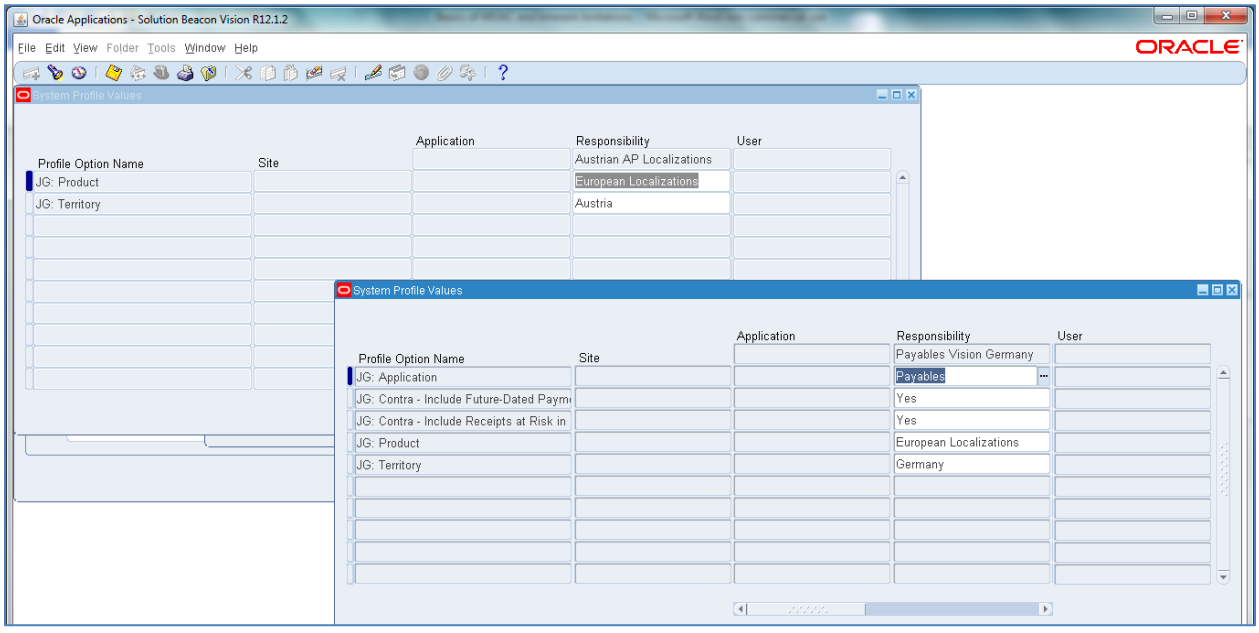
Basics of MOAC and Inherent limitations

In R12 of E-Business Suite, Oracle introduced Multi-Org Access Control (MOAC) to provide users with the ability to view data and process data across operating units. This new functionality is welcome by organizations that process data and want to view data across operating units – such as those that have a shared service environment. The implementation of MOAC is simple, but has some limitations. MOAC cannot be implemented in much of the world because of the need to use localizations and apply such localizations at the Responsibility level.

Here is an example:



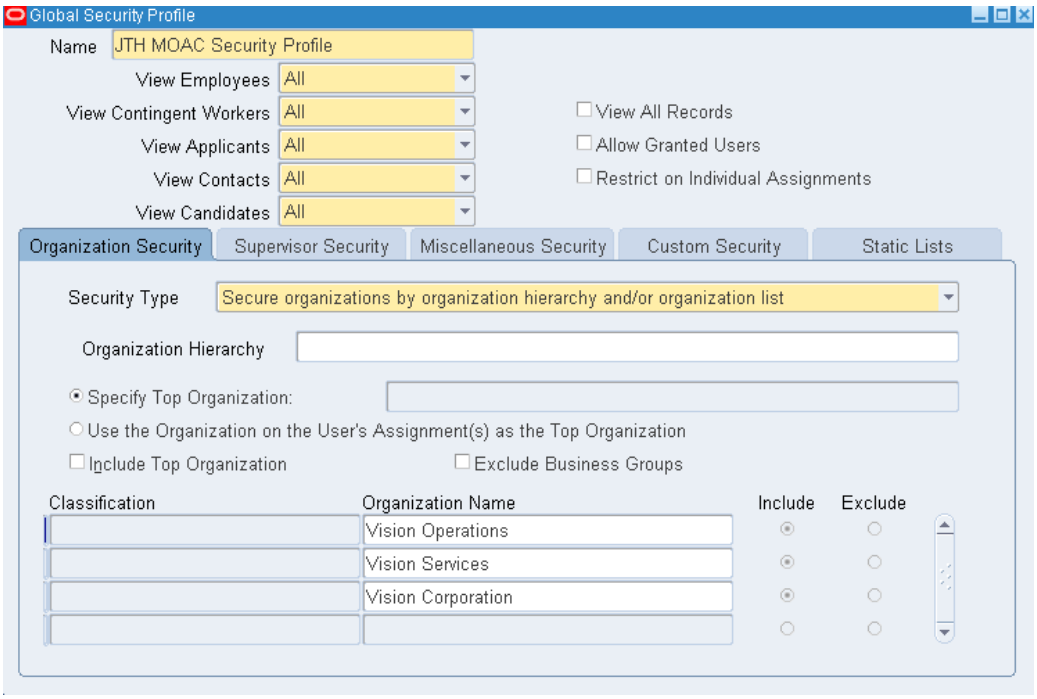
Inherent limitations

I queried two Payables users from in the Solution Beacon 12.1.2 Vision public domain environment – one for Austria and one for Germany. Localizations (JG: Territory and JG: Product) profile options were applied to these two responsibility in order to implement country-specific localizations for Austria and Germany. If you had a shared service center in Germany, for example, you wouldn't be able to combine these two countries into a single responsibility using MOAC because there is no way to apply the localizations to the combined responsibility because you'd need to set the JG: Territory profile option for both Germany and Austria which the profile options form doesn't currently support. I logged an enhancement request on behalf of client (Enhancement Request 10361672) that Oracle is currently considering. I encourage you to log an SR and throw your support behind this enhancement request.

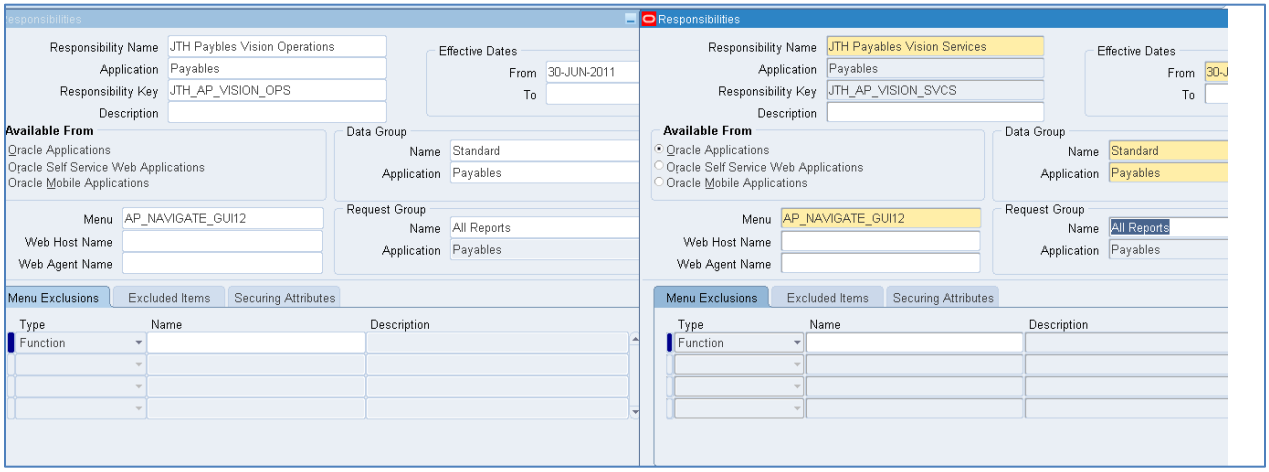
MOAC standard functionality

Let me now illustrate the basics of how MOAC is implemented. The process is rather quite simple. First, you need to set up a Global Security Profile. The Global Security Profile form can be accessed through the US HRMS user. This form along with the Security Profile form belongs in the menu of your Security Administrator (I typically recommend a custom menu and responsibility be built rather than using System Administrator), but Oracle hasn't added it there yet.

