originally requested page after resetting a password. For more information, see the *Oracle Access Manager Identity and Common Administration Guide*.
Reconfiguring the Logging Framework without a Restart	In 10*g* (10.1.4.0.1), you may reconfigure the logging framework without restarting the servers. To do this an administrator must manually update the logging configuration for each component: Identity Server WebPass Policy Manager Access Server WebGate Changes to logging parameters take affect within one minute, rather than requiring you to restart the server where the changes were made. For more information, see the *Oracle Access Manager Identity and Common Administration Guide*.
Support Changes	There have been a number of changes in supported platforms and third-party versions. You can now locate complete platform support details under the Certify tab at `https://metalink.oracle.com`. To use Metalink: ■ Log in to Metalink as directed. ■ Click the Certify tab. ■ Click View Certifications by Product. ■ Select the Application Server option and click Submit. ■ Choose Oracle Application Server and click Submit.

Table 5–1 (Cont.) General Oracle Access Manager Behavior Summary

Function	Behavior
Transport Security for the Directory Server	When you configure SSL mode for the directory server, only server authentication is supported. Client certificates are not supported. Oracle Access Manager verifies the server certificate against the Root CA certificate that you imported during product setup. For more information, see the *Oracle Access Manager Access Administration Guide*.
XML Catalogs and XSL Stylesheet Encoding	For non-English languages, XML message files have encoding set as UTF-8, because ISO-8859-1 encoding cannot represent all characters in all languages. When no encoding is specified, UTF-8 is used as the default. Some English-only files still use ISO-8859-1 encoding. For more information, see the *Oracle Access Manager Customization Guide*.
Web Server Configuration Files	There have been no changes for globalization and UTF-8 support in any Web server configuration files. However, the importantnotes.txt file has been removed and the information that was in this file is now documented in an appendix in the *Oracle Access Manager Installation Guide*.

Identity System Behavior Summary

Table 5–2 briefly summarizes 10*g* (10.1.4.0.1) Identity System behaviors.

Table 5–2 Identity System Behavior Summary

Function	Behavior
Challenge and Response Attributes	Starting with 10*g* (10.1.4.0.1), both the challenge phrase and response attributes must be on the same panel in Identity System applications. Challenge phrases and responses are displayed one after the other even though these are not configured one after the other in the panel. If a panel contains only the challenge attribute, it will be displayed in the Profile page without a response. If the panel contains only the response (without the challenge attribute), the response will not be displayed in the Profile Page at all. For details about configuring these, see the *Oracle Access Manager Identity and Common Administration Guide*. For details about combining these on a single panel after the upgrade, see the *Oracle Access Manager Upgrade Guide*. For changes to IdentityXML, see the *Oracle Access Manager Developer Guide*.
Identity Server Backward Compatibility	Starting with 10*g* (10.1.4.0.1), the Identity Server uses UTF-8 encoding and plug-in data will contain UTF-8 data. Earlier custom plug-ins send and receive data in Latin-1 encoding. Backward compatibility with earlier custom plug-ins is automatic. However, when you add a new 10*g* (10.1.4.0.1) Identity Server to an upgraded environment, you need manually set the encoding flag in the Identity Server oblixpppcatalog.lst to enable communication with earlier plug-ins and interfaces. For details, see the *Oracle Access Manager Installation Guide*.
Identity System Event Plug-ins	With release 10*g* (10.1.4.0.1), the Identity Server uses UTF-8 encoding; plug-in data will contain UTF-8 data. For more information, see the *Oracle Access Manager Developer Guide*. Backward compatibility between an upgraded Identity Server and earlier Identity Event plug-ins is automatic. For details about adding a new Identity Server to an upgraded environment, see the *Oracle Access Manager Installation Guide*.
IdentityXML and SOAP Requests	Starting with release 6.5, certain syntax changes were made for IdentityXML requests. Oracle recommends that you use the latest syntax for your customizations. However, the earlier syntax should still operate without problem. In 10*g* (10.1.4.0.1), UTF-8 encoding is used for XML pages, for SOAP/IdentityXML requests, and for Identity Event Plug-in data sent to executables. For more information and new syntax descriptions, see the *Oracle Access Manager Developer Guide*.

Table 5–2 (Cont.) Identity System Behavior Summary

Function	Behavior
Java Applets	A user working in an English locale cannot view applets in multi-byte languages. To work with applets in a multi-byte language, the locale on the user's machine must be set to the same language. Setting browser encoding will not work. There is a known limitation of Java applets in JDK1.1.7. Oracle Access Manager 10*g* (10.1.4.0.1), applets with non-ASCII data can only be displayed properly on machines running with a native encoded operating system. For more information about acquiring and using languages, see Table 5–1, " General Oracle Access Manager Behavior Summary". See also the *Oracle Access Manager Identity and Common Administration Guide*.
Mail Notification	In 10*g* (10.1.4.0.1) UTF-8 "B" (Base64 encoding) is used.MIME headers for all mails non-MHTML mail message are set as follows: MIME-Version: 1.0; Content-Type: text/plain; charset=UTF-8; Content-Transfer-Encoding: 8bit.
Minimum Number of Search Characters	In earlier releases, you needed to enter at least three characters when performing a search in Identity System applications (User Manager, Group Manager, and Organization Manager). In 10*g* (10.1.4.0.1) there is no minimum number of characters required. By default, you can enter no characters. As in earlier releases, to help users narrow their search criteria you can control the minimum number of characters that users must enter in the search field by setting the `searchStringMinimumLength` parameter in oblixadminparams.xml. See the *Oracle Access Manager Customization Guide* for details.
Multi-Step Identity Workflow Engine	You can model your business processes in the Identity System using workflows. In earlier releases, you could use a workflow to issue, revoke, and renew certificates. However, this is no longer supported.
Oracle Identity Protocol (OIP)	The Oracle Identity Protocol (formerly known as the NetPoint Identity Protocol) facilitates communication between Identity Servers and associated WebPass instances. There are no changes in the protocol for globalization.
Password Policies and Password Management Runtime	In 10*g* (10.1.4.0.1), internationalized characters are supported in password policies. In earlier releases, password policies worked only with Latin1 characters when enforcing policy constraints. There are no Password Management runtime changes.
Portal Inserts and URI Query Strings	In 10*g* (10.1.4.0.1), the encoding of data in the URI query string is UTF-8 encoding. However, earlier Portal Inserts in installations that have been upgraded to 10*g* (10.1.4.0.1) require modification after upgrading. For more information, see the *Oracle Access Manager Upgrade Guide*.
PresentationXML Directories	Before release 6.5, the PresentationXML library was provided under two directories and distributed depending upon how the files were likely to be used. For example, stylesheets that define the default Oracle Access Manager Classic Style were maintained in flat files in *\IdentityServer_install_dir*\identity\oblix\apps*AppName*. Starting with release 6.5 and continuing through 10*g* (10.1.4.0.1), the PresentationXML library is now stored in different directories. For more information, see the *Oracle Access Manager Customization Guide*.
Sorting User Search Results	In the User Manager, Group Manager and Org. Manager, search results are sorted using a locale-based case insensitive method when you click the column heading (Full Name, for example) in the search results table.
Web Services Code	The Oracle Access Manager product now provides sample code for implementing Web services using IdentityXML. For more information, see the *Oracle Access Manager Developer Guide*.

Access System Behavior Summary

Table 5–3 briefly summarizes 10*g* (10.1.4.0.1) Access System behaviors.

