Common Criteria

ORACLE
APPLICATION SERVER 10*g*

Evaluated Configuration for Oracle Identity and Access Management 10*g* (10.1.4.0.1)

May 2008

Security Evaluations
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065

Evaluated Configuration for Oracle Identity and Access Management 10*g* (10.1.4.0.1)

May 2008

Authors: Julian Skinner and James Belton.

Contributors: Adam O’Brien, Stephen Brooks, Peter Goatly, David Belfrage.

Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065.

The information in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. Oracle Corporation does not warrant that this document is error free.

Contents

Contents

CHAPTER

1

Introduction

This is the Evaluated Configuration Document (ECD) for the evaluation that has Oracle Identity and Access Management 10*g* (10.1.4.0.1) as its Target of Evaluation (TOE).

For this evaluation of Oracle Identity and Access Management the products which constitute the TOE are:

- Oracle Access Manager 10*g* (10.1.4.0.1)
- Oracle Virtual Directory 10*g* (10.1.4.0.1)
- Oracle Internet Directory 10*g* (10.1.4.0.1).

In addition, the TOE includes Patch 5912931, which is applied to Oracle Access Manager.

The TOE is hosted on the Red Hat Enterprise Linux AS Version 4 Update 5 operating system platform. The Web server platform used by Oracle Access Manager 10*g* (10.1.4.0.1) is Oracle HTTP Server 10*g* (10.1.3.1.0). Oracle Internet Directory 10*g* (10.1.4.0.1) uses the Oracle Database 10*g* Release 2 (10.1.0.5.0) Object-Relational Database Management System to hold its directory data.

This document explains the manner in which the TOE must be configured along with the host operating system, Web server, Oracle database, and network services so as to provide the security functionality and assurance as required under the Common Criteria for Information Technology Security Evaluation [CC].

As well as forming part of the TOE, Oracle Internet Directory (OID) is also being evaluated separately. As a result, this ECD refers to [OIDECD] to cover OID-specific evaluation topics.

The Evaluation Assurance Level for the TOE is EAL4 augmented with ALC_FLR.3. The Security Target used for the evaluation of the TOE is [ST].

1.1 Intended Audience

The intended audience for this document includes evaluators of the TOE, system integrators who will be integrating the TOE into systems, and accreditors of the systems into which the TOE has been integrated.

1.2 Organization

This document is composed of the following chapters:

Chapter 1 contains the introduction to the document;

Chapter 2 describes the preparatory actions to be undertaken before installing the software for the evaluated configuration;

Chapter 3 describes the installation of the software for the evaluated configuration;

Chapter 4 describes the post-installation actions to complete the evaluated configuration;

Chapter 5 describes the supporting procedures to ensure that the TOE is operated in a way that upholds the security objectives defined in [ST];

Annex A lists the TOE components installed as per Chapter 3;

Annex B contains instructions for configuring firewalls on the machines hosting the TOE, and

Annex C lists the references that are used in this document.

Change bars indicate changes since the previous issue of this document.

1.3 Format

Assertions about the configuration actions that are required to be performed are given identifiers to their left in bold Helvetica font, e.g. **[A-1]**. References to sections of documents listed in Annex C are in the format [*document, section*].

Mandatory evaluation configuration requirements use the words “must” and/or “shall” in each assertion.

Strongly recommended evaluation configuration requirements use the words “should” in each assertion.

CHAPTER

2

Preparation

This chapter describes the preparatory actions to be undertaken before installing the software for the evaluated configuration.

2.1 Machine Configuration

In the Evaluated Configuration the software was installed on 2 server machines.

Machine 1	SagDell4t
Specification	Dell PowerEdge 1950 2x Intel Xeon Dual Core Processors 16GB Memory RedHat Enterprise Linux AS Release 4 Update 5
Products to be installed	Oracle Internet Directory 10.1.4.0.1 Oracle Virtual Directory Server 10.1.4.0.1 Oracle Virtual Directory Manager 10.1.4.0.1 Oracle HTTP Server 10.1.3.1.0 version 2.x WebGate 10.1.4.0.1 WebPass 10.1.4.0.1 Policy Manager 10.1.4.0.1

Table 2-1: Configuration of Machine 1

Machine 2	SagDell5t
Specification	Dell PowerEdge 1950 2x Intel Xeon Dual Core Processors 16GB Memory RedHat Enterprise Linux AS Release 4 Update 5
Products to be installed	Oracle Internet Directory 10.1.4.0.1 Oracle Access Server 10.1.4.0.1 Oracle Identity Server 10.1.4.0.1

Table 2-2: Configuration of Machine 2

Note that two instances of OID were installed on Machine 2. These were used to store data accessed by Oracle Virtual Directory and are not part of the TOE.

In the Evaluated Configuration for the TOE these server machines run on a dedicated LAN with no connections to any other network. The client machines for use in testing the TOE also run on this LAN.

2.2 Physical Environmental Assumptions

This section describes physical requirements on the server machines so that the security of the TOE can be maintained.

[IM.A-1] The processing resources of the TOE shall be located within controlled access facilities which will prevent unauthorised physical access to the TOE by unprivileged users. Only authorised administrators for the system hosting the TOE shall have physical access to that system. Such administrators include the Operating System Administrators, Access and Identity Master Administrators, OID Directory Administrators and Database Administrators.

[IM.A-2] The media on which the TOE audit data resides shall not be physically removable from the underlying operating system by unauthorised users.

[IM.A-3] Any on-line and/or off-line storage media on which security relevant data resides shall be located within controlled access facilities which will prevent unauthorised physical access.

2.3 Electronic Delivery of the TOE

To receive electronic delivery of the TOE installation software, complete the following steps:

1. Access the Oracle's Technet Website at http://technet.oracle.com.
2. Click on the ‘Downloads’ link.
3. Scroll down to the Middleware section and click ‘Identity Management’.
4. Click the checkbox if you agree to the Licence Terms and export restrictions.
5. Click the ‘I Accept’ button to agree to the OTN licence terms.

