Access Control 5.3
User Access Review

Applies to:

Access Control 5.3

Summary

GRC Access Control identifies and prevents access and authorization risks in cross-enterprise IT systems to prevent fraud and reduce the cost of continuous compliance and control. This document discusses the User Access Review feature introduced in AC 5.3 including it benefits, configuration, use of the feature and workflow options.

Author: Ankur Baishya, Regional Implementation Group
Lori Donnelly, Customer Advisory Office

Company: Governance, Risk, and Compliance
SAP BusinessObjects Division

Created on: 1 June 2009

Version 1.0

Typographic Conventions

Type Style	Description
Example Text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation
Example text	Emphasized words or phrases in body text, graphic titles, and table titles
`Example text`	File and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example text`	User entry texts. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, F2 or ENTER.

Icons

Icon	Description
	Caution
	Note or Important
	Example
	Recommendation or Tip

Table of Contents

1. Management Overview

The User Access Review feature of Access Control (AC) automates and documents the periodic decentralized user access review by business managers or role owners. Requests are generated automatically based on the company's internal control policy. It provides a workflow-based review and approval process. This document provides details on functionality of the feature, its process options, configuration, and use.

The following abbreviations are used for the capabilities of AC:

- CUP Compliant User Provisioning
- ERM Enterprise Role Management
- RAR Risk Analysis and Remediation
- SPM Superuser Privilege Management

2. Key Features and Benefits

The key features of the User Access Review (UAR) in AC 5.3 are:

- An automated process for the periodic access review.
- Decentralized review of user access.
- Workflow of requests for review and approval.
- Automatic role removal, if desired.
- Status and history reports to assist in monitoring the review process.
- Audit trail and reports for supporting internal and external audits.
- Support for back-end systems integrated with Access Control as well as legacy systems.

The key benefits of the User Access Review are:

- A streamlined internal control process with collaboration among business managers, internal control, and information technology teams.
- Improved efficiency and visibility of the internal control process.

3. Technical Prerequisites

The User Access Review feature was introduced in Access Control 5.3. Therefore, you must have version 5.3 installed to utilize User Access Review (UAR) with SP06 or higher recommended. The screenshots provided in this document are from an AC 5.3 SP07 system. Use of the UAR feature requires configuration in multiple capabilities.

- Configuration of systems (connectors) in ERM is required for transaction usage and for user-role assignment information.
- Configuration of connectors in RAR is required for alert generation to provide transaction usage information.
- Configuration in CUP is more extensive. You must define connectors, configure the User Access Review feature, configure workflow, and define coordinators.

The configuration section of this document provides more details.

Another prerequisite is having a user detail data source to provide the manager relationship for the users included in the review. This data source may be an SAP ERP HR system or an LDAP (Lightweight Directory Access Protocol). Details are discussed in the AC 5.3 Configuration Guide.

4. Review Process

This section discusses the review process. It also discusses options in the process that require you to decide how to implement the review process. The next section will discuss how you configure the system to reflect your chosen process.

