

Migration Best Practices for OpenSSO 8 and SAM 7.1 deployments

ORACLE WHITE PAPER | MARCH 2015





Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.



Table of Contents

Disclaimer	1
Introduction	2
Migration Strategy	3
Migration Best Practices	5
Familiarize with Oracle Access Management 11gR2	5
Run Assessment Tool	6
Pre-Migration Tasks	6
Perform Migration for Large Deployments in Phases	7
Post-Migration Tasks	7
Server Co-existence	7
Co-existence Topology	7
Co-existence Limitations	8
Conclusion	9



Introduction

Oracle recognized the need for comprehensive access management and has delivered a solution that addresses the broadest set of access management capabilities ranging from Web Single Sign On, Identity Federation and Security Token Services to Mobile Security, Social Identity and Fraud Prevention under a single umbrella. Oracle's truly unique Oracle Access Management 11gR2 platform provides comprehensive and internet scale Access Management in a single product, with innovative new services and simplified deployment and management.

Oracle Access Management Oracle Access Management 11gR2 (referred to as simply Oracle Access Management 11gR2) is a service component and the foundation of Oracle Access Management that provides the core functionality of web single sign-on, authentication, authorization, centralized policy administration and agent management, real-time session management and auditing.

Oracle Access Management 11gR2 provides the following benefits:

- Centralized policy management and auditing reduces cost and improves compliance.
- Support for access management in a heterogeneous environment reduces total cost of ownership and accelerates deployment.
- Flexible and powerful policy model allows organizations to meet complex access management needs.
- Scalable deployment model supports most demanding, internet scale deployments.
- Extensible architecture enables easy customization to meet organization specific requirements.

Existing OpenSSO 8 and Sun Access Manager (SAM) 7.1 customers should consider migrating to Oracle Access Management 11gR2 to leverage the benefits described above as well as take advantage of the platform approach of Oracle Access Management 11g to address new requirements beyond Web-SSO like mobile access, fraud prevention, web services security, cloud-based solution etc. Finally, OpenSSO customers should migrate to the 11g platform before premium support ends.



This document describes the capabilities of Oracle Access Management 11gR2 that facilitate OpenSSO 8 and SAM 7.1 customers to move to the new platform, the various migration strategies they can adopt and the best practices they should follow to ensure a smooth and successful migration. To aid readability, the term OpenSSO is used to refer both OpenSSO 8 and SAM 7.1 in the rest of this document.

Capabilities to support migration

While existing OpenSSO customers would like to move to the new 11g platform to leverage the new benefits it provides, they will need a clear migration path that will ensure a smooth transition with minimal impact on their end users. Oracle Access Management 11gR2 provides the following three key capabilities to ease the migration for existing OpenSSO customers.

- » **Agent Compatibility.** Oracle Access Management 11gR2 provides Agent Compatibility in order to allow enterprises currently on OpenSSO to continue using their existing OpenSSO Policy Agents (2.2 or 3.0) while upgrading their server infrastructure to the new 11gR2 platform. A Protocol Compatibility Framework allows the Access Manager server to communicate with OpenSSO agents the same way it can communicate with the new 11g WebGates. This capability is especially important for OpenSSO customers with large deployments since they can focus on upgrading their server infrastructure first and adopt a more phased approach for replacing their existing OpenSSO agents with new 11g WebGates over time.
- » **Migration Utility.** In order to reduce the manual effort of migration, Oracle Access Management 11gR2 provides a set of command line utilities that includes:
 - » The OpenSSO Assessment tool goes through the policies and configuration of the existing OpenSSO server and generates a report listing out all the artifacts and whether they are fully compatible, partially compatible or incompatible with the 11g policy model. Customers can use this report to analyze the incompatibilities and decide the appropriate course of action to resolve them.
 - » The OpenSSO Migration tool performs the actual migration of policies and configuration from the existing OpenSSO server to the new Oracle Access Management 11gR2 server. The artifacts that get migrated include Policies, Agents, User Stores and Authentication Stores. This migration utility takes as an input a property file containing the details of the policy and configuration store of the existing OpenSSO server along with other migration parameters. It takes care of mapping the OpenSSO policy artifacts that are compatible to the new 11gR2 policy model.
- » **Server Co-existence Support.** In case of very large deployments with thousands of agents and applications spread across the enterprise, it may not be advisable to do the server migration at one go. To ensure zero down time migration, Oracle supports OpenSSO and Oracle Access Management 11gR2 server co-existence to enable customers to gradually migrate from OpenSSO servers to 11g over time. With server co-existence, both 10g and 11g servers can be live in production at the same time protecting different sets of applications while providing SSO across all applications.

