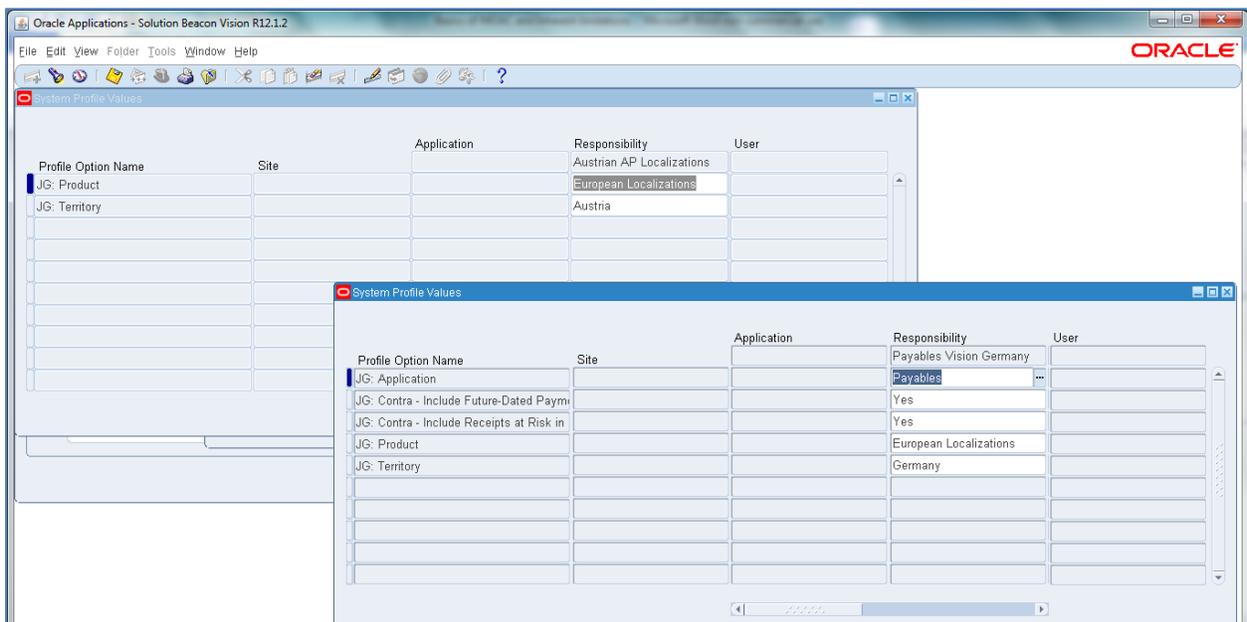


Basics of MOAC and Inherent limitations

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:



