FAQ

ORACLE FUSION MIDDLEWARE
Oracle Platform Security Services (OPSS) & Oracle Authorization Policy Manager (OAPM)
Frequently Asked Questions
July, 2010

This FAQ covers Oracle Platform Security Services (OPSS) and Oracle Authorization Policy Manager (OAPM) for Oracle Fusion Middleware 11gR1.

1.0 General Questions

1.1 What are the customer challenges addressed by OPSS?
Optimize development time, decrease development costs, increase development agility; Provide a consistent security experience on multiple platforms to developers and administrators; Facilitate administration tasks and simplify application maintenance; Provide common security services across applications; Support large enterprise deployments.

1.2 How do you describe OPSS?
OPSS is a standards-based, portable, integrated, enterprise-grade security platform for Java applications. Both Java EE and Java SE applications can use OPSS.

1.3 What security services does OPSS provide?
Security (authentication, authorization, SSO, credential store management, key store management); Audit; Cryptography (encryption and signature); Certificate lookup and validation; User roles; Credential mapping; Role mapping; Java EE policy and role deployment; Java2 and JAAS Policy Provider.

1.4 Who are the primary users of OPSS?
OPSS is designed for enterprise product development teams, systems integrators (SIs), and independent software vendors (ISVs). OPSS is used by Oracle developers to build Oracle Fusion Middleware (OFW) products and components (OPSS is “consumed” by multiple Oracle Fusion Middleware products such as Oracle SOA Suite, Oracle WebCenter, Oracle Application Development Framework (ADF), Oracle Web Services Manager (WSM), etc).

1.5 What are OPSS’s business benefits?
Thanks to OPSS, Oracle Fusion Middleware products, in-house developed applications, third-party applications, and integrated applications benefit from the same, uniform security, identity management, and audit services across the enterprise. OPSS provides a consistent security experience for developers and administrators.

1.6 What are OPSS’s benefits for developers?
OPSS provides an abstraction layer in the form of standards-based application programming interfaces (APIs) that insulate developers from security and identity management implementation details. For example, with OPSS, developers don’t need to know the nitty-gritty of cryptographic key management, developers don’t need to code to LDAP API and deal with user repositories and other identity management infrastructures.

1.7 What are OPSS’s benefits for SIs and ISVs?
OPSS provides SIs and ISVs with a ready-to-use enterprise security framework. OPSS facilitates integration with Oracle Fusion Middleware components such as Oracle Application Development Framework (ADF), Oracle SOA Suite, Oracle Virtual Directory (OVD), Oracle Internet Directory

(OID), etc. In addition, OPSS's security services provider interfaces (SSPI) allow SIs and ISVs to plug in their own security implementation if required.

1.8 How is OPSS delivered?

OPSS is delivered as a part of Oracle Fusion Middleware. If you install any of Oracle SOA, WebCenter or Oracle IdM you get OPSS.

1.9 Is OPSS available independent of Oracle Fusion Middleware?

Not in 11gR1. Post R1 there is a plan to make this possible.

1.10 Is OPSS portable to non-Oracle platforms?

OPSS is designed from the ground up to be portable to third-party application servers. As a result, developers can use OPSS as the single security framework for both Oracle and third-party environments, thus decreasing application development, administration, and maintenance costs.

1.11 The various components making up OPSS are scattered around the file system, will that be changed in the future?

Yes. In future 11g releases, OPSS's components will all be put together in the same directory for easier distribution.

1.12 Is OPSS the same as WebLogic Server security?

No. WebLogic Server "consumes" OPSS frameworks, for example for authentication, SSO, etc.

1.13 How much does OPSS cost?

OPSS is available with Oracle Fusion Middleware products. If you already have those products there is no additional cost for OPSS.

1.14 How does OPSS compare to ADF Security?

ADF Security is a consumer of OPSS. ADF security provides security to ADF based application whereas OPSS is web framework agnostic.

1.15 Does OPSS offer any IDE integration?

Oracle JDeveloper provides integration with OPSS and makes OPSS aware application development easier.