Migration Strategy

Leveraging the above capabilities, customers can plan their migration strategy based on the overall size of the deployment. Typically, customers with small to medium deployments should consider doing a complete migration

of the server in one shot though they can replace OpenSSO agents with 11g WebGates over a period of time. Large deployments should consider a phased approach for the server migration where the existing OpenSSO server and Oracle Access Management 11gR2 server would co-exist in the same environment till the migration completes.

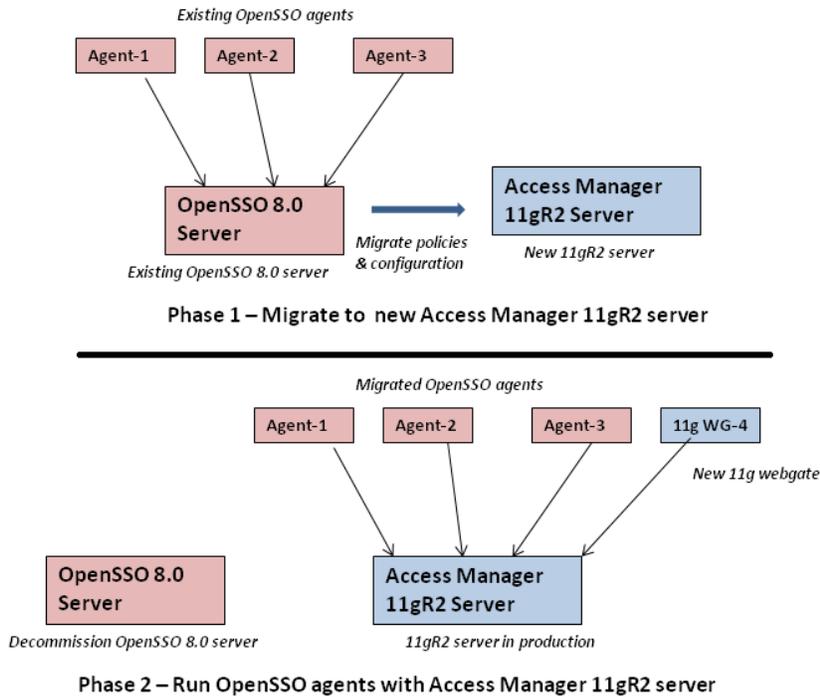
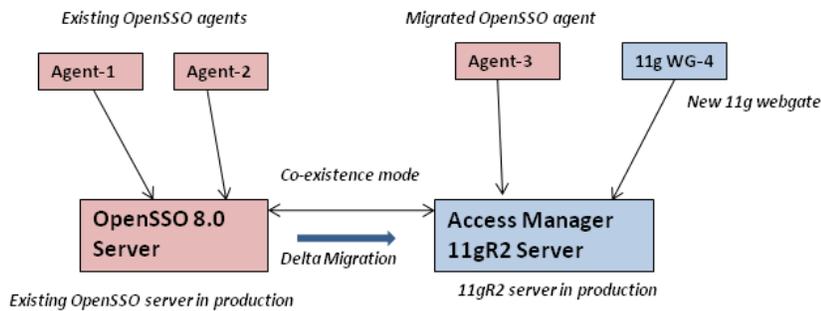


Figure 1. Migration from OpenSSO to 11gR2 without server co-existence

Figure 1 above depicts how an organization would migrate from their current OpenSSO platform to the new Oracle Access Management 11gR2 platform without using server co-existence mode. Using migration utilities, organizations will do a complete migration of policies and configuration from the existing OpenSSO server to the new Oracle Access Management 11gR2 server in Phase 1. Once migrated, the existing OpenSSO server will be decommissioned while the migrated OpenSSO agents will start working with the new Oracle Access Management 11gR2 server during Phase 2. Any new applications deployed during this phase can start using a new 11g WebGate that will communicate with the Oracle Access Management 11gR2 server.



Phase 2 with co-existence – Both OpenSSO and Access Manager 11gR2 server in production

Figure 2. Difference in Phase 2 by introducing server co-existence.