6. You should now be looking at the ‘Oracle Identity Management 10*g* 10.1.4.0.1 Downloads’ page: http://www.oracle.com/technology/software/products/ias/htdocs/10401.htm.
7. The following products need to be downloaded for the Linux operating system:

   - Oracle Identity Management Infrastructure and Oracle Federation
   - Oracle Access Manager
   - Oracle Virtual Directory
   - GCC Libraries for Oracle Access Manager

8. Hovering the mouse pointer over the link to the download will display the download's cksum number. This number should be recorded for later verification.

9. When the first download is requested, the OTN Sign-in page is presented.

10. Complete the form with your OTN login details, or create an account by clicking ‘sign up now’.

11.The download will start. Again, ensure that you download each disk.

12. Once the download is complete and the file has been transferred to the target environment, check the file with the cksum filename command to ensure that the download has not become corrupted. If the CKSUM numbers do not match, the file should be downloaded again.

For the Evaluated Configuration, the RedHat operating system software was obtained via download from the RedHat Network web site and made available to the host servers via an NFS mount.

2.4 Physical Delivery of the TOE

To request the media pack:

Go to www.oracle.com and select Shop Online. Choose the appropriate store and select Application Server. Select Application Server Enterprise Edition and chose your licensing terms. Select ‘Purchase Media Packs’. Select Linux x86. Then select Oracle® Application Server 10g Release 2 (10.1.2.0.2) Media Pack (with Oracle® Enterprise Manager 10g Release 3 Grid Control (10.2.0.3.0)) for Linux x86 (32-bit).

When the media pack arrives the relevant CDs / DVDs are:

B30971-01 – Oracle Identity Management Infrastructure and Oracle Identity Federation (10.1.4.0.1) (CD 1 of 2)

B30972-01 – Oracle Identity Management Infrastructure and Oracle Identity Federation (10.1.4.0.1) (CD 2of 2)

B30977-01 - Oracle Access Manager (10.1.4.0.1) (DVD 1 of 2)

B30978-01 - Oracle Access Manager (10.1.4.0.1) (DVD 2 of 2)

B30979-01 - Oracle Virtual Directory (10.1.4.0.1).

2.5 Download of the Patch

The patch can be obtained by downloading the p591293_101401_Linux-x86.zip file as follows:

1. Login to Metalink.

2. Select Patch Number from the Quick Find dropdown list and search for patch number 5912931

3. This will direct the browser to a download page. Select Linux x86 from the Platform dropdown list and click on the Download button.

CHAPTER

3 Installation

This chapter describes the installation of the software for the evaluated configuration.

3.1 Operating System Installation / Configuration

The actions **[IM.PRE-1]** to **[IM.PRE-5]** listed in this section are required on each server machine and before the installation of the TOE can be carried out.

[IM.PRE-1] The RedHat Operating System shall be installed as described in Annex B of [OIDECD].

[IM.PRE-2] In order that the Oracle Application Server 10*g* (10.1.4.0.1) installation process can install the TOE successfully, the following lines must be present in the file `/etc/sysctl.conf`:

```
kernel.shmall = 2097152
kernel.shmmax = 2147483648
kernel.shmmni = 4096
kernel.sem = 256 32000 100 142
fs.file-max = 131072
net.ipv4.ip_local_port_range = 1024 65000
kernel.msgmni = 2878
kernel.msgmax = 8192
kernel.msgmnb = 65535
```

[IM.PRE-3] An operating system group, which will be used by the Oracle software owner and database administrators, must be created before installing the TOE. Any legal name can be used for this group, but the convention is to use “oinstall”. The oinstall group can be created via the admintool GUI or with the Linux command:

```
$ groupadd oinstall
```

[IM.PRE-3] An operating system user that will be the Oracle software owner must be created before installing the TOE. The standard name used is “oracle”. When creating the user a primary group is required. The primary group should be oinstall. The oracle user can be created via the admintool GUI or with the Linux command:

```
$ useradd -g oinstall -c "Oracle Software Owner" oracle
```

```
$ passwd oracle
```

[IM.PRE-4] Each server machine should have a directory within which the TOE installation media will be stored. In the Evaluated Configuration this was: `/space/src/oracle`.

Also, each server should have a directory into which the software will be installed. In the Evaluated Configuration this was: `/space/oracle/product`

The following commands can be used to configure the ownership and access rights for these directories:

```
chown -R oracle:oinstall /space/src
chown -R oracle:oinstall /space/oracle
chmod 755 /space/src/oracle
chmod 755 /space/oracle/product
```

[IM.PRE-5] Under the `/space/src/oracle` directory the following sub-directories should be created on both Server machines:

```
AccessManager
OIM_ID_INFRA
OVD
GCC
```

Note, the OVD directory is only required on Machine 1.

If the installation files were obtained via cd/DVD then the contents of the cd/DVD's should be copied into the corresponding directory and uncompressed if required. If the installation files were obtained via download, the downloaded file should be copied into the corresponding directory and uncompressed using the following syntax:

```
$ cpio -idm < file_name.cpio
```

3.2 Logical TOE Software Configuration

3.2.1 Configuration of Oracle IAM

The logical configuration of the server software for Oracle Identity and Access Management is shown in the diagram on the next page. This configuration handles TOE administration functions as well as user requests to access resources that are controlled by the TOE.

The dotted line in the figure indicates the mechanism whereby Access Server can cause Identity Server to be entered via WebPass to enforce the TOE's password policy when an end user has requested access to a resource. To achieve this, Access Server redirects the end user's HTTP request to a Web page that causes WebPass to be entered. This occurs, for example, when the user's password has expired and the user has to supply a new one before the access request can be processed.

