Role Based Initiators: An Alternative to "Auto Approve Roles without Approvers" in Compliant User Provisioning

Applies to:

SAP BusinessObjects GRC Access Control v5.3.

Summary

A role or roles exist that per company policy does not need an approval to be provisioned to a user. However, it is deemed too risky to activate the ability to automatically approve roles without approvers because of the possibility of role approver data being missed in an upload or import of roles to Compliant User Provisioning (CUP). If that were to happen and the role was requested, then the role would automatically be provisioned without approval and therefore out of the IT security policy.

This document describes an alternative to activating the Auto Approve Roles without Approvers configuration by setting or using a No Role Owners or Roles with No Role Owner detour to effect the auto approval.

Author: Kevin Tucholke, Senior Consultant – Technology Services - SAP

Company: Capgemini

Created on: 2 April 2010

Author Bio

Kevin Tucholke is an SAP GRC Senior Consultant at Capgemini with 10 years of overall IT experience, 5 years of SAP GRC implementation and functional expertise and 6 years of Role and User provisioning expertise. He has completed multiple full life cycles of SAP GRC Access Control implementation and upgrade projects (version 3.0, 4.0, and 5.3). and has expert skills in GRC design and configuration in all components of Access Control (Risk Analysis and Remediation, Compliant User Provisioning, Superuser Privilege Management and Enterprise Role Management). He has extensive experience in leading remediation efforts to eliminate or remediate any unmitigated Segregation of Duties issues being reported by SAP GRC. This includes reviewing both security role and business process design and providing recommendations that effectively target trouble areas across the entire ERP system.

Table of Contents

Scenario

A role or roles exists that per company policy does not need an approval to be provisioned to a user. However, it is deemed too risky to activate the ability to automatically approve roles without approvers because of the possibility of role approver data being missed in an upload or import of roles to Compliant User Provisioning (CUP). If that were to happen and the role was requested, then the role would automatically be provisioned without approval and therefore out of the IT security policy.

This document describes an alternative to activating the Auto Approve Roles without Approvers configuration by setting or using a No Role Owners or Roles with No Role Owner detour to effect the auto approval.

Question:

How can CUP be configured to follow security policy and also approve certain roles automatically?

Solution:

Create a workflow path relevant to ONLY certain roles!

The following section will detail the current environment configuration and settings that are specifically relevant for this scenario.

Current Compliant User Provisioning (CUP) Relevant Information

This scenario is described for the production instance of GRC Access Control CUP. Some adjustments would need to be made for testing the solution in a non-production GRC instance. It is important to note that the information that follows directly pertains to this scenario and is not complete for an entire CUP implementation.

- **SAP ABAP Landscape and CUP Connectors**
  - •PRD_100 – Production ECC
  - •QAL_100 – Quality Assurance ECC
  - •DEV_100 – Development (Golden Configuration)
  - •DEV_200 – Development (Golden Development)
  - •DEV_300 – Development SANDBOX
  - •DEV_400 – Development (Golden Security)
- **Risk Analysis and Remediation (RAR) Connectors**
  - •PRD_100 – Production ECC
  - •DEV_100 – Development (Golden Configuration) (Basis Only / Cross System with PRD)
  - •DEV_200 – Development (Golden Development) (Basis Only / Cross System with PRD)
  - •DEV_400 – Development (Golden Security) (Basis Only / Cross System with PRD)
- **Request Types**
  - •NEW – New Account – contains actions of Create_User, Assign_Roles, User_Defaults
  - •CHANGE – Change Account – contains actions of Change_User, Assign_Roles
  - •NONPROD_USER – Non-Production Account (custom) – contains actions of Create_User, Change_User, Assign_Roles, User_Defaults
  - •FIREFIGHTID – Firefighter ID Maintenance (custom) – contain actions of Create_User, Change_User, Assign_Roles, User_Defaults
- **Default Role that is automatically applied to everyone in all connected systems**
  - •CG_EVERYONE – contains transactions that all users need (i.e. SU3, SU53, etc.). CUP Role information indicates that Joe Brown is the Role Owner and Role Approver as per

company policy and this information has been imported from Enterprise Role Management (ERM).

- **Roles that can be selected to be provisioned to a user**

  •These roles are display only and therefore the requirement for approval has been eliminated by the Internal Controls Department. Role Owner and Role Approver information exist on the role as per company policy and have been imported from ERM.