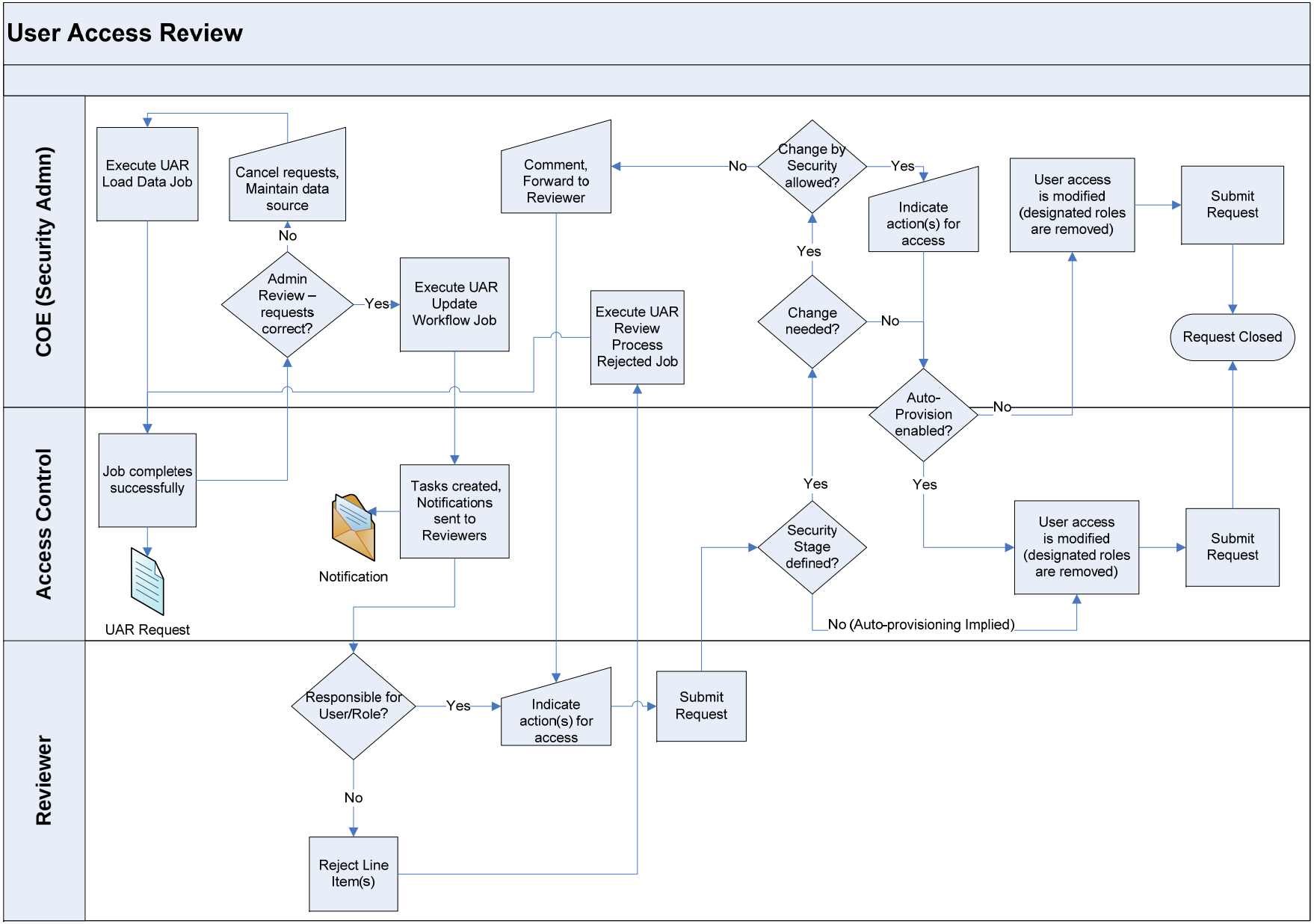
4.1 Overall Process

4.1.1 User Access Review Process Flow

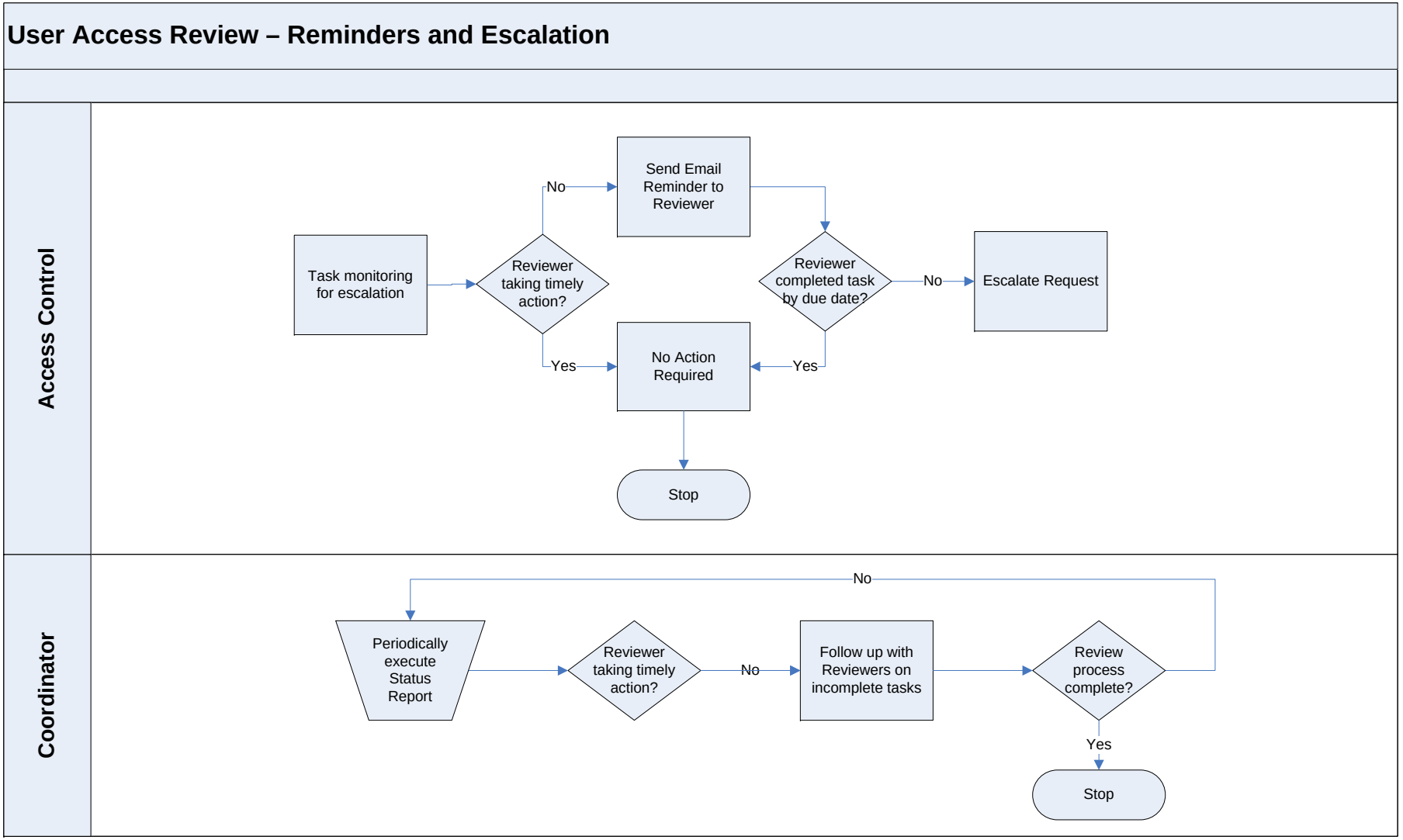
The high-level process for user access review is as follows.

- Access review requests are generated.
- E-mail notifications are sent to reviewers.
- Requests are reviewed and actions are noted by the reviewer.
- Roles marked for removal can be de–provisioned from the back-end system(s)

The detailed process for executing the User Access Review is depicted below. The first diagram shows the flow for a common User Access Review. The second diagram shows the activity being performed by Access Control to send reminder notifications or escalation requests as dictated by configuration when the stage approver does not submit completed requests and requests are not closed within the time defined in configuration.



4.1.2 Escalation Process Flow



4.1.3 Roles in the UAR Process

Administrator: This person has the AE_Admin UME role assigned for Access Control. They can perform general CUP administrator tasks in addition to UAR-specific administrator tasks, such as cancelling UAR requests and regenerating requests for rejected users.

User's Manager: The direct manager of a user as defined in the *User Details Data Source.*

Role Owner: The role owner specified in CUP master data.

Reviewer: This term refers to the approver at the *Reviewer* stage. The *Reviewer* may be the user's manager or the role owner.

Coordinator: The *Coordinator* specified in CUP master data. The *Coordinator* is assigned to *Reviewer*. They monitor the UAR process and coordinate activities to ensure the process is completed in a timely manner.

4.2 Process Options

Multiple process options will determine the approvers of the UAR requests.

4.2.1 Admin Review

You decide whether to enable *Admin Review.* This configuration option provides an opportunity for the administrator to validate the request data after the requests are generated (by the *UAR Load Data* job) but prior to generating workflow tasks (by the *UAR Update Workflow* job). If the *Reviewer* information is incorrect or missing, the administrator can modify the data prior to generating workflow tasks and notifications. The administrator can also delete requests.

4.2.2 Reviewer Stage

You decide whether the Reviewer stage will be addressed by the User's Manager or the Role Owner.

4.2.3 Security Stage

You decide whether to have a security stage. A security stage is mandatory if you do not have automatic provisioning enabled. The security stage may be desired even when automatic provisioning is enabled so that security personnel can ensure accurate data prior to provisioning.

If a security stage will be included in your approval workflow, you must decide whether security personnel will be able to modify the direction previously noted by an Approver. For instance, a security team member may decide to retain basic roles that have been inappropriately marked for removal by an approver.

4.2.4 Additional Approver Stage

You decide whether you will have an additional stage with the approver derived by a Custom Approver Determinator (CAD). The fields available in the UAR CAD differ from those available in the standard CUP CADs. The fields available are in the UAR CAD are:

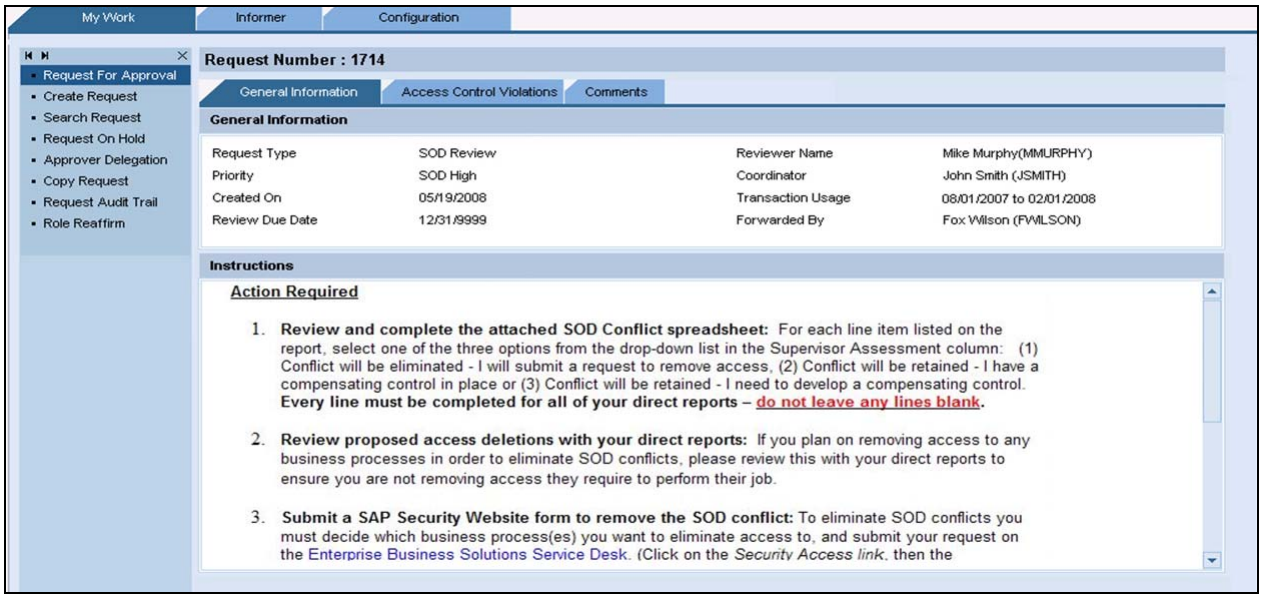
- Application
- Request type
- Role(s) being reviewed

For more details on the use of CADs, see the Configuration Guide.

