About Integrigy

Products

**AppSentry**
ERP Application and Database Security Auditing Tool

**AppDefend**
Enterprise Application Firewall for the Oracle E-Business Suite

Services

**Security Assessments**
- Oracle EBS, OBIEE, Databases, Sensitive Data, Penetration Testing

**Compliance Assistance**
- SOX, PCI, HIPAA

**Security Design Services**
- Auditing, Encryption, DMZ

You
generic privileged account

application, database, or operating system account used for administration by multiple people and has significant privileges
Generic Privileged Accounts

- Oracle E-Business Suite is defined by generic privileged accounts in each layer of the technology stack
  - Multiple highly privileged accounts
  - Generic accounts that must be used to manage the application and database

- Majority of all data breaches committed by insiders
  - Some intentional
  - Most accidental
# Oracle EBS Generic Privileged Accounts

<table>
<thead>
<tr>
<th>Oracle E-Business Suite</th>
<th>SYSADMIN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>seeded application accounts</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Oracle Database</th>
<th>APPS, APPLSYS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SYS, SYSTEM</td>
</tr>
<tr>
<td></td>
<td>Oracle EBS schemas (GL, AP, ...)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operating System (Unix and Linux)</th>
<th>root</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>oracle, applmgr</td>
</tr>
</tbody>
</table>
Generic Privileged Account Inter-Dependency

database
- APPS
  - execute SQL as SYS
    - database
      - SYS
  - can obtain SYSADMIN password
  - execute SQL as APPS
    - application
      - SYSADMIN
  - connect as SYSDBA
  - execute OS commands as oracle
    - operating system
      - oracle/applmgr
How Concerned About Privileged Accounts?

- Yes: 65%
- Somewhat: 26%
- No: 3%
- Don't Know: 6%
How Actively Managed are Privileged Accounts?

- **Very Actively Managed**: 38%
- **Somewhat Managed**: 35%
- **Not Managed**: 17%
- **Don't Know**: 10%
Generic
Privileged
Accounts

E-BUSINESS SUITE
SYSADMIN Oracle EBS User

- **SYSADMIN**
  - System Administrator responsibility + 13 more
  - Must be used certain functions
  - Cannot be disabled or end-dated
  - Access to everything in Oracle EBS

- **Who might have access to SYSADMIN?**
  - Application administrators
  - Application DBAs
  - Support and power users
  - Helpdesk
  - Consultants and subcontractors
| Control          | SYSADMIN should only be used for a few specific functions – named accounts for all other administration activities  
|                 | Change ticket required for all use in production  
|                 | Use custom generic, less privileged account for scheduled concurrent programs and proxy user  
|                 | Change password when cloning  
|                 | Frequently rotate password (90 days)  
|                 | **Manage password** in password vault [Vault]  
| Log & Monitor   | Implement auditing for all usage [Framework]  
|                 | Alert on login and monitor all usage  
| Audit           | Check last password change date  
|                 | Verify password complexity and length settings  
|                 | Interview to determine how password is controlled |
## 30+ Seeded Generic Application Accounts

<table>
<thead>
<tr>
<th>Active Application Account</th>
<th>Default Password</th>
<th>Active Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASGADM</td>
<td>WELCOME</td>
<td>SYSTEM_ADMINISTRATOR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ADG_MOBILE_DEVELOPER</td>
</tr>
<tr>
<td>IBE_ADMIN</td>
<td>WELCOME</td>
<td>IBE_ADMINISTRATOR</td>
</tr>
<tr>
<td>MOBADM</td>
<td>MOBADM</td>
<td>MOBILE_ADMIN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SYSTEM_ADMINISTRATOR</td>
</tr>
<tr>
<td>MOBILEADM</td>
<td>WELCOME</td>
<td>ASG_MOBILE_ADMINISTRATOR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SYSTEM_ADMINISTRATOR</td>
</tr>
<tr>
<td>OP_CUST_CARE_ADMIN</td>
<td>OP_CUST_CARE_ADMIN</td>
<td>OP_CUST_CARE_ADMIN</td>
</tr>
<tr>
<td>OP_SYSADMIN</td>
<td>OP_SYSADMIN</td>
<td>OP_SYSADMIN</td>
</tr>
<tr>
<td>WIZARD</td>
<td>WELCOME</td>
<td>AZ_ISETUP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>APPLICATIONS FINANCIALS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>APPLICATION IMPLEMENTATION</td>
</tr>
<tr>
<td>Control</td>
<td>End-date per best practices</td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change password to random string</td>
<td></td>
</tr>
<tr>
<td>Log &amp; Monitor</td>
<td>Implement auditing for all usage or access [Framework]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Alert on any attempt to access</td>
<td></td>
</tr>
<tr>
<td>Audit</td>
<td>Review usage of accounts for external access (DMZ)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Check end-date and last use</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Check last password change date</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Check for new seeded accounts after any major patches or upgrades</td>
<td></td>
</tr>
</tbody>
</table>
Generic Privileged Accounts

