

This FAQ addresses frequently asked questions relating to Oracle Access Manager 10gR3 and how it integrates with other Oracle Identity Management components.

- 1.0 General Information
- 2.0 Core Functionality
- 3.0 Technical Information
- 4.0 What's new in 10gR3?
- 5.0 Integration With Oracle AS SSO
- 6.0 Integration with Oracle and other 3rd party products
- 7.0 Product Availability and Pricing

1.0 General Information

1.1 What is Oracle Access Manager?

Oracle Access Manager (OAM) is Oracle Identity Management's solution for web access management and user identity administration. Out of the box, Oracle Access Manager is designed to support complex, heterogeneous enterprise environments. Oracle Access Manager consists of two tightly integrated components: the Access and Identity Systems. The Identity System provides delegated administration of user profiles and workflow for creating, updating, and deleting these profiles. It also provides applications for user self-registration, password management and dynamic group management. The Access System provides access control and single sign-on to Web applications and J2EE resources (EJBs, servlets, etc.) running on a variety of Web and Application servers.

1.2 What components are provided with Oracle Access Manager?

Oracle Access Manager consists of tightly coupled Identity and Access Systems. These two systems are integrated, so that a profile change made via the Identity System takes effect instantaneously for access evaluation by Access the System. The Access and Identity Systems also include web server agents namely, WebGate and WebPass, for all leading Web and Application servers. The following components are shipped with Oracle Access Manager:

- Identity Server
- WebPass
- Access Server
- WebGate
- Policy Manager

- Access Manager SDK
- Policy Manager API

1.3 What are WebGate and WebPass?

A WebPass is a web server plug-in (NSAPI filter, ISAPI filter or Apache Module) that passes information back and forth between a web server and the Identity Server. The WebPass provides two interfaces: the standard browser-based interface, which renders HTML-based content; and a SOAP web service interface called IdentityXML, which provides a programmatic interface into the Identity System functionality. Note that the HTML-based interface of WebPass also provides access to the Identity System Console, which is the administrative interface into the Identity System.

A WebGate is a web server plug-in (NSAPI filter, DSAPI filter, ISAPI filter or Apache Module) that intercepts HTTP requests from users for Web resources and forwards them to the Access Server for authentication and authorization. It is basically the Access System's Policy Enforcement Point (PEP).

1.4 What is Policy Manager?

The Policy Manager provides the policy administration interface for the Access System console. The Master Access Administrators and Delegated Access Administrators can use the Policy Manager to define policies and resources to be protected and to group resources into policy domains.

1.5 What are the Access and Identity System Consoles?

The Access Manager installation includes the Access and Identity System Consoles, which enable Oracle Access Manager administrators to perform Access and Identity system configuration and management.

1.6 What is the Access Manager Software Developer's Kit (SDK)?

The Access Manager Software Developer's Kit (SDK) enables developers to construct interfaces for other applications so that they can use the Access System for authentication and authorization. The SDK includes an Access Manager API that lets developers create custom access clients (also known as AccessGates) that interface with both Web and J2EE resources. The Access Manager SDK consists of libraries, build instructions, and examples to allow developers to build a custom AccessGate for web and Java resources.

1.7 What is the difference between AccessGate and WebGate?

A WebGate is an out-of-the-box Access Server client for web servers, which specializes in protecting HTTP resources. An AccessGate is a custom or general purpose Access Server client that processes user requests for Web and non-Web resources and is developed using the Access Manager SDK.

1.8 What is Oracle Access Manager Configuration Manager?

Oracle Access Manager Configuration Manager is a standalone Java application that is designed to work with Oracle Access Manager 10gR3 and Oracle COREid 7.0.4 to automate the process of migrating configuration data from one instance of Oracle Access Manager or COREid to another. This process, often referred to as horizontal data migration, allows you to migrate all of the configuration data stored in a LDAP directory across instances of Access Manager or COREid running in specific deployment environments, including:

- Development or sandbox type environments
- QA or other testing environments
- Pre-production or staging environments
- Production environments
- Other custom environments

1.9 How does Oracle Access Manager Configuration Manager work?

Oracle Access Manager Configuration Manager is a new, optional add-on component that enables you to automate the task of pushing configuration data changes from a specified source directory in one deployment to an associated target directory in another deployment. It does this by connecting to the LDAP directories in each deployment.