Figure 2 above shows how Phase 2 would differ in case an organization chooses to do the server migration over time and therefore configures the existing OpenSSO server and the new Oracle Access Management 11gR2 server in a server co-existence mode. In this case, customers will do a complete migration of policies and configuration from OpenSSO server to the new Oracle Access Management 11gR2 server in the beginning but will selectively point some of the migrated agents to the new Oracle Access Management 11gR2 server. At any point in time, some of the OpenSSO agents will continue to work with the existing OpenSSO server whereas the remaining OpenSSO agents along with any new 11g WebGates will work with the Oracle Access Management 11gR2 server. Agents pointing to the OpenSSO server can be updated to point to the Oracle Access Management 11gR2 server over time. During this co-existence phase, if new artifacts are created on the OpenSSO server, they can be migrated to Oracle Access Management 11gR2 using the Delta mode of migration. This phase will continue till all the OpenSSO agents are pointing to the Oracle Access Management 11gR2 server at which point the OpenSSO server can be decommissioned. Any new applications deployed during this phase can start using a new 11g WebGate that will communicate with the Oracle Access Management 11gR2 server.

While the migration utility provides a simple way to move policies from OpenSSO to the 11g platform, it may not necessarily be the optimal solution for very small deployments where the number of agents and policies are low (less than 20). In such cases, customers can choose to manually recreate policies in the 11g server and register either existing OpenSSO agents or new 11g WebGates against it.

Migration Best Practices

Following are some recommended best practices to ensure a smooth migration from OpenSSO to Oracle Access Management 11gR2.

Familiarize with Oracle Access Management 11gR2

The console user interface and navigation as well as a number of artifact names in the 11gR2 platform are significantly different from the old OpenSSO platform. It is highly recommended that customers planning to migrate to the new 11gR2 platform invest time to acquaint themselves with new terminology and user interface. Administrators should go through the 11gR2 product documentation to familiarize themselves with concepts and terminology in 11gR2 and how this maps to their existing OpenSSO nomenclature.

For example, Oracle Access Management 11gR2 has no concept of “Referral” policies like OpenSSO does. So these policies would not get migrated. Similarly, in OpenSSO one can have a policy without any artifacts or a policy with rules but no subjects or conditions whereas one cannot create such policies in 11gR2.

Understanding these differences and familiarizing oneself with the 11g interface and policy model before starting on the migration would go a long way in ensuring a smooth migration.

Run Assessment Tool

The OpenSSO Assessment Tool provides a powerful tool for OpenSSO customers to get an idea of what the migration entails. It goes through the policy and configuration store of OpenSSO and creates a set of assessment reports on all the artifacts to be migrated including Agents, Policies, Authentication Stores and User Stores. The Excel-based report provides details on every artifact, whether it is fully compatible (Auto-Policies), partially compatible (Semi-Policies) or incompatible (Manual-Policies) with the 11g policy model and what manual action, if any, will be required post-migration. For example, OpenSSO policies having no artifacts or having only rules but no subjects or conditions are considered incompatible and cannot be migrated. Separate reports are created for Agents, Policies, Authentication Stores, User Stores and Dashboard Info. Figure 3 below depicts a screenshot of the excel-based assessment report. Running the OpenSSO Assessment Tool can provide customers with a lot of useful insight on what manual effort, if any, will be required after the migration and an approximate idea of how long the actual migration would take. It is recommended that OpenSSO customers should first run the OpenSSO Assessment Tool and use the generated reports to create a migration plan. For policies that are incompatible, administrators can decide appropriate course of action like creating them manually in 11g after the migration.

Policies:						
Realm Name:	/					
Policy:						
	Name	Description	isReferral	isActive		OAMCompatible
	Policy1_LDAP1	Policy1 with LDAP1, under Top Realm	FALSE	TRUE		Auto
	Details:					
	Rules:					
	Name	Service Type	Resource Name	Action Value		OAMMapping
	rule1	iPlanetAMWebAgent Service	http://adc2140266.us.oracle.com:8003/agentapp/index1.html	{POST=[deny], GET=[allow]}		Yes
	rule3	iPlanetAMWebAgent Service	http://adc2140266.us.oracle.com:8003/agentapp/index3.html	{GET=[allow]}		Yes
	rule2	iPlanetAMWebAgent Service	http://adc2140266.us.oracle.com:8003/agentapp/index2.html	{POST=[allow], GET=[allow]}		Yes
	Subjects :					
	Name	Type	isExclusive			OAMMapping
	sub2	AMIdentitySubject	FALSE			Yes
	sub1	AMIdentitySubject	FALSE			Yes
	subGroup1	AMIdentitySubject	FALSE			Yes
	Conditions:					
	Name	Type	ConditionValue			COND_OAMMapping
	LDAP1	AuthSchemeCondition	{AuthScheme!=[LDAP]}			Yes
	Response Providers :					
	Name	Type	OAMMapping			
	response1	IDRepoResponseProv	Yes			
	response2	IDRepoResponseProv	Yes			
	Policy:					
	Name	Description	isReferral	isActive		OAMCompatible
	Policy2_LDAP_WindowsDesktopSSO	policy with LDAP, Windows Desktop SSO in authn store	FALSE	TRUE		Auto

Figure 3. Excel-based Assessment Report generated by migration tool.