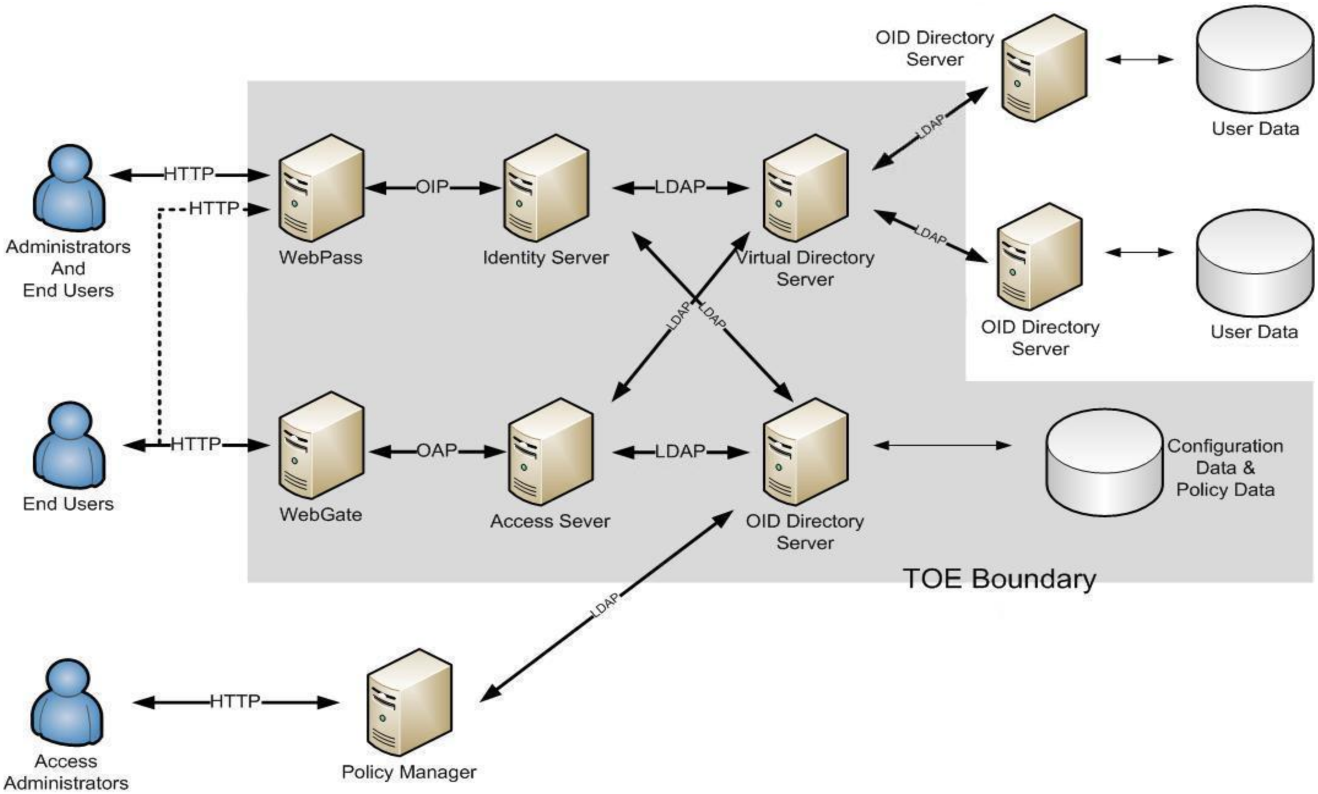

Figure 1: Oracle IAM Configuration

3.2.2 Configuration of the TOE

The logical configuration of the TOE software in its operational state is shown in the diagram on the next page. This configuration only handles user requests to access resources that are controlled by the TOE (administration functions are not part of the TOE in its operational state).

As described in the section above, the dotted line in Figure 2 indicates the mechanism whereby Access Server can cause Identity Server to be entered via WebPass to enforce the TOE's password policy when an end user has requested access to a resource.

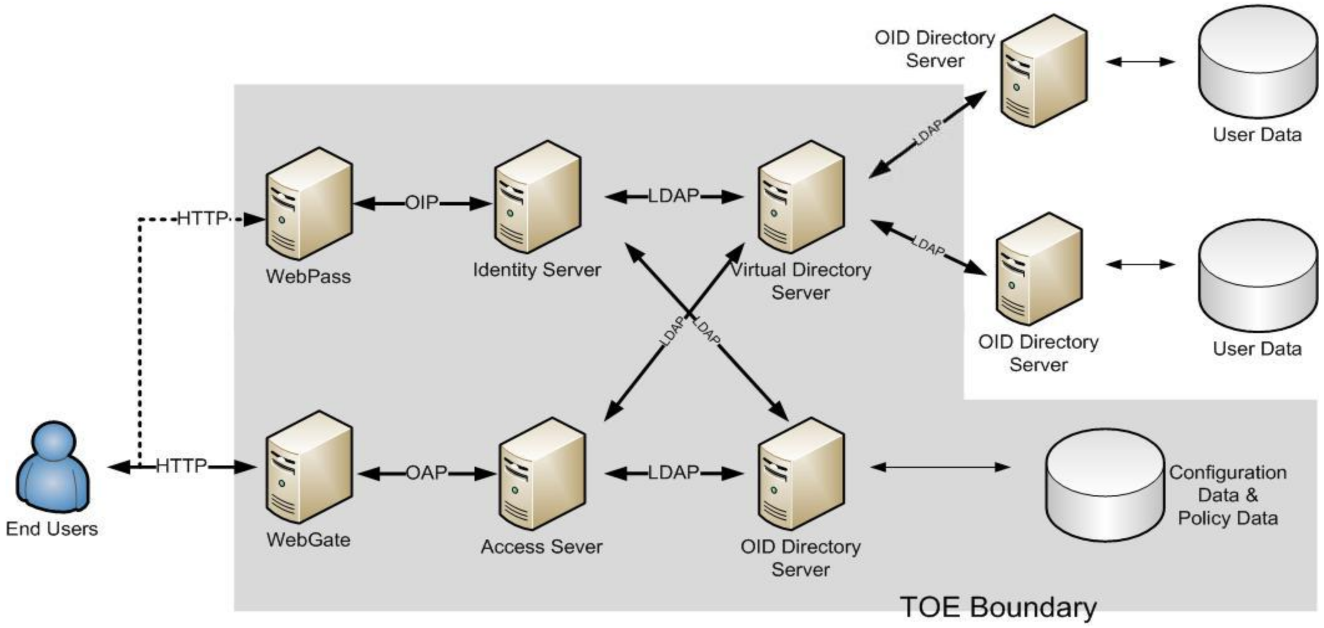

Figure 2: TOE Configuration

3.3 Oracle IAM Installation

3.3.1 Step by Step Installation of Oracle IAM

This section details the steps needed to set up the TOE's evaluated configuration on Red Hat Enterprise Linux AS Version 4 Update 5, and on which server the instructions must be followed.

