International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991
Vol. 6, No. 1
February 2017

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 6, No. 1, February 2017

Research Paper

ACCESS MANAGEMENT AND SINGLE SIGN ON

Md Muzaffar Shariff[1]* and Basha[2]

*Corresponding Author: Md Muzaffar Shariff ✉ shariffsh25@gmail.com

This paper describes the the requirement specification for Authentication and Authorization Security and forms the basis from which the technology solutions will be designed. The document contains description of the features to be implemented as well as requirements for the Authentication and Authorization.

Keywords: Identity and access management, SSO, Authentication, Authorization

INTRODUCTION

This paper describes the the requirement specification for Authentication and Authorization Security and forms the basis from which the technology solutions will be designed. The document contains description of the features to be implemented as well as requirements for the Authentication and Authorization.

OBJECTIVES

- Creating applications.
- Achieving Access management by integrating all resources and systems in an organization.
- Implementing strong authentication using two factor authentication.
- Providing authorization in order to secure the resources.
- Implementing SSO technique for every user to have access over various applications within the system.
- Having Centralised access control.

EXISTING SYSTEM

- Where everything is manually operated.
- Every employee enter into the organization and into their respective departments are handled by the people in admin section.
- The daily log of employee and management is maintained in manual registers which are later entered into the systems by other persons.

Requires a Lot of Time-Effort

- Distributed control.

[1] Department of Computer Science and Engineering, Vishwa Bharathi PG College of Engineering & Management (Approved by Aicte, New Delhi, Ministry of HRD, Govt. of India), Kuppenakuntla (V), Penuballi (M), R.R. District 501503, India.

[2] Assistant Professor, Department of Computer Science and Engineering, Vishwa Bharathi Pg College of Engineering & Management (Approved by Aicte, New Delhi, Ministry of Hrd, Govt. of India), Kuppenakuntla (V), Penuballi (M), R.R. District 501503, India.

Limitations of Existing System

- Completely handled by humans where there are lot of chances to do manipulations.
- No security to any of the organization resources.
- Distributed system so any information that has to be informed to all is not possible.
- Access to any resource of any user may not be monitored each and every minute.

PROPOSED SYSTEM

- Automating every operation by implementing IAM.
- Employee once they join into the organization will be automatically identified and their access over any resource will be pre-defined.
- So trying for any resource which the person is not authorized will be denied by checking.
- Security is provided for each and every resource present in the organization.
- Notification regarding any event or information will be directed to the respective persons with reduced time effort compared to existing system.
- Centralised system.

OVERVIEW

Authentication

Oracle Access Manager 11 g application domains aggregate resources and security policies (one policy per resource). Oracle Access Manager 11 g authentication policies include a specific scheme. Supported authentication modules include LDAP, X.509, and Kerberos. Authentication user mapping is performed against the primary user-identity provider by the centralized credential collector.

Authorization

Oracle Access Manager 11 g performs authorization based on security policies defined in the application domain and persisted in the database. Authorization policies define the resource and constraint evaluation.

Responses

Administrators can set session attributes using authentication and authorization Responses. Aside from session attributes, a Response can also obtain user-related data and request-related data. Responses, once set, are then sent as either HTTP Headers or Cookies to the agent that helps manifest them. For cookie values and header variables, Responses can retrieve session attributes previously set by another Response. For example, session attributes set by a Response upon authentication can be retrieved as a header value during authorization.

Session Management

Oracle Access Manager 11 g session management services track active user sessions through a high performance distributed cache system based on technology from Oracle Coherence. Each Oracle Access Manager runtime instance is a node within the distributed cache system. Secure communication between the nodes is facilitated using a symmetric key. The Oracle Access Manager runtime instances move user session data in the local cache into the distributed cache for other nodes to pick up. Each Oracle Access Manager runtime instance can also configure the replication factor and determine how session data is distributed. Administrators can configure the session lifecycle, locate and remove specific active sessions, and set a limit on the number of

concurrent sessions a user can have at any time. Out-of-band session termination prevents unauthorized access to systems when a user has been terminated.

Keys

The Oracle Access Manager 11 g runtime is deployed as an application to a WebLogic Managed Server or Cluster. New Oracle Access Manager 11 g WebGates support a shared secret per agent trust model. 11 g WebGates use agent/ host specific cookies, which offers superior security. Oracle Access Manager 11 g WebGates are all trusted at the same level; a cookie specific for the WebGate is set and cannot be used to access any other WebGate-protected applications on a user's behalf. Cookie-replay types of attacks are prevented.