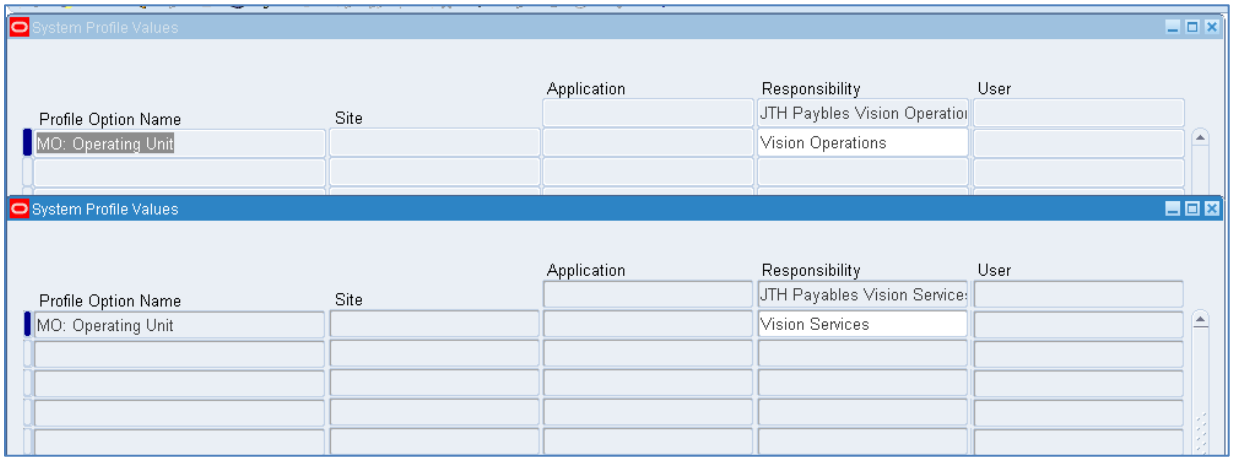
Here is an example of a Global Security Profile:



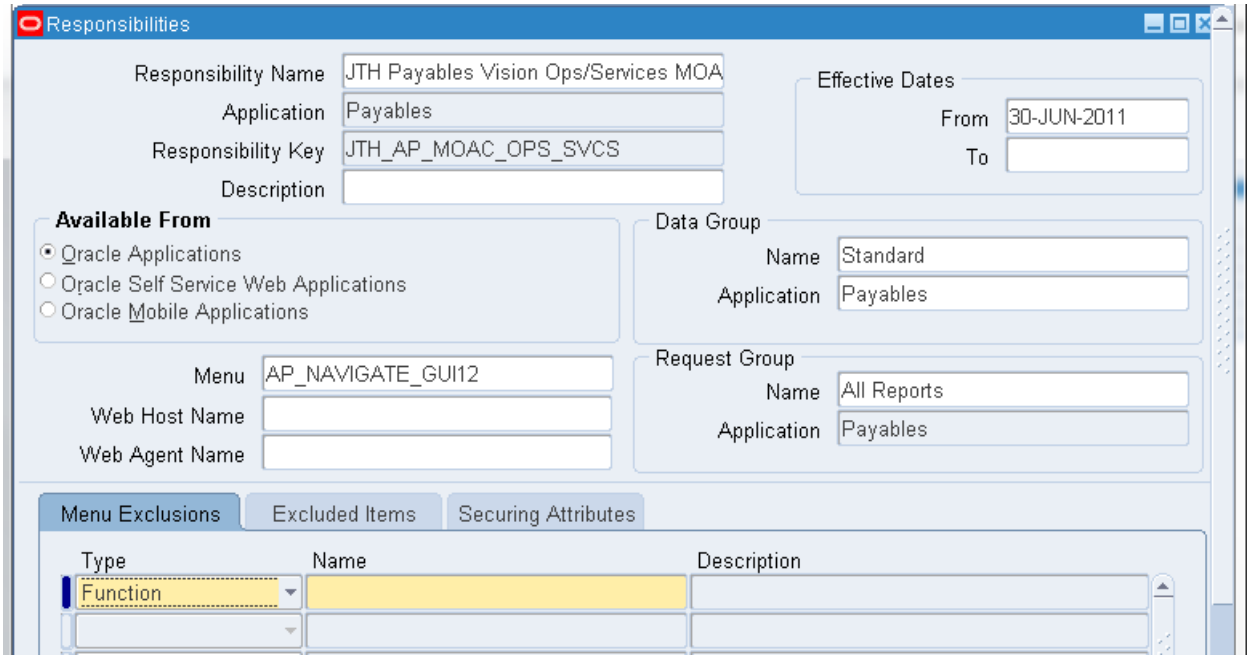
Here are two responsibilities that are set up to manage two of these operating units (Vision Operations and Vision Services):