Oracle Access Manager Configuration Manager allows you to create a snapshot backup of your existing configuration data, create associations (Directory Pairs) between your existing configuration directory and a new configuration directory, and then migrate that configuration data between the two directory instances. When you migrate data, all entries that you select in the configuration tree are copied from the source directory server to the associated target directory server. Configuration Manager migrates only LDAP data, not files. You can migrate both physical entries and logical objects between your source and target directory environments. (Workflow Definitions are an example of logical objects that may be migrated between directory environments.) Configuration Manager provides a mechanism to preview logical objects in tree-view form prior to migration, and to define and apply transformation rules, giving you the tools to easily identify and manipulate the objects to be migrated.

1.10 How is Oracle Access Manager Configuration Manager licensed?

Oracle Access Manager Configuration Manager is a Java application that requires Oracle Application Server (OC4J) for deployment and runtime support and an Oracle Database as the Configuration Manager repository. An instance of Oracle Database and OC4J are provided with the Configuration Manager installation. For customers that do not already have a license to use OC4J, they are entitled to use it, at no additional cost. This limited use license restricts the use of this OC4J instance to use with Configuration Manager only. We do not bundle license of Oracle Database. The customer is expected to either already own or purchase a license to use Oracle Database with Configuration Manager.

1.11 Where can I find documentation for Oracle Access Manager?

Oracle Access Manager's documentation consists of a number of distinct books:

- Introduction
- Installation Guide
- Upgrade Guide
- Identity and Common Administration Guide
- Access Administration Guide
- Deployment Guide
- Customization Guide
- Developer Guide
- Integration Guide
- Schema Description

Product documentation is available here:

10.1.4.0.1 Documentation:

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

10.1.4.2.0 Documentation:

http://download.oracle.com/docs/cd/E10761_01/welcome.html

10.1.4.3.0 Documentation:

http://download.oracle.com/docs/cd/E15217_01/index.htm

2.0 Core Functionality

2.1 What are the main features of Identity System?

The Identity System provides

- Centralized user, group and organization management
- Integrated Identity Workflow engine
- User self-registration and self-service
- Password Management
- Extensive APIs for customization

2.2 What are the features provided by the Identity System for customization?

The Identity System provides the following components to enable customization.

- Identity Event plug-in APIs – these APIs enable the development of small applications called actions that enable the customization of the Identity System business logic.
- Identity XML – Allows interaction with the Identity Server without a browser.
- Portal Inserts – These are embeddable pieces of Identity System functionality that are available as URLs and can be inserted into other applications without programming
- PresentationXML – Enables Identity System User Interface customization.

2.3 What are the main features of the Access System?

The Access System provides

- Centralized authentication and Single Sign-on
- Policy-based authorization to HTTP and J2EE resources
- Centralized auditing and reporting
- APIs for custom plug-ins
- Connectors to integrate with various 3rd party platforms

2.4 What are the different Authentication mechanisms that are supported?

Oracle Access Manager supports the following authentication schemes: basic username/password authentication, X.509 certificate-based authentication, HTML form-based authentication, RSA SecurID, and Smart Cards.

2.6 What are the different resource types that can be protected by the Access System?

The Access System can be configured to protect HTTP and J2EE resources. The resource type to be protected can be specified using the Access Manager. The HTTP resource types include web pages, directories, web applications and query strings. The J2EE resources include, Java server pages, EJBs and servlets. Other resource types that can be protected include standalone Java/C++/C programs, ERP and CRM applications.

2.7 What is a policy domain and how do I configure it?

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

2.8 What is an Authentication plug-in?

An authentication *plug-in* is a shared library that participates in the user authentication process. Plug-ins are used to implement customized authentication schemes. They implement challenge methods, map user credentials to user profile entries in a directory, process user credentials, perform custom tasks related to the authentication process, and so on. The Access System provides out-of-the-box authentication plug-ins for all the

authentication schemes it supports by default. The default plug-ins can be replaced with custom authentication plug-ins to serve other purposes involved in the authentication process

2.9 How do I create a custom Authentication plug-in?

Custom authentication plug-ins can be created using the plug-in APIs that are shipped with the Access Server. These APIs are located in the install directory, typically `<Access_server_install_dir>/access/oblix`. The APIs support the development of both C/C++ and .Net (C# and Visual Basic). The Oracle Access Manager Developer's Guide contains detailed information about plug-in development.