Table 5–3 Access System Behavior Summary

Function	Behavior
Access Server Backward Compatibility	Earlier custom plug-ins sent and received data in Latin-1 encoding. In 10*g* (10.1.4.0.1), Access Servers use UTF-8 encoding and 10*g* (10.1.4.0.1) custom plug-in data will be UTF-8 encoded. In 10*g* (10.1.4.0.1), cookie encryption and decryption is accomplished by the Access Server. When you upgrade an earlier Access Server to 10*g* (10.1.4.0.1), a new parameter is set in the Access Server globalparams.xml file automatically. This provides backward compatibility with earlier custom plug-ins and interfaces, as well as earlier WebGates and custom AccessGates. For more information, see the *Oracle Access Manager Upgrade Guide* When you add a new Access Server to an upgraded environment, you need manually set the value in the Access Server globalparams.xml to enable backward compatibility. For more information, see the *Oracle Access Manager Installation Guide*.
Access Manager SDK, Access Manager API, and Custom AccessGates	10*g* (10.1.4.0.1) Access Servers use UTF-8 encoding automatically. In addition, the Access Manager SDK (formerly the Access Server SDK) and Access Manager API (formerly known as the Access Server API) are used to create custom AccessGates. Custom AccessGates use UTF-8 encoding automatically. For Java interfaces and the Java implementation of the Access Manager API, there have been no external changes for 10*g* (10.1.4.0.1). JNI calls use UTF-16 encoded Java string objects. Earlier Oracle Access Manager releases converted this data to Latin-1. 10*g* (10.1.4.0.1) Access Servers and AccessGates use UTF-8 encoding automatically. The 10*g* (10.1.4.0.1) Access Manager SDK and custom 10*g* (10.1.4.0.1) AccessGates are **not** backward compatible with earlier Access Servers, nor with the earlier Access Manager SDK and AccessGates. However, you can use earlier AccessGates with 10*g* (10.1.4.0.1) Access Servers that are enabled to be backward compatible.
Authentication Scheme Updates	In 10*g* (10.1.4.0.1) it is no longer necessary to disable an authentication scheme before you modify it. Also, in 10*g* (10.1.4.0.1) you can configure an authentication scheme that allows the user to log in for a period of time rather than a single session.
Authorization Rules and Access Policies	Starting with release 6.5, Authorization rules are grouped under a tab named "Authorization Rules". Also, a new authorization inconclusive state was introduced in release 7.x (apart from authorization success and failure states). During an upgrade the rules are renamed using a combination of the Policy Domain name to which the rule belongs, followed by the Authorization Rule name: *PolicyDomain_AuthorizationRuleName.*When your earlier installation included authorization failure redirects, you need to complete a procedure after the upgrade to assure proper authorization failure re-directs. For more information, see the *Oracle Access Manager Upgrade Guide*.
Custom Authentication and Authorization Plug-in Interfaces	Before 10g (10.1.4.0.1), the Authentication Plug-In API and Authorization Plug-In API for C used Latin-1 encoding for data exchanged between the Access Server and the custom plug-ins. In 10*g* (10.1.4.0.1), the Authentication Plug-In API and Authorization Plug-In API for C use UTF-8 encoding for plug-in processing. There is no change for .NET (managed code) plug-ins.
Directory Profiles	Release 6.5 introduced support for directory server profiles for the Access Server and Policy Manager. During a Policy Manager upgrade from any release before 7.x, a new directory server profile is added automatically. However, the values for `Initial Connections` and `Maximum Connections` are not retained during the Policy Manager upgrade. After upgrading, Oracle recommends that you verify and validate that new directory server profiles were properly created and that load-balancing and failover settings in Access System directory server profiles are configured as expected. For more information about directory profiles, see Table 5–1, " General Oracle Access Manager Behavior Summary".
Form-based Authentication	10*g* (10.1.4.0.1) WebGates accept input data only in UTF-8 encoding. To ensure that character set encoding for the login form is set to UTF-8, add the following META tag to the HEAD tag of the login form HTML page: <META http-equiv="Content-Type" content="text/html;charset=utf-8">. For more information, see the *Oracle Access Manager Access Administration Guide*.
Maximum Elements in Session Token Cache	In earlier releases, the default value for this parameter was 100000. However, in Oracle Access Manager 10g (10.1.4.0.1), the default value has changed to 10000. You can find this parameter by navigating to the Access System Console, Access System Configuration tab, Access Server Configuration function. Look on the Details for Access Server page. For more information, see the *Oracle Access Manager Access Administration Guide*.
Oracle Access Protocol	In 10*g* (10.1.4.0.1), UTF-8 encoding is used to for communication between Access System components to accommodate globalization. The OAP was formerly known as the NetPoint Access Protocol (NAP). For information about the Access Server and backward compatibility, see earlier discussions in this table.

Table 5–3 (Cont.) Access System Behavior Summary

Function	Behavior
Policy Manager API	The Policy Manager API was formerly known as the Access Management API. In 10*g* (10.1.4.0.1), ■ In the C language API, the `ObAMMasterAuditRule_getEscapeCharacter` remains and you may continue using this. However, the audit escape character must be an ASCII character; otherwise the return value is incorrect. In this case, you must modify your C code to use the new API. ■ On Java clients, the `ObAMMasterAuditRule_getEscapeCharacter` works correctly and you can continue using this even when the audit escape character is not an ASCII character. ■ In the C language API, a new `ObAMMasterAuditRule_getUTF8EscapeCharacter` has been added, which returns a pointer to the UTF-8 encoded audit escape character. For more information, see the *Oracle Access Manager Developer Guide*.
Preferred HTTP Host	This WebGate configuration parameter is now mandatory before WebGate installation and must be configured with an appropriate value whenever a WebGate is added. (From the Access System Console, select Access System Configuration, Add New AccessGate.) This parameter defines how the hostname appears in all HTTP requests as users attempt to access the protected Web server. The hostname within the HTTP request is translated into the value entered into this field (regardless of the way the hostname was defined in an HTTP request from a user). For more information, see the *Oracle Access Manager Installation Guide*.
Shared Secret	The location of the shared secret key remains unchanged from earlier releases. However, in 10*g* (10.1.4.0.1), cookie encryption/decryption is handled by the Access Server. During an upgrade to 10*g* (10.1.4.0.1), the earlier encryption scheme is retained. For more information about Access Servers and WebGates, see other items in this table. If you change the shared secret during a user session, the user does not need to re-authenticate. If a cookie is being decrypted with the old shared secret and the cookie is refreshed, it is encrypted with the new shared secret. For more information, see the *Oracle Access Manager Access Administration Guide*.
Triggering Authentication Actions After the ObSSOCookie Is Set	You can cause authentication actions to be executed after the ObSSOCookie is set. Typically, authentication actions are triggered after authentication has been processed and before the ObSSOCookie is set. However, in a complex environment, the ObSSOCookie may be set before a user is redirected to a page containing a resource. In this case, you can configure an authentication scheme to trigger these events. See also *Oracle Access Manager Access Administration Guide*.
WebGates	In earlier releases, cookie encryption and decryption was accomplished by WebGates and AccessGates. In 10*g* (10.1.4.0.1), cookie encryption and decryption is accomplished by the Access Server. WebGates and AccessGates no longer need the shared secret key. 10*g* (10.1.4.0.1) WebGates have been redesigned and the WebGatestatic.lst file has been replaced with options you can configure using the Access System Console, Access System Configuration tab. See the *Oracle Access Manager Access Administration Guide* for details. Earlier WebGates may coexist with 10*g* (10.1.4.0.1) Access Servers. However, each Access Server must be backward compatible with earlier WebGates. For more information, see details about Access Servers in this table, and the *Oracle Access Manager Upgrade Guide*. The code for WebGates has been rewritten so that 10*g* (10.1.4.0.1) WebGates and AccessGates share the same code base. For more information, see the *Oracle Access Manager Developer Guide*.

6

Road Map to Manuals

Each product manual is written to help the individuals responsible for certain tasks complete their work. Each Oracle Access Manager implementation may involve the following individuals at various times during the overall process:

- Technical architects
- Network, system, database, and Web administrators
- IT and application developers
- Quality Assurance (QA) engineers
- Business analysts

This chapter provides a brief overview of each manual in the suite, its intended audience, and recommended prerequisite knowledge and skills, as outlined in Table 6–1. Look for an overview of each manual following the table.

Table 6–1 Oracle Access Manager Manuals

Title	Purpose
Oracle Application Server Release Notes	Provide up-to-the-minute details about the product, changes and new features, and more.
Oracle Access Manager Introduction	Acquaints you with Oracle Access Manager 10*g* (10.1.4.0.1) concepts, features, and applications.
Oracle Access Manager Installation Guide	Guide you as you prepare your environment, then install and set up Oracle Access Manager.
Oracle Access Manager Upgrade Guide	Guide you as you upgrade an earlier Oracle Access Manager installation to the latest version.
Oracle Access Manager Identity and Common Administration Guide	Provides details you need to perform Identity System and common administration tasks.
Oracle Access Manager Access Administration Guide	Provides details you need to perform Access System administration tasks.
Oracle Access Manager Deployment Guide	Helps you fine tune and manage the Oracle Access Manager installation.
Oracle Access Manager Customization Guide	Provides details to help you customize Oracle Access Manager to change the appearance of applications or change how to control Oracle Access Manager.
Oracle Access Manager Developer Guide	Acquaints you with the application programming interfaces (APIs) provided by Oracle Access Manager and how to write custom applications and plug-ins that use the programmatic access provided to gain access toOracle Access Manager functionality, and, in some cases, to extend that functionality
Oracle Access Manager Integration Guide	Guides you as you integrate Oracle Access Manager with one or more supported third-party products.

Table 6–1 (Cont.) Oracle Access Manager Manuals

Title	Purpose
Oracle Access Manager Schema Description	Acquaints you with the Oracle-provided objects and attributes that control the behavior of Oracle Access Manager.

Oracle Application Server Release Notes

For up-to-the-minute details about the product release, see the *Oracle Application Server Release Notes* where you will find information about:

- Oracle Access Manager changes and new features
- Known issues
- Documentation updates and resolved issues

Audiences

Everyone should review the latest *Oracle Application Server Release Notes* for their product and installation.

- If you are new to Oracle Access Manager and want to ensure you have the latest details, check the *Oracle Application Server Release Notes*.
- If you have used Oracle Access Manager and want to quickly update your knowledge, *Oracle Application Server Release Notes* summarize the latest enhancements and changes.

Prerequisites

None.