4.2.5 Instruction for Reviewers

You can provide detailed instructions for reviewers to supplement the content of the notification emails. The level of instruction for approval of periodic access reviews might be more extensive since it is an infrequent process and may involve reviewers who do not perform routine approval of requests to create or change accounts.

The *Instructions* area of the UAR requests is an HTML viewer. An example of a UAR request with an HTML page provided in the request is shown here.



4.3 Workflow Stage Configuration

Now that you have decided which stages to include in your UAR workflow, you must decide on specific behavior for each stage to reflect your review process. The items to be addressed in configuration are listed below.

4.3.1 Email Notification

You decide on the content of email notifications to be sent to the approvers at each stage. You determine the recipient(s), the content of the notification header and the email body. For more details, see the email notification configuration section below or see the Access Control 5.3 Configuration Guide.

4.3.2 Reminders

You decide whether to send reminders to the reviewers who have not completed their portion of the request by the date specified in configuration. You can specify the interval of reminder notifications in days, the reminder notification header, and body content. For details on configuring reminders, see the configuration Guide.

4.3.3 Escalation

You decide whether to escalate UAR requests in each stage's details. Therefore, escalation is based on the time spent in a particular stage. If a reviewer does not complete their review of a request according to the date parameter defined in configuration, then the request is escalated. Escalation of a request will show in the request's audit trail.

You also determine whether escalation will include automatically removing access that is not approved by a certain date.

4.4 Automatic Provisioning

You decide whether to automatically provision requests at the end of the request's workflow. If chosen, roles that are marked for removal in the User Access Review will be automatically de-provisioned in the target system.

If you do not choose to automatically provision, a security stage must be placed in the workflow to allow the security team to modify access according to the review.

5. Configuration and Master Data

This section contains Instructions for configuring the User Access Review and providing the necessary master data. It includes many excerpts from the *AC 5.3 Configuration Guide.* For more information on general configuration, please review the corresponding section of the configuration guide.

5.1 Alert Generation in RAR

There are two methods for providing role usage information for UAR requests. You may define connectors and execute alert generation in RAR. The alternative is to define connectors only in ERM and upload role usage and role assignment information there.

5.1.1 Back-end Systems with RAR Connectors and RTAs

Alert Generation data in Risk Analysis and Remediation provides the foundation of the usage information in the User Access Review requests for connected back-end systems. To allow the system to obtain usage information automatically, you must configure alert generation and execute the alert generation job in RAR. If there is no alert generation information obtained from RAR by the ERM Role Usage Synchronization job, you must upload role usage information in ERM or the usage column in UAR requests will contain zeroes (0).

For Access Control to automatically obtain the transaction and role usage information, please ensure that the connector ID in RAR is identical to the connector ID in CUP and the system (connector) ID in ERM.

5.1.2 Back-end Systems without RAR Connectors and RTAs

You may upload role usage information for the back-end system when you upload role assignment information in ERM. Please refer to the following section on Role Usage Synchronization.

5.2 Role Usage Synchronization in ERM

The *Role Usage Synchronization* job in ERM provides role usage information and the user to role relationship for the user access review. The usage of each role is calculated from the action usage data of the *Alert Generation* job in RAR and the actions defined in each role. For each back-end system to be included in the UAR review, the role assignment information must be either obtained from the back-end system using a real-time agent or uploaded manually. Either approach requires definition of a system (connector) in ERM. You define ERM connectors in *Configuration* > *System Landscape* > *Systems.*

For information on creating connectors or the populating role usage information in ERM, please refer to the *AC 5.3 Configuration Guide.*

5.3 Configuration and Master Data in CUP

5.3.1 Initial Data File for UAR

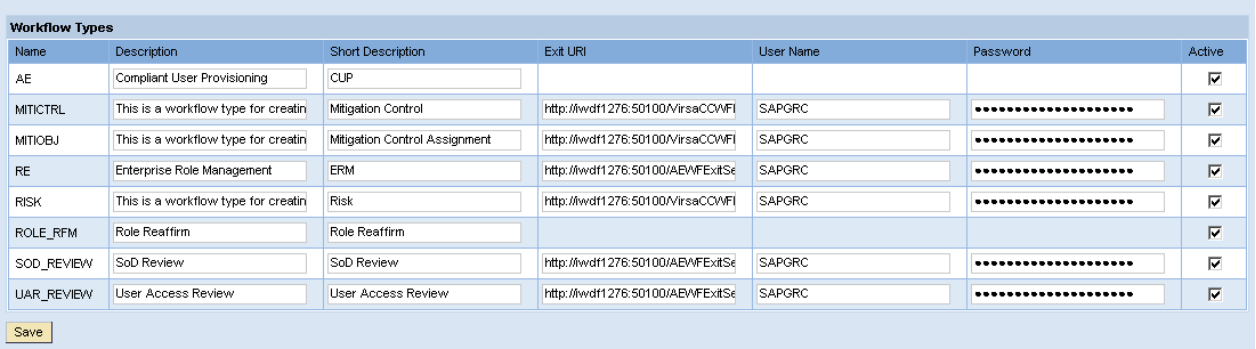
Ensure that the *AE_init_append_data_ForSODDUARReview.xml* file has been uploaded in *Configuration* > *Initial System Data.* This .xml file is one of the initial data files included with Access Control.

Support Packages may deliver subsequent versions of the initial data files and you must be sure that you have the data files that correspond to your AC support package level. Upload the specified initial data file in CUP using the *Append* option. If you are configuring a new Access control installation, then you will need to upload all initial data files.

5.3.2 Workflow Type

You must activate the UAR Workflow Type, which was created by the initial data files. If the workflow type is not available, you may need to upload the AE_init_append_data_ForSODDUARReview.xml file again.

Navigate to Configuration > Miscellaneous. In the Workflow Types pane, maintain the entry UAR_REVIEW.



Workflow Types

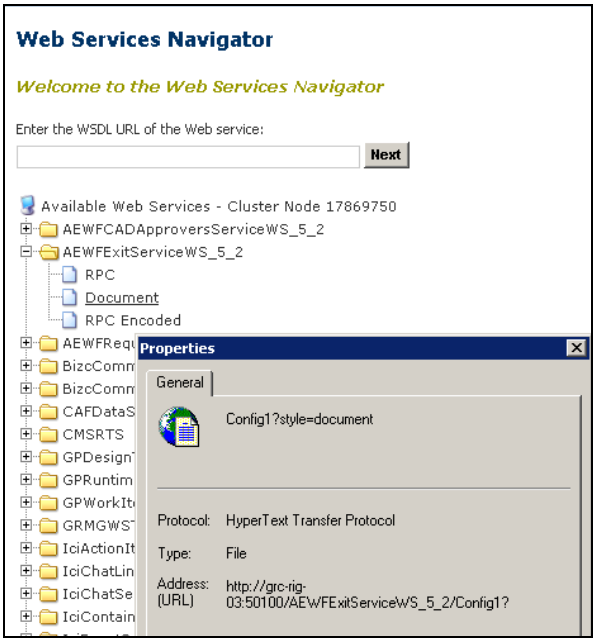
Name	Description	Short Description	Exit URI	User Name	Password	Active
AE	Compliant User Provisioning	CUP				☑
MITICTRL	This is a workflow type for creatin	Mitigation Control	http://wdf1276:50100/VirsaCCWFI	SAPGRC	••••••••••••••••••••	☑
MITIOBJ	This is a workflow type for creatin	Mitigation Control Assignment	http://wdf1276:50100/VirsaCCWFI	SAPGRC	••••••••••••••••••••	☑
RE	Enterprise Role Management	ERM	http://wdf1276:50100/AEWFExitSe	SAPGRC	••••••••••••••••••••	☑
RISK	This is a workflow type for creatin	Risk	http://wdf1276:50100/VirsaCCWFI	SAPGRC	••••••••••••••••••••	☑
ROLE_RFM	Role Reaffirm	Role Reaffirm				☑
SOD_REVIEW	SoD Review	SoD Review	http://wdf1276:50100/AEWFExitSe	SAPGRC	••••••••••••••••••••	☑
UAR_REVIEW	User Access Review	User Access Review	http://wdf1276:50100/AEWFExitSe	SAPGRC	••••••••••••••••••••	☑

Save

- Description fields
- *Exit URI* of the web service *AEWFExitServiceWS_5_2*.