SSO

The Oracle Access Manager 11 g Server Session Token forms the basis for SSO between Oracle Access Manager and OSSO Agents. Logout is driven through Oracle Access Manager 11 g Server Global Logout, which terminates the central session and logs out the user from each agent that was visited.

Implementation

Integration

This integration scenario enables you to manage identities with Oracle Identity Manager and control access to resources with Access Manager. Access Manager provides a centralized and automated Single Sign-On (SSO) solution. Access Manager uses a database for policy and configuration data and a single directory for identity data. This integration scenario assumes a single directory server, namely Oracle Internet Directory, is front-ended by Oracle Virtual Directory. Oracle Identity Manager is a user provisioning and administration solution that automates user account management.

Integrating Access Manager and Oracle Identity Manager

- Create a new AccessGate by completing the following steps:
- After logging in to the console, click on the Access System Configuration link.
- Now open the Access System Configuration tab.
- Click on the Add New AccessGate link.
- Complete the following fields on the Add New AccessGate page:
  - AccessGate Name: Enter a suitable name for this Access Gate.
  - Hostname: Type in the hostname of the AccessGate machine.
  - AccessGate Password: Specify a password.
  - Preferred HTTP Host: The hostname entered here will appear in all HTTP requests as they attempt to access the protected resource, regardless of the way the hostname was defined by the client in the HTTP request.
- You can leave all the other fields as default.
- Click Save when you have finished.
- Identify a host to install EM12cR3. Install EM12cR3.
- Create OUD Authenticator and OAM ID Asserter using the EM Weblogic Admin Console.
- Change the Order of Authenticators and AssertersAs the web tier utilities have already

been installed with EM12c, the only product installation is Webgate.

- Configure the Webgate installed in previous step to rely on OAM for authentication.
- Configure OMS for OAM integration

Single Sign On (SSO)

Single sign on can be implemented for WebCenter applications using several solutions This section describes their benefits and recommended application.

Oracle Access Manager (OAM), part of Oracle's enterprise class suite of products for identity management and security, provides awide range of identity administration and security functions, including several single sign on options for WebCenter Spaces and WebCenter Portal applications. OAM (in particular, OAM 11 g) is the recommendedsingle signonsolution for Oracle WebCenter 11 g installations.

- Users sign onto a site only once and are given access to one or more applications in a single domain or across multiple domains.
- "In any client/server relationship, single sign-on is a session/user authentication process that permits a user to enter one name and password in order to access multiple applications."
- SSO gathers the various authentication credentials of a user from each security domain into a central repository. The repository is accessed by a single set of authentication credentials for a user. When a user requests access to a known security domain the credentials for that domain are passed in to gain access.
- The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.

Concept of SSO can be used within an Intranet, Extranet or Internet.