Oracle Access Manager Introduction

Look to the introduction (the guide you are now reading) for:

- A complete list of what is new in this release
- An introduction to product concepts, features, components, applications, and functions
- An overview of integration and customization options
- An introduction to globalization, localization, and multibyte language support that includes a summary of system behavior
- A brief introduction to system behaviors
- An introduction to installation and multi-language environments
- A road map to all Oracle Access Manager manuals and their audiences, with suggested prerequisite knowledge and skills
- A glossary of terms

Audiences

Anyone interested in learning about Oracle Access Manager should begin with the *Oracle Access Manager Introduction*.

Prerequisites

None

Oracle Access Manager Installation Guide

The *Oracle Access Manager Installation Guide* helps you prepare your environment, then install and set up Oracle Access Manager. The guide includes:

- An introduction to installation and the sequence of tasks that you must perform
- Installation prerequisites, considerations, and options
- Preparation worksheets that you can complete to help streamline your experience and document your Oracle Access Manager installation
- Step-by-step instructions to help ensure a successful Oracle Access Manager installation
- Troubleshooting tips

Audiences

The *Oracle Access Manager Installation Guide* is required for anyone who is responsible for:

- An overview of installation and configuration tasks and where to find more information about each one
- Details about how to prepare your environment before installation
- Identity Server installation and setup
- WebPass installation to enable communication with the Identity Server
- Policy Manager installation and setup, which includes the Access System Console
- Access Server installation to enable communication with the directory server and WebGate
- WebGate installation to enable communication with the Access Server
- Optional component installation, including the Oracle Virtual Directory, SNMP agent, and Language Packs

Prerequisites

Be sure to read the *Oracle Access Manager Introduction* before starting the installation. This guide presumes that you have knowledge of and experience with the following:

- Operating and file systems: Windows or Unix based
- Sites connected to the Internet and networking protocols
- Network security: building firewalls, deploying authentication systems, and so on
- Host security: passwords, uids, file permissions, file system integrity, and the like
- Web server, Web browser, and configuration details
- Database administration

Oracle Access Manager Upgrade Guide

The *Oracle Access Manager Upgrade Guide* provides information to help you upgrade an existing Oblix NetPoint or Oracle COREid installation to Oracle Access Manager 10*g* (10.1.4.0.1). The guide includes:

- An introduction to upgrade tasks, planning, and deployment scenarios
- An overview of upgrade concepts and methods
- Upgrade prerequisites, considerations, and preparation steps
- A summary of changes from earlier system behaviors to 10*g* (10.1.4.0.1) system behaviors to help you easily recognize differences
- Step-by-step instructions to help ensure a successful upgrade of all components and instances to 10*g* (10.1.4.0.1)
- Post upgrade steps that you need to complete to ensure compatibility with any earlier customizations in the upgraded environment
- Troubleshooting tips

Audiences

The *Oracle Access Manager Upgrade Guide* is required for anyone who needs to upgrade an earlier Oblix NetPoint or Oracle COREid installation to Oracle Access Manager 10*g* (10.1.4.0.1), which includes:

- Preparing and taking inventory in your older installation
- Upgrading the Identity System components and ensuring backward compatibility with custom plug-ins and customizations
- Upgrading the Access System components and ensuring backward compatibility with custom access clients and plug-ins
- Integration component upgrades

Prerequisites

The *Oracle Access Manager Upgrade Guide* presumes that you have knowledge of and experience with the following:

- Your earlier Oblix NetPoint or Oracle COREid installation
- Operating and file systems: Windows or Unix based
- Sites connected to the Internet and networking protocols
- Network security: building firewalls, deploying authentication systems, and so on
- Host security: passwords, uids, file permissions, file system integrity, and the like
- Web server, Web browser, and configuration details
- Database administration

Oracle Access Manager Identity and Common Administration Guide

The *Oracle Access Manager Identity and Common Administration Guide* focuses on Identity System administration. It also includes tasks that are common to both the Identity System and Access System. The *Oracle Access Manager Identity and Common Administration Guide* provides information on how to:

- Configure the rights and tasks available to administrators and end users
- Prepare for administration
- Specify Identity System administrators
- Make schema data available to the Identity System
- Configure User, Group, and Organization Managers
- Chain Identity functions into workflows
- Configure global settings for Oracle Access Manager
- Change transport security modes
- Set up auditing, access reporting, logging, and the SNMP monitor
- Deploy with Active Directory
- Implement .NET Features

During this phase of the implementation, the "Oracle Access Manager Schema Description" on page 6-10 may also be useful.

Audiences

The *Oracle Access Manager Identity and Common Administration Guide* targets the following audiences:

- Identity administrators and delegated Identity administrators
- Individuals who enter or manage information about users, groups, and resources
- Individuals who manage servers
- Individuals who audit or monitor system events and user-session activity
- Individuals who generate reports

Prerequisites

Oracle Access Manager should be installed and its operation confirmed, as described in the *Oracle Access Manager Installation Guide* or the *Oracle Access Manager Upgrade Guide*.

To complete activities in the *Oracle Access Manager Identity and Common Administration Guide*, the reader should have some knowledge of and experience with the following:

- Browser-based interfaces, windows, and menus
- Your Web servers and LDAP directory server
- Data entry
- Policy setting
- Report generation

Helpful

- Knowledge of authentication and authorization concepts
- System or database administration

Oracle Access Manager Access Administration Guide

The *Oracle Access Manager Access Administration Guide* focuses on Access System administration. It includes details on how to:

- Configure access administrators and server settings
- Configure AccessGates and Access Servers
- Protect resources with policy domains
- Configure user authentication
- Configure user authorization
- Set up single sign-on
- Use the Access System with other Oracle products
- Access System configuration and management
- Set up form-based authentication
- Enable Impersonation with the Access System

During this phase of the implementation, the "Oracle Access Manager Schema Description" on page 6-10 may also be useful.

Audiences

The *Oracle Access Manager Access Administration Guide* targets the following audiences:

- Access administrators and delegated Access administrators
- Individuals who create and manage policy domains
- Individuals who configure and manage servers, WebGates, and Access System configuration
- Individuals who create and manage authentication and authorization schemes
- Individuals who audit or monitor system events and user-session activity, and generate reports

Prerequisites

Oracle Access Manager should be installed and its operation confirmed, as described in the *Oracle Access Manager Installation Guide* or the *Oracle Access Manager Upgrade Guide*.

To complete activities in the *Oracle Access Manager Access Administration Guide*, the reader should have some knowledge of and experience with the following:

- Browser-based interfaces, windows, and menus
- Your Web servers and LDAP directory server
- Data entry
- Policy setting
- Report generation

Helpful

- Knowledge of authentication and authorization concepts
- System or database administration

Oracle Access Manager Deployment Guide

The *Oracle Access Manager Deployment Guide* provides the information needed to fine-tune and manage the Oracle Access Manager installation. The scope of this guide encompasses:

- Capacity planning
- System tuning
- Performance and scalability considerations
- Failover and load balancing
- Caching
- Migration planning to move Oracle Access Manager from a test environment to a production environment

Audiences

The *Oracle Access Manager Deployment Guide* targets the knowledge and skill requirements of system, network, or Master Administrators responsible for optimizing the Oracle Access Manager implementation.

Prerequisites

To complete activities in the *Oracle Access Manager Deployment Guide* the reader should have strong knowledge of and experience with the following:

- Network, site planning, and networking concepts
- Distributed computing environment concepts
- Consistent network-wide file system layout design
- Routing principles
- Client/server programming
- Operating system details and inter-process communication
- System performance tuning
- Firewall and Internet security
- Computing policies

Helpful

- Familiarity with failover concepts and practices
- Network communications

Oracle Access Manager Customization Guide

The *Oracle Access Manager Customization Guide* explains how to control the way Oracle Access Manager looks and operates, without programming. Topics in this guide include:

- Changing the appearance of Oracle Access Manager applications
- Tuning catalog files
- Designing the graphical user interface (GUI) by editing XML files

- Connecting CGI files or JavaScripts to Oracle Access Manager screens
- Controlling how Oracle Access Manager operates by making configuration changes to the operating system, Web or directory servers, or directory content
- Introducing the Access Manager API (formerly known as the Access Server API) and the Authorization and Authentication Plug-in APIs from an administrator's point of view

Audiences

The *Oracle Access Manager Customization Guide* is a valuable asset to anyone responsible for customizing Oracle Access Manager to control operations.

Prerequisites

Techniques provided here are vulnerable to error and should be used with the utmost care. This guide assumes that you have some prior knowledge of and experience with:

- Using Oracle Access Manager
- Logical connections between the Identity and Access systems
- General working knowledge of directories and LDAP
- Comfort manipulating files and running applications at the command-line level

Oracle Access Manager should be installed and its operation confirmed, as described in the *Oracle Access Manager Installation Guide* or the *Oracle Access Manager Upgrade Guide*.