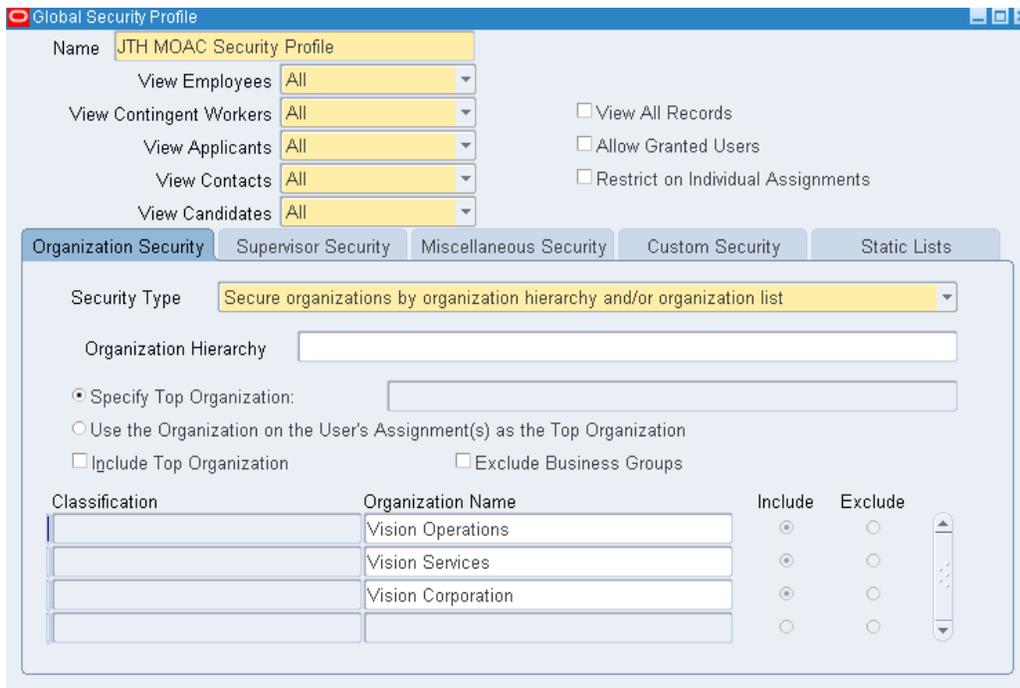
Inherent limitations

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:



Global Security Profile

Name: JTH MOAC Security Profile

View Employees: All

View Contingent Workers: All

View Applicants: All

View Contacts: All

View Candidates: All

View All Records

Allow Granted Users

Restrict on Individual Assignments

Organization Security | Supervisor Security | Miscellaneous Security | Custom Security | Static Lists

Security Type: Secure organizations by organization hierarchy and/or organization list

Organization Hierarchy: []

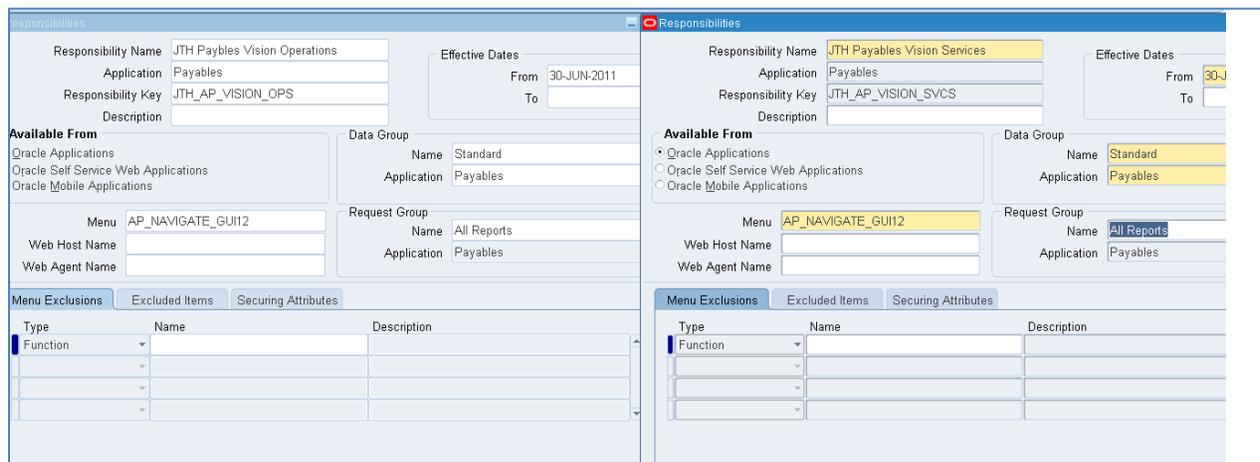
Specify Top Organization: []

Use the Organization on the User's Assignment(s) as the Top Organization

Include Top Organization Exclude Business Groups

Classification	Organization Name	Include	Exclude
	Vision Operations	<input checked="" type="radio"/>	<input type="radio"/>
	Vision Services	<input checked="" type="radio"/>	<input type="radio"/>
	Vision Corporation	<input checked="" type="radio"/>	<input type="radio"/>
		<input type="radio"/>	<input type="radio"/>

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



Responsibilities

Responsibility Name: JTH Payables Vision Operations

Application: Payables

Responsibility Key: JTH_AP_VISION_OPS

Effective Dates: From 30-JUN-2011 To []

