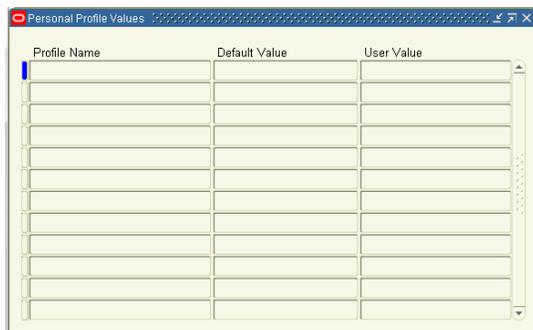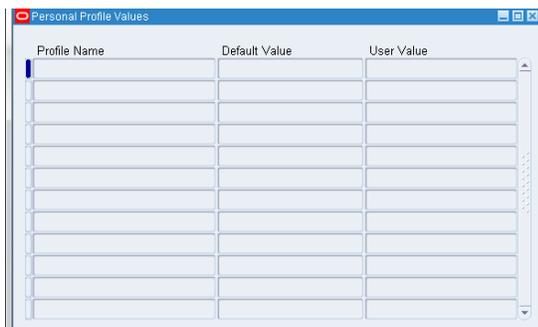# Risks and Controls related to User Profile Values

Background: Oracle provides a form to allow users to maintain certain profile options. The form is called "Personal Profile Values" and the function is "Profile User Values". Here is an 11i screen shot of the form:

And an R12 version of the same form:

This form allows an application user to set profile options where they can be set at the user level. Setting a profile option at the user level overrides any values set at 'higher' levels – Site, Application and Responsibility levels.

Here is a screen shot of the form where Profile Options are defined (via Application Developer responsibility):

The profile option above (Account Generator:Run in Debug Mode) is defined to allow it to be overridden by a user in the Personal Profile Values form.

I queried a 12.1.3 environment and noted that there are 8, 485 different profile options (see screen shot below). While not all of these allow users to override the value at the User level through the Personal Profile Values form, there are likely thousands of profile options that provide a user the ability to override a profile value.

Here are some examples of profile options that typically organizations wouldn't allow users to override:

Account Generator:Run in Debug Mode, Account Generator:Purge Runtime Data. In the 12.1.3 test environment, I scrolled through the Define Profile Options form and found hundreds, if not thousands of profile options that could be maintained by the user. Unless a thorough analysis is done on each of these that can be set at the User level through the User Profile Values form, it is prudent to restrict access to this form.
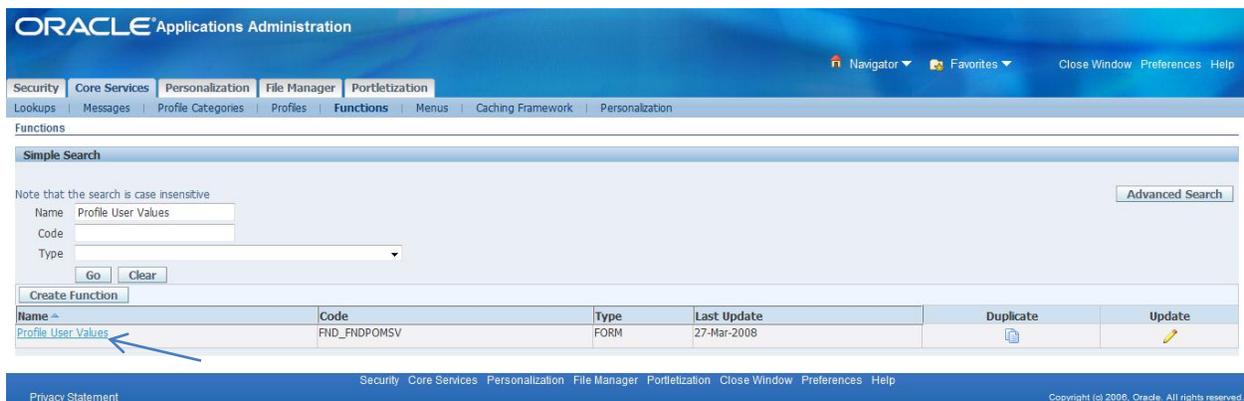
Recommendations:
Based on the risks associated with users having the ability to override these values, we do NOT recommend this form be accessible by users. All changes to profile options should go through a centralized process. Because many of the profile options could have a significant impact on key controls and/or are critical to the design of the application, we recommend that most profile options go through a formal IT change management process. The assumption should be that all profile options go through a formal IT change management process other than those that have been specifically exempted from the policy. Some examples of low-impact profile options that may be exempted from the change management process are: Java Color Scheme, Printer, and Concurrent:Report Copies. Only those profile options that have been properly evaluated with respect to their risk and that management has deemed the risk to be tolerable should be exempted from being required to go through the change management process.

Remediation:
If your organization uses R12, Oracle has (finally) provided a way to identify which responsibilities have access to this function. Here are the details…

Responsibility: Functional Administrator
Navigation: Core Services -> Functions

Query on the Name "Profile User Values" and you will receive this screen:

Click on the Profile User Values link and you will receive this screen:

Click on the Menus tab and you will receive this information:

This provides you with the menus that contain this function. In this 12.1.2 environment (public domain environment hosted by Solution Beacon – thanks to SB!!!) there are 194 menus that contain this function. Note that this query does not show the main or top-level menus that contain these submenus so further research would be needed to determine how to remove access to these functions from end users if you decide to remove access to this function rather than personalizing the form.

Contact: Feel free to contact the author, Jeffrey T. Hare, CPA CISA CIA, at jhare@erpra.net with further questions or comments related to this subject.