**Triggering Parametrized Certification Campaigns from Identity Portal**

This document describes how to configure parametrized campaigns from Identity Portal that allow a manager to request an ad-hoc certification campaign based on desired criteria. These use cases are built on Identity Suite 14.0 Virtual Appliance and work with 14.1 VApp as well (I have tested both versions). Therefore the IM tasks assume the existence of user attributes that are provided out of the box in the VApp. If you want to make the use cases work with a non-VApp IDS installation, you either need to configure the required screen user attributes by extending the CA Directory schema, Directory.xml and task profiles, or you need to rename the screen attributes in the IM tasks file based on your user directory configuration.

Web Services examples are provided for generating 3 types of campaigns in Identity Governance:

* User Privileges Campaign
* Role Definition Campaign
* Resource Campaign

All of the web service examples provided include support for Continuous Export which allows to automatically de-provision entitlements that have been rejected through any of these campaigns. If you do not desire this functionality, make sure you change the following setting from True to False in the XML files:

<ns3:Property xmlns:ns3="<http://dto.eurekify.com>">

<name xmlns="<http://dto.eurekify.com>">flow.nofitications.boolean.isModelChangeNotificationOn</name>

<value xmlns="<http://dto.eurekify.com>">true</value>

</ns3:Property>

All of these certification campaigns assume that you are using ConnectedUniverse\_Model for certifications. If you want to use a different universe make sure that you update the SOAP actions with the right universe name as described in step 6 of this document.

Remember to also update the IP Address of your IDG installation (this document assumes IP address of 172.17.17.145 but for sure you have your own Identity Governance IP address). Follow the instructions in Step 7 to update SOAP actions with the right IP address information.

1. Identity Manager Tasks and Policy xPress Policies

Import IMCampaignTasksAndPX.xml into your IdentityEnv environment’s “Role and Task Settings” from immanage console.

This will import 3 tasks, 1 screen and 3 policy xpress policies triggered on completion of the related 3 tasks to call Identity Governance with CreateCampaign web service.

These Identity Manager tasks and Policy xPress policies assume existence of the following well-known attributes (which are configured by default in IdentityEnv environment on Virtual Appliance):

* %STRING\_08%
* %STRING\_09%
* %STRING\_01%
* %CASE\_EXACT\_STRING00%
* %CASE\_EXACT\_STRING01%

If you are not using the default IdentityEnv environment in VApp, change the attribute mappings to suite your own user directory schema. In this case, the attributes would need to be update in both tasks and policy xpress policies.

1. Identity Manager Admin Role

Make sure you add the 3 imported IM tasks to the Admin Role you have mapped to Sigma Managers. Only the users that are authorized to use these tasks can request ad-hoc campaigns from Identity Portal. Make sure you add the following 3 tasks to your Admin Role:

* Trigger User Certification Campaign
* Trigger Role Certification Campaign
* Trigger Resource Certification Campaign
1. Identity Portal Task mappings

**REMEMBER TO RESTART IM CONNECTOR IN IDENTITY PORTAL ADMIN UI. THIS WAY THE 3 TASKS IMPORTED ABOVE WILL BE VISIBLE TO THE END USERS INTERACTING WITH THE PORTAL.**

From Identity Portal Admin UI, Tools, Import SigmaTasks.txt. This will map each of the above 3 IM tasks in Identity Portal as tasks. So you will have 3 new Identity Portal tasks created.

If you are not using the Virtual Appliance, you may need to change the name of your Identity Manager connector in the SigmaTasks.txt, in particular if you are getting an error that the IDM connector is down while in reality it is up. This may happen because the Identity Manager connector name specified in the SigmaTasks.txt file does not exist.

1. Identity Portal Forms:

From Identity Portal Admin UI, Tools, Import the 3 forms in SIGMAFORMS.zip file. This will create 3 new forms in Identity Portal that are mapped to the above 3 tasks to send parametrized SOAP queries to IDG. I have created 1 file per form because it’s easier to edit in case you need to modify something (task tag or form name)

When Identity Portal forms are imported, it also imports the mapping between the IM task attributes and the form properties. If you are not using the default IdentityEnv environment on the Virtual Appliance and have updated your Identity Manager tasks and PX policies in Step 1 above to use other user attributes, then make sure that you update the each of the form files with the right attribute names.