This section should be used in conjunction with the relevant installation manuals and assumes any prior installations of Oracle Application Server have been removed before the new installation starts.

1. Install the GCC libraries on each machine, as follows:
   --Navigate to the `/space/src/oracle/GCC` directory;
   -- unzip the zip file;
   -- copy the lib files to the `/usr/lib` directory (this must be performed via an account with administrator privileges).

2. Machine 1. Install Oracle Internet Directory as described in [OIDIG]. This instance of OID will be used to store Configuration and Policy data. In the Evaluated Configuration the following values were used as inputs during the installation:
   --Destination Path: /space/oracle/product/10.1.4/IM_INFRA_POLICY
   --Global Database Name: polOID.saglab.uk.oracle.com

   Following installation an LDAP object, which we will name as 'OAM', needs to be created in the Policy/Configuration directory for Access Manager to store data (the dn of this object will be required during the configuration of Access Manager). This is done using the following steps:

create a file with the following contents:

```
dn: cn=OAM, cn=Products, cn=OracleContext, dc=oracle,dc=com
changetype: add
cn: OAM
objectClass: top
objectClass: orclContainer
```

Save this file as 'add_oam.ldif' in the `$HOME` directory.
Set the ORACLE_HOME environment variable:

```
$export ORACLE_HOME=/space/oracle/product/10.1.4/
IM_INFRA_POLICY.
```

Navigate to the `$ORACLE_HOME/bin` directory and run the following command:

```
$ ./ldapmodify -h sagdell4t -p389 -D "cn=orcladmin" -w
password -f /home/oracle/add_oam.ldif
```

3. Machine 2. Install 2 instances of Oracle Internet Directory as described in [OIDIG]. These 2 instances of OID are not part of the TOE but are used to store User data which will be used to test the security functions of the TOE. In the Evaluated Configuration the following values were used as inputs during the installation:

   OID Instance 1:
   --Destination Path: /space/oracle/product/10.1.4/IM_INFRA_USER1
   --Global Database Name: user1OID.saglab.uk.oracle.com

   OID Instance 2:
   --Destination Path: /space/oracle/product/10.1.4/IM_INFRA_USER2
   --Global Database Name: user2OID.saglab.uk.oracle.com

   Note that OID Instance 2 will, by default, be configured to listen on port 13060 rather than the standard LDAP port of 389.

4. Create user accounts in each of the OID User instances that will be the “Master Access Administrators” in the Identity and Access Systems and remove the PUBLIC account. In the test system this was achieved using Oracle Directory Manager (ODM), as follows;

   --login to ODM as the superuser (cn=orcladmin);
   --Navigate to Entry Management -> dc=com -> dc=oracle -> cn = Users
   --Select the account cn=orcladmin
   --Right-click and select ‘Create Like’.
   --Edit all occurrences of ‘orcladmin’ to a new name for the account (in the test system these were renamed to orcladmin1 and orcladmin2 in the respective instances of OID) and change the password.
   --Click ‘OK’.
   --Delete the orcladmin and PUBLIC user accounts.

5. Machine 1. Install Oracle Virtual Directory Server as described in [OVDIG].

6. Machine 1. Install Oracle Virtual Directory Manager as described in [OVDIG].

7. Machine 1. Configure OVD as described in [OVDIG].

8. Machine 1. Install Oracle HTTP Server as described in [OHSIG].
   Oracle HTTP Server is not part of the TOE, but is the platform used for running the WebPass and WebGate components of Oracle Access Manager.

9. Install and configure all of the components of Oracle Access Manager as described in [OAMIG].

10. Unzip and install the Patch on Machine 1 as follows:

    - first shut down OHS using opmnctl
    - create a directory in which to unzip the Patch e.g

    ```
    $cd /space/src/oracle
    $mkdir PatchWebGate
    ```

    - move the p5912931_101401_Linux-x86.zip to this directory and unzip it.
    - this will extract 4 more zip files. Unzip the OHS2 version, which will create a new directory (with a name ending binary_parameter).
    - navigate to the newly created directory and run the tool to install the patch i.e.

    ```
    $cd *binary_parameter
    $./patchinst
    ```

    - the patchinst will prompt for the installation directory of Webgate. Enter the full path thus:

    ```
    /space/oracle/product/10.1.4/webgate/access
    ```

    - when the installation is finished restart OHS.

3.4 Client Installation

The TOE scope does not include any Oracle Identity and Access Management client software. During the evaluation of the TOE, client software can be used to send HTTP messages to the TOE in order to test its security features and can be used to configure the TOE's environment in preparation for the use of the TOE in its operational state.

Administrators are to prevent other client software being installed on any machine in the network that includes the evaluated configuration of the TOE as per the following assertion:

[IM.CA-1] No applications, other than those which communicate with the TOE by sending HTTP messages (such as browsers), shall be permitted to run on any machine that accesses the network other than those listed in section 2.1, unless they have been shown not to compromise the TOE's security objectives as stated in [ST].

CHAPTER

4 Configuration

This chapter describes the post-installation actions to complete the evaluated configuration.

4.1 TOE Requirements

The actions listed in this section are required to be performed to increase the security of the evaluated configuration after installation of the TOE has been carried out as described in the previous chapter.

Throughout this section the term “administrator” is used to mean either the Master Administrator in OIAM or the Directory Administrator in OID.