Available From: Oracle Applications Oracle Self Service Web Applications Oracle Mobile Applications

Data Group: Name Standard Application Payables

Menu: AP_NAVIGATE_GUI12

Request Group: Name All Reports Application Payables

Web Host Name: []

Web Agent Name: []

Menu Exclusions: Excluded Items Securing Attributes

Type	Name	Description
Function		

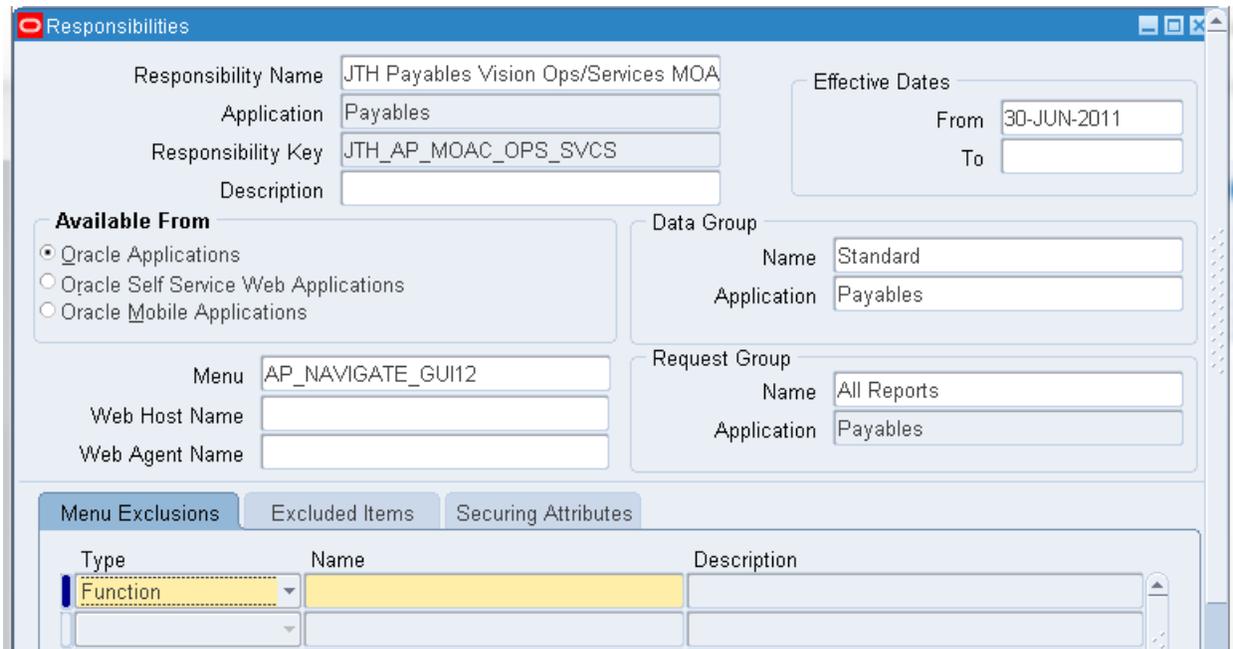
Normally you'd set the MO: Operating Units for these as follows:



Profile Option Name	Site	Application	Responsibility	User
MO: Operating Unit			JTH Payables Vision Operations	
			Vision Operations	

Profile Option Name	Site	Application	Responsibility	User
MO: Operating Unit			JTH Payables Vision Service: Vision Services	
			Vision Services	