DATABASE
| Oracle Database | SYS | - Owner of database  
| | | - Must be used for some operations  
| | SYSTEM | - Generic DBA account  
| | | - Must be used for EBS adpatch & adadmin  
| Oracle E-Business Suite | APPS | - Application account for all access – users, concurrent manager, and maintenance  
| | | - Must be used for maintenance  
| | | - APPS can access all data, including encrypted sensitive data  
| | APPLSYS | - Same password as APPS  
| | | - Should not be directly accessed  
| | Schema Owners (GL, AP, etc.) | - 250+ schema accounts  
| | | - All active and have default passwords  
| | | - Significant privileges  

# Oracle Database Account Passwords

<table>
<thead>
<tr>
<th>Database Account</th>
<th>Default Password</th>
<th>Exists in Database %</th>
<th>Default Password %</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS</td>
<td>CHANGE_ON_INSTALL</td>
<td>100%</td>
<td>3%</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>MANAGER</td>
<td>100%</td>
<td>4%</td>
</tr>
<tr>
<td>DBSNMP</td>
<td>DBSNMP</td>
<td>99%</td>
<td>52%</td>
</tr>
<tr>
<td>OUTLN</td>
<td>OUTLN</td>
<td>98%</td>
<td>43%</td>
</tr>
<tr>
<td>MDSYS</td>
<td>MDSYS</td>
<td>77%</td>
<td>18%</td>
</tr>
<tr>
<td>ORDPLUGINNS</td>
<td>ORDPLUGINNS</td>
<td>77%</td>
<td>16%</td>
</tr>
<tr>
<td>ORDSYS</td>
<td>ORDSYS</td>
<td>77%</td>
<td>16%</td>
</tr>
<tr>
<td>XDB</td>
<td>CHANGE_ON_INSTALL</td>
<td>75%</td>
<td>15%</td>
</tr>
<tr>
<td>DIP</td>
<td>DIP</td>
<td>63%</td>
<td>19%</td>
</tr>
<tr>
<td>WMSYS</td>
<td>WMSYS</td>
<td>63%</td>
<td>12%</td>
</tr>
<tr>
<td>CTXSYS</td>
<td>CTXSYS</td>
<td>54%</td>
<td>32%</td>
</tr>
</tbody>
</table>

* Sample of 120 production databases
# SYS Database Account

| Control | ■ **Control password** with password vault *[Vault]*  
|         | ■ SYS should only be used for a few specific functions – named DBA accounts for all other database management activities  
|         | ■ Change ticket required for use in production  
|         | ■ Change password when cloning |
| Log & Monitor | ■ Implement auditing for logins, key security and change management events *[Framework]*  
|             | ■ AUDIT_SYS_OPERATIONS = TRUE  
|             | ■ Reconcile usage to change tickets |
| Audit | ■ Check last password change date  
|       | ■ Interview to determine how password is controlled |
## SYSTEM Database Account

<table>
<thead>
<tr>
<th>Control</th>
<th>SYSTEM should only be used for EBS administration and patching — named DBA accounts for all other database management functions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Change password when cloning</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Log &amp; Monitor</th>
<th>Implement auditing for logins, key security and change management events [Framework]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Reconcile usage to change tickets</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Audit</th>
<th>Check last password change date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Interview to determine how password is controlled</td>
</tr>
</tbody>
</table>
### APPS Database Account