Helpful

- System or database administration
- Familiarity with CGI files or JavaScripts
- Your Web server, Web browser, operating system, and configuration details

Oracle Access Manager Developer Guide

The *Oracle Access Manager Developer Guide* describes the application programming interfaces (APIs) provided by Oracle Access Manager. It also explains how to write custom applications and plug-ins that use the programmatic access provided by Oracle Access Manager to gain access to Oracle Access Manager functionality (and, in some cases, to extend that functionality). This guide shows you how to:

- Use IdentityXML to interact with the Oracle Access Manager Identity System without using a browser.
- Use the Identity Event Plug-in API to implement functions and executables triggered by events within the Identity System.
- Use AccessXML to gain access to the Oracle Access Manager Access System without using a browser.
- Develop custom AccessGates using the Access Manager API (a subset of the Access Manager Software Developer Kit) in Java, C, C++, and C# (.NET managed code).
- Write applications using the Policy Manager API (a subset of the Access Manager Software Developer Kit) that use a programmatic interface (Java, C, and C# (.NET

managed code)) to create, modify, delete, and retrieve policy domains and their content.

- Develop server-side plug-ins to apply custom filters and logic using the Authentication and Authorization Plug-in APIs.

Audiences

The *Oracle Access Manager Developer Guide* is for Administrators and experienced developers who want to write applications that extend the capabilities of Oracle Access Manager.

Prerequisites

This guide presumes that you have knowledge of and experience with the following:

- Concepts and fundamentals of supported programming languages (C, C++, Java code, C# (.NET managed code)
- APIs, wrappers, variables, constructors
- Extensions, events, parameters, and exceptions
- Cookies
- Certificates

Oracle Access Manager Integration Guide

The *Oracle Access Manager Integration Guide* explains how to integrate Oracle Access Manager with one or more third-party products, such as:

- Oracle Application Server
- Siebel
- Security Provider for WebLogic SSPI
- IBM WebSphere
- Plumtree portal
- RSA SecurID
- SharePoint Portal Server, Content Management Server
- and others

For a complete list of supported integrations, see the latest *Oracle Access Manager Integration Guide* which includes both considerations and steps to complete each integration.

Audiences

Anyone who is responsible to integrate Oracle Access Manager with another supported product.

Prerequisites

Oracle Access Manager should be installed and its operation confirmed as described in *Oracle Access Manager Installation Guide* or the *Oracle Access Manager Upgrade Guide*.

The *Oracle Access Manager Integration Guide* presumes that you have knowledge of and experience with the product you are integrating as well as with Oracle Access Manager.

Oracle Access Manager Schema Description

The *Oracle Access Manager Schema Description* identifies the Oracle-provided objects and attributes that control the behavior of Oracle Access Manager. This information is being provided to help you understand the structure and behavior of the product.

Audiences

The *Oracle Access Manager Schema Description* is intended for anyone who needs to understand the structure and behavior of the Oracle Access Manager product.

WARNING: Oracle does not support modified versions of its schema.

Prerequisites

The *Oracle Access Manager Schema Description* assumes that you are familiar with your LDAP directory and concepts.

Glossary

access administrator

A user able to modify data within the Access System. The Master Administrator and Master Access Administrators can modify any of this data. Delegated Access Administrators may modify only subsets of this data.

access client

An Access System component that monitors attempts to access a Web site and uses the Access Server to provide authorization and authentication services prior to completing the access requests. It can be either the Access System-provided client (WebGate) or a client that is built into an application server or standalone application by using the Access Manager API. See also **AccessGate**.

access control

The protection of system resources against unauthorized use. The process is regulated according to a security policy and permits only authorized system entities (users, programs, processes, or other systems) to access the resource. See also **ACL (access control list)**.

Access Manager API

A collection of libraries, build instructions, and examples that can be used to build a customer-specific AccessGate for non-Web resources. This helps the customer to extend authorization and authentication rules to other resources in addition to URLs, and to control user interaction with applications outside of Oracle Access Manager. In this way, customers can have centralized policy information in a single system that can be leveraged across both Web and non-Web resources. This API can integrate with Java and C/C++ applications. The Java API allows application servers and other Java-based systems to leverage Oracle Access Manager infrastructure. The C/C++ API allows client/server or non-Java applications to leverage Oracle Access Manager infrastructure. The API is available as a distinct product. See also **API (Application Programming Interface)**.

Access Manager SDK

Also known as the Software Developer Kit, is an optional component that is installed independently as described in the *Oracle Access Manager Developer Guide*. The SDK provides all the information and resources you need to build a custom access client (AccessGate) (as well as the Policy Manager API). In addition to the files that make up the various implementations of the Access Manager API, the SDK includes documentation and code samples, which show how to construct simple AccessGate servlets or applications for each of the supported development platforms.

Access Server

This standalone server (of which there can be several instances) provides dynamic policy evaluation services for both Web-based and non-Web resources and applications. Different applications and web servers can make use of the authentication, authorization, and auditing services it provides.

Access System

This system allows companies to do policy-based authorization and Web single sign-on. Companies can set up security policies to control access to Web and non-Web resources and audit the usage (such as applications, content, services, and objects in applications). It provides the following applications and components:

Policy Manager

Access Server

WebGate/AccessGate

Despite the change in product name from NetPoint to Oracle Access Manager, you may see the term NPAS.

Access Tester

The Policy Manager tool used to determine whether a policy domain's authentication, authorization, and auditing rules deliver the level of access control required.

AccessGate

A custom WebGate developed using the Access Manager SDK. An AccessGate is a form of access client that processes requests for Web and non-Web resources from users or applications and uses the Access Server to provide authorization and authentication services to monitor and control attempts to access a Web site. Customers can also use the Access Manager API to build a client into an application server or standalone application. Oracle Access Manager provides an out-of-the-box WebGate client. See also **WebGate**.

ACI (access control item)

An entry in an access control list (ACL) specifying users, their access rights, and the target entries or attributes to which those rights apply.

ACL (access control list)

The set of roles and policies used for controlling access to resources such as directories and Oracle Access Manager applications. The ACL describes the users or groups, the type of access permitted and the attributes being accessed.

action

A task within a Oracle Access Manager workflow that results in changed information (for example, a change to a user's phone number).

activate

The process followed to make a user's directory information accessible within Oracle Access Manager. See also **deactivate**.

actor

The participant who performs a specific action in a Oracle Access Manager workflow.

AL32UTF8

The Oracle UTF-8 character set that maps to the latest version of the Unicode Standard (Unicode 4.0) and provides support for newly defined supplementary characters.

API (Application Programming Interface)

A set of commands used to extend the capabilities of an existing application. APIs contain a library of functions and an interface that can be easily added to the application.

application

A program that performs any one of the tasks for which a computer is used. Oracle Access Manager applications include User Manager, Group Manager, Org. Manager, Policy Manager.

ASCII

Most modern character encodings have an historical basis in ASCII, which is the most common format for text files in computers and on the Internet. In an ASCII file, each alphabetic, numeric, or special character is represented with a 7-bit binary number.

attribute

A characteristic or trait associated with a directory object, which can have one or more values. For example, the object class “person” can be identified with the attribute “cn” with the specific value: “Joe Smith”.

audit

The process of collecting information on Oracle Access Manager system events such as authentication success or authorization failure, and which user or administrator triggered them. This data, when presented in report form, helps Master Administrators understand Oracle Access Manager usage patterns.

audit files

Disk files that record audit information. Each Access Server and Identity Server can record audit information to a file, to the consolidated audit database, or to both.

audit file rotation

The process by which a specified audit file is closed, stamped with the date and time, and given a new name. When an audit log is closed, a new audit log file is created.

audit rule

A named filter that determines the tracking level of the authentication and authorization activities performed by an Access Server.

Auditing Services

Provide flexible and detailed recording of events in the Access System and Identity System. You can use this information both for security purposes and for monitoring Oracle Access Manager system usage. Audit files enable you to detect intrusion threats, monitor security, and create business-level reports by integrating with third party products such as Crystal Reports.

authentication

The process of establishing and proving a user’s identity. In the world of brick-and-mortar business transactions, this process is often a visual one (comparing the information on a document such as a driver’s license with the bearer of that

document.) Electronic, online transactions require a more complex authentication method.

authentication plug-in

A set of instructions for performing authentication. Oracle Access Manager provides default authentication instructions. Customers can also write their own plug-ins using the Authentication Plug-in API.

Authentication Plug-in API

An Access System standard API used to create customer-defined authentication plug-ins. For use within authentication schemes and chained authentication processes to be used by Oracle Access Manager.

authentication rule

A named logic flow that describes the process to get an authentication result, generally over a set of resources within a Oracle Access Manager policy domain. An authentication rule generally contains an authentication scheme.

authentication scheme

A named set of plug-ins that defines the challenge method and steps required to authenticate a user.

Authentication Services

Provide a generalized means to authenticate users and systems when they try to access resources protected by Oracle Access Manager. These services support not only the basic username and password authentication method but also stronger methods such as digital certificates or SecurID cards. You can further expand the authentication capabilities with the Oracle Access Manager Authentication Plug-in API. Once a user is authenticated by the authentication services, Oracle Access Manager creates a single-sign-on session for the client that frees the user from having to sign on again to access other resources or applications.

authorization

The process that determines the access permitted to users after they have been authenticated.

authorization plug-in

A set of instructions for performing authorization, which can be included in an authorization scheme to extend the set of Oracle Access Manager default authorization schemes. Customers can write their own plug-ins using the Authorization Plug-in API.