2.10 What is an Authorization plug-in?

Similar to an authentication plug-in, an authorization plug-in is a shared library (.dll or .so) that the Access Server uses to make outbound calls to external business logic for determining user authorization privileges and actions. An Authorization plug-in provides customized authorization functionality. An authorization plug-in can accept user parameters, configuration parameters and context specific information such as HTTP header variables.

2.11 Does Oracle Access Manager provide Self-Service and Delegated Administration?

Yes. Oracle Access Manager includes the Identity System, which allows customers 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 Identity System features a flexible and powerful workflow engine across all three of the following modules:

- **User Manager** – This application provides users with a web interface to create, remove, and modify user accounts and access privileges based on their entitlements, role, or group. User Manager also provides user account self-registration, password management, and a multi-step workflow engine for managing requests. User identity administration can be delegated to any number of users (i.e. n-delegation).
- **Group Manager** - This application provides users with a web interface to create, modify and delete groups. Groups can be static, dynamic, nested or any combination thereof. It allows users to subscribe/unsubscribe from groups with a workflow engine that controls requests. Group management can also be delegated out to other users.
- **Organization Manager** - This application provides users with a web interface to create, modify, and delete organizations and any generic data that are defined in the directory. Organization Manager also has workflow and delegation capability.

2.12 Can I centrally manage Oracle Access Manager's WebGates and AccessGates?

The WebGate and AccessGate components are centrally managed through the Access System's Administration Console, which is a web-based interface that allows administrators to create, update and remove agent configuration, including:

- Agent identifiers, which includes host name, port number, internal component ID assigned to this component in the system, and the shared secret it uses to authenticate to the Access Server.
- Configuration data, such as, which Access Server to connect to (or to which cluster), failover and load-balancing configuration, failover thresholds, keep-alive interval for connection keeping, number of elements and lifespan of the policy cache.
- Session based parameters, such as maximum session timeout, DNS domain on which the session cookie is to be bound.
- Security based parameters, transport level encryption, enabling/disabled IP address validation checking, session token encryption keys and ciphers.

3.0 Technical Information

3.1 How does Authentication work in Oracle Access Manager?

Oracle Access Manager's authentication architecture consists of 3 main areas:

- The authentication challenge mechanism – the challenge mechanism determines how credentials are gathered from the end user. For WebGates, these are basic HTTP challenge, HTML Form-based challenge, X.509 certificate challenge, External authentication challenge (which instructs the WebGate to fetch a HTTP header variable within the memory context of the web server, such as REMOTE_USER, as a credential), and no-challenge (which is particularly relevant for “unprotecting” public content).
- The authentication flow – defines the sequence of steps that the authentication scheme should follow to authenticate the user. For example, the first step could be to map the user against a unique entry in the directory based on the users' credential, and the second could be to validate the user's password through an LDAP bind. However, if this second step fails, the third step could be to try to authenticate the user against NT or SecurID. The authentication flow allows for orchestrating and arranging various authentication steps in any way that make sense for the end user. At the end of a successful authentication flow, the user session is established with the authentication level associated to the particular authentication flow.
- The authentication steps – these are Authentication plug-ins that the Access Server instantiates and invokes within its memory context. These are the actual working modules that implement the authentication logic. For example, there is a plug-in that maps user entries against the directory through LDAP search calls, there is another that performs an LDAP bind operation, likewise there is a plug-in to decode and parse an X.509 certificate, etc. Authentication plug-ins can be custom developed using the Authentication API, and customers have relied on this API to effectively

extend the authentication options, in some cases to integrate with legacy systems, or in others to integrate new authentication technology. Also, Oracle partners who are part of the extended IdM ecosystem program, which Oracle announced on June 14, 2006, are leveraging this API to build integration between Oracle Access Manager and their particular authentication technology.