METHODOLOGY

Figure 1: Login to Oracle Access Manager

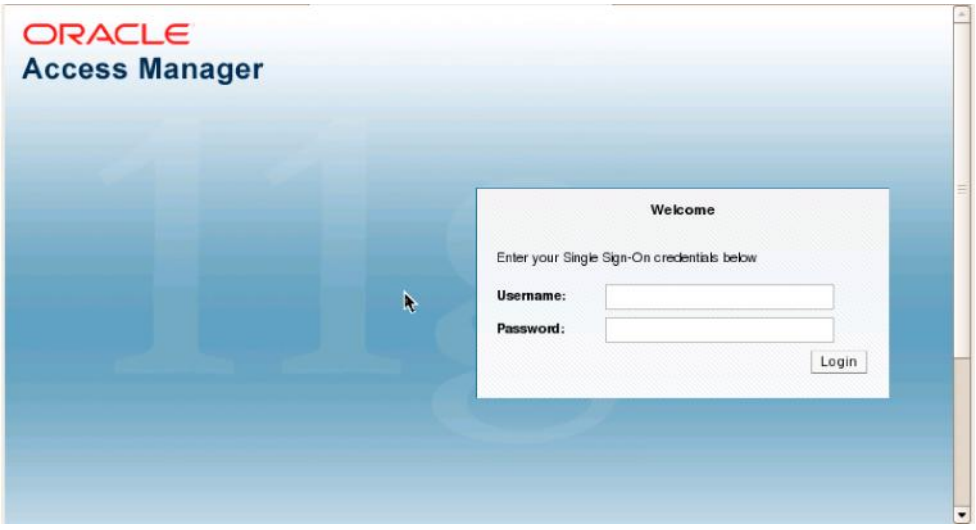


Figure 2: Go to System Configuration

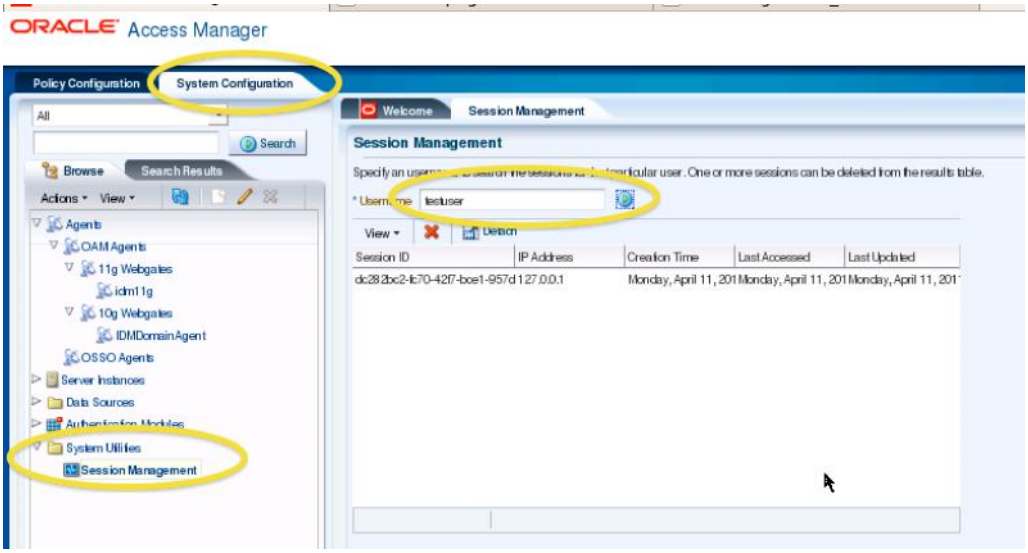


Figure 3: URL Protection

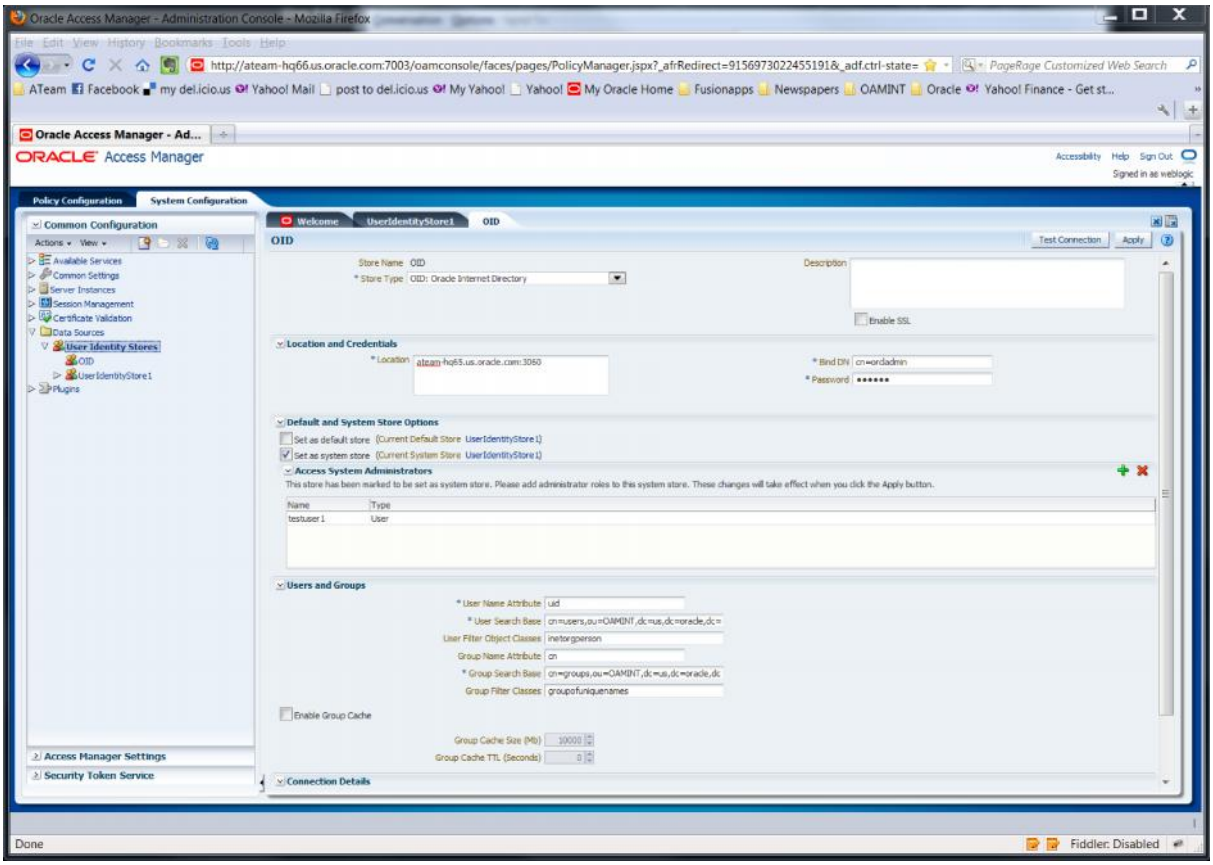


Figure 4: Audit Policy

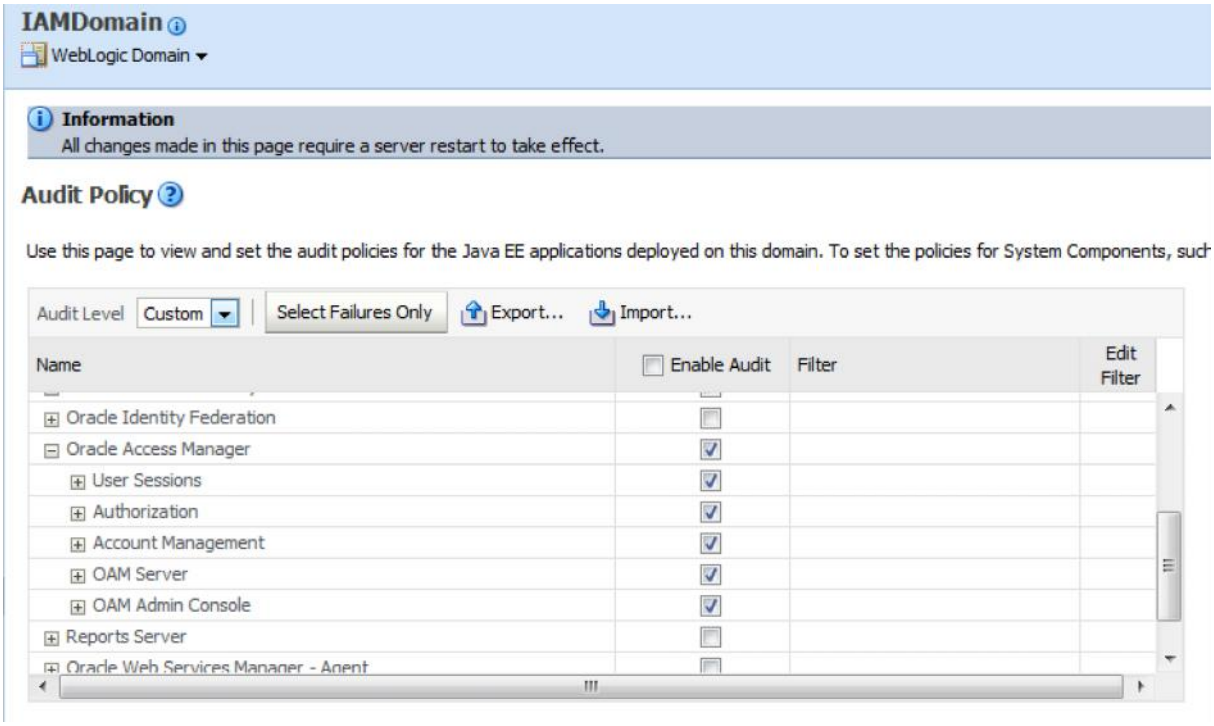


Figure 5: USSO Agent

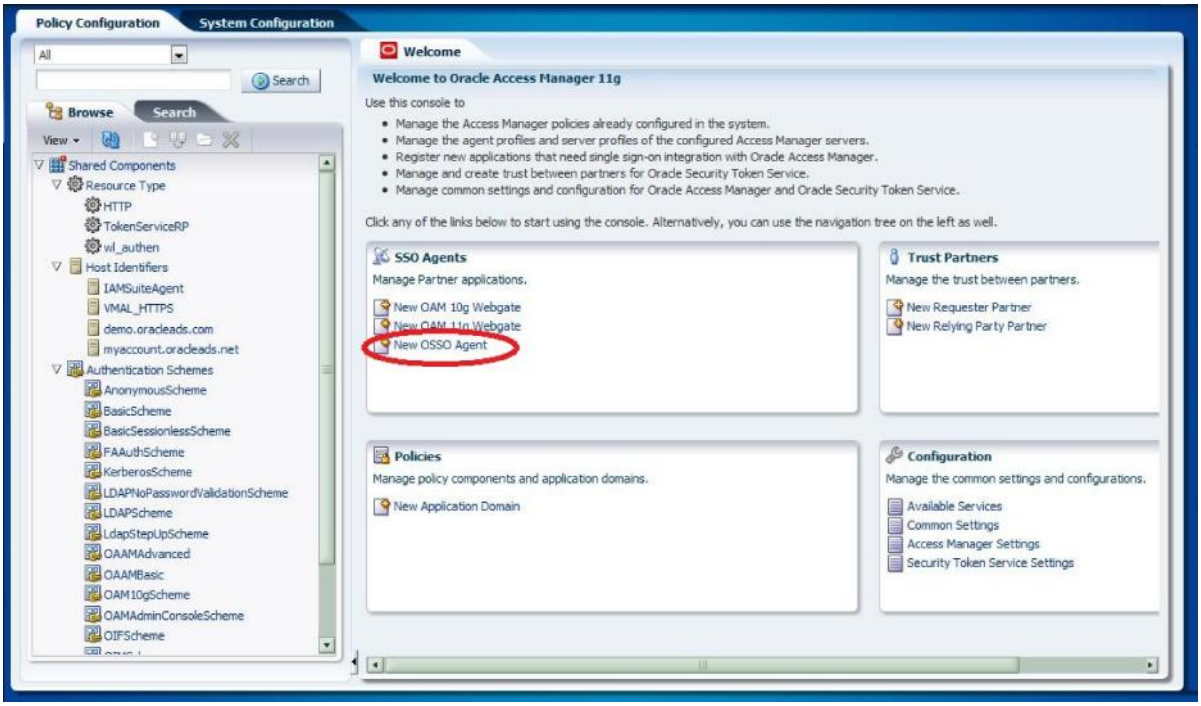


Figure 6: Authentication Schemes

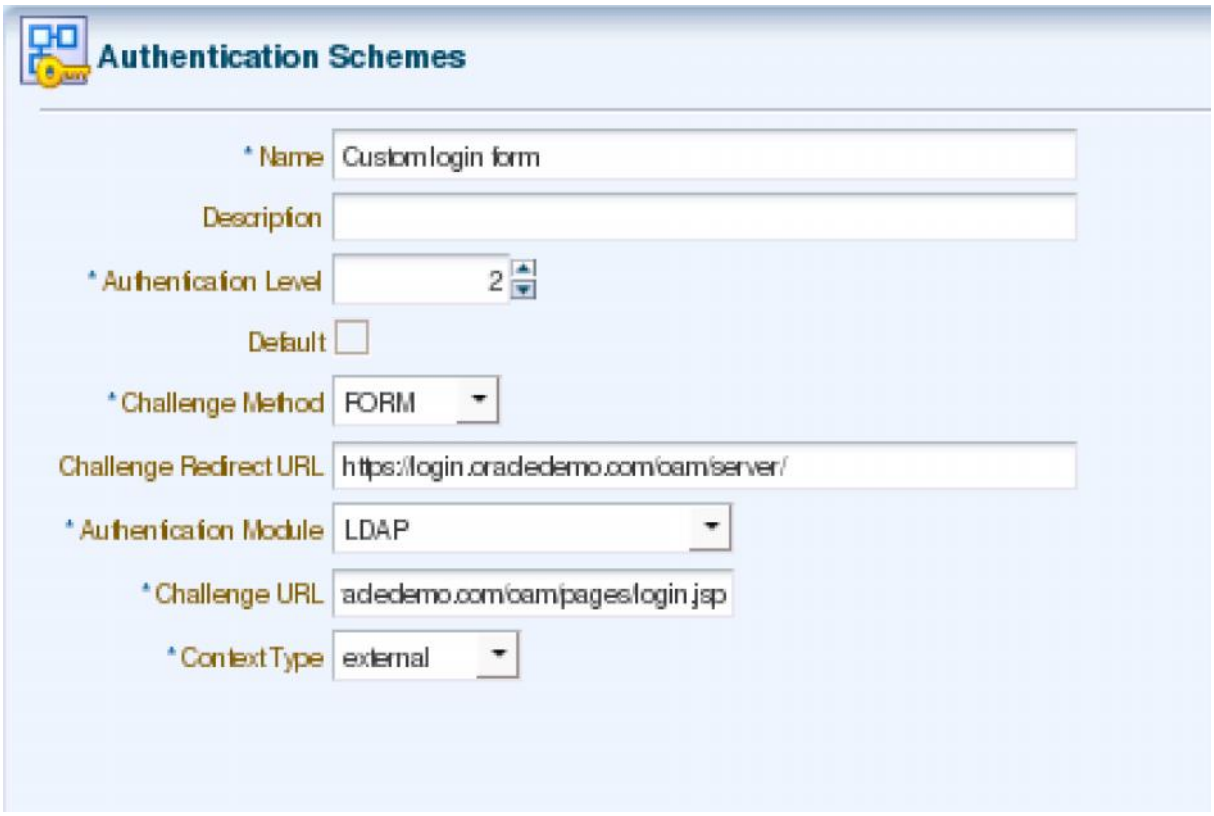


Figure 7: Internet Identity Services