#### Control
- **Manage password** with password vault *[Vault]*
- **APPS should only be used for EBS administration and patching** – named DBA accounts for all other database management functions
- Use custom database profile with no lockout but strong password controls
- Change password when cloning

#### Log & Monitor
- Implement auditing for logins, key security and change management events *[Framework]*
- Monitor closely for failed logins *[Framework]*
- **Attempt to reconcile** DBA usage to change tickets

#### Audit
- Check last password change date
- Review logins to see who else is using
- Interview to determine how password is controlled
### EBS Schema Database Accounts

<table>
<thead>
<tr>
<th>Control</th>
<th>Log &amp; Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Change all passwords using FNDCPASS and throw the password away</td>
<td>▪ Implement auditing for all logins, key security and change management events [Framework]</td>
</tr>
<tr>
<td>▪ Control the APPLSYS account same as APPS</td>
<td>▪ Alert on any logins to the schema accounts</td>
</tr>
<tr>
<td>▪ R12 = lock all the schema accounts using the utility AFPASSWD –L</td>
<td>▪ Alert on any logins to APPLSYS</td>
</tr>
<tr>
<td>▪ Change passwords when cloning</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Audit</td>
<td></td>
</tr>
<tr>
<td>▪ Check last password change date</td>
<td></td>
</tr>
<tr>
<td>▪ Interview to determine how password is controlled</td>
<td></td>
</tr>
</tbody>
</table>
Database Accounts – General IT Controls

**Database Password Profiles**

- Create organizational database password profiles for service and named users
- Assign these profiles to all accounts
- Never use the DEFAULT profile – routinely check for any accounts assigned
- Use custom password verify function that meets organizational password policy
Default Database Passwords

- Routinely check for default database passwords
- Check after all database upgrades and after major EBS patches
- Use a tool like AppSentry rather than DBA_USER_WITH_DEFPWD that checks all accounts for many passwords
Generic
Privileged
Accounts

OPERATING SYSTEM
## oracle and applmgr Operating System Accounts

| Control | ▪ **Control password** with password vault [Vault]  
▪ **Prevent direct logins to oracle and applmgr**  
▪ DBAs should have named OS accounts  
▪ Require DBAs to use `su`, `sudo`, or PowerBroker to access oracle and applmgr accounts  
▪ Enforce a chain-of-trust – named user → generic user  
▪ No developer access to production server OS |
|---|---|
| Log & Monitor | ▪ Implement auditing at the OS level for all user logins  
▪ Use keystroke or command logging if required  
▪ Alert on direct logins to oracle or applmgr |
| Audit | ▪ Check last password change date  
▪ Interview to determine how password is controlled |
**Operating System – General IT Controls**

- **DBAs should never have root access**
  - Require segregation of duties for operating system

- **DBAs should have named OS accounts**
  - Integrate with LDAP or Active Directory for authentication and access control

- **Avoid SSH key or trust logins**
  - Limit any use of password-less logins between servers
  - Do not allow for highly privileged accounts
  - Always use passphrases
Overview

EBS Privileged Accounts

Best Practices

Logging Auditing & Monitoring

Q&A
Best Practices to Control Privileged Accounts

- **Use a Bastion host (virtual desktop) for direct O/S and/or database access**
  - Restrict network access and/or database ACLs
  - Two-factor authentication to access
  - Use SSH Keys for appropriate O/S accounts
  - Install key logger

- **Consider Oracle Database Vault**
  - Additional license but comes with pack for E-Business Suite schemas
Control Passwords to Control Privileged Accounts

- **Change defaults and don’t use weak passwords**
  - Use a random password generator

- **Use different passwords for production**
  - Change all passwords when clone

- **No hardcoding of passwords**
  - E.g. where possible consider password vault APIs and Oracle Wallet(s)

- **Use approach of need-to-know and least privilege**
  - Separation of duties and job function
  - Minimum of EBS, Database and O/S
Control Passwords to Control Privileged Accounts

- **Periodically inventory privileged and generic accounts**
  - Ask questions, cull and document
  - Take names and assign owners

- **Control passwords per risk classification of the account**
  - Rotate, expiry, complexity, length and half-passwords
  - One size does not fit all

- **Adopt formal privileged account and password policy**
  - Train and enforce
  - Make it real
Best Practices to Control Privileged Accounts

- Do you have a policy to change privileged password when somebody leaves?
  - Vendors included: managed services, hosting and cloud providers

- Does your password policy govern generic privileged accounts or does it forbid them?