  The format of the URI is http://***<server>:<port>***/AEWFExitServiceWS_5_2/Config1?wsdl.

  You can use the *Web Services Navigator t*o identify the *Exit URI.* Expand the entry for AEWFExitServiceWS, right-click on *Document,* and select *Properties* to display the URI.

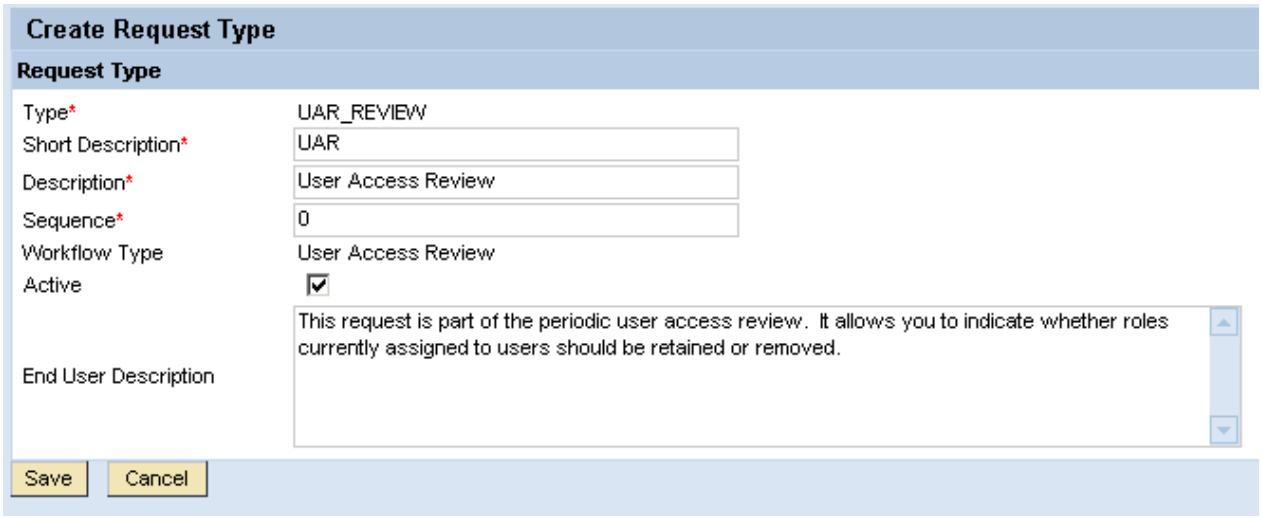


- *User Name* and *Password:* Enter the account and password to be used accessing the capability
- *Active* indictor: Select the indicator to enable the connector.

5.3.3 Request Type

The initial data files include the *UAR_HIGH* request type. You must activate the UAR request type.

- Go to *Configuration > Request Configuration > Request Type.*
- Select the *UAR_REVIEW* request type and select *Change.*
- Maintain the descriptions.
- Ensure that the *Active* indicator is selected.



5.3.4 Request Priority

Confirm that the *UAR_HIGH* priority is present and is associated with the UAR *Workflow Type.* Navigate to *Configuration > Request Configuration > Priority.*

Request Configuration

Priority

Priority	Short Description	Description	Workflow Type
HIGH	CUP - High	Compliant User Provisioning - High Priority	CUP
LOW	CUP - Low	Compliant User Provisioning - Low Priority	CUP
MC_HIGH	MITICTRL High	MITICTRL High	Mitigation Control
MEDIUM	CUP - Medium	Compliant User Provisioning - Medium Priority	CUP
MO_HIGH	MITIOBJ High	MITIOBJ High	Mitigation Control Assignment
RE_HIGH	RE High	RE High	ERM
RS_HIGH	High	High Priority for Create/Modify CC Risk	Risk
SOD_HIGH	SOD High	SOD High	SoD Review
UAR_HIGH	UAR	UAR High	User Access Review

5.3.5 Number Range

Ensure there is an active number range in CUP. The number range is applicable to all CUP requests and is not specific to any request type(s).

Go to *Configuration > Number Ranges* to maintain number ranges.

5.3.6 User Data Source

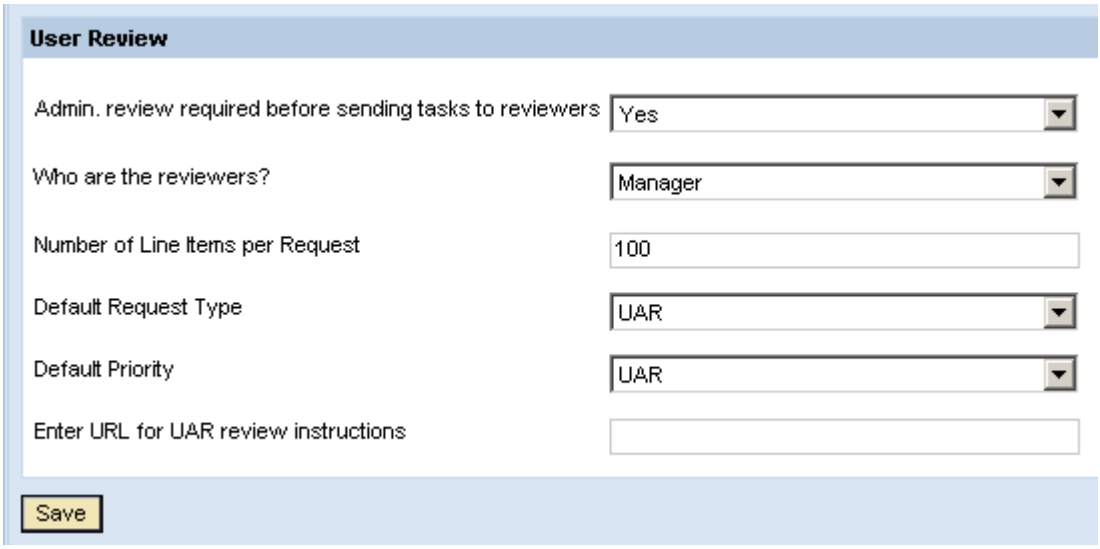
There are multiple types of data sources in CUP. You must identify a *Search Data Source* to be the source of all user IDs returned when performing a search. You may also identify a *User Details Data Source* that will be the source of all user-to-manager relationships.

Go to *Configuration* > *User Data Source* to configure both types of data sources. For details on this configuration, see the *AC 5.3 Configuration Guide*.

5.3.7 User Review Configuration

5.3.7.1 UAR Request Options

Go to *Configuration* > *User Review* > *Options* and specify the parameters for the UAR requests to be generated in the *User Review* pane.