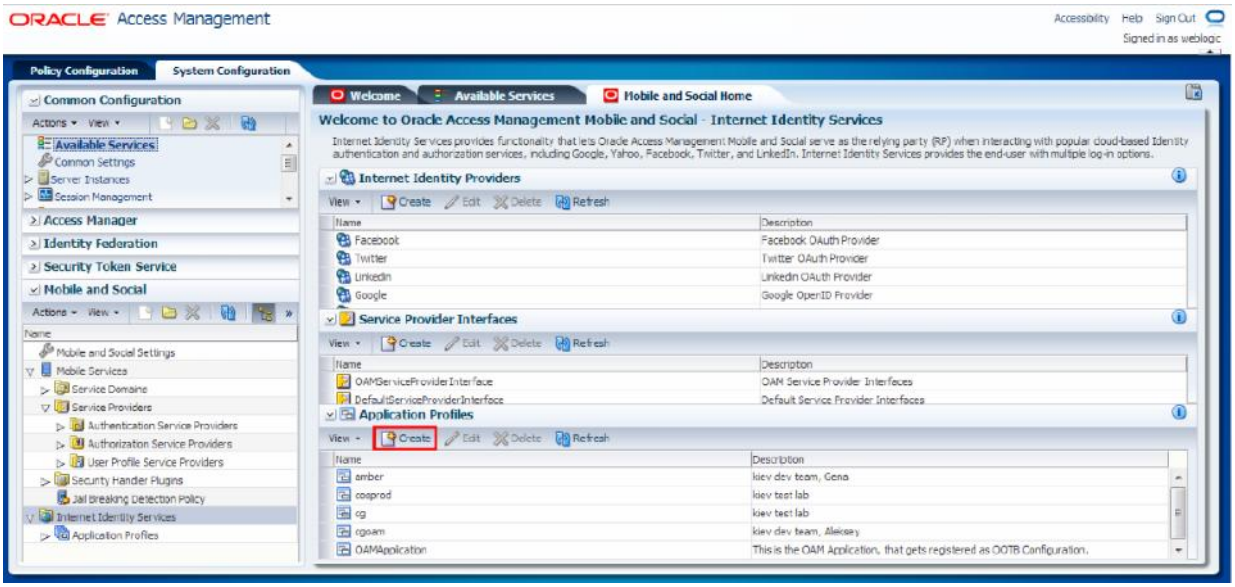


Figure 8: Web Gate

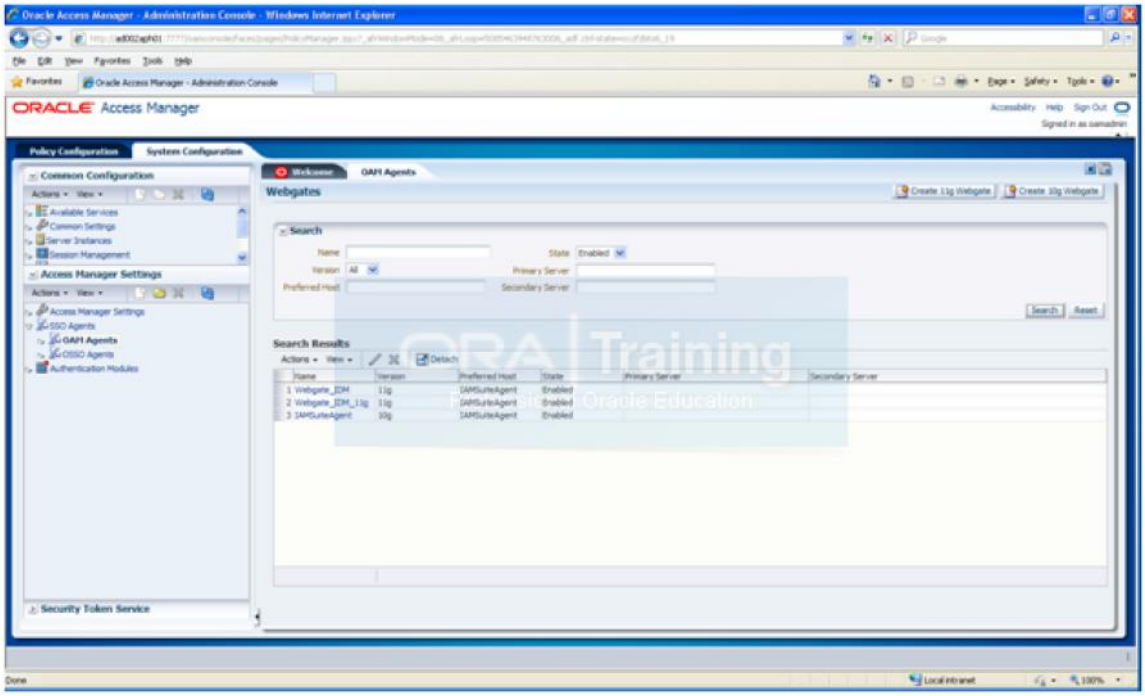


Figure 9: Web Gate Creating

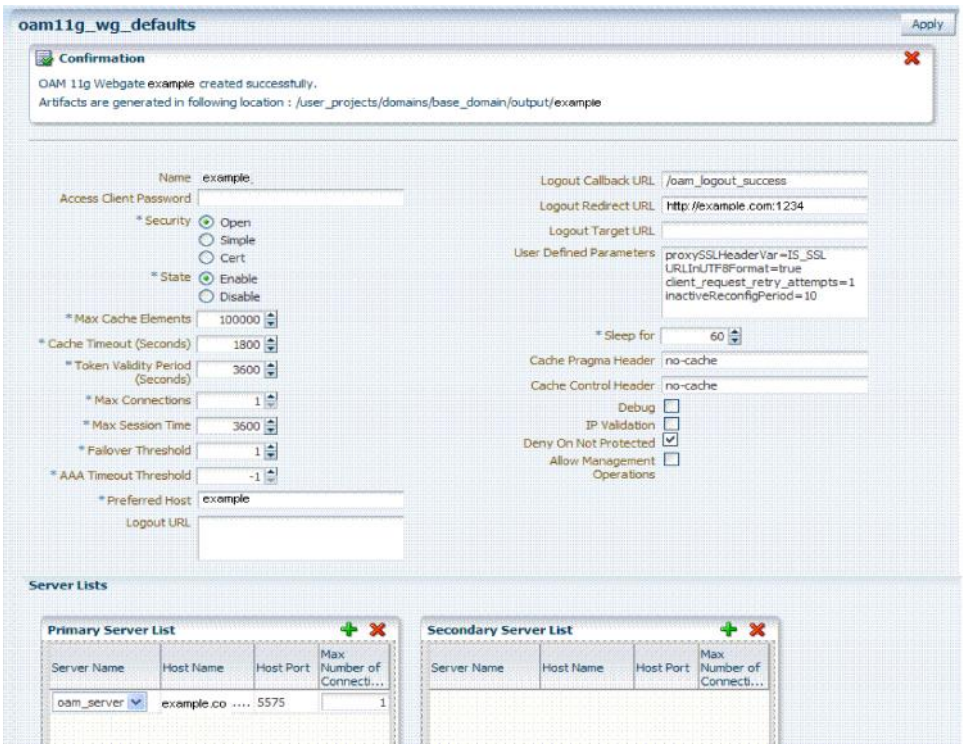
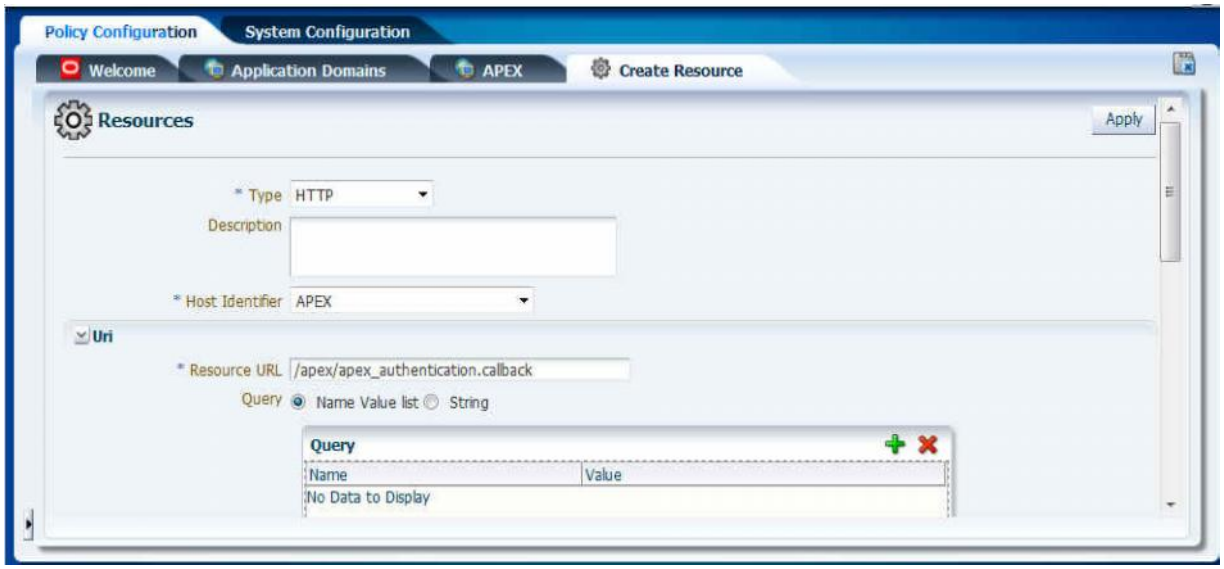


Figure 10: Policy Configuration



CONCLUSION

Access Management System provides single sign-on for users by central maintenance, support for multiple authentication methods and authorization for resources, and centralized policy evaluation and