[IM.POST-1] The administrator must ensure all the assertions in [OIDECD, 4] have been met on the OID instance used to store Configuration and Policy data.

[IM.POST-2] The administrator must change the “Shared Secret”, following the instructions in [OAMAG, 8: Creating a Shared Secret Key] and must ensure the Shared Secret is never set to NULL.

[IM.POST-3a] The administrator must create a suitable password policy. Directions for doing this are given in [OAMICAG, 7: Creating Password Policies for a Specific Domain]. The password policy must use the following minimum values (except for the Number of login tries allowed which is a maximum value). Where values are not given the default value can be used:

Password Policy Name = “ECD Password Policy”

Password Policy Domain = “dc=oracle,dc=com”

Password Minimum Length = 6

Minimum Number of Uppercase Characters = 0

Minimum number of Lowercase Characters = 0

Minimum number of Nonalphanumeric Characters = 0

Minimum Number of Numeric Characters = 0

Password Expiry Notice Period = “” (i.e. blank)

Number of login tries allowed = 10.

Lockout Duration = 1 (hour).

[IM.POST-3b] The administrator must create a Password Change Redirect URL. Information on doing so is given in [OAMICAG, 7: Configuring Password Redirect URLs]. In the evaluated configuration the Redirect URL used was:

http://sagdell4t.saglab.uk.oracle.com:7778/identity/oblix/apps/lost_pwd_mgmt/bin/lost_pwd_mgmt.cgi?program=redirectforchangepwd&login=%login%%userid%&backURL=%HostTarget%%RESOURCE% &target=top

In addition, a policy domain will need to be created to grant access to the URL. The policy that was used in the Evaluated Configuration is described in Appendix B.3.

[IM.POST-4] The administrator must configure Cache timeouts on both the Access Server and the WebGate to be a suitably small value, as follows:

Login to sagdell4:7778/access/oblix/

To change the Access Server Configuration, click on:

- Acesss System Console hyperlink
- Access Server Configuration tab
- Access1 hyperlink
- Modify button

Then change the following values:

- URL Prefix Reload Period (seconds) to 5
- Password Policy Reload Period (seconds) to 5
- User Cache Timeout (seconds) to 5
- Policy Cache Timeout (seconds) to 5

Then click the "Save" button and "OK" to commit the changes.

To alter the WebGate configuration, click on:

- Acesss System Console hyperlink
- Access System Configuration tab
- AccessGate Configuration hyperlink
- Go button
- AccessGate1 hyperlink
- Modify button
- Change the "Cache timeout" value to 5
- Click the "Save" button and "OK" to commit the changes.

[IM.POST-5] The administrator must configure the Access Server and the Identity Server to write their Audit records to file, as follows:

Login to the Access Server and click on:

- Access Server Configuration tab
- Access1 hyperlink
- Modify button

Then change the following values.

- Audit to File (on/off)* to ON
- Audit File Name to "/space/oracle/product/10.1.4/AccessServer/AccessServerAudit.log"
- Buffer Size 100

Then click the "Save" button and "OK" to commit the changes.

Login to the Identity Server and click on:

- System Configuration tab
- Identity Servers hyperlink
- identity hyperlink
- Modify button

Then change the following values.

- Audit to File (on/off)* to ON
- Audit File Name to "/space/oracle/product/10.1.4/Identity_Server/IdentityServerAudit.log"
- Buffer Size 100
- Then click the "Save" button and "OK" to commit the changes.

[IM.POST-6] The administrator must not change the Log Level or the Access Log to File settings for OVD server auditing (see [OVDPM, 6]). The default Log Level is “Info” and Access Log to File is enabled by default.

[IM.POST-7] The administrator must create a Form-based Authentication Scheme and a Policy domain that will use the Scheme to restrict access to resources that require authentication. A Policy domain using anonymous authentication must also be created in order to allow access to the html page containing the form.

In addition the administrator must create a Policy domain that will use the Form-based Authentication Scheme to restrict access to the Access and Identity Servers to administrators.

An example of how this can be achieved is provided in Annex B. Also see [OAMAG, Appendix A] for more details.

[IM.POST-8] Administrators must ensure that when creating or amending policies the Update Cache box is always selected to ensure the new or amended policy is applied.

[IM.POST-9] The administrator must enable `DenyOnNotProtected` in the WebGate and ensure the WebGate is configured for UTF-8 (see [OAMAG,3-27]), as follows:

login to the Access System Console

http://sagdell4t:7778/access/oblix/

Then click

1.Acesss System Console

2.Access System Configuration

3.AccessGate Configuration

4.Go

5.AccessGate1

6.Modify

Select the “On” radio button for the `DenyOnNotProtecteded` parameter.

Under “User Defined Parameters” add a Parameter of URLInUTF8Format an set the Values field to true.

Click on save.

Note, [IM.POST-7] must have been correctly performed before enabling `DenyOnNotProtecteded`.

[IM.POST-10a] The administrator must configure the Master Audit Rule, following the instructions in [OAMAG, 4: Configuring the Master Audit Rule] and ensuring all of the "Audit Events” and the “Update Cache” options are selected.

[IM.POST-10b] The administrator must ensure that the operating system’s auditing is started by using the following command:

```
$ /etc/init.d/auditd start
```

In addition the administrator must ensure auditing is automatically started on reboot as follows:

```
$/sbin/chkconfig auditd on
```

[IM.POST-11] The administrator shall perform regular checks of the audit trail, looking for evidence of attacks against the TOE’s security policy. Particular items to look for are:

• anonymous web users accessing web resources for which they are not intended to be authorized.

• evidence of any access to non-public information via web user accounts that are no longer intended to be used to access web resources.

• if the Access Server audit log (configured as per assertion [IM.POST-5]) includes many entries in a short period of time showing access to the Password Change Redirect URL mentioned in assertion [IM.POST-3b].
Such evidence will require investigation as it is likely to indicate that a user has been making a password-guessing attack to try to gain access as another user.

