

Chapter 7: Application Users Best Practices

...

Use and Care of Generic User Accounts

As a general rule, generic user accounts are not to be established or used. This includes accounts for temporary employees such as AP Clerks. Generic accounts hide the employee’s accountability over the data entry performed and are an auditing 101 “no-no.”

Oracle comes seeded with a lot of generic user accounts. You can review Metalink Note 189367.1 (Best Practices for Securing your E-Business Suite) for a list of such accounts and recommendations from Oracle. Be aware that some generic users may not be documented in this Metalink Note. I have attempted to keep a current list of known generic users available to end users in the Internal Controls Repository (ICR).

For many companies, all seeded Oracle users can be end-dated (disabled) other than GUEST and SYSADMIN. Before disabling any of the accounts, you should test the disabling of such accounts in a non-production environment and analyze the impact of disabling such accounts. Unfortunately, detailed documentation on the impact of disabling such accounts doesn’t exist currently. When in doubt, you should test, test, test and then check with others that have tried it. You can use listservers like OAUG’s DBA and generic listserver as well as the Oracle Internal Controls and Security listserver that ERP Seminars hosts.

Even if you disable the accounts of these generic users, you should also change the seeded password. This is necessary because of the risk of decrypting passwords. The decryption risk will be more fully addressed later in the book. More on this topic can also be found in the Integriqy white paper called “Oracle Applications 11i Password Encryption.”¹

For the remaining active generic user accounts, ongoing monitoring of activity related to each account should continue.

Regarding the GUEST account, it should not have responsibilities assigned to it, and there should never be a direct login using this account. The GUEST account doesn’t even show up as an account in the Users form, so it cannot be used to directly log into the applications. So, the risk here is minimal. However, to be on the

¹ http://www.integriqy.com/security-resources/advisories/Integriqy_Encrypted_Password_Disclosure.pdf

safe side, include the GUEST account in login activity monitoring as well as in a regular review of assigned responsibilities.

The SYSADMIN user login is a hotly debated topic. Many system patches provided by Oracle refer to needing to use the SYSADMIN account to perform activities and maintenance during patching. Most of the time, they really mean that the user needs to perform activities via the use of the System Administrator responsibility. When patches call for specific processes to be performed by an Apps DBA or DBA, they should do so via a named login assigned to them to maintain clear accountability for performing the process or entering the data.

As it relates to the SYSADMIN login, the following controls need to be put in place to monitor the use of it:

- Assign only the System Administrator responsibility and User Management role to the SYSADMIN login. If there are any other responsibilities or roles, they should be end-dated.
- Review the active assigned responsibilities at least monthly or, preferably develop an alert or detailed audit trail (log or trigger based) to monitor the assignment of new responsibilities and roles or the removal of end dates on disabled responsibilities or roles.
- Require the use of the SYSADMIN login to be manually logged each time it is used.
- Establish a policy or develop security standards for the owner of the SYSADMIN login to understand the SYSADMIN login should be used only when it is absolutely required by Oracle.
- Treat the SYSADMIN password similarly to Apps - one person (or small group) should know the password, and the password should be sealed in an envelope and held securely by an IT manager.
- Reset the SYSADMIN password according to a corporate password reset policy (I have seen some clients not reset their SYSADMIN password) - note that even if the password expires, the SYSADMIN login is still active.
- Most importantly, NEVER end date the SYSADMIN login as it is needed internally in many places. End-dating the SYSADMIN login may shut down your system or certain processes within your system (i.e. workflow processes).
- Routine maintenance that can be performed using a named login and the System Administrator responsibility should NEVER be done using the SYSADMIN login.

Apart from the SYSADMIN login, I have seen one other type of generic user account utilized by organizations – a job scheduling login with a user name similar to JOBSCHLR. This generic job scheduling login is used for scheduling concurrent programs and reports rather than scheduling them under a user’s login and risking the possibility of the user leaving the organization. The job scheduling user account also allows multiple users to log in and see activity such as log files and output files.

Controls should be put in place for the JOBSCHLR login as follows:

- The only responsibility granted to the user should be a job scheduling responsibility with a single function “Requests: Submit” assigned to the menu. No other functions are to be granted, particularly any functions that update data or allow access to sensitive data. If support users need

access to other forms, they should access those forms through their own named login and “Support” responsibilities designed for supporting the applications.

- Review the active assigned responsibilities to make sure no other responsibilities have been assigned to this login no less frequently than monthly. If the person(s) responsible for maintaining this login also has access to the System Administrator responsibility, consider developing an Alert or detailed audit trail to monitor for new responsibilities or roles being assigned or for assigned responsibilities or roles having their end date removed.
- Narrowly define the requests and reports that this responsibility can use to only schedule jobs. No reports with sensitive data should be contained in the request group.
- Changes to security related to this login should be required to go through the Change Management process. This would include changes to the responsibility definition, underlying menu, and the request group.

...