3.2 Can I programmatically manage Oracle Access Manager policies?

Oracle Access Manager provides the Policy Manager API, which is an API that developers can use to programmatically manage Oracle Access Manager access policies. The most common scenarios requiring these custom policy administration interfaces include:

- Automation of the policy creation process as a downstream step in publishing content – a Financial Services customer who published financial reports (as PDF files) has a very complex set of access rules tied to who can view a particular report, which can be tedious and error-prone for an administrator to do. Hence, they have automated the process of creating these access policies as a step right after the content is published.
- Bulk load policy creation – for cases in which customers have a batch of applications or resources that need to be protected. A custom policy administration interface can be built to process the many requests for policy creation at once and map them into the appropriate format.
- Specialized UI/Replacing homegrown system – for cases where customers are delegating the administration of access policies to a set of end users, who have grown used to a particular interface to manage policies, customers choose to build a specialized UI which leverages the Policy Manager API on the backend, such that the impact on the end users is minimized, thus minimizing any customer or administrator retraining required.

3.3 What APIs are available to customize or extend Oracle Access Manager?

Oracle Access Manager offers a comprehensive set of integration options for its solution. These 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.

- Authentication Plug-in API – API to extend number of available authentication methods not provided out-of-the-box, and for chained authentication processes. In essence, this allows the Access Server to utilize a custom authentication method or to use an external authentication provider.
- Authorization Plug-in API – This API allows customers to extend policy evaluations through dynamic callouts to custom code. As an example, a policy administrator can set a policy that allows an end user to access some resource if his/her bank balance exceeds a certain amount. Moreover, this allows the Access Server to utilize an external authorization source.

- Access Manager API – This API gives customers the ability to extend Oracle Access Manager’s authentication, authorization, and auditing services to non-web resources such as client-server applications.
- Policy Manager API – This API allows application to programmatically manage access policies as opposed to utilizing the UI.
- IdentityXML – allows applications to programmatically utilize identity administration functionality available in the Identity System through a SOAP-based web services interface.
- Event Plug-in API – This API allows customers to extend the business logic of the Oracle Access Manager 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 Oracle Access Manager, to do data validation, or to pre-populate fields based on other information provided.

The Oracle Access Manager Developer Guide has a complete list of APIs and customization points.

3.4 What standards does Oracle Access Manager support?

Below is a list of standards supported by Oracle Access Manager:

- Web/SOA Protocols - SMTP, HTTP(S), SOAP
- Identity Management - LDAP, ADSI, XACML (Future)
- Security Standards - Kerberos, PKI (X.509, AES, SHA-1, RC6, PKCS), SSL , TLS, JAAS
- J2EE, Web Services, Integration and XML Standards - EJB, J2EE Connector, JNDI, JDBC, ODBC, OCI, WSDL, UDDI, WS-Trust (future)
- Development Standards - J2EE, .NET, C/C++, XML DTD, HTML, HTMLCSS, XML Namespaces, XML Schema, XPATH, XSD, XSLT

3.5 What are the installation pre-requisites for Oracle Access Manager?

- Server Platform – OS and hardware requirements are published (and updated periodically) in the [Oracle Access Manager platform support matrix](#). These outline the OS and HW support options for the Identity and Access Servers.
- Depending on the system (Windows vs. Unix), topology and the expected performance requirements, the memory and disk space requirements would vary. A minimal of 512MB of RAM and 1GB of HDD is required for most Oracle Access Manager components.
- LDAP Directory – Oracle Access Manager relies on an LDAP directory server as the identity and configuration (including policy) store. The [list of supported directory servers](#) is updated periodically, so customers need to verify version and platform requirements before installing. Administrative access to the directory is required during install.
- Web Server – The management interfaces of Oracle Access Manager install as plug-ins to leading web servers, hence at least one available instance of a supported web

server is required. The [list of supported web servers](#) is updated periodically, so customers need to verify version and platform requirements before installing.

- Network – When deployed in a distributed environment, Oracle Access Manager requires TCP/IP network access so that each component can connect. Depending on the TLS option chosen to encrypt the communication between components, time synchronization (i.e. NTP) between the various servers will be required. Likewise, if SSL encryption is required, valid server digital certificates may be required.
- (Optional) Audit Database – If audit information is to be stored in a database, an instance of a supported database will be required. Oracle Access Manager supports MS SQL Server and Oracle databases for auditing.

3.6 Does Oracle Access Manager provide auditing and reporting capabilities?

Oracle Access Manager supports auditing, logging, SNMP monitoring, and other reporting features.

Auditing - Through a completely configurable log format, Oracle Access Manager allows administrators to choose the fields and format to log the information in. Logging and tracking can also be selected on a granular basis, allowing the logging of only those resources that are sensitive or of the usage patterns of particular web servers.