1.16 What is Oracle Authorization Policy Manager (OAPM)?

Oracle Authorization Policy Manager is a graphical user interface to manage authorization policy for applications that use Oracle Platform Security Services.It gives security administrators a business friendly way to manage authorization policy for multiple applications from one tool.

1.17 What is the difference between OPSS & Oracle Entitlements Server?

OPSS is a standards-based, portable, integrated, enterprise-grade security platform that provides security and IDM integration in the area of authentication, authorization, audit, credentials, crypto, key storage etc. OPSS based applications can seamlessly integrate with Oracle Entitlements Server, Oracle Access Manager, Oracle Web Services Manager, Secure Token Servers, directory servers and other identity backends & in future with Oracle Adaptive Access Manager & Oracle Identity Manager.

Oracle Entitlements Server is Oracle's commercial full featured fine grained authorization product and includes advanced policy capabilities such as attribute based access control, conditions, obligations, XACML, controlled policy distribution, support for a wide variety of programming environments and platforms, and offers integrations with Oracle and 3rd party commercial off the self applications such as Microsoft SharePoint. The next version of OES will include OPSS and OAPM will evolve into the OES management console.

1.18 What is the difference between OAPM & Oracle Entitlements Server (OES)?

OAPM is the policy management tool for applications built using ADF Security, Fusion Applications or built with OPSS.

Oracle Entitlements Server is Oracle's commercial full featured fine grained authorization product and includes advanced policy capabilities such as attribute based access control, conditions, obligations, XACML, controlled policy distribution, support for a wide variety of programming environments and platforms, and offers integrations with Oracle and 3rd party commercial off the self applications such as Microsoft SharePoint. The next version of OES will include OPSS and OAPM will evolve into the OES management console.

1.19 What is the difference between OAPM & Fusion Middleware Control based policy management?

OAPM provide a business friendly interface to security administrators with human readable policies based on a registry of protected application resources - the resource catalog. OAPM has other features like entitlement management and delegated policy administrations not provided by Fusion Middleware Control.

1.20 How can I get Oracle Authorization Policy Manager?

OAPM is shipped with Oracle Identity Management 11*g* Release 1.

2.0 Technical Questions

2.1 What are the choices for authentication?

For most Java EE applications, container based authentication is the right choice. For Java EE applications with need for programmatic authentication, WLS's Authenticate API is a choice. For Java SE application OPSS offers API.

2.2 What are the choices for authorization?

For many Java EE applications, the standard role based authentication (declarative & programmatic) is a reasonable choice. Oracle's Application Development Framework, ADF, among many features also offers ADF security that may be used to implement authorization in an application. Non-ADF based application, may use the standard checkPermission API or OPSS authorization API for JAAS based authorization.

Oracle Entitlements Server is Oracle's commercial full featured fine grained authorization product and includes advanced policy capabilities such as attribute based access control, conditions, obligations, XACML, controlled policy distribution, support for a wide variety of programming environments and platforms, and offers integrations with Oracle and 3rd party commercial off the self applications such as Microsoft SharePoint. The next version of OES will include OPSS and OAPM will evolve into the OES management console.

2.3 What is Credential Store Framework?

Application developers often need to store credentials (username/password) to various system/services (e.g. credential for database, website, web service, a privileged account etc). OPSS provides an abstraction of Credential store that is used to securely store credentials. OFW offers various tools (GUI & Command line) to manage these credentials. Credential Store Framework (CSF) API is used by application to access the credentials stored in a credential store.

2.4 What is User Role API?

User Role (U/R) API provides access to a user's attribute stored in an Identity Store (LDAP, RDBMS, custom). This API frees application developer from knowing the details of identity store.

2.5 What is Identity Governance Framework?

The Identity Governance Framework (IGF) is a standard to address governance of identity related information across enterprise IT systems.
IGF provides a common framework for defining usage policies, attribute requirements, and developer APIs pertaining to the use of identity related information. These enable businesses to ensure full documentation, control, and auditing regarding the use, storage and propagation of identity-related data across systems and applications.