- When was the last time audited all privileged generic accounts?

- What is your policy for SSH logins?
Best Practice: Use a Password Vault

- Vaults are purpose built solutions for enterprise password management
  - Sophisticated security
  - Robust standard reports
  - Built to support meet compliance requirements

- Shrink trust perimeter and increase governance of privileged accounts
  - Add all accounts passwords except those owned by named individuals
  - All service accounts
  - All generic accounts
  - Phased implementation (controlled vs. managed)
Password Vault Recommendations

- Add field for ticket number for password pulls
  - Required freeform text field to start

- Use for password expiry and rotation process

- Use for password creation and reset process

- Use for Rescue ID workflow process

- Log using Syslog (e.g. to Splunk)
  - Pass ticket number for password pull
Best Practice: Access Management Policy

- Implement an overall access management policy based on IT Security policies and compliance requirements
  - E.g. SOX/CoBit, PCI, HIPAA, 21 CFR 11

- Make part of overall Database security Program
  - Access Management is only one component

- Consider Access Management engagement
  - Audit and recommendations
Agenda

1. Overview
2. EBS Privileged Accounts
3. Best Practices
4. Logging Auditing & Monitoring
5. Q&A
Access management success or failure largely based on logging and auditing
  - No other way

Constantly log activity
  - Focus on key events
  - Audit with reports
  - Alert in real-time
The Oracle database and Oracle E-Business Suite offer rich log and audit functionality
- Most organizations do not fully take advantage

Requirements are difficult
- Technical, Compliance, Audit, and Security

Integrigy has a framework
- Already mapped to PCI, HIPAA, SOX and 21 CFR 11
Integrigy Framework for Auditing and Logging

Payment Card (PCI DSS)
SOX (COBIT)
HIPAA (NIST 800-66)
FDA 21 CFR 11
IT Security (ISO 27001)

Foundation security events and actions
(logins, logoffs, account creation, privileges, etc.)

Oracle Database
- Native Auditing
- Syslog
- DB log files

Oracle E-Business Suite
- Signon
- AuditTrails
- Page Tracking

Centralized Logging Solution
- Protected Audit Data
- Alerting & Monitoring
- Reporting
- Correlation

Integrigy Framework for Auditing and Logging
The foundation of the framework is a set of key security events and actions derived from and mapped to compliance and security requirements that are critical for all organizations.

<table>
<thead>
<tr>
<th>E1 - Login</th>
<th>E8 - Modify role</th>
</tr>
</thead>
<tbody>
<tr>
<td>E2 - Logoff</td>
<td>E9 - Grant/revoke user privileges</td>
</tr>
<tr>
<td>E3 - Unsuccessful login</td>
<td>E10 - Grant/revoke role privileges</td>
</tr>
<tr>
<td>E4 - Modify auth mechanisms</td>
<td>E11 - Privileged commands</td>
</tr>
<tr>
<td>E5 - Create user account</td>
<td>E12 - Modify audit and logging</td>
</tr>
<tr>
<td>E6 - Modify user account</td>
<td>E13 - Create, Modify or Delete object</td>
</tr>
<tr>
<td>E7 - Create role</td>
<td>E14 - Modify configuration settings</td>
</tr>
</tbody>
</table>
## Foundation Security Events Mapping