The Access System automatically audits administrative events, such as clearing information from caches. Audit policies set in the Master Audit Rule and audit rules derived from it determine what is tracked. Audit policies can be configured for:

- Authentication and authorization success or failure
- Resource access
- Policy modification

The administrator can customize audit output to include user profile attributes.

Reporting - The auditing feature collects and presents data pertaining to policy and profile settings, system events, and usage patterns. This information can be used for reporting. Oracle Access Manager can generate two types of audit reports:

- Static: These reports are derived from policy and profile information that is stored on the backend directory server.
- Dynamic: These reports are derived from Access System and Identity System events that are collected from the servers through auditing.

At the most detailed level, dynamic audit reports reveal when a system event was triggered and who triggered it. At a higher level, these reports can reveal component load levels, resource request patterns, system intrusion attempts, and overall system performance.

All dynamic audit reports and some static audit reports can be exported to a file, to a relational database, or both.

3.7 What reports are provided out of the box?

Oracle Access Manager provides a set of pre-defined Crystal Reports templates, which have been defined based on the most common reports used in meeting compliance requirements. These include:

- Authentication Statistics (success/failed rates across all Access Servers)
- Authorization Statistics (success/failed rates across all Access Servers)
- Failed Authorizations (by user)
- Failed Authorizations (by resource)
- Access testing
- Group History (all changes to all Group profiles)
- Identity History (by user)
- Locked-out users
- Password Changes (in a particular interval of time)
- Users Created/Deactivated/Reactivated/Deleted
- User profile modification history (for all users)
- Deactivated users report
- Workflow execution time

3.8 What logging and diagnostic tools does Oracle Access Manager provide?

Oracle Access Manager collects a wide range of program execution data such that administrators can troubleshoot system performance issues and diagnose component health problems. Administrators can control logging activity for components by specifying log output for individual Access Servers, Identity Servers, Policy Managers, WebPasses, WebGates, custom AccessGates, and custom plug-ins.

The parameters that control logging activity reside in configuration files stored with each component. The log output for each component can be configured through the administrative UI or configuration files. The log data generated by a specific component can be output to either of the following destinations, or neither, or both:

- A log file stored in the directory tree under the root installation directory of the component generating the data.
- The system file of the machine hosting the component's logging data. (When more than one component resides on the same host, all components can send data to the system log file on that machine).

For convenience, the many thousands of program events and states reportable through logging are classified within an eight-level, pyramidal hierarchy. At the highest level, the Fatal category includes about 60 catastrophic events that usually force a component to exit. At the bottom of the pyramid, the Trace level reports about 900 Access Manager API and 150 third-party API calls and their outcomes. In most cases, these Trace level messages are meaningful only to developers and plug-in programmers.

Oracle Access Manager 10gR3 also includes a command-line diagnostic tool that allows the production of real-time server status information in a XML format. The information includes status of caches, threads, and mutex objects within the servers.

3.9 What monitoring capabilities does Oracle Access Manager provide?

The Simple Network Management Protocol (SNMP) enables monitoring component activity on the network that hosts the Oracle Access Manager system by collecting and displaying server-related SNMP data on a network management station. Oracle Access Manager supports version 2 of the SNMP protocol. SNMP statistics commonly include data such as:

- The hosts, routers, and servers on the network.
- The number of requests being processed on a particular device.
- Whether or not a particular device is running.
- Whether requests were processed successfully.

SNMP data is displayed on a network management station (NMS), such as HP OpenView or IBM Tivoli, which can capture SNMP statistics for the Identity Server and the Access Server running on any supported platform.

Oracle Access Manager supports SNMP polling and trapping. Polling collects information such as:

- The version number of a component
- Configuration status
- Connection status
- Statistics on actions the component has processed

Event traps include information such as:

- Component failure
- Event failure
- Connection status
- Failure to complete actions

The SNMP information is gathered through Management Information Base (MIB), which is a specification file that contains variables relevant to the status of different Oracle Access Manager components. The SNMP Agent collects values for fields in the MIB.

4.0 What's new in 10gR3?

4.1 Globalization and Localization

Oracle Access Manager supports multi-byte [utf-8] characters in 10gR3. All the existing features (user management, password management, access control, and etc) have been enhanced to allow users to input, process and output internationalized data. To increase the

global outreach, Oracle Access Manager is also being localized to 27 languages for end-users and 9 languages for Administrators.