enforcement along with event logs of the users which completely form a secured system.

FUTURE ENHANCEMENTS

The nexus of forces (cloud, mobile, information, and social) is driving complex shifts in identity and access management. In this article the author describes a set of five key predictions for the future of identity and access management, setting a horizon date of the year 2020.

The nexus of forces (cloud, mobile, information, and social) is driving complex shifts in Identity and Access Management (IAM). Where once the IT manager responsible for IAM had only to worry about the efficiency and effectiveness of his program for internal systems and internal users, the new reality makes every business one of global relationships, cloud- and mobile-based users and data, and often distributed ownership and control of resources and participants. Against this shifting landscape, the Gartner IAM research team has developed a set of five key predictions for the future of identity and access management, setting a horizon date of the year 2020.

REFERENCES

1. An XML-Based Single Sign-On Scheme Supporting Mobile and Home Network Service Environments, IEEE.
2. farroha@ieee.org, deborah.l.farroha@ugov.gov, IAM, IEEE.
3. http://www.2ab.com/pdf/Access Management
4. http://www.karingroup.com/eng/about/what_is_identity
5. http://www.niso.org/publications/rp/RP-11-2011_ESPReSSO

6. http://www.oracle.com/technetwork/testcontent/access-manager-wp-10gr3-131015
7. http://www.safenetinc.com/uploadedFiles/About_SafeNet/Resource_Library/Resource_Items/White_Papers_-_SFDC_Protected_EDP
8. httpS://www.owasp.org/images/2/26/OWASPSanAntonio_2006_08_SingleSignOn.ppt+&cd=3&hl=en&ct=clnk&gl=in
9. Identity Management, Access Specs are Rolling Along-IEEE.
10. IEEE Strong authentication using dynamic biometric signature.
11. Springer computer n/w security

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com