    - CG_FI_DISPLAY
    - CG_SD_DISPLAY
    - CG_CO_DISPLAY

- **Existing Workflows – Path/Stages/Initiator**

  •PRDC_USER_ACCESS – New User Access for Production System(s)

    - 2 Approval Stages – Manager; Role Owner with SoD Detour;
    - Risk Analysis Mandatory in Each Stage
    - Initiated by PRDC_USER_REQUEST initiator with conditions
      - Application | PRD_100 | AND
      - Request Type | New Account | AND

  •PRDU_USER_ACCESS – Change User Access for Production System(s)

    - 2 Approval Stages – Manager; Role Owner with SoD Detour;
    - Risk Analysis Mandatory in Each Stage
    - Initiated by PRDU_USER_REQUEST initiator with conditions
      - Application | PRD_100 | AND
      - Request Type | Change Account | AND

  •NONP_USER_ACCESS – User Access for Non-Production System(s) (New and Change Requests)

    - 2 Approval Stages – Application Owner; Role Owner;
    - Risk Analysis NOT Mandatory
    - Initiated by NPRD_USER_REQUEST initiator with conditions
      - Application | QAL_100 | OR
      - Application | DEV_300 | OR
      - Request Type | Non-Production Account | AND

  •NONP_USER_ACCESS_RA – User Access for Configuration/Development Non Production System(s)

    - 3 Approval Stages – Manager; Application Owner; Role Owner;
    - Risk Analysis Mandatory in Each Stage
    - Initiated by NPRD_RA_USER_REQUEST initiator with conditions
      - Application | DEV_100 | OR
      - Application | DEV_200 | OR
      - Application | DEV_400 | OR

- Request Type | Non-Production Account | AND

•FFID_USERID_CREATE – Maintenance of Firefight IDs (Service Users)

- 3 Approval Stages – Manager; Role Owner; Security or FF Administrator;
- Risk Analysis NOT Mandatory
- Initiated by FFID_USER_REQUEST initiator with conditions
  - Application | PRD_100 | AND
  - Request Type | Firefighter ID Maintenance | AND
  - USER TYPE (Custom Field) | S | AND
    - This forces that the FFID's are created as SERVICE users

- **Role Selection Settings**

•"Auto Approve Roles without Approvers" is INACTIVE (unchecked)

The additional configuration to implement the solution follows in the next section.

Solution Configuration

1) Create a new initiator for the intended roles to be auto-approved.

- •DEFAULT_ROLES_NO_APPROVAL – Default Roles No Approval Initiator
  - Conditions:
    - Role | CG_EVERYONE | OR
    - Role | CG_FI_DISPLAY| OR
    - Role | CG_SD_DISPLAY | OR
    - Role | CG_CO_DISPLAY | OR

2) Create a new stage with No Stage as the approver

- •DEFAULT_ROLES - Default Roles No Stage Approval
  - Major Configuration Settings
    - Risk Analysis Mandatory - NO
    - Approve Request Despite Risks - NO
  - See TIPS Section below for additional information on configuration settings.

3) Create a new workflow path

- •DEFAULT_ROLES_PATH – Default Roles No Approval Path
  - Initiator – DEFAULT_ROLES_NO_APPROVAL
  - Stage – DEFAULT_ROLES

4) Review and maintain each initiator that handles a request type that has the ASSIGN_ROLES action.

- •For Example, the SAP delivered Request Types New Hire, New Account, Change Account would contain this action, whereas Information, Lock Account, Unlock Account, Delete, and Super User Access would not.
- •From the scenario above each of the initiators listed would need the following conditions added:
  - Conditions:
    - Role | CG_EVERYONE | NOT
    - Role | CG_FI_DISPLAY| NOT
    - Role | CG_SD_DISPLAY | NOT
    - Role | CG_CO_DISPLAY | NOT
- •IMPORTANT: Remember that the order of the Condition statements (OR, NOT, AND) is important in CUP initiators. The order must be OR statements, then NOT statements, then AND statements.
- •This additional configuration is needed so that the request does not satisfy multiple initiators.
  - Example: If a request to create a new account in PRD_100 was submitted and it contained the CG_EVERYONE role and the NOT statements above did not exist, the initiators that would be satisfied would be PRDC_USER_REQUEST for the entire request and DEFAULT_ROLES_NO_APPROVAL for the role CG_EVERYONE. CUP would not be able to determine how to handle the CG_EVERYONE role. However, by adding the NOT statements into the PRDC_USER_ACCESS initiator, CUP can identify the exact and ONLY initiator for the CG_EVERYONE role.

5) DO NOT change the "Auto Approve Roles without Approvers" configuration setting. This setting will remain INACTIVE (unchecked).

6) See Appendix for full examples of the UPDATED configuration.

The Result

After the above changes have been applied, when a request is submitted that contains one or more of the roles CG_EVERYONE, CG_FI_DISPLAY, CG_SD_DISPLAY, CG_CO_DISPLAY, these roles will be split into a parallel path and be automatically approved by the system user and either remain pending or auto provision based on the configuration settings in Auto-Provisioning – Provisioning Options.

Additional Information and Tips

Attaching an SoD Detour:

If there is a possibility that any of the roles that are included in this "no-approver" process would create a Segregation of Duties (SoD) issue, it is possible to attach the SOD Detour path to the DEFAULT_ROLES stage. It would also then be REQUIRED to set CUP to perform a Risk Analysis upon Submission in the Risk Analysis section of the configuration tab.

For Example, if a request containing CG_FI_DISPLAY was submitted, and for the sake of this example, it creates an SoD issue when added, the request would be auto approved in the DEFAULT_ROLES stage and then would be detoured to the SOD Approver stage where it would need to be manually approved. This would also mean that an approver must be found for that stage (i.e. Mitigation Approver as the Approver Determinator would not be possible since the mitigation control would not be assigned). If using an Approver Determinator such as Mitigation Approver, a separate SoD Detour could be created specifically for this situation to have a specific approver assigned.

