INTEGRIGY

Oracle PeopleSoft Security Quick Reference

Version 2.0 – April 2016

1. Critical Patch Updates

Oracle Critical Patch Updates (security patches) are delivered through PeopleTools. CPUs PeopleTools releases are provided for up to 24 months after the next minor release is generally available.

PeopleTools	GA Date	CPU End Date
PT8.51	9/10/10	Jan 2014
PT8.52	10/28/11	Jan 2015
PT8.53	2/1/13	7/19/16
PT8.54	7/11/14	12/4/17
PT8.55	12/4/15	TBD

To find PeopleTools release –

```
SQL> SELECT * FROM sysadm.psstatus;
```

2. Supported Databases and WebLogic

RDBMS and WebLogic Critical Patch Updates patches are separate and are applied NOT through PeopleTools updates.

PeopleTools	Database	WebLogic	Tuxedo
PT8.51	11.2.0.4	10.3.6.0	10.3.0.0
PT8.52	11.2.0.4	10.3.6.0	10.3.0.0
PT8.53	11.2.0.4 12.1.0.2	10.3.6.0	11.1.3.0 11.1.1.2
PT8.54	11.2.0.4 12.1.0.2	12.1.3.0 12.1.2.0	12.1.1.0
PT8.55	11.2.0.4 12.1.0.2	12.1.3.0	12.1.1.0 12.1.3.0

- RDBMS 12.1.0.1 supported through July 2016.
- RDBMS 12.1.0.2 supported through July 2021.
- RDBMS 11.2.0.4 supported through December 2020.
- WebLogic 10.3.6.x is supported through December 2018.
- WebLogic 12.1.2.0 is supported through June 2016.
- WebLogic 12.1.3.0 is supported through December 2017 and will be the terminal release of 12.1.x.
- Tuxedo support dates – 10.3 December 2016, 12.1.3 in 2020, all 11.x and 12.1.1 end in 2018.
- WebLogic version can be found running –

```
java weblogic.version -verboseChange default
```

3. Default Oracle Database Accounts

All database passwords should be changed. No default passwords should be used. Default Oracle database accounts should be expired & locked.

Account	Account Status	Change Method
SYS, SYSTEM	Open	Manual
CTXSYS, APPQOSSYS, OUTLN	Expired & Locked	Manual
DIP, ORACLE_OCM, DBSNMP	Expired & Locked	Manual

To test for default database account passwords –

```
SQL> SELECT * FROM sys.dba_users_with_defpwd;
```

4. Change Owner ID Password

1. For the Access ID (SYSADM), in Application Designer, select Tools, Miscellaneous Definitions, Access Profiles.
2. Highlight the Access Profile enter the old password and the new password. Always use a complex password of the maximum 8 characters allowed.

5. Remove Unneeded Default Super Users

Seeded PeopleSoft application user accounts with super user privileges, where possible, should be removed or have the password changed. Refer to documentation for details.

Default Oracle PeopleSoft Users		
BELHR	JCADMIN1	PSJPN
CAN	NLDHR	PSPOR
CFR	PS	TIME
CNHR	PSCFR	UKHR
ESP	PSDUT	UKNI
FRA	PSESP	USA
FRHR	PSFRA	HSHR
GER	PSGER	WEBGUEST
GRHR	PSINE	WEBMODEL

6. Change IB Gateway Properties Password

Change the password using the Integration Broker Gateway Authentication page. Select the check box to change password from default.

7. Change Connect ID Password

1. Change the 'PEOPLE' database account password following RDBMS specific instructions.
2. Update application server configuration using PSADMIN utility. Be sure to select option to encrypt password.
3. Update password in Configuration Manager.

The Connect ID password should –

- not exceed eight characters.
- (Windows) should not contain forward-slash (/).
- (UNIX) should not contain percent (%).

8. CONNECT ID Permissions

The Connect ID (PEOPLE) account should have only these database grants –

```
CREATE SESSION
GRANT SELECT ON psstatus TO people;
GRANT SELECT ON psoprdefn TO people;
GRANT SELECT ON psaccessprfl TO people;
```

To check permissions –

```
SQL> SELECT * FROM sys.dba_tab_privs
     WHERE grantee = 'PEOPLE';
```

9. Delete or Disable Unused User IDs

Disable or remove stale user accounts –

1. Select PeopleTools > Security > User Profiles > User Profiles.
2. Select user to disable or delete.
3. If disabling, check Account Locked Out check box.

Use the following SQL to locate stale users:

```
SQL> SELECT * FROM sysadm.psptloginaudit;
```

10. Oracle Support (MOS) Security Notes

Useful PeopleSoft Security Links	2060772.1
Lifetime support summary for PeopleSoft	1348959.1
Master Note PT Known Security Issues	1348934.1
PeopleSoft Security Auditing	1963774.1
PeopleTools Certifications	759851.1

11. Controls – Security Related

PeopleTools > Security > Password Configuration > Password Controls to access the Password Controls page.