1. Identity Portal Module for On-demand Certifications.

From Identity Portal Admin UI, Tools, Import SigmaModuleCertificationActions.txt. this will create a new module with the required actions and form mappings. A new module with the name On-Demand Certifications will be created. Change the module name in the SigmaModule.txt file if you want to use a different module name.

Give access to this module to the necessary Identity Portal Profiles so your users can see it. By default this Module is NOT assigned to any user and therefore is not visible to anyone.

1. Identity Governance Universe:

The use cases assume that the Universe is named ConnectedUniverse. To make it work with your own universe make sure you replace ConnectedUniverse with your Universe name in the SOAP actions in 2 places as described below (Universe Name is Case Sensitive, therefore make sure you indicate the Universe name exactly as it appears in Identity Governance. For example, ConnectedUniverse\_Model is NOT the same as ConnectedUniverse\_model

Policy xPress Action needs to be updated in all 3 policy xpress policies (if you want to change the universe):

* TriggerUserCertificationCampaign
* TriggerRoleCertificationCampaign
* TriggerResourceCertificationCampaign

**TWO CHANGES NEED TO BE MADE IN THE SOAP BODY:**

In the SOAP Request Message as highlighted below, search for ConnectedUniverse\_Model and replace with your Universe\_Model name.



The search for ConnectedUniverse (without model) and replace that one with your Universe name as highlighted below:



1. Identity Governance IP Address in SOAP actions:

Make sure you change the IP address in the policy xpress SOAP actions to point to the IP address for your Identity Governance server installation. The IP address needs to be updated in the action of all 3 policy xpress policies:

* TriggerUserCertificationCampaign
* TriggerRoleCertificationCampaign
* TriggerResourceCertificationCampaign

Modify each of the policy xpress policies by going to action and updating the IP address (and port if needed) as indicated with the WSDL URL in the below image:



1. Identity Governance Certification Campaign Reviewer

The PX policies are configured to set the campaign reviewer to the user called “imadmin”. Replace this user with the userID of your own reviewer by editing the DefaultManager setting in the action of the 3 policy xpress policies:



In Identity Governance USER\_CERTIFICATION campaigns will go to the user’s manager based on RACI. ROLE\_CERTIFICATION campaigns will go to the role owner based on RACI. DefaultManager setting is used when user manager or role manager cannot be resolved by RACI or when RACI is not defined.

1. Identity Governance Certification Campaign Owner:

The campaign owner in Identity Suite 14.1 has the capability to view the progress of certification campaigns from the campaign dashboard. The Policy Xpress policies are set to create campaigns with the original requester as owner of these campaigns. Which means the requester of the campaign can monitor the progress of campaigns from Identity Portal. If you want to use another user as campaign owner, edit the Owner setting in the actions in the 3 policy xpress policies by replacing the below value with your own userID. I am using a variable that resolves based on the submitting user’s UserID but you can replace with another existing Identity Governance user.



1. Update parameters in Forms.

As you have seen already 3 forms are imported by this configuration (I apologize for non-standardized names, you can rename the forms before importing):

* SantanderTriggerCertificationCampaign1
* TriggerCampaignByRole1
* TrygResourceCampaign1

Modify the attributes of these forms if you want to add / modify parameters.

For example, TriggerCampaignByRole1 is used for ROLE\_DEFINITION campaigns, I have added 4 Provisioning Role names to the list and All (\*) option to run role\_definition campaign for all roles. You can edit the options of the field labeled “Please Select Role” to add/remove provisioning role names. The provisioning role names are case sensitive and they need to match exactly the way they appear in Identity Governance.



On the other hand, TrygResourceCampaign1 form has the drop down options populated based on the initialization and change handlers, add / remove desired values (remember that these are case sensitive and need to match the names exactly in Identity Governance). Don’t change Endpoint Type and Endpoint Name. These are the names of the resource fields in Identity Governance. But you can add additional Endpoint Types to the list or additional Endpoint Names.



Change handler:



SantanderTriggerCertificationCampaign1 has just a user selector field. A USER\_CERTIFICATION campaign is generated for the chosen user. Only the user’s manager can run the campaign for his / her subordinate user.