4.2 Password Policy enhancements

- Track the last login time
- Lost Password Management using multiple password hints
- Password policies that are configurable for different domains (e.g. one for intranet users and another for extranet users)
- Improved Password composition rules
 - Check for numeric characters in a password
 - Check for user id in a password
- Redirect user to the Back URL after password reset
- Improved tracking of inactive user accounts

4.3 Downtime reductions

Oracle Access Manager 10gR3 provides a zero downtime migration approach for customers. The approach will eliminate server outages throughout the migration. LDAP calls have been enhanced to be asynchronous calls, thereby preventing downtime due to server hang-ups when LDAP servers are unresponsive. Changing the LDAP bind passwords no longer require restarting components of Oracle Access Manager.

4.4 Shared secret enhancements

This allows crypto operations related to security tokens to be performed on the Access Server instead of at the web gate.

4.5 Oracle HTTP Server (OHS) support for Oracle Access Manager Web components

The Oracle Access Manager web server components – WebPass, WebGate and Policy Manager – are integrated out of the box with Oracle HTTP Server.

4.6 Performance enhancements

There have been several enhancements to increase the performance of Oracle Access Manager. Performance increases are made to various operations including GUI display operations, large static group operations, and Access Management SDK calls.

5.0 Integration with Oracle Single Sign-on

5.1 How does Oracle Access Manager differ from OracleAS Single Sign-on?

They are similar products in that both perform user authentication. However Oracle Access Manager also provides powerful policy-based authorization functionality to web and J2EE

resources, which OracleAS Single Sign-on does not. They are currently separate products and can be used together in a single environment if required. Oracle Access Manager access also provides integrations with a broad set of non-Oracle products and platforms.

5.2 When would I buy Oracle Access Manager vs. OracleAS SSO?

Oracle Access Manager is ideally suited for deployment in a non-Oracle or a heterogeneous environment. Currently, Oracle Access Manager can also be deployed with 3rd party Application Servers such as Oracle WebLogic and IBM WebSphere. Oracle Access Manager also supports a number of 3rd party web servers, Portal servers and packaged ERP and CRM applications. It is also best suited for policy-based URL-authorization, and can be used in conjunction with OracleAS SSO's authentication functions.

OracleAS SSO is best suited to be deployed with Oracle infrastructure and applications.

5.3 How will Oracle Access Manager and OracleAS SSO evolve in the future?

OracleAS SSO will be “fused” with Oracle Access Manager to provide authentication and authorization across both Oracle and non-Oracle products.

6.0 Integration with Oracle and other 3rd party products

6.1 How does Oracle Access Manager integrate with other Oracle products?

As a part of Oracle Fusion Middleware, Oracle Access Manager is pre-integrated with

- Oracle Fusion Applications (Oracle eBusiness Suite, PeopleSoft, JD Edwards and Retek, Siebel)
- Oracle Fusion Middleware components (Oracle HTTP Server, Oracle Portal, and Oracle Container for J2EE (OC4J))
- Oracle Collaboration Suite

6.2 How Does Oracle Access Manager integrate with Oracle's Enterprise Single Sign On (eSSO) Suite?

Oracle Access Manager is integrated with the Oracle Enterprise Single Sign-On Suite (Oracle eSSO). There are 3 points of integration between these two: a) Oracle eSSO can automatically log in a user into Access Manager to effectively provide non-web and web SSO; b) Oracle eSSO and Access Manager can leverage the same backend user directory for identity and credential store; c) Oracle eSSO password reset and self-service capabilities from the desktop (GINA-based) can be leveraged to effectively reset the user password's in the underlying directory, used by Oracle Access Manager. Hence, the user can use this route to unlock and regain access to web applications.

6.3 How does Oracle Access Manager integrate with Oracle Virtual Directory?

Oracle Access Manager is certified to leverage Oracle Virtual Directory as an identity store, this way Access Manager can leverage any backend configuration that is virtualized through Virtual Directory. The integration includes pre-tested schema mapping templates that can be leveraged by customers to address the most common Virtual Directory topologies (i.e. virtualizing internal and external user directories).

6.4 How does Oracle Access Manager integrate with Oracle Internet Directory?

Oracle Access Manager integrates with Oracle Internet Directory as a backend data store, using it to store server configuration data, policy data, and user identities or groups data. Oracle Access Manager provides schema files out-of-the-box for Oracle Internet Directory (and other supported directory servers) to simplify the deployment of a complete identity and access management system.