Authorization Plug-in API

An Access System standard API, used to create customer-defined plug-ins for use within authorization schemes to be used by Oracle Access Manager. This API allows customers to extend policy evaluations through dynamic call outs to custom code. As an example, a policy administrator can set a policy that allows an end user to access some resource if their bank balance exceeds a certain amount. Use the Authorization Plug-in API to check the bank balance that resides in a database.

authorization rule

A named logic flow that describes the process to be followed to get an authorization result, generally over a set of resources within a Oracle Access Manager policy domain. An authorization rule usually contains an authorization scheme.

authorization scheme

A named link to a shared library holding an authorization plug-in that defines a method to be used to authorize a user.

Authorization Services

Once a user or system is authenticated, these services specify what information they can access. They deliver the centralized, consistent management of policies across applications, while providing users granular access to Web-based content and resources. This capability gives growing e-business organizations the control and consistency they require for secure, sensitive information, while helping ensure that users and systems have easy access to the information and applications they need.

auxiliary object class

An object class that contains supplementary attributes not necessarily found in a structural object class; also called mix-in classes because they allow additional attributes to be "mixed into" an existing class. An auxiliary object class cannot stand by itself. Its attributes must be assigned to an entry that is based on an existing object class.

CA (Certification Authority)

Certifies the mapping of the public and private key pair with the subject identity (user name, email, machine name, and so on) by digital signature.

cert

A transport security mode under which the data transferred between points is encrypted using SSL and a public key certificate. Transport security between all Identity System components must match. Transport security between all Access System components must match.

certificate

A collection of data used for authentication, which uniquely associates an entity (for example, an individual, a company, or a machine) with a public encryption key. The ITU-T Recommendation X.509 is the most widely used format for providing this information. A certificate is issued by a CA.

class

In object-oriented programming, a class is a template definition of the method and variable in a particular kind of object. Specific to Oracle Access Manager, the Access Manager API uses a library based on Java classes. For directories, see **object class**.

class attribute

The attribute that links search results to a profile.

Cloning

Instead of using the command line or the installation GUI to install a Oracle Access Manager component, you can automatically install a component by cloning the configuration of an already-installed component. Cloning creates a copy of a component on a remote system using an already-installed component as a template.

CMS (Cryptographic Message Syntax)

The Internet standards track protocol that is used to digitally sign, digest, authenticate, or encrypt arbitrary messages.

component

A part. For Oracle Access Manager, any of its major out of the box parts, such as the Identity Server, WebPass, Policy Manager, WebGate, Access Server.

configuration data

Oracle Access Manager configuration settings (also known as Oracle specific data). See also **Oracle Specific Data (OSD)**.

configuration DN

The node in the directory tree under which the schema information that defines all Oracle Access Manager operations is stored.

container

An object in an LDAP directory that contains other objects. For example, the object dc=yourcompany may contain the ou=marketing and ou=engineering objects. These objects may in turn contain other objects.

container limit

Specifies the maximum number of objects that a container can hold.

CSV (character-separated value)

A method of representing data that was originally stored as a number of variable length fields within a record. The data is extracted as a series of variable length text strings, separated by some defined character (often a comma). Also a file extension type, as in myfile.csv.

Data Anywhere

The data management layer (formerly known as COREid Data Anywhere) aggregates and consolidates data from RDBMS and LDAP directories into a virtual LDAP tree that can be managed by the Identity System and used to support authentication and authorization using the Access System. Data Anywhere supports multiple LDAP environments, RDBMS databases, and split directory profiles using the Oracle Virtual Directory Server (VDS, formerly OctetString VDE). See the *Oracle Access Manager Installation Guide*.

Data Management Services

Allow companies to set fine-grained attribute-level access controls for managing users, groups, and organizations. Setting attribute-level access controls determines self-service and modify rights. Customers can also specify a restricted searchbase used for display and modification of information for different audiences. These services reduce the costs of identity administration and enforce security for data changes.

data transport mode

See **transport security mode**.

data type

A syntax type describing how the values for an attribute are stored. Oracle Access Manager supports the following data types: Binary, Distinguished Name, Integer, Postal Address, String Case-insensitive, String Case-sensitive, and Telephone. The data type helps determine what display type Oracle Access Manager uses to portray that attribute.

deactivate

In the Oracle Access Manager environment, deactivate means to make objects inaccessible but not remove them from the directory. For example, users who have had their identity profiles deactivated cannot log in to the system, and their identities are not found during searches.

deactivate user

The immediate removal of a user's access privileges. Deactivation is done system-wide and without going through standard workflow processes.

default audit rule

The audit rule that applies to a policy domain if there are no more specific audit rules defined for the domain. Also called the master audit rule.

default authentication rule

The authentication rule that applies to a policy domain unless there are more specific authentication rules defined for the domain.

default authorization rule

The authorization rule that applies to a policy domain unless there are more specific authorization rules defined for the domain.

default rules

Blanket rules that apply to all resources within a policy domain, created to ensure that access is always controlled. The default rules apply for authentication, authorization, and auditing, unless overridden by more specific rules.

delegated access administrator

Administrators who have only the right to perform tasks that a Master Access Administrator delegates to them. See **access administrator**.

delegated identity administrator

Administrator with responsibilities delegated by the Master Identity Administrator. Delegated Identity Administrators have responsibilities for functions under the Configuration tab in each Identity System application (User Manager, Group Manager, and Organization Manager). This includes delegation administration, attribute access control, and workflow definition.

delegation

The sharing of authority. The authority to change directory information or perform tasks can be delegated. Also, the authority to delegate can itself be delegated. For example, the Oracle Access Manager Administrator delegates responsibility for the Identity System and the power to delegate to a master identity administrator who might then delegate the power to start certain workflows to a delegated identity administrator.

delete

To remove the profile information for an object from the LDAP directory. User profiles must be deactivated before you can delete them. Oracle recommends you archive your profiles before you delete them.

derived attribute

A stored pointer from an entry in one object class to a target entry in another object class, based upon matching information in the two classes.

directory

A directory is a specialized database optimized for frequent read operations. A directory organizes data in a hierarchical information model, represented as a directory tree. A tree contains entries, which are made up of attributes and their values.

directory administrator

The user responsible for maintaining the directory.

directory server

A server specifically designed to manage a directory of users and resources. The directory server provides for the retrieval and storage of data, in contrast to a web server that serves up pages from a Web site.

directory service

The collection of hardware, software, processes, and administrative policies required to make the directory's information available to users.

disable

User Manager only. Deactivates a user, which means the user cannot be recognized by the Identity System once the user's current session has ended. Deactivation takes effect the next time the user attempts to log in. Deactivating does not delete the object from the directory. This action does not require a participant.

display name

For Oracle Access Manager, the user-provided descriptive text associated with an attribute that appears in reports and screens in place of the formal directory attribute name. For example, an attribute with the name `departmentnumber` could be shown as "Dept. #," "Department Number," or "DEP-ID" in the Display Name field.

display type

The format in which Oracle Access Manager displays stored directory information. Display types available to an attribute are determined by its associated data type and semantic type. Examples of display types are Check Box, Multi-Line Text, and Radio Buttons.

distinguished name (DN)

A string that uniquely identifies each entry in an LDAP directory. DNs are organized in a hierarchy; each consisting of the name of an entry plus a path of names tracing the DIT (directory information tree) entry back to the root of the DIT.

DIT (directory information tree)

The directory's hierarchical structure, containing all data objects.

DLL (dynamically linked library)

See **DSO (dynamic shared object)**. The term DLL is more common in the Windows environment, but the two terms are synonymous.

DN

Distinguished name. A string that uniquely identifies each entry in an LDAP directory. DNs are organized in a hierarchy; each consisting of the name of an entry plus a path of names tracing the entry back to the root of the directory information tree (DIT).

domain

See **policy domain**.

domain attribute

Domain attributes help you specify mutually exclusive sets of users, regardless of their location on the directory tree.

DSO (dynamic shared object)

The generic term for a library of software routines or data resources that has been specifically packaged to be linked with application programs when they are loaded by the operating system, or later when explicitly requested by the applications. If many running programs require services from the same library, the operating system can share elements of the library, and achieve significant savings in resources. Synonym: DLL (dynamically shared library).

dynamic group

A group whose list of members is dynamically generated (for example, by exercising an LDAP rule). Group membership can vary as users meet or do not meet the membership criteria

dynamic member

A member of a dynamic group.