Additional Uses

This configuration will also work for any roles that require a separate approval process other than the request would normally take. However, for each role that is specifically identified in any role based initiator, the same role must be included with a condition of NOT in all other initiators that handle request types that are assigned the action of ASSIGN_ROLES.

Appendix

Updated Workflows – Path/Stages/Initiators with new configuration

- The additional configuration is **Bolded** and **Highlighted**
- NOTE: Placement of the Initiator Conditions is INTENTIONAL to conform with the requirement that initiator conditions are to be listed in order by OR, NOT, AND

•DEFAULT_ROLES_PATH – Default Roles No Approval Path

- **1 Approval Stage – NoStage approver**
- **Risk Analysis NOT Mandatory in Stage**
  - **See Optional Configuration for additional info**
- **Initiated by DEFAULT_ROLES_NO_APPROVAL initiator with conditions**
  - **Role | CG_EVERYONE | OR**
  - **Role | CG_FI_DISPLAY| OR**
  - **Role | CG_SD_DISPLAY | OR**
  - **Role | CG_CO_DISPLAY | OR**

•PRDC_USER_ACCESS – New User Access for Production System(s) (New and Change Requests)

- 2 Approval Stages – Manager; Role Owner with SoD Detour;
- Risk Analysis Mandatory in Each Stage
- Initiated by PRDC_USER_REQUEST initiator with conditions
  - **Role | CG_EVERYONE | NOT**
  - **Role | CG_FI_DISPLAY| NOT**
  - **Role | CG_SD_DISPLAY | NOT**
  - **Role | CG_CO_DISPLAY | NOT**
  - Application | PRD_100 | AND
  - Request Type | New Account | AND

•PRDU_USER_ACCESS – Change User Access for Production System(s) (New and Change Requests)

- 2 Approval Stages – Manager; Role Owner with SoD Detour;
- Risk Analysis Mandatory in Each Stage
- Initiated by PRDU_USER_REQUEST initiator with conditions
  - **Role | CG_EVERYONE | NOT**
  - **Role | CG_FI_DISPLAY| NOT**
  - **Role | CG_SD_DISPLAY | NOT**
  - **Role | CG_CO_DISPLAY | NOT**
  - Application | PRD_100 | AND
  - Request Type | Change Account | AND

•NONP_USER_ACCESS – User Access for Non-Production System(s) (New and Change Requests)

- 2 Approval Stages – Application Owner; Role Owner;
- Risk Analysis NOT Mandatory
- Initiated by NPRD_USER_REQUEST initiator with conditions
  - Application | QAL_100 | OR
  - Application | DEV_300 | OR
  - **Role | CG_EVERYONE | NOT**
  - **Role | CG_FI_DISPLAY| NOT**
  - **Role | CG_SD_DISPLAY | NOT**
  - **Role | CG_CO_DISPLAY | NOT**
  - Request Type | Non-Production Account | AND

•NONP_USER_ACCESS_RA – User Access for Configuration/Development Non Production System(s)

- 3 Approval Stages – Manager; Application Owner; Role Owner;
- Risk Analysis Mandatory in Each Stage
- Initiated by NPRD_RA_USER_REQUEST initiator with conditions
  - Application | DEV_100 | OR
  - Application | DEV_200 | OR
  - Application | DEV_400 | OR
  - **Role | CG_EVERYONE | NOT**
  - **Role | CG_FI_DISPLAY| NOT**
  - **Role | CG_SD_DISPLAY | NOT**
  - **Role | CG_CO_DISPLAY | NOT**
  - Request Type | Non-Production Account | AND

•FFID_USERID_CREATE – Maintenance of Firefight IDs (Service Users)

- 3 Approval Stages – Manager; Role Owner; Security or FF Administrator;
- Risk Analysis NOT Mandatory
- Initiated by FFID_USER_REQUEST initiator with conditions
  - **Role | CG_EVERYONE | NOT**
  - **Role | CG_FI_DISPLAY| NOT**
  - **Role | CG_SD_DISPLAY | NOT**
  - **Role | CG_CO_DISPLAY | NOT**
  - Application | PRD_100 | AND
  - Request Type | Firefighter ID Maintenance | AND
  - USER TYPE (Custom Field) | S | AND
    - This forces that the FFID's are created as SERVICE users

Disclaimer and Liability Notice

This document may discuss sample coding or other information that does not include SAP official interfaces and therefore is not supported by SAP. Changes made based on this information are not supported and can be overwritten during an upgrade.

SAP will not be held liable for any damages caused by using or misusing the information, code or methods suggested in this document, and anyone using these methods does so at his/her own risk.

SAP offers no guarantees and assumes no responsibility or liability of any type with respect to the content of this technical article or code sample, including any liability resulting from incompatibility between the content within this document and the materials and services offered by SAP. You agree that you will not hold, or seek to hold, SAP responsible or liable with respect to the content of this document.