6.5 How does Oracle Access Manager integrate with Oracle Identity Manager?

Oracle Access Manager is part of the Oracle Access and Identity Management Suite, which also includes Oracle Identity Manager. Identity Manager is a market leading provisioning and identity administration solution, with differentiating functionality around auditing and reporting. Oracle Access Manager integrates with Oracle Identity Manager to protect Identity Manager's web interface, as well as to provide web SSO. Oracle Identity Manager on the other hand can manage the underlying directory upon which Oracle Access Manager is deployed, such that user provisioning functionality translates to real-time access to applications and resources protected by Oracle Access Manager. The coupling of the two products makes for a complete end-to-end identity and access management solution with support for heterogeneous platforms and directory services.

6.6 How does Oracle Access Manager integrate with Oracle Identity Federation?

Oracle Access Manager provides out-of-the-box integration with Oracle Identity Federation, which supports all major protocols, including SAML, Liberty ID-FF, and WS-Federation. Both products can share a common user repository and Oracle Identity Federation can delegate Authentication and Authorization decisions to Oracle Access Manager. Oracle Identity Federation deploys as a self-contained stand-alone federation server and can seamlessly integrate with Oracle Access Manager – or other Web Access Management systems – deployed at either an identity provider or service provider site to manage user sessions.

6.7 Is Oracle Access Manager supported on Oracle Unbreakable Linux?

Yes. Oracle Access Manager 10gR3, when deployed on Red Hat Linux 3.0 or 4.0 is supported through the Oracle Unbreakable Linux support program. For more information on Oracle Unbreakable Linux, please visit: <http://www.oracle.com/technologies/linux>

6.8 What 3rd party products and platforms does Oracle Access Manager integrate with?

Oracle Access Manager integrates with a wide set of 3rd party Application servers, Web servers, Directory servers and Portal servers. The following support matrix summarizes the 3rd party product and platform support.

Applications	Application Servers	Web Servers	Directory Servers	Portal Servers	Operating Systems
Oracle eBusiness Suite	Oracle Application Server	Oracle HTTP Server	Oracle Internet Directory	Oracle Portal Server	RedHat Linux SUSE Linux
PeopleSoft	IBM WebSphere	IBM HTTP Server	Oracle Virtual Directory	IBM WebSphere	NT/Win 2000/Win 2003
JD Edwards	Oracle WebLogic	Apache	IBM Tivoli Directory	Oracle WebLogic	Solaris
Retek		Domino	Novell eDirectory	Plumtree (BEA AquaLogic)	
Siebel		Microsoft IIS	Microsoft Active Directory	Oracle WebCenter	
SAP		Sun Java System Web Server	Microsoft ADAM		
Oracle Business Intelligence			Sun Java System Directory		

6.9 Where can current and planned platform support information for Oracle Access Manager be found?

Detailed platform support information for both base OS platform support as well as integration with 3rd party products is periodically updated and published externally at: http://www.oracle.com/technology/products/id_mgmt/coreid_acc/pdf/oracle_access_manager_certification_10.1.4_r3_matrix.xls

6.10 Is Oracle Access Manager supported on VMWare virtualized environments?

Oracle Access Manager has not been certified on VMWare virtualized environments. Support will be provided only in the following manner: Oracle will only provide support for issues that either are known to occur on the native OS platform, or can be demonstrated not to be as a result of running on VMWare.

For more information, please refer to Metalink under [note 249212.1](#).

7.0 Product Availability and Pricing

7.1 Where can I find more information about Oracle Access Manager and Oracle Identity Management products?

For general information about Oracle and its products and services, see <http://www.oracle.com/>. For specific information about Oracle's Application Server products see <http://www.oracle.com/technology/products/ias/index.html>. For specific information about Oracle Identity Management see http://www.oracle.com/technology/products/id_mgmt/index.html

7.2 Where can I find more information about Oracle Access Manager pricing?

Pricing information is available at <http://www.oracle.com/corporate/pricing/index.html>

ORACLE FUSION MIDDLEWARE

Oracle Application Server 10g: Oracle Access Manager 10gR3 FAQ

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Copyright © 2009, Oracle. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice.

This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission. Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.