Dynamic Participants

One or more users selected based on runtime LDAP-attribute values or business logic. All possible sets of dynamic participants for a given step are specified by person, group, role, or rule in a workflow plug-in or application, which executes when workflow execution reaches that step.

embedded virtual data source

A virtual object that VDS "sees" as a target data store it can present to Oracle Access Manager or federate in a virtual directory, then present to Oracle Access Manager. Each embedded virtual data store aggregates two or more target data stores. The three types of embedded virtual data stores are: split profile, native RDBMS Join, and native RDBMS View. In general, embedded virtual data stores are suitable for authentication and authorization activities only, because they necessarily involve secondary data sources, which are sometimes not available for the full range of Oracle Access Manager identity management activities.

enable

The automated process that makes a user's directory information accessible within the Identity System. This process does not require user intervention. See also **activate**, **deactivate**, and **disable**.

End User

The basic Oracle Access Manager user-type.

entry

The most basic unit of information stored in a directory. Consists of one or more attributes and their values.

fat tree

A directory tree structure that contains many container objects all at the same level. For example, a fat tree may contain150 organizations, each holding a few people, within a company.

federation

A term used to describe the method by which Oracle Virtual Directory Server (VDS) makes a data source visible in the virtual directory it presents to Oracle Access Manager. All the data for a given user profile comes from a single data store such as an LDAP directory, a single-table database, or an embedded virtual data source. Different user profiles can come from different federated data stores.

Filter Builder

Oracle Access Manager feature that helps users create dynamic LDAP filters.

flat tree

A directory tree structure that contains a large number of objects under one container. For example, a flat tree may consist of 150 people within a single organization within a company.

globalization

Provides multi-lingual applications and software products that can be accessed and run anywhere simultaneously, without modification, while rendering content in the native user's language and locale preferences. Oracle Access Manager 10*g* (10.1.4.0.1) has undergone a globalization process.

granting rights

The process of assigning view, modify, and change rights to other users.

Group Manager

This application allows companies to create/delete groups, delegate group administration, and allow users to subscribe/unsubscribe from groups. Group management can be delegated.

group type

A label describing how group content is constructed. The Group Manager supports static, nested, and dynamic group types.

host ID

The label by which a computer can be identified. Labels include a host URL (such as oracle.com:80) and IP address (such as 111.111.11.1:80).

Identity Event Plug-in API

A standard component installed with the Identity Server. It enables you to extend the business logic of the Identity System by calling out to other systems before or after an event happens in the Identity System. Some of the uses of this API are to: bring data from external systems back into the Identity System; perform data validation; and pre-populate fields based on other information provided.

identity management

The creation, removal, and ongoing changes of identity information relating to individual users, groups, and organizations. The determination of whether or not a person qualifies for an access privilege. This can be determined by a specific user attribute value, membership in a group, or association with an organization.

identity profile

A collection of directory information describing a user object, such as a telephone number, password, location, and reporting relationship. See also **profile**.

Identity Server

This standalone server (of which there can be several instances) processes all the requests related to user identity, group, organization, and credentials management requests

Identity System

(Formerly the NetPoint COREid Identity System) Allows companies to create, remove, and manage ongoing changes of identity information relating to individual users, groups, and organizations. It also allows companies to manage which access privileges a user should get. The system provides the following applications and components:

User Manager

Group Manager

Organization Manager

Identity Server

WebPass

Identity Workflow

Allow customers to have a flexible workflow engine to which they can map their business processes without restrictions. Users and systems can submit requests that can go through multiple steps and be routed internally or externally. Customers can set workflow definitions for:

Creating, deleting, and modifying users, groups and organizations

Subscribing to groups and unsubscribing Self-registration of users and organizations

Issuing, revoking, and renewing certificates

IdentityXML

Allows applications and systems to access Identity System functionality programmatically through XML. You can access the Identity System functionality without having to go through a Web browser. Applications and systems can access or modify centralized information about users, groups, organizations through XML. IdentityXML allows for cross firewall integration without the need to expose the customer directory.

idle session

A session that has generated no requests from the browser for a specified time period known as the idle session timeout. Oracle Access Manager considers such sessions to be inactive or idle. Oracle Access Manager terminates idle sessions automatically after the idle session timeout elapses.

idle session timeout

The number of minutes that must pass with no requests from the browser to consider the session to be inactive or idle. The Identity System terminates idle sessions automatically after the idle session timeout elapses. The default idle session timeout is 180 minutes. You can change this value in the Identity System Console.

Integration Services

Allow developers to leverage the capabilities of Oracle Access Manager across all of their applications and e-business efforts and extend the value of Oracle Access Manager by providing integration points with other vendors' systems and applications. These services consist of: Access Manager API, Authentication Plug-in API, Authorization Plug-in API, Identity Event Plug-in API, IdentityXML, Policy Manager API.

internationalization

The Oracle internationalization standard requires software products and applications, such as Oracle Access Manager, to be usable on any language operating system with non-US keyboards or other country specific hardware. Applications do not have hard-coded dependencies on language strings, do inter-operate with non-US versions of other products, can handle multibyte characters and differences in a distributed environment, and can detect the user's desired locale. Oracle Access Manager10*g* (10.1.4.0.1) meets these requirements.

ISAPI (Internet Server Application Programming Interface)

An Internet Web server extension, which Oracle Access Manager uses to communicate with Microsoft Internet Information Server (IIS). ISAPI extends the functionality of IIS by allowing programmers to create modules that add or replace functionality, such as authentication, authorization, error logging, or content generation.

Latin-1

Earlier releases of Oracle Access Manager (originally known as Oblix NetPoint) supported only the Latin-1 encoding and character set, known formally as ISO/IEC 8859 and informally as ISO 8859. ISO 8859-1 Latin-1 encodings can be represented in a single byte (8-bits) in computer memory and enable support for various Western European languages. Oracle Access Manager 10*g* (10.1.4.0.1) supports UTF-8 and supports backward compatibility with older environments upgraded to 10*g* (10.1.4.0.1). See also **UTF-8**.

LCA (Local Certificate Authority)

A CA located within the same firewall as your Oracle Access Manager installation.

LDAP (lightweight directory access protocol)

A standard protocol for managing information in a directory.

LDAP filter

A string of characters interpreted by LDAP to generate custom search results. Also known as an LDAP rule.

LDAP rule

Also known as an LDAP filter. See **LDAP filter**.

LDAP URL rule

In the Access System, a rule which follows the formal LDAP URL syntax and specifies a host, port and user combination that can be accessed.

LDIF (LDAP Data Interchange Format)

A file format used to import or export data from an LDAP directory or database. LDIF files are ASCII text files that represent data in a format that is recognizable to an LDAP directory or database.

localization

Includes translation of separated file text. In Oracle products, including Oracle Access Manager, information is presented to the user in a manner consistent with the user's local cultural conventions, including data formatting, collation, currency, date, time, and directionality of text (right-to-left or left-to-right).

localized access control

An Oracle Access Manager feature that lets an administrator restrict users and groups to searching only a permitted domain within the LDAP directory. It also restricts delegated administrators to hiring only within permitted domains.

logging

The process of collecting information about Oracle Access Manager program execution to assess the health of Oracle Access Manager system components, administrative changes to policies, configuration, and other events. Oracle Access Manager helps administrators to specify the types of events that are logged for each Oracle Access Manager application.

Master Access Administrator

The administrator who configures the Access System, including WebGates, Access Servers, authentication parameters, and the initial set of policy domains. In addition, master access administrators assign individuals to the delegated access administrator role. Master access administrators are assigned by the Oracle Access Manager Administrator. See also **access administrator**.

Master Administrator

The superuser, who is empowered to configure the deployment and assign administrative tasks. The Master Administrator is assigned when the Identity System is initially installed and set up. Through the System Console, this person can create additional Master Administrators as well as Master Access Administrators and Master Identity Administrators.

master audit rule

The audit rule that applies in the absence of audit rules created at the policy domain level.

master identity administrator

The administrator authorized to configure the Identity System. In addition, master identity administrators assign individuals to be delegated identity administrators. Master identity administrators are assigned by the Master Administrator.

monitoring

The process of collecting Small Network Monitoring Protocol (SNMP) data for assessing the health of a network hosting an Oracle Access Manager system. See also **SNMP Agent**.

multibyte

Refers to an encoding scheme or character set wherein a single codepoint value generates a bit pattern that is distributed over one to four bytes. For example, Unicode 8-bit encoding standard UTF-8 characters can be 1 byte, 2 bytes, 3 bytes, or 4 bytes. In contrast, each 7-bit ASCII character occupies 1 byte.

Multi-level Identity Delegation

Enables the delegation of identity administration to multiple levels of individuals throughout an e-business network. You can delegate rights such that some users can pass on the rights they have been given or a subset of them (delegate rights), or you can prevent someone who has received rights from passing them on to others (grant rights). There is no restriction on the number of delegation levels. Delegated identity management lowers overall administrative costs by distributing work across the entire e-business network.

Multi-level Policy Delegation

Enables the delegation of access policy administration to multiple levels of individuals throughout an e-business network. You can delegate rights such that some users can pass on the rights they have been given or a subset of them (delegate rights), or you can prevent someone who has received rights from passing them on to others (grant rights). There is no restriction on the number of delegation levels. Delegated policy management lowers overall administrative costs by distributing work across the entire e-business network.

multi-table database

A database that stores in more than one table the user profile attributes that get mapped into the virtual directory.