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>E1 - Login</td>
<td>10.2.5</td>
<td>11.10 (e) (d)</td>
<td>A12.3</td>
<td>164.312(c)(2)</td>
<td>A 10.10.1</td>
<td>AU-2</td>
</tr>
<tr>
<td>E2 - Logoff</td>
<td>10.2.5</td>
<td>11.10 (e)</td>
<td>DS5.5</td>
<td>164.312(c)(2)</td>
<td>A 10.10.1</td>
<td>AU-2</td>
</tr>
<tr>
<td>E3 - Unsuccessful login</td>
<td>10.2.4</td>
<td>11.10 (e) 11.300 (d)</td>
<td>DS5.5</td>
<td>164.312(c)(2)</td>
<td>A 10.10.1</td>
<td>A.11.5.1</td>
</tr>
<tr>
<td>E4 - Modify authentication mechanisms</td>
<td>10.2.5</td>
<td>11.10 (e) (d) 11.300 (b)</td>
<td>DS5.5</td>
<td>164.312(c)(2)</td>
<td>A 10.10.1</td>
<td>AU-2</td>
</tr>
<tr>
<td>E5 - Create user account</td>
<td>10.2.5</td>
<td>11.10 (e) 11.100 (a)</td>
<td>DS5.5</td>
<td>164.312(c)(2)</td>
<td>A 10.10.1</td>
<td>AU-2</td>
</tr>
<tr>
<td>E6 - Modify user account</td>
<td>10.2.5</td>
<td>11.10 (e) 11.100 (a)</td>
<td>DS5.5</td>
<td>164.312(c)(2)</td>
<td>A 10.10.1</td>
<td>AU-2</td>
</tr>
<tr>
<td>E7 - Create role</td>
<td>10.2.5</td>
<td>11.10 (e)</td>
<td>DS5.5</td>
<td>164.312(c)(2)</td>
<td>A 10.10.1</td>
<td>AU-2</td>
</tr>
<tr>
<td>E8 - Modify role</td>
<td>10.2.5</td>
<td>11.10 (e)</td>
<td>DS5.5</td>
<td>164.312(c)(2)</td>
<td>A 10.10.1</td>
<td>AU-2</td>
</tr>
<tr>
<td>E9 - Grant/revoke user privileges</td>
<td>10.2.5</td>
<td>11.10 (e)</td>
<td>DS5.5</td>
<td>164.312(c)(2)</td>
<td>A 10.10.1</td>
<td>AU-2</td>
</tr>
<tr>
<td>E10 - Grant/revoke role privileges</td>
<td>10.2.5</td>
<td>11.10 (e)</td>
<td>DS5.5</td>
<td>164.312(c)(2)</td>
<td>A 10.10.1</td>
<td>AU-2</td>
</tr>
<tr>
<td>E11 - Privileged commands</td>
<td>10.2.2</td>
<td>11.10 (e)</td>
<td>DS5.5</td>
<td>164.312(c)(2)</td>
<td>A 10.10.1</td>
<td>AU-2</td>
</tr>
<tr>
<td>E12 - Modify audit and logging</td>
<td>10.2.6</td>
<td>11.10 (e)</td>
<td>DS5.5</td>
<td>164.312(c)(2)</td>
<td>A 10.10.1</td>
<td>AU-2 AU-9</td>
</tr>
<tr>
<td>E13 - Objects Create/Modify/Delete</td>
<td>10.2.7</td>
<td>11.10 (e)</td>
<td>DS5.5</td>
<td>164.312(c)(2)</td>
<td>A 10.10.1</td>
<td>AU-2 AU-14</td>
</tr>
<tr>
<td>E14 - Modify configuration settings</td>
<td>10.2.2</td>
<td>11.10 (e)</td>
<td>DS5.5</td>
<td>164.312(c)(2)</td>
<td>A 10.10.1</td>
<td>AU-2</td>
</tr>
<tr>
<td>Level 1</td>
<td>Enable <strong>baseline auditing and logging</strong> for application/database and implement security monitoring and auditing alerts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 2</td>
<td>Send audit and log data to a <strong>centralized logging</strong> solution outside the Oracle Database and E-Business Suite</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 3</td>
<td>Extend logging to include <strong>functional logging</strong> and more complex alerting and monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Logging and Auditing is the Key
Integrigy Log and Audit Framework

More information on Integrigy’s Log and Auditing Framework is available in our Auditing and Logging whitepaper at –

www.integrigy.com/security-resources
Contact Information

Mike Miller
Chief Security Officer
Integrigy Corporation

web: www.integrigy.com
e-mail: mike.miller@integrigy.com
blog: integrigy.com/oracle-security-blog
youtube: youtube.com/integrigy