[IM.POST-12] The administrator shall ensure that the TOE audit trail is kept to a reasonable size by archiving audit material when necessary and by purging the TOE audit trail (after first-checking its contents as described in the assertion above).

The administrator must note that, if the TOE audit trail is not regularly purged, it can cause the disk space to fill up. The administrator must therefore monitor disk usage and must take action to prevent the disk space allocated to hold the audit trail getting full. The audit records for Oracle Access Manager and Oracle Virtual Directory are put to files (see [IM.POST-5] and [IM.POST-6]). The actions to prevent the audit trail becoming full for OID are covered in assertion [DI.POST-6] in [OIDECD, 4.2].

[IM.POST-13] The administrator must configure Firewalls on each server machine as described in Annex B of this document.

[IM.POST-14] Administrators must ensure that any LDAP filters used in authorization rules (see [OAMAG, 6]) do not contain unnecessary space characters.

[IM.POST-15] Administrators must ensure that the name of the OID super user is not changed from `orcladmin`.

[IM.POST-16] Administrators must ensure that all UID's are unique across all user data stores accessed by Oracle Access Manager via OVD.

[IM.POST-17] Administrators must ensure that the Anonymous authentication scheme is only used for resources that are to be accessible by all TOE users.

[IM.POST-18] Administrators must ensure that they read the following explanation of the "Allow Takes Precedence" feature to avoid inadvertently configuring authorization rules that do not always operate in the way that the administrator intended:

[OAMAG, 6: About Actions for Inconclusive Results] states that an Inconclusive result can be returned for an authorization expression if the user qualified for conflicting Allow Access and Deny Access rules, and [OAMAG, 6: About Authorization Expression Evaluation] states that, in the case of an Inconclusive result, the user is denied access to the resource.
However, the administrator must bear in mind when devising authorization expressions that such an Inconclusive result does not necessarily deny the user access to the resource. [OAMAG, 6: About the AND Operator] explains that, if a user qualifies for both the Allow Access condition and the Deny Access condition of the same authorization rule, whichever condition is configured to take precedence in the Allow Takes Precedence field for the authorization rule is the one that is honoured.

[IM.POST-19a] Administrators must ensure the following modules are removed from or commented out of the OHS `httpd.conf` file:

- mod_rewrite
- mod_imap
- mod_status
- mod_proxy

OHS should then be restarted using the opmnctl tool.

[IM.POST-19b] Administrators must use the `LimitRequestBody` directive in the `httpd.conf` file to limit the amount of information that can be POSTed to the web server during form-based authentication. The `LimitRequestBody` directive must be applied to any directories containing the form action URL of any form-based authentication pages. In the evaluated configuration the following lines were added to the `httpd.conf` file:

```
<Directory "/space/oracle/product/10.1.3.1/OHS/ohs/htdocs/form_protected">
LimitRequestBody 100
</Directory>
```

[IM.POST-20] Administrators must remove all file permissions on all installed files from user accounts that are not in the same Group as the software owner, as follows:

```
$ cd /space/oracle
$ chmod -R o-rwx product
```

This must be performed on all server machines listed in section 2.1.

4.2 TOE Restart Procedure

Should it become necessary to restart the TOE the following are the steps that must be followed:

Machine 1

Start the database as follows:

```
$ export ORACLE_SID = polOID
$ export ORACLE_HOME = /space/oracle/product/10.1.4/IM_INFRA_POLICY
$ cd $ORACLE_HOME/bin
$ ./sqlplus /nolog
SQL> connect / as sysdba;
SQL> startup;
SQL> exit;
```

Start the listener as follows:

```
$ ./lsnrctl start
```

Start OID as follows:

```
$./oidctl server=oidldapd instance=1 start
```

Machine 2

Start both databases as follows:

```
$ export ORACLE_SID = user1OID
$ export ORACLE_HOME = /space/oracle/product/10.1.4/IM_INFRA_USER1
$ cd $ORACLE_HOME/bin
$ ./sqlplus /nolog
SQL> connect / as sysdba;
SQL> startup;
SQL> exit;
```

Start the listener as follows:

```
$ ./lsnrctl start
```

Start OID as follows:

```
$./oidctl server=oidldapd instance=1 start
```

```
$ export ORACLE_SID = user2OID
$ export ORACLE_HOME = /space/oracle/product/10.1.4/IM_INFRA_USER2
$ cd $ORACLE_HOME/bin
$ ./sqlplus /nolog
```

```
SQL> connect / as sysdba;
SQL> startup;
SQL> exit;
```

Start OID as follows:

```
$./oidctl server=oidldapd instance=1 start
```

Machine 1

Start OVD as follows:

```
$ cd /space/oracle/product/10.1.4/OViD
$ ./vde.sh start
```

Start OHS as follows:

```
$ cd /space/oracle/product/10.1.3.1/OHS/opmn
$./opmnctl startall
```

Machine 2

Start Identity Server as follows:

```
$ cd /space/oracle/product/10.1.4/Identity_Server/identity/oblix/apps/common/bin
$./start_ois_server
```

Start Access Server as follows:

```
$ cd /space/oracle/product/10.1.4/AccessServer/access/oblix/apps/common/bin
$./start_access_server
```

This Page Intentionally Blank

CHAPTER

5

Procedures

The procedural requirements for maintaining the security of the Oracle Internet Directory instance that is part of the TOE are given in [OIDECD, 5]. This chapter describes additional procedural requirements for maintaining the security of the TOE.

5.1 Operating System Procedures

5.1.1 General Procedures

[OS-2] The operating system administrator shall ensure that only designated users are able to perform administrative tasks within the operating system. In addition, the only local operating system user accounts on the server machines listed in section 2.1 shall be those for the TOE software administrator (e.g. the oracle user account) and the operating system administrator account (e.g. the root account).

[OS-3] The operating system administrator shall ensure that there are no general purpose computing capabilities (e.g. compilers or user applications) available on the TOE servers other than those services necessary for the operation, support and administration of the TOE software.