NAP (NetPoint Access Protocol)

The original name for the Oracle Access Protocol. See **Oracle Access Protocol (OAP)**

nested group

A group that contains other groups as members.

nested member

A member of a nested group. Membership indicates the nested group contains one or more groups that the member belongs to (either statically or dynamically).

NetPoint Access System (NPAS)

Despite the change in product name from NetPoint to Oracle Access Manager, you may see references to NPAS. See also **Access System**

NetPoint System Administrator (NPSA)

The component used for Web-based administration and configuration of the overall Oracle Access Manager system. Despite the change in product name from NetPoint to Oracle Access Manager, you may see references to NPSA.

NIP (NetPoint Identity Protocol)

The original name for the Oracle Access Protocol. See **Oracle Identity Protocol (OIP)**

NSAPI (Netscape Server Application Programming Interface)

The Internet web server extension that Oracle Access Manager uses to communicate with Netscape. NSAPI extends the functionality of Netscape servers by allowing programmers to create modules that add or replace functionality, such as authentication, authorization, error logging, or content generation.

object

An entity in an LDAP directory, such as a person, group, or other resources.

object class

A group of common objects in an LDAP directory. An example is the person object class, which groups all attributes describing individuals.

object class attribute

The attribute the Oracle Access Manager applications use to reference object profiles during operations (such as search). User Manager uses an attribute that contains a user's name. Group Manager uses an attribute that contains a group's name. Organization Manager uses an attribute that contains an organization's name.

OID (Object Identifier)

A unique value identifying an LDAP attribute.

OIS (Oracle Identity Server)

The service name for the Oracle Identity Server (also known as the Identity Server). This component routes requests from the web server to perform transactions in the User Manager, Group Manager, and Organization Manager applications. This component is referred to as OIS.

open

A transport security mode where no authentication and no encryption is performed. For example, the AccessGate does not demand any proof of the Access Server's identity, and the Access Server accepts connections from all WebGates connected to it. Transport security between all Identity System components must match. Transport security between all Access System components must match.

optional attributes

During request processing, those attributes whose value specifications are defined as optional.

Oracle Access Manager

The Oracle unified solution, integrating identity management and Web access management for E-business networks. It contains two integrated modules: the Identity System (required) and the Access System (optional).

Oracle Access Protocol (OAP)

The protocol governing communications between Access System components (Policy Manager, Access Server, WebGate) and a Web server.

Oracle Identity Federation

Organizes an enterprise's user identification policies to allow a wide range of associates such as vendors, distributors and customers to access protected resources using authentication proofs from a variety of sources.

Oracle Identity Protocol (OIP)

The protocol governing communications between Identity System components (Identity Server, WebPass) and a Web server.

Oracle Specific Data (OSD)

Oracle Access Manager configuration settings (also known simply as configuration data). See also **configuration data**.

Organization Manager

This application allows companies to create and delete organizations and manage their ongoing changes. Organization management can be delegated.

Password Management Services

Provide comprehensive password management. Customers can specify multiple password policies, constraints on password composition, configurable password validity period and notification, forced password change, lost password management setup, and password creation/change rules.

Personalization Services

Oracle Access Manager enables personalization and Web SSO for other applications through HTTP header variables and redirection URLs. When Oracle Access Manager authenticates or authorizes user requests, the URL it returns can contain HTTP header variables, redirection URLs, or encrypted cookies. The HTTP header variables can contain any user data stored under the authenticated user's ID in the directory, thereby providing a rich source of information for personalization purposes on that particular user. The downstream application can decode this information and use it to personalize the user experience. You can also include a redirection URL in the URL returned by Oracle Access Manager after an authentication or authorization event. This redirection URL may take the user to another Web page, for example, tailored to the identity of the user. In addition to providing personalization services, an encrypted cookie can be included in the URL returned by Oracle Access Manager to enable Web single sign-on.

PKI (Public-Key Infrastructure)

A security infrastructure that provides services implemented by public key concepts and techniques.

plug-in

A component added to Oracle Access Manager to change or enhance its behavior.

policy

The set of authentication, authorization, and auditing rules that apply to one or more resource types within a policy domain. In the absence of a policy for a specific resource type, the default rules for all resource types in the policy domain apply.

policy base

The location in the DIT under which all policy data is stored.

policy-based authorization

The use of security policies for controlling access to Web and non-Web resources (such as applications, content, services, and objects in applications).

policy domain

A policy domain encompasses the resources you want to protect, the rules for protection, the policies for protection, and the administrative rights. Policy domains are defined in the Policy Manager.

Policy Manager

The application through which users can perform policy management, designation of resources (both Web and non-Web), and policy testing through simulated user access.

Policy Manager API

An Oracle Access Manager standard API (a subset of the Access Manager SDK) used to write applications that use the programmatic interface instead of the Policy Manager user interface to create, modify, delete, and retrieve policy domains and their contents and to allow custom applications to access the authentication, authorization, and auditing services of the Access Server. For more information, see Oracle Access Manager Developer Guide.

pooling

The process of defining a hierarchy of primary and secondary Access Servers. NetPoint Access System (NPAS) opens and closes connections to these Access Servers in order to evenly distribute the work load. See also **NetPoint Access System (NPAS)** on page Glossary-14.

pooling Access Servers

The process of an Access Server opening or closing connections to Access Servers in order to maintain adequate load balancing.

Portal Inserts

Embeddable pieces of Oracle Access Manager functionality and workflows that are available as URLs and can be placed anywhere on a customer site or portal.

pre and post processing (PPP)

External actions that can take place before or after a step in an Identity System workflow. For example, an administrator can choose to have specific persons emailed after a workflow step takes place. Associated with the Identity Event Plug-in API.

Presentation Services

Allow companies to customize the user interface for the Identity System end-user applications and to integrate Oracle Access Manager functionality seamlessly into their portals. These services include: Portal Inserts and PresentationXML.

PresentationXML

Allows the Oracle Access Manager product user interface to be completely customized. The product outputs XML, and you can combine this output the with the XSL style sheets that Oracle provides to allow the customer to change the interface to fit their needs.

profile

A set of attributes that describe an object.

Query Builder

Oracle Access Manager feature that helps users create dynamic LDAP filters. Also known as the Filter Builder.

query string variables

Variables that allow you to determine who can send certain input parameters to a program, which in turn can control the behavior of the program itself.

relative distinguished name (RDN)

The left-most (bottom) attribute value in the DN.

reporting

The process of collecting Oracle Access Manager audit information in an SQL-compatible database and presenting this using one of the specially configured Crystal Report templates supplied by Oracle Access Manager.

request

An in-process workflow definition that was initiated by a user. Requests can include multiple tickets.

request ticket

See **ticket**.

Required attributes

When you are defining a workflow step, any attributes you set as required must have values assigned to them when a user processes this workflow.

resource

Within Oracle Access Manager, the information or activity that can be protected by the Access Server. A policy domain is an example of a protected information resource, a method within an application is an example of a protected activity.

rights

An Oracle Access Manager Administrator (also known as the Master Administrator) can assign the following kinds of rights:

View: Users with View rights can view the name and value of an assigned attribute in an object profile.

Modify: Users with Modify rights can change the value of an assigned attribute in an object profile.

Notify: Users with Notify rights receive an email notification whenever an assigned attribute is changed.

Basic: Administrators with Basic rights can assign View, Modify, or Notify permissions to users for all attributes under their control.

Grant: Administrators with Grant rights can assign basic rights to users and other administrators for all attributes under their control.

Delegate: Administrators with Delegate rights can assign grant and delegate rights to users and other administrators for all attributes under their control.

roles

The predefined lists of users. Roles can include all users, all managers, direct reports, and so on.

root directory

The first URL prefix entered into the system. This is the starting point for all policy domains.

rule, LDAP

See **LDAP filter**.

rule, URL

See **LDAP URL rule**.

rules

In Oracle Access Manager, the list of conditions during which access is allowed or denied and to which end user(s) these conditions apply. Rules also govern the way in which auditing is done.

SASL (simple authentication and security layer)

SASL provides a means for clients and servers to negotiate an authentication mechanism dynamically.

schema

A schema defines the type of information stored in a directory. It consists of object classes and attributes.

searchbase

The location in the DIT where users can begin their searches.

Security Services

Services that provide authentication, authorization, and auditing to all your applications and e-business efforts, as well as help users and administrators to manage passwords and certificates. These services include: Authentication Services, Authorization Services, Auditing Services, Password Management Services, and Certificate Management Services.