1. *Admin. review required before sending tasks to reviewers:* Maintain this parameter based on the decision made when considering the process options.
   - *Yes:* The administrator reviews the UAR requests prior to the generation of workflow tasks. The administrator makes the required approver modifications and cancels any UAR requests that are not desired.
   - *No:* The administrator does not have an opportunity to review UAR requests prior to sending the workflow notifications to reviewers.

   Note: If there are user records without a manager identified in the User Detail Data Source, then you must enable Admin Review to generate requests.
2. *Who are the reviewers?*
   - *Manager* represents the manager of the user as identified in the User Detail Data Source.
   - *Role Approvers* represents the role approver identified in Compliant User Provisioning master data.
3. *Number of lines items per Request* This is the maximum number of lines for user role assignments permitted on a request. If more lines are required than the maximum number allowed, then another request is required for the remaining items. Therefore, each reviewer may receive one, several or many requests depending on how many user-role assignments they have to approve.

   If a user's access causes the total lines of the request to exceed the maximum number of lines for a request, then that user's role assignments will cross requests.
4. *Default Request Type:* The dropdown list includes any request type in the system that has the *User Access Review* workflow type.

5. *Default Priority* Set the default priority of the request to the value configured or confirmed earlier.
6. *Enter URL for UAR review instructions:* If an HTML page with detailed instructions for reviewers was created to supplement any instruction in the email notification, enter the URL of that page. The page can be saved to a local directory of your choice on your internal server.
7. Click *Save*.

5.3.8 Rejection Reasons

The *Reject User* functionality was introduced in SP06. This section is not applicable if your version of Access Control is lower than AC 5.3 SP06.

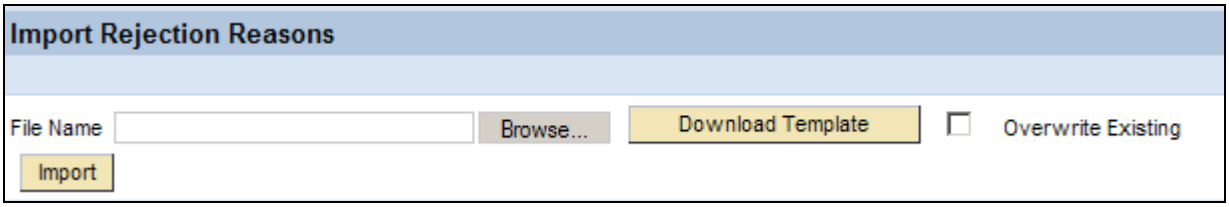
Rejection reasons are mandatory when rejecting a review request. You must upload the reason codes and descriptions using a template.

Procedure

1. Go to *Configuration -> User Review -> Reason for Rejection*. The *Reason for Rejection* screen appears.
2. Under *Import Rejection Reasons,* click *Download Template*. The template opens in Excel.
3. Complete the required information and save the template.

Field	Max Field Length	Recommendation	Possible Values
ReasonCode (required)	10 characters	All UPPER case No special characters, no spaces	Letters and numbers
ReasonEnable	n/a	Have some desired value.	Yes/yes/y/YES/Y No/no/n/NO/N *(When empty default value No)*
ShortDescription_xx (XX – language code such as EN, DE etc.)	100 characters, including spaces	Recommended to have some desired value for at least for application default language	Letters and numbers

4. Under *Import Rejection Reasons,* click *Browse.*



5. Select the Rejection Reasons file and click *Import.*

> **Note**
>
> You cannot delete reason codes from the application. To deactivate a reason code, populate the *ReasonEnable* field with **No**, choose the *Overwrite Existing* option, and import the upload file.

5.3.9 Workflow

You can configure a UAR workflow based on your organization's requirements. For example, the UAR workflow may consist of a primary path with a single stage for *Reviewer* approval and a detour path. A common detour path has a single stage for *Security* approval with a detour condition for action of *Marked for Removal.*

To configure this simple example of a User Access Review workflow, perform the following:

- Define an Initiator.
- Define Stages (one stage for Reviewer and another stage for Security).
- Define Paths (the example configuration has a primary path for the Reviewer and a detour path for Security).
- Define a Detour with condition.

5.3.9.1 Defining an Initiator

The initiator specifies the conditions for sending access requests down a particular path. In this case, we will create an initiator for UAR requests.

In the *Initiator* pane, perform the following steps.

1. Go to the *Configuration* tab > *Workflow* > *Initiator.* The *Initiators* screen appears.
2. Click *Create*. The *Create Initiator* screen appears.
3. In the *Name* field, enter a name for your initiator. For example, enter '*UAR Initiator*'.
4. In the *Short Description* field, enter a brief description for this initiator.
5. In the *Description* field, enter a long description for this initiator.
6. In the *Workflow Type* dropdown menu, select *User Access Review*.

In the *Select Attributes* pane, perform the following steps. The suggested values will provide a simple initiator for the User Access Review process.

7. In the *Condition* dropdown menu, select *AND*.
8. In the *Attribute* dropdown menu, select *Request Type.*
9. In the *Value* field, select *UAR.*
10. Click *Add Attribute*.
11. Click *Save*.

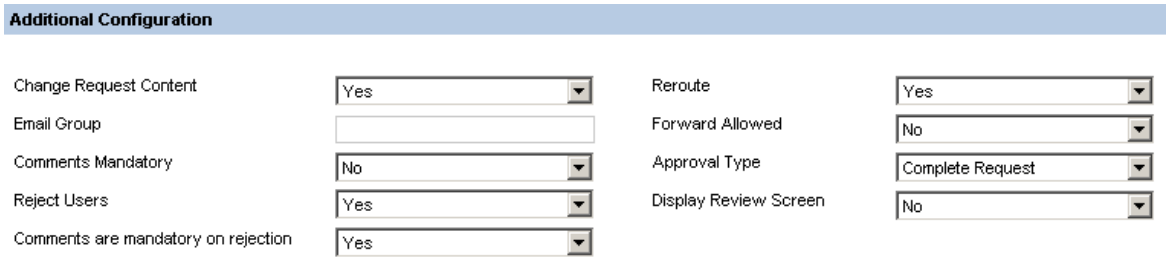
5.3.9.2 Defining Stages

For the simple example workflow provided, you will define one stage for the Reviewer (which is either the user's Manager or the Role Owner) and one stage for Security.

1. Go to the *Configuration* tab > *Workflow* > *Stage*. The *Workflow Stages* screen appears.
2. Click *Create*. The *Stage Configuration* screen appears.
3. In the *Name* field, enter a name for your stage. For example, enter <UAR REVIEWER> or <UAR SECURITY>.
4. In the *Short Description* field, enter a brief description for this stage.
5. In the *Description* field, enter a long description for this stage.
6. In the *Workflow Type* dropdown menu, select *User Access Review*.
7. In the *Approver Determinator* dropdown menu, select *Reviewer* (for Managers or Role Owner).