2.6 What solution does OPSS provides for Audit?

OPSS uses an internal framework to provide audit functionality. OPSS API invocation causes audit events generation. Using the provided OFW Control GUI an admin can configure audit events and use Oracle BI Publisher to view audit reports. Various Oracle products like OID, OVD & DIP etc, also use the OPSS audit framework.

2.7 What are the management tools for OPSS?

There are three tools, Oracle Fusion Middleware Control, WLST & WLS Admin Console. In a SOA, ADF or WebCenter domain to manage JAAS policy, Application Policy, Credential Store & Audit one can use the OFW Control GUI or WLST commands. To manage standard Java EE security constructs and to manage container security the tool of choice is WLS Admin Console.

2.8 How does one manage authorization policy?

For Java EE applications using JAAS/OPSS based authorization, you can use OFW Control or WLST commands to manage authorization policy including application role to enterprise group mapping, application role hierarchy and permission grants.
For Java SE applications using JAAS/OPSS based authorization, you can use MBeans or directly edit system-jazn-data.xml.
To manage authorization policy of application using only Java EE based authorization use WLS admin console.
With Oracle Identity Management 11*g* Release 1 APM is available and is the preferred tool to manage authorization policies for OPSS and ADF Security based applications.

2.9 What is IdStore?

IDStore/IdStore/IdentityStore/UserStore is a logical name. It represents a trusted repository where users and groups are stored and the repository is used to validate users during authentication. Out the box OFW and Oracle WebLogic Server use embedded LDAP as IdStore. However it could be changed to other LDAP servers or RDBMS supported by OFW.

2.10 How does one manage Credentials?

You can use OFW Control or WLST command to manage credentials.

2.11 What is the default Policy Store?

Out of the box, the default policy store is an XML file, which is only recommended for testing or small deployments. For most production deployments the Policy store should be changed to LDAP (OID).

2.12 What is the default Credential Store?

Out of the box, the default credential store is a file. When policy store is changed to LDAP, the credential store is implicitly changed to same LDAP.

2.13 What is the meaning of term "re-association"?

The term means changing the actual store where authorization policies and credentials are stored from file to LDAP or from one LDAP instance to another LDAP instance.

2.14 Do content of policy and credential store get migrated during "re-association"?
Yes.

2.15 How does one create user and groups for OPSS?
OPSS uses the "Authenticators" provided by Oracle WebLogic server for authentication. If your IdStore is embedded LDAP use Admin Console, if using other LDAP server as IdStore you will need to use that LDAP server provided tool to create users and groups. For programmatic user and group creation User and Role is a choice. An enterprise solution will typically use a Provisioning solution like Oracle Identity Manager for this.

2.16 What are the choices for Single Sign-On in OFW11gR1?
Out of the box SSO between apps within a domain is automatic provided the cookies share a domain. Another choice is Oracle WLS SAML that is good for departmental SSO use cases. For enterprise SSO, 11gR1 provides Oracle Single Sign On & Oracle Access Manager as two options. OSSO is preferred enterprise SSO for existing OSSO and Oracle Classic customers. For new deployments customers should choose OAM.

2.17 What is OSDT?
Oracle Security Developer Toolkit (OSDT) is a part of OPSS. OSDT is a set of standard compliant java libraries that can be used for crypto, XML security, SMIME & SAML.

2.18 What Policy Store does OAPM support?
OAPM requires Oracle Internet Directory (OID) as a policy store.

2.19 Does OAPM integrate with Oracle Identity Manager?
Oracle Identity Manager is used to provision users and group. OAPM uses Identity Governance Framework (IGF) to read users & groups created with OIM.

2.20 Does OAPM manage users and groups?
No, OAPM only provides read only access to users and groups. Typically an Identity Manager (like Oracle Identity Manager) is used to provision users and groups in an enterprise.

2.21 Does OAPM support XML based policy store?
No, OAPM requires Oracle Internet Directory for policy store.

ORACLE FUSION MIDDLEWARE

Oracle Platform Security Services (OPSS) FAQ

July 2010
Author: Marc Chanliau & Vinay Shukla
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

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.