This FAQ is for questions on the Oracle Authentication Services for Operating Systems 11.1.1.3.

### 1.0 Core Functionality Questions

#### 1.1 What is Oracle Authentication Services for Operating Systems?

Oracle Authentication Services for Operating Systems (OAS4OS) enables enterprises to centralize the management of Unix and Linux authentication, user accounts, password policies, and Sudo authorization policies using Oracle Internet Directory (OID). Based on open standards interfaces, OAS4OS provides full automation of client configuration and user migration and serves as LDAP based naming server to replace NIS.

#### 1.2 When is the OAS4OS 11.1.1.3 available?

April 27, 2010

#### 1.3 What is new with OAS4OS 11.1.1.3?

- Full integration with Fusion Middleware Release 11g R1 patchset 2 (11.1.1.3). OAS4OS was not available with FMW 11g R1 or FMW 11g R1 patchset 1.
- Extended client OS support, for a full list see 1.10
- New configuration scripts to enable PAM proxy user based access to OID for enhanced security
- Easy configuration of OID SSL using customer provided certificates for production deployments, or use of self signed certificates to test OID SSL connections
- Restricting client access based on IP address
- Easy reset of client configuration to support testing

For further details see the OAS4OS Admin Guide.

#### 1.4 Where can I download the software?

OAS4OS 11.1.1.3 ship’s as part of the Oracle Fusion Middleware 11g R1 patchset 2 (11.1.1.3).

In order to use OID 11.1.1.3 you have to install or upgrade to OID 11.1.1.2 first before applying FMW 11g R1 patchset 2. For further details see the FMW Upgrade Guide.
Customers who already have installed OID 11.1.1.2 can use the OAS4OS 11.1.1.3 software without upgrading to OID 11.1.1.3, if they wish. For OID 11.1.1.2 the OAS4OS software is available for download on OTN at


1.5 Which version of OID is supported with OAS4OS 11.1.1.3?

The supported OID versions are 11.1.1.2.0 or 11.1.1.3.0. New customers must install OID 11.1.1.2.0 to use the scripts available on OTN.

Customers having installed OID 11.1.1 must upgrade to OID 11.1.1.2, or OID 11.1.1.3. When upgrading to OID 11.1.1.3 the OAS4OS software is included in the upgrade, and no other software download is required.

OAS4OS 11.1.1.3 is not backward compatible with OID 10g.

1.6 How can I verify that OAS4OS is installed on my system?

OAS4OS software components are installed into $ORACLE_HOME/oas4os directory.

1.7 What are the software prerequisites for the OID server?

See Oracle® Fusion Middleware System Requirements and Specifications 11g Release 1 (11.1.1)

1.8 Does OAS4OS support other directories besides OID?

No. Currently OAS4OS requires OID.

1.9 Where can I find a matrix of certified OID and client OS versions for PAM authentication?

See Oracle Fusion Middleware Supported System Configurations

1.10 What is included in OAS4OS?

In a nutshell OAS4OS is software to easy applicable configuration automation for client side PAM, and OID server configuration.

1.11 What is PAM?

PAM stands for Pluggable Authentication Modules and is a standard, documented set of interfaces available on most modern Linux and Unix variants that allows extension of common login and related functionality. Common plug-ins include those that access LDAP, NIS, Kerberos, and even Strong Authentication.

1.12 What is NIS?
NIS (Network Information System) is a network naming and administration service for networks. NIS is being deprecated, hence the support for OAS4OS to replace NIS deployments with an LDAP based solution.

See also “A Planning Guide for Moving to LDAP as Naming Service on Solaris”

1.13 What is sudo?

Sudo (“superuser do”) allows system administrators to work using their own accounts and switch to root (or other user identities) only for commands that are permitted by Sudo policies. Sudo provides policy management and named user based auditing for privileged accounts.

1.14 What is a typical use case for sudo?

For example, an installation of the Oracle DB is done by an administrator with privileges only to install the Oracle software. At some point during the installation superuser (root) privileges are required to execute a “root.sh” script which changes ownership of programs (like OID) to be owned and executed by root.

The “root.sh” script has to be run as user “root”. In this case the administrator executes the `sudo` command that will effectively grant him “root” privileges to execute only “root.sh” without disclosing the password of the “root” user on this system.

1.15 How can customers migrate account information?

Automation tools are provided to migrate user and group information from existing NIS databases or file based repositories, as well as from existing directories, to Oracle Internet Directory. For further details consult the OAS4OS Administrator Guide on http://www.oracle.com/technology/products/oid/oracleauthenticationservices.html

1.16 Does OAS4OS support auditing?

Auditing is based on the audit features of OID. All authentication operations are audited when auditing is enabled.

1.17 What is the Architecture for Oracle Authentication Services for Operating Systems?

The Oracle Authentication Services for Operating Systems leverages three major components:

- Pluggable Authentication Modules (PAM) – Standard operating system modules available on most Linux and Unix-based systems that support externalized authentication.
- **Oracle Internet Directory (OID)** – Highly scalable, available, and secure standards-based directory server that leverages Oracle Database to store users, groups, roles, and entitlements.

- **Automation** – New tools that configure both PAM and OID components, simplify user migration, and ensure strong default security between network endpoints. The automated pre-configuration removes complexity and reduces errors that can often occur during installation and SSL configuration.

The diagram below shows these components in a typical deployment. The authentication services reside primarily on the server-side with the Oracle Internet Directory server while leveraging existing PAM technology on the client-side. All connectivity occurs over secure SSL sessions.

1.21 **How does this Architecture tie into the overall Oracle Architecture?**

The solution can be combined with existing security solutions to authenticate database, web, and application users. The solution can be extended with Oracle Identity Manager to incorporate robust account reconciliation and compliance reporting, as well as complete, workflow-based user provisioning.
1.22 What types of support are available to customers?

Customer can open SR with Oracle support or post questions on the OTN forum at http://forums.oracle.com/forums/forum.jspa?forumID=398

1.23 Are there any white papers or demos available?


1.24 What is the product roadmap?


1.25 Where do I find more information?