   Compliant User Provisioning provides two standard approvers for the UAR process. The first is the *Reviewer*, which can be the user's manager or the role owner. The second is *Security*. Optionally, you can define a Custom Approver Determinator (CAD) for a custom approver if an additional approver/stage is required.
8. Specify the time desired for escalation in *Request Wait Time (Days)* and *Request Wait Time (Hours)*. This is the number of days and hours the request may stay in the stage before the request is escalated.
9. In the *Escalation Configuration* dropdown menu, select the type of action taken by the system when escalation is triggered. The following options are available:
   - *No Escalation:* Choose this setting when no escalation is required.
   - *Forward to Administrator:* Upon escalation, the request is sent to the administrator for approval.
   - *Forward to Next Stage:* Upon escalation, the request is sent to the next stage.
   - *Deactivate; Forward To Next Stage:* Upon escalation, the role assignments for users on the request are deactivated with the validity date is set to the current date. Then, the request is forwarded to the next stage.
   - *Deactivate; Lock, Forward To Next Stage:* Upon escalation, the users on the request are locked in addition to being deactivated and the request is forwarded to the next stage.
   - *Lock, Forward To Next Stage*: Upon escalation, the users on the request are locked and the request is forwarded to the next stage
10. In the *Notification Configuration* pane,
    - Select the person(s) to receive a notification when the request is *Approved.*
    - Select the person(s) to receive a notification when the request is *Escalated.*
11. In the individual tabs for *Approved, Escalation* and *Next Approver* email notifications, specify the email *Subject* (header) and the email *Content*.
12. In the *Additional Configuration* pane, you maintain multiple parameters. The items discussed here are of specific interest during user access review.



a. *Change Request Content*

- *Yes: Enables the Approve and Remove buttons during request review. This is required for the Reviewer stage and is optional for the Security stage.*
- *No: Disables the Approve and Remove buttons during request review. This is optional for the Security stage. The reviewer will not be able to specify an action but will only take action on direction already noted or comment and sent the request to another reviewer for update.*

b. *Email Group: Obsolete field that is not supported for AC 5.3.*

c. *Comments Mandatory*

- *Yes: Enforces entry of comments regardless of any action taken.*
- *No: Any entry of a comment is optional.*

d. *Reject Users*

The ability to reject users is required for the *Reviewer* stage and is optional for the *Security* stage.

- *Yes: Enables the Reject User button during request review.*
- *No: Disables the Reject User button during request review.*

e. *Comments are Mandatory on Rejection*

- *Yes: Requires the reviewer rejecting users to enter a comment. Information related to the reason for rejection may assist the administrator or coordinators in correcting information for users/roles that are still relevant for review.*
- *No: Entering a comment is not enforced when a user is rejected from a UAR request.*

f. *Reroute*

- *Yes: Enables the Reroute button during request review.*
- *No: Disables the Reroute button during request review.*

g. *Forward Allowed*

Forwarding a UAR request is supported only when the entire request is forwarded. To have individual user records reviewed by someone other than the stage reviewer, it is recommended to *Reject* the user and manage the user through the alternate process. See the section *Manage Rejected Users* for more information.

- *Yes: This option is not recommended.*
- *No: This option is recommended.*

h. *Approval Type*

- *Complete Request: All lines of the request are visible at the stage. This is required for the Reviewer stage and is optional for the Security stage.*
- *Only Remove Items: Only the items of the request that have been previously marked for removal will be visible at the stage. This is commonly used for the Security stage. This allows Security to easily perform manual provisioning or to confirm that appropriate roles have been marked for removal.*

i. *Display Review Screen*

- *Yes: An approval screen will be shown after the request has been submitted. This approval screen is redundant in the case of the User Access Review. This selection is required if risk analysis is mandatory at the stage.*
- *No: The last approval screen will be bypassed after the request has been submitted. In the case of the User Access Review requests, the approve or remove action has already been indicated for each line item and this review screen is redundant. This option is not supported where risk analysis is mandatory at the stage.*

> **Caution**
>
> For stages with *Risk Analysis Mandatory* set to *Yes*, then *Display Review Screen* must also be set to *YES*. Otherwise, risk analysis will be bypassed.

13. Specify a value for the *Additional Security Configuration (Approval Reaffirm)* parameter, if necessary.

    If *Display Review Screen* is set to *No* as suggested, then this field is not editable.

    - *Yes:* The approver must confirm their identity before submission of the review request by entering their password when prompted.
    - *No:* The approver is not prompted to confirm their identity upon submission of the review request.

14. Click *Save* to store the stage definition.

5.3.9.3 Defining the Reviewer Path

You must define the primary path for UAR request approval by reviewers.

1. Go to *Configuration* tab > *Workflow* > *Path*. The *Workflow Paths* screen appears.
2. Click *Create*. The *Create Path* screen appears.
3. In the *Create Path* pane, perform the following steps.
   a. In the *Name* field, enter a name for your path. For example, enter <UAR Primary>.
   b. In the *Short Description* field, enter a brief description of the stage.
   c. In the *Description* field, enter a long description of the stage.
   d. In the *Workflow Type* dropdown menu, select *User Access Review*.
   e. In the *Number of Stages* field, enter the number of stages for the primary path. The example workflow has *Number of Stages* equal to *1*.

f. In the *Initiator* dropdown menu, select the initiator name that you previously created. In this example, the initiator name is *UAR Initiator.*

g. Select the *Active* checkbox.

h. Leave the Detour checkbox unselected.

4. In the *Path Definition* pane, select the stage name for each stage of the path. In the workflow example, *Stage 1* is the <UAR REVIEWER stage.

5. Click Save.

5.3.9.4 Defining the Detour (Security) Path

For the example workflow, you will define a detour for line items on the UAR request that have been selected for removal. You create the detour path with the following steps.

1. Go to *Configuration* tab > *Workflow* > *Path*. The *Workflow Paths* screen appears.
2. Click *Create*. The *Create Path* screen appears.
3. In the *Create Path* pane, perform the following steps.
   a. In the *Name* field, enter a name for your path. For example, enter <UAR DETOUR>.
   b. In the *Short Description* field, enter a brief description of the stage.
   c. In the *Description* field, enter a long description of the stage.
   d. In the *Workflow Type* dropdown menu, select *User Access Review*.
   e. In the *Number of Stages* field, enter the number of stages for the detour path. The example workflow has *Number of Stages* equal to 1.
   f. In the *Initiator* dropdown menu, leave the *Select* instruction. There is no initiator specified since this is a detour path.
   g. Select the *Active* checkbox.
   h. Select the *Detour* checkbox.
4. In the *Path Definition* pane, select the appropriate name for each stage. For this example workflow, the stage name is UAR *SECURITY. .*
5. Click *Save*.

5.3.9.5 Custom Approver Determinator

You can define custom approver determinators (CADs) to be used for additional stages in approval of UAR requests. If definition of the process resulted in stages other than the Reviewer (Role Owner or User's manager) and Security stages, then define a CAD to be sued at this additional stage. The example being used in this document does not involve a stage utilizing a CAD.

5.3.9.6 Defining a Detour

For the example workflow, you will define the detour for line items selected for removal using the following steps.

1. Go to *Configuration* tab > *Workflow* > *Detour/Fork*. The *Workflow Stage Detour* screen appears. The screen defaults to the *Stage Detour* tab.
2. Click *Create*. At the bottom of the table, the entry fields become active.

3. In the *Workflow Type* dropdown menu, select *User Access Review*.
4. In the *Path* dropdown menu, select the UAR path. In this workflow example, the path is <UAR PRIMARY PATH>.
5. In the *Stage* dropdown menu, select the appropriate stage. In this workflow example, the detour will occur at the <UAR REVIEWER> stage.
6. In the *Action* dropdown menu, select *Save*.
7. In the *Condition* dropdown menu, select *Items with Remove Action*.
8. In the *Value* dropdown menu, select *Yes*. The *Yes* value indicates that the request will follow the detour if the condition is true.
9. In the *Detour Path* dropdown menu, select the appropriate detour path to be followed. In the example workflow, the *Detour Path* is the <UAR DETOUR> path.
10. Click *Save.*

5.3.9.7 Defining an Email Reminder

You define whether notifications will be sent for UAR requests upon request submission, upon request close and as reminders. You may define the timing for reminder notifications and the content for the relevant notifications. These notifications are optional and you may ignore this section.