Passwords	
Enable Signon PeopleCode	Enable
Age	365
Account Lockout	3
Miscellaneous (Password = User ID)	True
Minimum Length	8
Character Requirement	2
Other Security	
Purge User Profiles	730
Expire at Next Logon	After password reset
Can Start Application Server[1]	Heavily restrict
Allow password to be emailed	Not for privileged users

[1] Password controls do not apply to users who can start the application server. Permission also applies to Process Scheduler.

12. Monitoring and Auditing

Use PSADMIN (psappsrv.cfg) ensure the following domain parameters are set for auditing.

Parameter	Description	Value
Enable Login Audit option	User logon/off and attempts. Log written to table PSPTLOGINAUDIT	Y
Suppress SQL Error	Specify whether SQL errors appear to the user	1=disable 0=display
EnableDBMonitoring	DB level auditing set. Triggers will populate tables with a 'AUDIT_prefix'. Then need to create a record definition in Application Designer and build the SQL table in which you store audit information	1

13. Disable Config Re-Initialization

Dynamic re-initialization is enabled by default only for the PROD profile. Ensure no other profiles have it set. If they do, remove it –

1. In PIA, PeopleTools > Web Profile > Web Profile Configuration. Select the web profile (e.g., PROD).
2. Select the Custom Properties page. Delete any property with the name auditPWD.

14. Harden WebLogic Web server

1. **Change default WebLogic Passwords.** Do for key default WebLogic accounts such as: System, operator, monitor. This is critical to secure anyone with access to http://server:port/console.

2. **Disable console access based on IP whitelist.** Domain > Security > Filter > Connection Filter. Specify connection filter rules such as –

```
10.1.1.1  * 7001 allow https #allow only 10.1.1.1
0.0.0.0/0 * 7001 deny        #deny everyone else
```

3. **Enable SSL (HTTPS).** Follow instructions in Enterprise PeopleTools PeopleBook: *System and Server Administration, Working with Oracle WebLogic, Defining SSL Certificates on WebLogic*. Recommend allowing only TLS 1.1 and 1.2.

4. **PeopleSoft recommended steps.** Follow instructions in Enterprise PeopleTools PeopleBook: *System and Server Administration, Working with Oracle WebLogic*.
    a. Change the WebLogic server user password.
    b. Restrict access to a servlet.

5. **Harden WebLogic per best practice.** Follow the recommended security steps under *Securing the WebLogic Server Host* at –
    http://download.oracle.com/docs/cd/E14571_01/wls.htm

15. Enable Tuxedo Encryption

Tuxedo is controlled by the psadmin utility in $PS_HOME/appserv. Edit the configuration file psappsrv.cfg for the domain. The default value of zero (0) does not encrypt. Change the value to 64 for 64-bit encryption or to 128 for 128-bit encryption under the Encryption property for the **Workstation Listener** and **JOLT Listener**.

16. Encrypt Web Config & Template Files

1. Run the PTEM_CONFIG Application Engine program with the property encrypt_password set to True in the template file. Generates a new template file named **_encrypted.*

2. Generate a new PSCipher key to encrypt values in the web server config files – `pscipher -buildkey`

17. Change Default PSKEY Password

The PSKEY is keystore contains all root and node certificates used by the Integration Gateway and PIA. The default password is 'password' and the keystore is located here in PS_HOME\webserv\domain\keystore directory.

1. Use pskeymanager.sh to change the default password –
    `pskeymanager.sh -changeKeystorePassword`
2. Update the secureFileKeystorePasswd property in the integration.properties file and WebLogic with password.

18. Default Oracle PeopleSoft Ports

Component	Port # + x
Database	1521
WebLogic	90, 443
Tuxedo	3050
WSL	7000
WebLogic Admin	7001-7005
PS Real Time Event Server	7180, 7143
JSL	9000, 9010
Jolt connections from web server	9001-9005
PS Debugging	9500
Jolt relay	9100
PIA	8101

19. Key Tables and Configuration Files

Table	Description
PSOPRDEFN	PeopleSoft Users
PSUSERATTR	User security attributes, includes mobile
PSOPRALIAS	Various ids: emplid, cust_id, vendor_id,
PSROLEUSER	Lists a user's static and dynamic roles
PSPTLOGINAUDIT	User login activity
PSAUDITEXT	Field level auditing (replaces PSAUDIT)
File	**Description**
psappsrv.cfg	Parm file for Tuxedo and app servers
psappsrv.val	Validation file for interactive config
psappsrv.env	Environment file and variables

INTEGRIGY
http://www.integrigy.com

PeopleSoft Security Quick Reference

Version 2.0 – April 2016