5.1.2 Identification and Authentication

Procedures relating to user passwords are covered in section 5.2 below.

5.1.3 Protection of Resources

[PR-1] The operating system shall protect all of the installed TOE-related files and directories by means of its Access Control Mechanisms to ensure that they are accessible to their authorised users only. The Oracle Universal Installer sets file permissions when the Oracle software is installed, so no further action in this respect is required.

[PR-2] To maintain the integrity of the audit timestamp, only registered system administrators shall have access to the operating system clock configuration. All other users shall have no access permissions for the operating system clock configuration.

[PR-3] Authorised administrators of the TOE are non-hostile, are appropriately trained and follow administrator best practice and guidance.

5.1.4 Accounting and Auditing

[AA-1] The operating system shall protect operating system audit trails against unauthorised modification and deletion by means of its Discretionary Access Control mechanisms.

[AA-2] Administrators shall only delete or modify the TOE-generated audit log files in order to comply with assertion [IM.POST-12].

[AA-3] The operating system administrator shall adopt procedures to archive audit log files prior to audit trail size or disk space exhaustion.

5.2 TOE Administration Procedures

Procedures for the administration of TOE security shall be established based on the contents of this document, the Security Target [ST], any site security policy that may be in force and [OIDECD]. In particular, procedures for the TOE shall be established as follows:

- The administrator shall instruct users not to disclose their TOE passwords to other individuals.
- The administrator shall advise users of the restrictions on the passwords they can use as a result of the settings in the password policies that apply to them.
- User passwords generated by the system administrator shall be distributed in a secure manner.
- Procedures and/or mechanisms shall assure that, after system failure or other discontinuity, recovery without a protection (i.e. security) compromise is obtained.
- The on-line and off-line storage media on which security related data (such as audit trails) is held shall be properly stored and maintained, and routinely checked to ensure the integrity and availability of the security related data;
- The Oracle Virtual Directory root user is a highly trusted user, who is required by the architecture of the TOE to be able to perform privileged adminisration operations. It is necessary that appropriate personnel and procedural measures will be provided to ensure that operations performed under this trusted user account conform to the system security policy.
- For routine administration tasks it is recommended that alternative, less privileged, accounts are used rather than the OID super user or the OVD root user. These accounts should be configured as members of administrative groups and should be used to perform a set of resticted administrative operations for the directory.
- Administrators, through the use of password policies, shall ensure that password controls for all users (including trusted administrative users, but excluding the OVD root user for which password policies do not apply) are strong enough to satisfy the TOE’s CC Strength of Function rating of SOF-*high*.
- Administrators should be aware of the factors influencing the strength of user passwords when creating or updating password policies. **[IM.POST-3]** ensures that certain limits are set in every password policy. However, suitable use of the other available password controls normally strengthens the TOE’s overall password mechanism strength.
  For example, setting Password Validity Period in conjunction with Password

Expiry Notice Period will limit the opportunity of an attacker to guess a particular password. In addition, using the Password History password policy field will ensure passwords held in the history store cannot be re-used, again limiting the opportunity for a particular password to be guessed.

Note that Password policies are described in [OAMICAG, 7: Managing Password Policies].

This Page Intentionally Blank

ANNEX A TOE Components

A.1 Server components

The components that are installed on the server by the Oracle Universal Installer during the installation of Oracle Internet Directory 10*g* (10.1.4.0.1) are listed in the install log. This can be located in the following directory:

`/space/oracle/oraInventory/logs`

The components that are installed on the server during the installation of Oracle Access Manager 10*g* (10.1.4.0.1) are listed in files named comps.xml, which can be located in the following subdirectories of the `/space/oracle/product/10.1.4` directory:

Component Name: OracleAS Identity Management aaa 10.1.4
Directory: `/AccessServer/access/inventory/ContentsXML`

Component Name: OracleAS Identity Management Identity 10.1.4
Directory: `/Identity_Server/identity/inventory/ContentsXML`

Component Name: OracleAS Identity Management manager 10.1.4
Directory: `/webcomponent/access/inventory/ContentsXML`

Component Name: OracleAS Identity Management WebPass 10.1.4
Directory: `/webcomponent/identity/inventory/ContentsXML`

Component Name: OracleAS Identity Management WebGate 10.1.4
Directory: `/webgate/access/inventory/ContentsXML`

The components that are installed on the server during the installation of Oracle Virtual Directory 10*g* (10.1.4.0.1) are listed in the Oracle_Virtual_Directory_InstallLog.log file. This can be located in the following directory:

`/space/oracle/product/10.1.4/OViD/log`

A.2 Evaluated Configuration Boundaries

The evaluated configuration of the TOE shall comprise exactly the following software components:

- Oracle Internet Directory Server 10.1.4.0.1
- Oracle Internet Directory Tools 10.1.4.0.1
- Oracle Virtual Directory Server 10.1.4.0.1
- OracleAS Identity Management aaa 10.1.4
- OracleAS Identity Management Identity 10.1.4
- OracleAS Identity Management WebPass 10.1.4
- OracleAS Identity Management WebGate 10.1.4

A.3 Client components

There are no client components in the TOE.

B Authentication

This Annex describes how to configure the Form-based Authentication Scheme and the policies that were used in the TOE in its Evaluated Configuration. In addition, the HTML forms and resources are described to provide an example of how form-based authentication could be used.

B.1 Create a Form-based Authentication Scheme

From the Access System Configuration tab click on the "Authentication Management" link in the left-hand frame and click on the "Add" button. Enter the following information:

Name: Form-Based Over LDAP

Descirption: Form-Based Authentication

Level: 1

Challenge Method: Form

Challenge Parameter: (click the '+' button to add the following Challenge Parameters)

- form: /forms/login.html
- creds: login password
- action: /form_protected/dummy
- passthrough: no

SSL Required: No

Challenge Redirect: Null

Select the Plugins tab followed by the Modify button. From the Plugin Name drop-down list select "credential_mapping". In the Plugin Parameters field enter the following:

obMappingBase=”dc=oracle,dc=com”, obMappingFilter=”(&(objectclass= inetorgperson)(uid=%login%)(|(!(obuseraccountcontrol=*)) (obuseraccountcontrol=ACTIVATED)))”

Click on the Add button and create the validate_password plugin with a Plugin Parameter of: ObCredentailPassword=”password”,obReadPasswdMode=”LDAP”, obWritePasswdMode=”LDAP”.