1. Go to *Configuration* tab > *Workflow* > *Email Reminder*. The *Email Reminder screen* appears.
2. In the *Workflow Type* dropdown menu, select, *User Access Review*.
3. In the *Days* field, enter the number of days to elapse from the time that the request was first submitted to the approver's inbox before reminder notifications are generated. If you do not wish to
4. Click *Save* under the *Select No. of Days* pane.
5. In the *Request Submission and Closing Email* Configuration pane, choose the tab for which you wish to configure notifications. For example, choose the *Reminder* tab.
6. In the *Subject* field, enter an email header statement for the notification recipient, such as the *Reviewer.*
7. In the *Content* field, define the email body for the recipient.
8. While defining content, you may select *Email Arguments* from the dropdown menu to be included in the content.

> **Note**
>
> You can copy *Email Arguments* from the body of the email to the email *Subject.*

9. In the *Notification Configuration* pane, choose the recipients for the notification being defined on this tab. The type of notification you are maintaining determines the possible recipients.
10. Repeat steps 5 through 9 for each type of notification you wish to generate.
11. Click *Save* under the *Request Submission and Closing Email* Configuration pane.

5.3.9.8 Auto Provisioning

You can define whether roles approved for removal are de-provisioned from the user manually or automatically. The configuration setting for auto-provisioning is global. If CUP is being used, then

provisioning for the user access review should follow your corporate policy for auto-provisioning. See the *AC 5.3 Configuration Guide* for more instruction on configuring auto provisioning.

5.3.10 Service Level (Escalation)

You may define the conditions that will cause an escalation, the action taken for the escalation and the content of the escalation email.

1. Go to the *Configuration* tab > *Service Level.*
2. Click *Create*. The *Create Service Level* screen appears.
3. In the *Service Level* pane, populate the following fields.
   a. In the *Name* field, enter a name for your service level. For example, enter *UAR Escalation.*
   b. In the Short Description field, enter a brief description for this service level.
   c. In the Description field, enter a long description for this service level.
   d. In the Workflow Type dropdown menu, select User Access Review.
   e. In the Type dropdown menu, select either Formula or Fixed.
      - Formula allows you to specify criteria for the escalation of the request. Fields available to determine the formula are time (in days and hours) and attributes (including custom attributes).
      - Fixed allows you to specify a date upon which the request will be escalated. You also specify whether this is a *Global Escalation Date*. If it is a *Global Escalation Date,* then the date defined here takes precedence over the escalation date configured at the workflow stage level. For more information about configuring escalation, see the *AC 5.3 Configuration Guide* and *AC 5.3 SP06 Supplemental Note*.
4. Complete definition based on the escalation type chosen.
5. Click *Save*.

Note: Modify the Due Date and Global Escalation Date for new review cycles. If the request generation date is later than the due date, the background jobs for request generation will error.

5.3.11 Configuring an SMTP Server

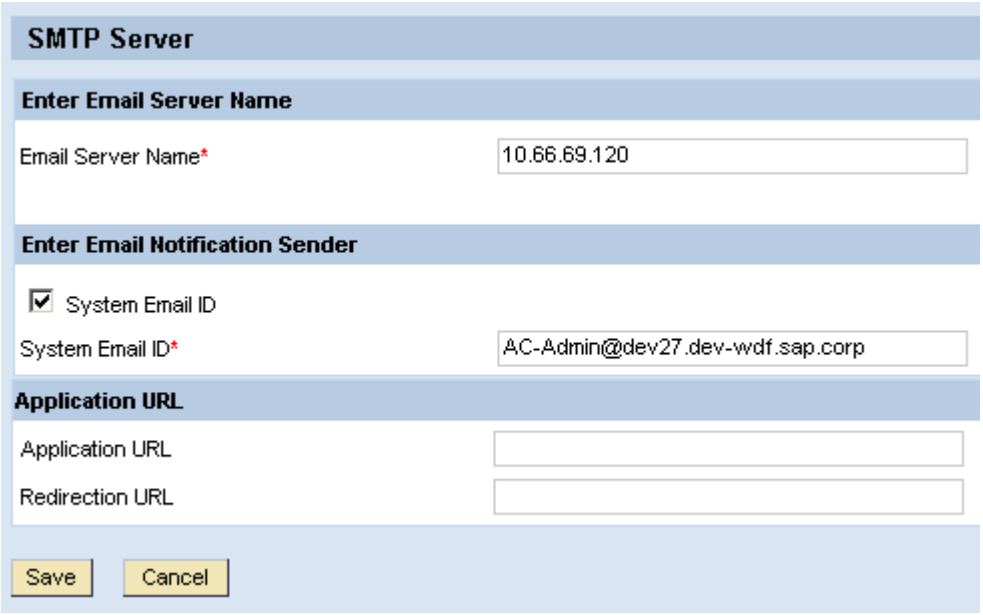
Compliant User Provisioning uses an SMTP server to send email notifications and reminders to users, requestors, and approvers of requests.

⚠ If this setting is not properly configured, the entire approval process might be jeopardized. If approvers are not getting the email notifications that a request is waiting for their approval, the approvers must log on to Compliant User Provisioning and check their email.

1. On the *Configuration* tab, navigate to *Workflow* > *SMTP Server*.

   The *SMTP Server* screen appears.
2. In the *Email Server Name* field, enter the name of the SMTP server that Compliant User Provisioning uses to transmit messages.
3. In the *System Email ID* field, enter the system account to be used as the sender of email notices from Access Control. If no system account is to be used, the email notifications will have the previous stage owner as the sender of the email.

4. Entries in the *Application URL* and *Redirection URL* fields are not required for the UAR.
5. Click *Save*.



- Emails are not sent automatically. To send the emails, execute the *Email Dispatcher* background job. For more information, see Setting Up Background Jobs.

5.3.12 Field Mapping

If you are using an LDAP as the *User Detail Data Source* and UAR requests will be approved by users' managers, then you must specify a field mapping for *Manager* so that Access Control can determine the reviewer for workflow. You define this in *Configuration* > *Field Mapping* > *LDAP Mapping.*

If you are auto-provisioning as part of the UAR process, you must perform field mapping for provisioning. You define this in *Configuration* > *Field Mapping* > *Provisioning.*

For more information, see the *Field Mapping* section of the *AC 5.3 Configuration Guide*.

5.3.13 Security Lead

You can specify a group email or approver IDs to be used in the security approval stages. On the *Configuration* tab, go to *Approvers* > *Security Lead* to configure the security lead information.

5.3.14 Coordinator

You identify a *Coordinator* for each *Reviewer*, regardless of whether the reviewer is a *User's Manager* or a *Role Owner*. Access Control uses the coordinator information to generate reports that can be used while managing the review process.

1. Go to the *Configuration* tab > *User Review* > *Coordinator.*
2. Choose *Search.*
3. The list of coordinators is shown. Choose Create to identify new coordinators or associate coordinators with additional Reviewers.

4. Enter a *Coordinator ID* and a *Reviewer ID.* (Note that wildcards are not support in the ID fields.)
5. Choose *Save.*

If you are not using *Admin. Review*, then you must have a *Coordinator* associated with the *Reviewer* to get a UAR request to generate. For example, user MWONG with Reviewer BLAW must have a Coordinator associated for BLAW to get MWONG included on a UAR request.

5.3.15 Defining Connectors

For each back-end system to be included in the user access review, you must define a connector. The *Connector ID* in CUP must be identical to the *System* (connector) in ERM so that user-to-role relationship information may be transferred to CUP. It should also be identical to the Sys

5.3.16 Roles

Roles that will be included on the UAR requests must be imported into CUP so that role descriptions can be provided in requests and to support drilling down to the actions included in the roles. You may import roles from a back-end system supported by an RTA or from a spreadsheet file.