Pre-Migration Tasks

There are a few steps administrators should pay close attention to before running the actual migration. Migration for large deployments with thousands of policy artifacts will need sufficient memory for processing. The Java heap size



for the WebLogic Administration Server should be increased as needed prior to running the migration. Also, the size of the log file should be increased to ensure the migration logs are not lost during rotation of the log files.

Like any software migration process, it is recommended to take adequate back-ups of the source and target environments to restore in case of unforeseen failures.

Perform Migration for Large Deployments in Phases

In case of very large OpenSSO deployments with thousands of agents and applications spread across the enterprise, it may not be advisable to do the server migration at one go. In such cases, customers can choose to perform the migration in a phased manner over a period of time. Customers would start by setting up a new Oracle Access Management 11gR2 infrastructure and configuring it to work with OpenSSO server in a co-existence mode. After verifying SSO works between the two, they will run a complete migration of all the artifacts from OpenSSO to Oracle Access Management 11gR2. But instead of pointing all the agents to the new Oracle Access Management 11gR2, customers can choose to point just some of the migrated agents while the others can continue to point to the existing OpenSSO server. They can plan to update these remaining agents to point to Oracle Access Management 11gR2 in batches over a period of time. For example, a customer with an OpenSSO deployment having 1000 agents can choose to update 50 agents at a time to point to the new 11gR2 server and complete the migration in 20 increments over a period of 6 months. During this period, if new agents or policies are configured in OpenSSO, the customer can leverage the Delta mode of migration to synchronize the new artifacts with the 11gR2 server.

In order to ensure an SSO experience for end users, customers would need to manually update the authentication scheme of the migrated applications previously using LDAPScheme to OAM10gScheme. The authentication schemes of migrated applications that were previously using other schemes like X509Scheme need not be updated to OAM10gScheme so end users would still get challenged for credentials as expected (step up authentication).

Customers with very large deployments can thus take advantage of the Delta mode of migration and Co-existence support to mitigate the risk of a single “big-bang” migration.

Post-Migration Tasks

The migration takes care of copying the artifacts from the OpenSSO store to the 11g2 store. But there are a few manual steps needed after migration run to actually associate a specific migrated OpenSSO Agent to the Oracle Access Management 11gR2 server. This includes manually copying the properties file for every agent. Also, passwords for User Stores are not migrated and need to be manually updated after the migration. Finally, the Minimum and Maximum Connection Pool Size need to be configured manually.

Needless to say, the most critical post-migration task is to verify whether the migration has been performed correctly. Administrators should also login to the admin console and visually verify whether all artifacts have gotten migrated properly and check the log files for any errors or warnings. They should plan to test various migrated policies and verify whether runtime behavior is as expected. The Access Tester utility that ships with 11gR2 can be leveraged for this testing.

Server Co-existence

Co-existence Topology

As explained in the previous section, customers with large deployments that choose to perform their migration in increments will need to configure their OpenSSO and Oracle Access Management 11gR2 servers in co-existence

mode till they complete the migration. The co-existence mode configuration essentially ensures that authentication always happens at the OpenSSO instance irrespective of whether application that is being accessed is protected by OpenSSO server or Oracle Access Management 11gR2 server. This is done by protecting all resources in Oracle Access Management 11gR2 by a specific Authentication scheme called OAM10gScheme. Also, the Oracle Access Management 11gR2 server itself is protected by an OpenSSO agent which redirects to the OpenSSO server for authentication

Figure 4 below depicts the topology for co-existence between OpenSSO and Oracle Access Management 11gR2 servers. Both are configured to use the same User and Authentication Store. When the user tries to access a resource R protected by the Oracle Access Management 11gR2 server, it gets intercepted by Agent 1 which tries to contact the 11g server. But since the server is protected by Agent 2, the latter intercepts that request and redirects to the OpenSSO server which throws the login page. Once the user enters his credentials, the LDAP module of the OpenSSO server authenticates the user against the Authentication Store and if successful, establishes an OpenSSO session and redirects back to Agent 2. Agent 2 verifies the OpenSSO Cookie 1 from the browser and sets the header OAM_REMOTE_USER to the User ID. Oracle Access Management 11gR2 now invokes the OAM10g Scheme, asserts the user based on the header and establishes an Access Manager 11g session. It also creates the OAM Id cookie and OpenSSO cookie 2 using the OpenSSO Proxy before redirecting the user to the requested resource. Since the browser now has cookies to satisfy both OpenSSO and Oracle Access Management 11gR2 servers, the user can navigate between applications protected by either of them without being challenged.