Click the Save button.

Select the General tab, click Modify and select the “Yes” radio button adjacent to the Enabled field.

B.2 HTML Forms and Resource

On Machine 1 navigate to the `/space/oracle/product/10.1.3.1/OHS/ohs/htdocs` directory and create the following:

Create a directory called `forms`. Within this directory create an html page named `login.html`. This page must contain an html form based on the following:

action=”/form_protected/dummy”
method=”post”
input type=”text” name=”login” size=”20” maxlength=”50”
input type=”password” name=”password” size=”20” maxlength=”50”

Create another directory called `form_protected`. Within this directory create 2 html pages named `resource1.html` and `resource2.html`.

B.3 Policies

Access to the Identity Server and Policy Manager must be restricted to Administrators by creating a policy based on the following values:

Resources
URL Prefix: /access and /identity

Authorization Rules
Select Allow Access and select the Administrators.
Enabled: Yes
Allow takes precendence: Yes

Default Rules
Authentication Scheme: Form-Based Over LDAP
Authorization Expression: Select the one created in the Authorization Rules

A policy must be configured to grant anonymous access to the html file containing the login form:

Resources
URL Prefix: /forms/login.html

Authorization Rules
Select Allow Access and select the “Any one” option in the Role dropdown list.
Enabled: Yes
Allow takes precendence: Yes

Default Rules
Authentication Scheme: Anonymous Authentication
Authorization Expression: Select the one created in the Authorization Rules

A policy must be configured to enable form-based protection for the form_protected directory:

Resources
URL Prefix: /form_protected

Authorization Rules
Select Allow Access and select the “Any one” option in the Role dropdown list (or, alternatively, select the users to whom access is to be granted).
Enabled: Yes
Allow takes precendence: Yes

Default Rules
Authentication Scheme: Form-Based Over LDAP
Authorization Expression: Select the one created in the Authorization Rules

A policy must be configured to grant all users access to the password change URL:

Resources
URL Prefix: /identity/oblix/apps/lost_pwd_mgmt and /identity/oblix/lang

Authorization Rules
Select Allow Access and select the “Any one” option in the Role dropdown list.
Enabled: Yes
Allow takes precendence: Yes

Default Rules
Authentication Scheme: Anonymous Authentication
Authorization Expression: Select the one created in the Authorization Rules

This Page Intentionally Blank

C Firewalls

Firewalls must be configured on all servers in the TOE such that all ports, with the exception of the ports required by the software in the TOE, are closed.

C.1 Configuring Firewalls for Machine 1

Login to Machine 1 and create a file called `/etc/sysconfig/iptables` with the following content (note that 172.20.16.139 is the IP address of Machine 2 in the evaluated configuration):

```
# Firewall configuration for Oracle access server
# DO NOT USE system-config-securitylevel to edit
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 7778 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp -s 172.20.16.139 --dport 389 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp -s 172.20.16.139 --dport 1389 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Once this is complete start the restart the firewall with the following command.

```
/etc/init.d/iptables restart
```

C.2 Configuring Firewalls for Machine 2

Login to Machine 2 as an Administrator and create a file called `/etc/sysconfig/iptables` with the following content (note that 172.20.16.138 is the IP address of Machine 1 in the evaluated configuration):

```
# Firewall configuration for Oracle access server
# DO NOT USE system-config-securitylevel to edit
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp -s 172.20.16.138 --dport 389 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp -s 172.20.16.138 --dport 6021 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp -s 172.20.16.138 --dport
```

```
6022 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp -s 172.20.16.138 --dport 13060 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Once this is complete start the restart the firewall with the following command:

```
/etc/init.d/iptables restart
```

This Page Intentionally Blank

D References

[CC] *Common Criteria for Information Technology Security Evaluation,*
Version 2.3, August 2005.

[LDAP3] *Lightweight Directory Access Protocol (v3),*
Request For Comments (RFC) 2251 of the Internet Engineering Task Force,
December 1997,
available on the World Wide Web at http://www.ietf.org/rfc.htm.

[OAMAG] *Oracle Access Manager Access Administration Guide 10g (10.1.4.0.1),*
Part No. B25990-01, Oracle Corporation.

[OAMICAG] *Oracle Access Manager Identity and Common Administration Guide 10g (10.1.4.0.1),*
Part No. B25343-01, Oracle Corporation.

[OAMIG] *Evaluated Configuration for Oracle Identity and Access Management 10g (10.1.4.0.1): Oracle Access Manager Installation ,*
Oracle Corporation.

[OHSIG] *Evaluated Configuration for Oracle Identity and Access Management 10g (10.1.4.0.1):Oracle HTTP Server Installation ,*
Oracle Corporation.

[OIDAG] *Oracle Internet Directory Administrator's Guide 10g (10.1.4.0.1),*
Part No. B15991-01, Oracle Corporation

[OIDECD] *Evaluated Configuration for Oracle Internet Directory 10g (10.1.4.0.1),*
Oracle Corporation.

[OIDIG] *Evaluated Configuration for Oracle Identity and Access Management 10g (10.1.4.0.1): Oracle Internet Directory Installation,*
Oracle Corporation.

[OIMUR] *Oracle Identity Management User Reference 10g (10.1.4.0.1),*
Part No. B15998-01, Oracle Corporation.

[OVDIG] *Evaluated Configuration for Oracle Identity and Access Management 10g (10.1.4.0.1): Oracle Virtual Directory Installation,*
Oracle Corporation

[ST] *Security Target for Identity and Access Management 10g (10.1.4.0.1),*
Oracle Corporation.