Selector

The Oracle Access Manager utility used to locate and select one or more users and groups.

self registration

The process a new user can employ to gain limited access to your system through the initiation and processing of a self-registration workflow.

self-service

The process of modifying attributes without the use of a workflow.

semantic type

Semantic types apply an Oracle Access Manager business rule to an attribute. Examples of business rules are reporting relationship and on-screen location of an end user's photo and job title.

shared secret

The feature that allows administrators to generate a cryptographic key that encrypts cookies sent from a WebGate to a browser.

signing authority

RSA signing identity that is hosted by the main domain site and can issue digital certificates to the associate domain site.

simple

A transport security mode where the communication between the Oracle Access Manager Web clients (Identity Server and WebPass, WebGate/AccessGate and Access Server, and Policy Manager and WebPass) is encrypted using TLS v1 (Transport Layer Security, RFC 2246) and protected with X.509 digital certificates and a global password. Transport security between all Identity System components must match. Transport security between all Access System components must match.

single sign-on (SSO)

The method of transparently accessing multiple protected web servers with only a single login. Users needing access to single-domain servers store a generated cookie, used for subsequent requests to the Web site. Users needing access to multi-domain servers store a cookie generated by a central Web login server; this is transparently done for each accessed server within the associated Web system.

single-table database

A single-table database does not necessarily refer to a database that contains just one table, but rather, a database that stores in just one table all the user profile attributes that get mapped into the top level virtual directory.

SNMP Agent

The Simple Network Management Protocol (SNMP) is an application-layer protocol that enables network devices to exchange information. By using SNMP-transported data (such as successful operations and failure conditions), administrators can monitor network performance and solve problems. The Oracle Access Manager SNMP agent enables you to implement SNMP-based data collection for the Identity Server and Access Server.

split profile

A special type of embedded virtual data source created from more than one data source. Each data store contributes some of the attributes necessary to complete the full set of user profile attributes that gets mapped into the VDS virtual directory. These attributes can come from LDAP directories or database tables. All the Oracle Access Manager user schema attributes must reside in the primary data store, because not all Oracle Access Manager operations can be performed on the attributes in the secondary stores.

VDS can make a split profile visible to Oracle Access Manager as a standard LDAP directory. Alternatively, a split profile can be federated as part of a virtual directory. For an illustration, see the *Oracle Access Manager Installation Guide*.

SSL (Secure Sockets Layer)

A method for establishing an encrypted connection between a client and a server.

static group

A group whose member list is explicitly defined.

static member

A member of a static group.

Static Participants

One or more users assigned responsibility for completing a given workflow step. These users are specified in the workflow applet by person, group, role or rule.

structural object class

Structural object classes contain basic attributes required for use within Identity applications. When you create a tab within an Identity application, you must assign a structural object class to it.

subclassing

The process of creating a new object class based on an existing object class and specifying that the existing class is its superior. The new object class inherits the set of required attribute types, the set of optional attribute types, and the kind of object class from its superior.

subflow

Subflows are workflows spawned by another workflow. Subflows operate independently and can spawn subflows of their own.

substitute administrator

Substitute administrators are users who have permission to temporarily take all of your rights and responsibilities. This is useful in the case of vacations or extended leaves, where the job needs to be done but it would be too difficult administratively to remove all permissions from the absent employee and assign them to someone else.

super directory

A special type of virtual directory that facilitates namespace mapping and directory-wise searches. It can contain any combination of federated LDAP directories, RDBMS databases, and embedded virtual data sources. The embedded virtual data sources can be split profiles, native RDBMS Joins, and native RDBMS Views. The super directory, which is the only supported method for producing a single, contiguous searchbase aggregated from multiple data stores, connects to Oracle Access Manager by means of a VDS local store adapter. For details, see the *Oracle Access Manager Installation Guide*.

superior

The class that another class inherits some of its characteristics from in the subclassing process.

Surrogate Participants

One or more users assigned workflow ticket-processing responsibilities whenever a given static participant or dynamic participant activates the Out of Office flag in his or her user profile. The surrogate receives incoming tickets as long as that Out of Office flag remains active.

synchronizing

Synchronizing enables you to harmonize two installations of the same Oracle Access Manager component when one is more up-to-date than the other. Synchronization can be used to upgrade or repair installations on similar platforms.

ticket

A pending activity for a user to perform (usually an administrator or delegated administrator). For workflows, the ticket ID contains an appended step ID number.

Time-based Escalation

Whenever a workflow ticket is not processed within a specified interval, responsibility for processing the ticket is transferred from the original participant who failed to act to a new participant, such as the manager of the original participant. If the new participant fails to process the ticket within the specified interval, the ticket is escalated again, and so on, until it ultimately reaches the Oracle Access Manager Administrator.

transport security mode

The method used to protect the information transfer path between two points, often a client and a server. In Oracle Access Manager, the transport security mode is most often used to highlight that the transfer path is secured (for example with SSL encryption) rather than left in the clear. See the Oracle Access Manager security modes: Open, Simple, and Cert. Transport security between all Identity System components must match. Transport security between all Access System components must match. Transport security between all Identity System components must match.

Unicode

A universal encoded character set that enables you to store information from any language using a single character set. Unicode provides a unique code value for every character, regardless of the platform, program, or language.

Unicode standard

The universal character encoding standard that provides a unique number for every character in any language (for example, English, European languages, Asian languages. This standard forms the basis for consistency in processing, storing, and interchanging text data for software and information technology protocols on any platform, for any program. See the Unicode Consortium Web site at `http://www.unicode.org/` for more information.

URI

Uniform Resource Identifier - the generic term for the unique name of any resource on a network. A URL is one kind of URI.

URL

Uniform Resource Locator - a type of URI specific to the World Wide Web.

URL pattern

The fine-grained portion of the policy domain's Web namespace is specified as a pattern. The specific URL pattern syntax is described in the *Oracle Access Manager Identity and Common Administration Guide*.

URL prefix

Starting point for your policy domain. The URL prefix maps to a directory on your web server's file system.

User Action Steps

Workflow steps that require explicit (non-automated) processing by a step participant.

User Manager

This application allows companies to create, remove, and manage ongoing changes in user identities and access privileges based on the user profile. User identity administration can be delegated.

UTF-8

Unicode Transformation Format 8(UTF-8). UTF-8 is a reasonably compact, variable-width encoding scheme. Oracle Access Manager supports UTF-8 encoded data in directory servers. The UTF-8 encoding form assigns each Unicode scalar value to an unsigned byte sequence of one to four bytes in length. The UTF-8 encoding scheme serializes a UTF-8 code-unit sequence in precisely the same order as the code-unit sequence itself.The UTF-8 encoding scheme, defined in Annex D of ISO/IEC 10646:2003, is a technical equivalent to definitions in the Unicode Standard.

UTF8

The UTF-8 encoded character set, by Oracle, based on Unicode version 2.1. Introduced with Oracle8 and 8 *i*. Oracle9i included an updated version of the Oracle UTF8 character set to support Unicode standard 3.0. To maintain compatibility with existing installations, the UTF8 character set will remain at Unicode version 3.0.

virtual directory

A logical, aggregated directory that presents user data drawn from multiple sources, just as if all that data came from a standard LDAP directory to which a customer-defined schema has been uniformly applied. For the purposes of integration, the Oracle Virtual Directory Server (VDS) does *not* create permanent copies of user profiles outside the native data sources. Rather, VDS retrieves and transforms each user profile as it is requested by an Oracle Access Manager application. For details, see the *Oracle Access Manager Installation Guide*.

virtual directory schema

This is the schema developed by the customer for use by the top-level directory that the Oracle Virtual Directory Server (VDS) makes visible to Oracle Access Manager. It must be extended with the Oracle Access Manager user schema. Optionally, you can further extend the virtual directory schema with customer attributes drawn from the target data sources. For details, see the *Oracle Access Manager Installation Guide*.

Web resources

Any subset of an HTTP URL. Typically, they can be Web pages, directories, CGI scripts, or Web-enabled applications.

Web server

Program that, using the client/server model and the World Wide Web's Hypertext Transfer Protocol (Hypertext Transfer Protocol), serves the files that form Web pages to Web users (whose computers contain HTTP clients that forward their requests).

Web single sign-on

Single authentication to multiple resources (applications, content, services, objects in applications). To achieve single sign-on, customers centralize the security for various resources, so that developers can reuse the centralized information and avoid having a different security scheme and user database associated with each application.

WebGate

An Oracle-provided out-of-the-box Web server plug-in access client that acts as the interface between individual Web servers and the Access Server. The WebGate

intercepts HTTP requests for Web resources and forwards them to the Access Server for authentication and authorization. You can create a custom WebGate, known as an AccessGate, using the Access Manager SDK. See also **AccessGate**.

WebPass

This component is a plug-in that is placed on the web server to shuttle information back and forth between the web server and the Identity Server.

workflow

The automation of procedures where information or tasks are passed between participants and programs according to a defined set of business rules. Introduced into Identity applications to enable customers to automate their business processes.

workflow actions

Each step within a workflow allows one action (approval, provide info, and so on).

workflow definition

The flow of responsibility, defined actions, and responsible individuals combined together to perform the process necessary to complete a workflow type.

workflow participant

All of the people, groups, roles, and so om that can take part in a workflow step, therefore receiving a ticket.

Workflow Services

Users and systems can submit requests that can go through multiple steps and be routed internally or externally. Customers can set workflow definitions for:

Creating, deleting, and modifying users, groups and organizations

Self registration of users and organizations

Subscribing to groups and unsubscribing

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

X