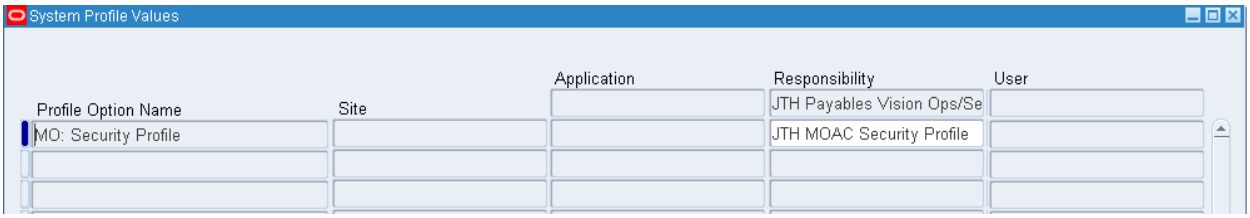
Normally you'd set the MO: Operating Units for these as follows:



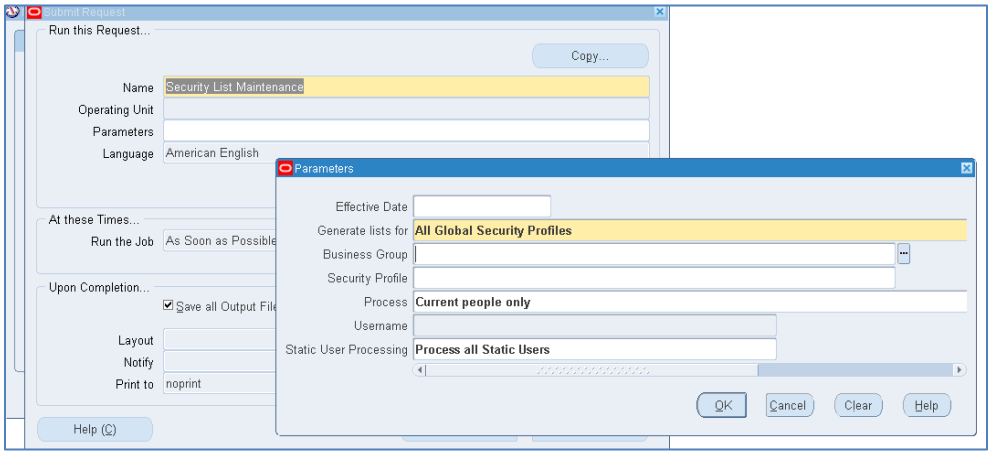
For a MOAC implementation, here is the responsibility definition:



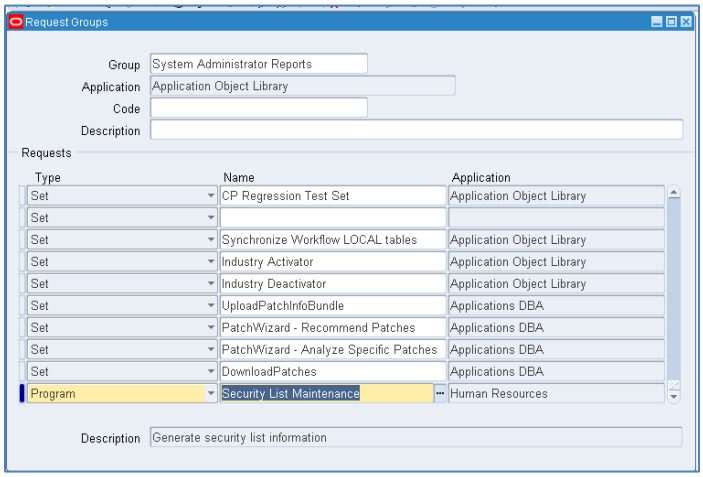
For the MOAC responsibility, you set the MO: Security Profile rather than the MO: Operating Unit as follows:



When implementing MOAC for a responsibility or making changes to the Global Security Profile definitions, you need to run the “Security List Maintenance” request with the following parameters:

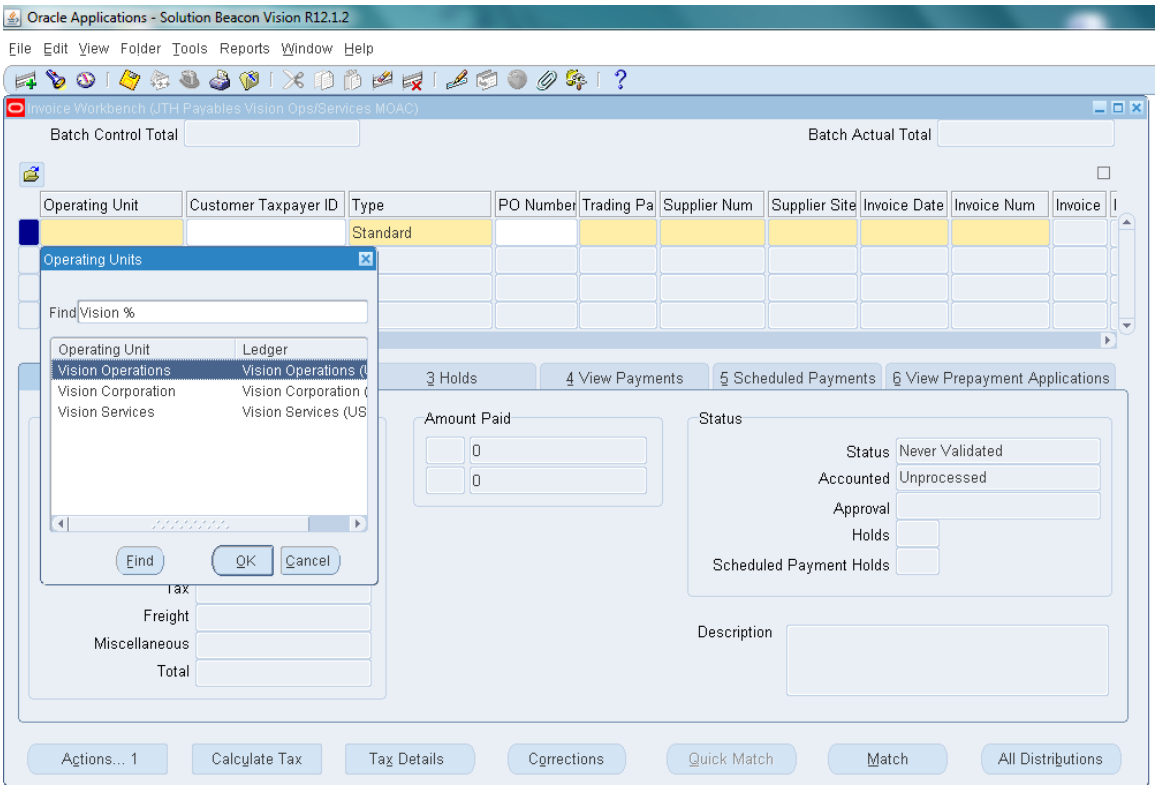


For the sake of this illustration, I added the Security List Maintenance program to the request group associated with the System Administrator responsibility as follows:



However, best practices would dictate the creation of a custom request group for your custom Security Administrator Responsibility where this program then gets included.

Here is what the forms look like in a MOAC world:



Notice you now have the ability to enter data into three different operating units.

Conclusion: Oracle's MOAC functionality introduced in R12 is a powerful tool to combine access to multiple operating units. Implementing MOAC should be part of all organization's upgrade or implementation plans. If you are a multi-national company running Oracle E-Business Suite and use localizations, please log an SR in support of the enhancement request noted earlier.

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.