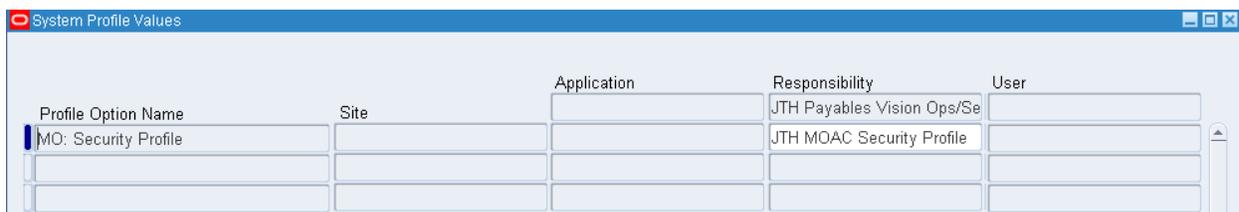
For a MOAC implementation, here is the responsibility definition:



Responsibility Name: JTH Payables Vision Ops/Services MOA
 Application: Payables
 Responsibility Key: JTH_AP_MOAC_OPS_SVCS
 Description:
 Effective Dates: From 30-JUN-2011 To
 Available From: Oracle Applications
 Oracle Self Service Web Applications
 Oracle Mobile Applications
 Menu: AP_NAVIGATE_GUI12
 Web Host Name:
 Web Agent Name:
 Data Group: Name Standard Application Payables
 Request Group: Name All Reports Application Payables

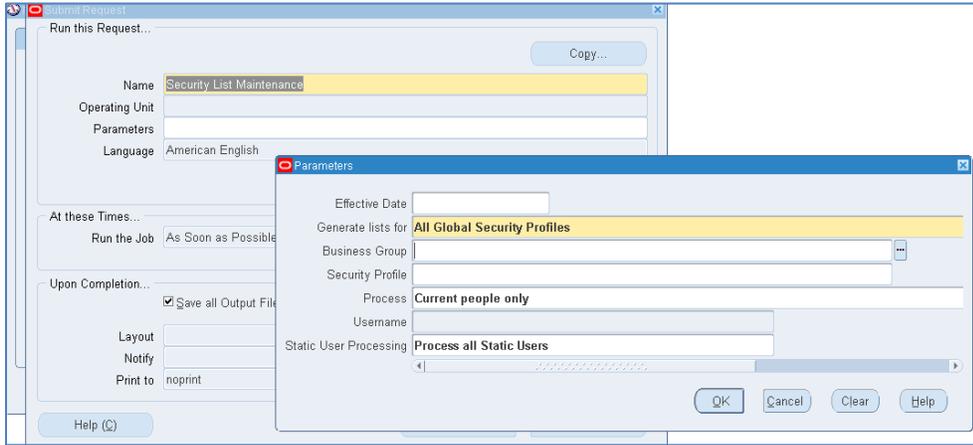
Type	Name	Description
Function		

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



Profile Option Name	Site	Application	Responsibility	User
MO: Security Profile			JTH Payables Vision Ops/Se	
			JTH MOAC Security Profile	

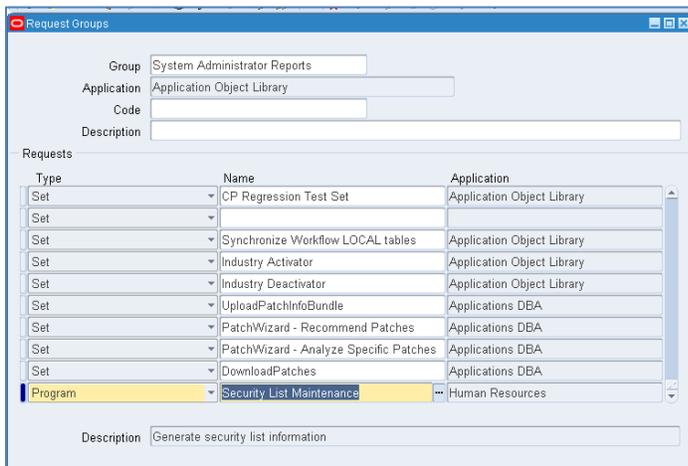
When implementing MOAC for a responsibility or making changes to the Global Security Profile definitions, you need to run the “Security List Maintenance” request with the following parameters:



The screenshot shows the 'Run this Request...' dialog box with the 'Parameters' sub-dialog open. The 'Parameters' dialog has the following fields:

- Effective Date: [Empty]
- Generate lists for: **All Global Security Profiles**
- Business Group: [Empty]
- Security Profile: [Empty]
- Process: **Current people only**
- Username: [Empty]
- Static User Processing: **Process all Static Users**

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:



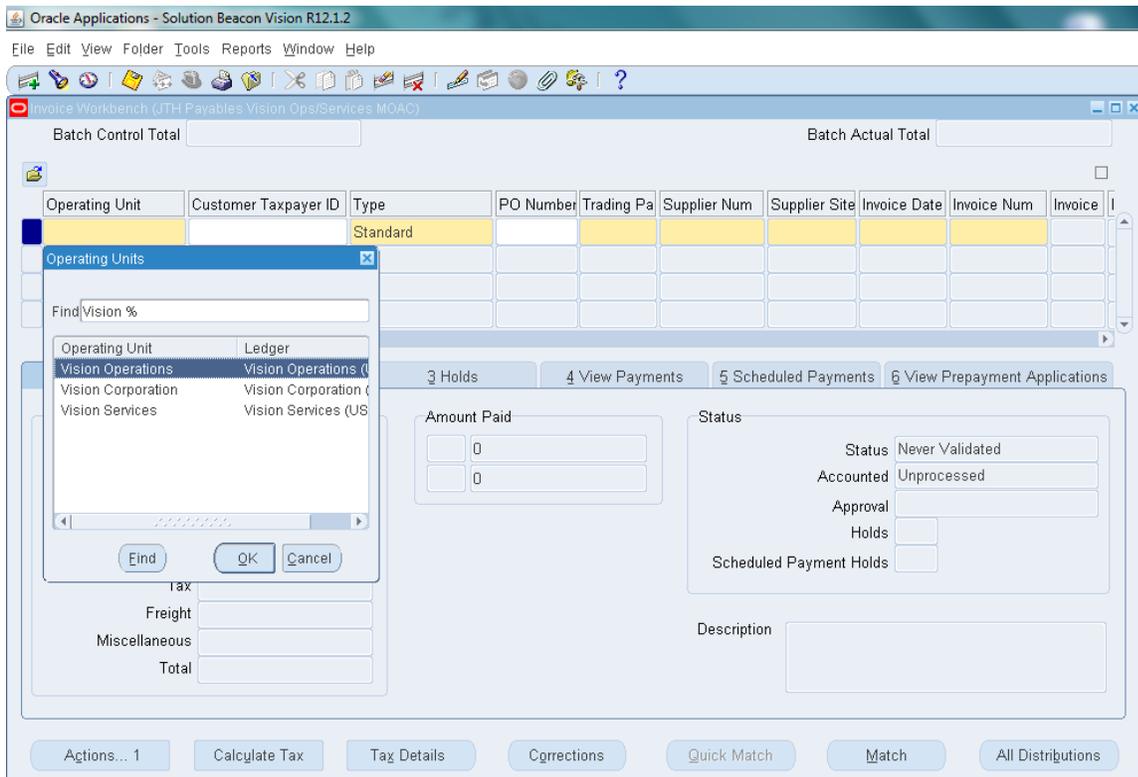
The screenshot shows the 'Request Groups' dialog box. The 'Group' is 'System Administrator Reports', 'Application' is 'Application Object Library', and 'Code' is empty. The 'Requests' table lists several requests, with 'Security List Maintenance' highlighted as a 'Program' request under the 'Human Resources' application.

Type	Name	Application
Set	CP Regression Test Set	Application Object Library
Set	Synchronize Workflow LOCAL tables	Application Object Library
Set	Industry Activator	Application Object Library
Set	Industry Deactivator	Application Object Library
Set	UploadPatchInfoBundle	Applications DBA
Set	PatchWizard - Recommend Patches	Applications DBA
Set	PatchWizard - Analyze Specific Patches	Applications DBA
Set	DownloadPatches	Applications DBA
Program	Security List Maintenance	Human Resources

Description: Generate security list information

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.