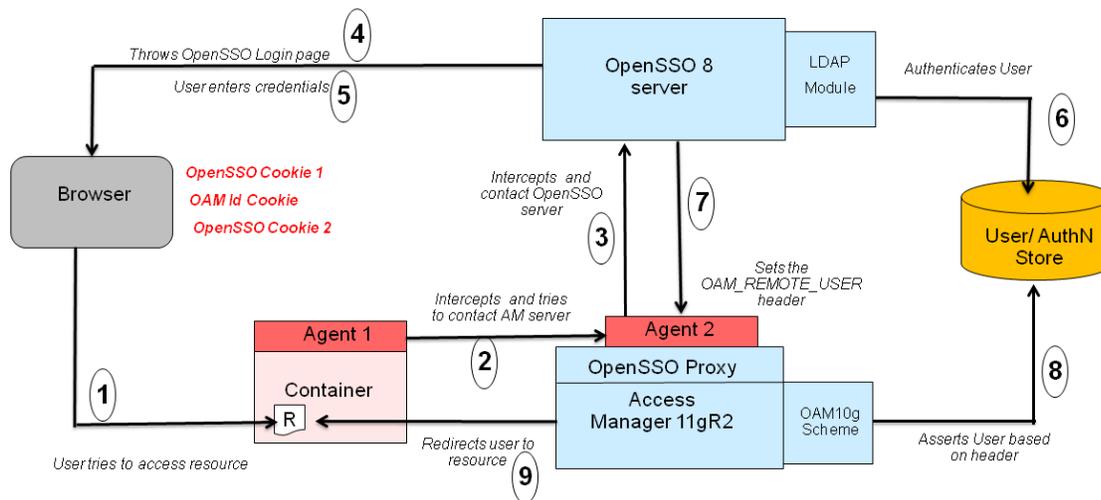


Figure 4. Topology for Co-existence between OpenSSO and Oracle Access Management 11gR2

Co-existence Limitations

While server co-existence provides a convenient mechanism for customers to run their OpenSSO and 11g platforms in parallel during the migration while keeping it transparent to end users, they need to be aware of the limitations and restrictions it presents. Since all the authentication is essentially delegated to the existing OpenSSO platform, customers cannot take advantage of any new authentication related feature of the new 11gR2 platform like



Detached Credential Collector (DCC) or Password Policy as long as they are running in a co-existence mode. Also, customers would need to manually update the authentication scheme of the migrated applications using LDAPScheme to OAM10gScheme in order to enable the single sign on behavior.

Further, since Oracle Access Management 11gR2 creates sessions based on authentication at the OpenSSO end, it limits the session management capabilities of Oracle Access Management 11gR2. For example, even if an administrator terminates all the 11g sessions of a particular user through the admin console to lock out the user, new sessions would get automatically re-created as long as the user has valid cookies to login to the OpenSSO server. There are also certain limitations introduced in the Session Lifetime and Idle Timeout parameters as well as the logout settings to facilitate seamless SSO experience for the end user between the two servers.

Customers should take these limitations into account before deciding whether a phased incremental migration approach with co-existence would be a practical approach for them.

Conclusion

Oracle's new, innovative Oracle Access Management 11gR2 platform is the most complete and scalable access management solutions in the market and customers on existing OpenSSO platforms should strongly consider migrating to the new 11g platform to take advantage of the various benefits it has to offer. Oracle Access Management 11gR2 also provides a clear migration path consisting of agent compatibility, migration utility and server co-existence support which can enable customers to have a smooth and successful migration.



CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com

Oracle Corporation, World Headquarters

500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries

Phone: +1.650.506.7000
Fax: +1.650.506.7200

Hardware and Software, Engineered to Work Together

Copyright © 2015, Oracle and/or its affiliates. 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.0115

MIGRATION BEST PRACTICES FOR OPENSOURCE 8 AND SAM 7.1 DEPLOYMENTS

March 2015

Author: Venu Shastri

Contributing Authors: Svetlana Kolomeskaya, Forest Yin



Oracle is committed to developing practices and products that help protect the environment