5.3.16.1 Importing Roles from RTA-Supported Systems

To import roles:

1. On the *Configuration* tab, navigate to *Roles* > *Import Roles*.

   The *Import Roles* screen appears.
2. From the *System* dropdown list, select the system that contains the roles you want to import.
3. From the *Role Source* dropdown list, select either the SAP backend or Enterprise Role Management.
4. In the *Last Sync Date* field, select the date when the roles were last changed and selected for synchronization. Click the calendar icon to set the date.

   All roles that have been changed since the specified date are selected for import.
5. Select the appropriate setting in which to import your roles from the following table.

Role Import Settings	
Role Import Setting	**Description**
All Roles	Imports all roles from the specified system, including delivered roles. Use caution when importing roles, you might not want to import all roles from the backend system into Compliant User Provisioning. The only roles you should import should be the roles that you want requestors to select for provisioning.
All Roles Except SAP Predefined Roles	Imports all the roles, excluding delivered roles, in the specified SAP system.

Role Import Settings	
Role Import Setting	**Description**
Selected Roles	Imports individual roles. You must know the names of the roles you want to import. Enter the roles one at time in the *Role Name* field, or use a wildcard option (an asterisk - *) to specify a number of similarly named roles.
From File	Use this setting to load roles from an Excel spreadsheet file. The spreadsheet file can be on your local host or on another system. You can use *Browse* to navigate to the appropriate file.

In your development system, where you create roles to transport, there might be some roles used for testing which you do not want users to request. If you do not import these roles, they are not available for selection, approval, and provisioning.

For SAP systems: If you do not want users requesting access to *SAP_ALL* in your production system, do not import *SAP_ALL* for the production system.

6. Select the *Overwrite Existing Roles* checkbox to overwrite any existing roles of the same name as those you import or add any new roles to the system.

   The *Overwrite Existing Roles* option does not affect any roles that are not listed in the spreadsheet or included in the import.

7. Click *Import*.

   The following message appears:

   `Import Status: xx successfully imported from yy records found.`

   Where *xx* is the number of roles successfully imported from the records found.

5.3.16.2 Importing Roles from non-RTA-Supported Systems

You may import roles for systems that are not supported by an RTA. See the appendix for details on using the Role Import/Export Template.

5.3.17 UME Security

As of SP06, UME actions for managing the rejected user process are introduced and must be assigned to the appropriate individuals. These actions were provided in the initial data files as of SP06. The general security requirements for Access Control are not discussed here. If you need information on general security, please see the *AC 5.3 Security Guide*.

UME Action	Permission Included
ViewManageRejectionReasons	Provides the ability to configure *Rejection Reasons* to be used in reviews
ViewRejectUsers	Enables the *Reject Users* button in review requests

ViewManageRejections	Provides the ability to view the *Manage Rejections* functionality for UAR
ManageRejectionsGenerationAction	Provides the ability to generate new requests for rejected users
ManageRejectionsCancelGenerationAction	Provides the ability to cancel the generation of new requests for rejected users

6. Review Execution

6.1 UAR Request Creation

Identified below are the steps and jobs executed to generate requests for the periodic user access review. (Please note that generating new requests for users rejected from earlier requests is discussed in the section *Managing Rejected Users*)

Before beginning the user review process, all supporting information for generating requests should be current to ensure accurate workflow of requests. For example, if the Reviewer is configured to be the User's Manager, then the user to manager relationships should be current in the detail data source.

Note: If there are users with no manager identified in the *User Detail Data Source* and the *Reviewe*r is defined as the *User's Manager*, then *Admin Review* is required. This allows the administrator to maintain the missing data prior to sending workflow tasks to reviewers.

6.1.1 Purge Usage Information

If more transaction usage information is stored in RAR than is desired for User Access Review or SOD Review requests, then the data should be archived. For example, if your UAR process states that the prior twelve months' usage information should be provided in UAR requests and RAR has fifteen months available, then the oldest three months information should be purged (archived) in RAR. It is important to note that usage information purged in RAR is still accessible to RAR from the flat file that is produced but is not accessible by ERM or CUP.

This requires configuration of the location for writing the purge file in RAR *Configuration* > *Miscellaneous* > *Alert Log File Name and Location.* For more information on purging usage information, refer to the *AC 5.3 Configuration Guide*.

6.1.2 Alert Generation

Ensure that the RAR Alert Generation job has been executed if your role usage information will be obtained automatically rather than being uploaded.

To generate alerts:

1. On the *Configuration* tab, navigate to *Background Job* > *Alert Generation*.
2. In the *Action Monitoring* pane, select *Generate Action Log*.
3. Select the SAP single or cross systems for which to generate alerts. Only SAP servers that have connectors created appear in the dropdown list.

4. Select all types of alerts to include in the action log.
   - *Conflicting Action*

     Select *Risk ID* equal to *'*'.

     Select *Risk Level* equal to *All*.

     Select *Consider Mitigated Users*.
   - *Critical Action*

     Select *Risk ID* equal to *'*'.

     Select *Risk Level* equal to *All*.

     Select *Consider Mitigated Users*.
   - *Control Monitoring*

     Select the *Mitigating Control ID* equal to *'*'.
5. In the *Alert Notification* pane, select the appropriate items according to company policy.
6. Click *Schedule*. The *Schedule Background Job* screen appears.
7. In the Job Name field, enter a name for this job.
8. Select *Immediate Start* or *Delayed Start.* Indicate the date and time to begin.
9. If the job should be performed multiple times, select *Schedule Periodically* and indicate the frequency as well as the *End Date* past which no jobs will execute.
10. Click *Schedule* to accept your input or *Reset* to begin again.

    Upon completion of scheduling, the following message displays: `Background job scheduled successfully, Job ID: XX.` Table VIRSA_CC_ACTUSAGE will be updated with the chosen transaction usage information,

6.1.3 Role Usage Synchronization

The next step in generating data for the User Access Review is to identify the roles assigned to users, the transactions included in the roles, and the use of those transactions and roles.

6.1.3.1 Back-end Systems with RAR Connectors and RTAs

The ERM Role Usage Synchronization job gathers multiple types of data.

For SAP ERP backend systems connected to RAR, the Role Usage Synchronization job will obtain transaction usage information from RAR alert data. The job also obtains role to user assignments and role content information from the back-end systems. Access Control then translates the transaction usage information into role usage.

You execute the job in ERM by following the path *Configuration* > *Role Usage Synchronization*. Select the system(s) for which role usage synchronization is to be executed.

To execute the *Role Usage Synchronization*:

1. On the *Configuration* tab, navigate to *Role Usage Synchronization*.
2. From the *Role Usage Synchronization* pane, select the system from which you want to synchronize the role usage.

3. Enter the *Synchronization Start Date* with which you want the synchronization to begin. If you leave this field blank, it defaults to the date of the last synchronization job. For the initial execution of the job, you should leave the date field blank so that all existing data will be obtained.
4. Click *Schedule*.

   The system displays the message `Role usage synchronization job scheduled successfully; job ID ##` if the synchronization is scheduled successfully.

6.1.3.2 Back-end Systems without RAR Connectors and RTAs

For systems where automatic generation of the user to role assignments and/or role usage information is not available, you can upload the data. See the *AC 5.3 Configuration Guide* for more information on uploading the data.

To perform manual upload:

1. On the *Configuration* tab, navigate *to Role Usage Synchronization*.
2. From the *Upload Role Usage* section, select the system type of the source system where the role usage information is being uploaded.
3. In the File Name field, click *Browse* to locate the file you want to import.

   You can click the red arrow next to the *Browse* button to download the Role Usage Import Template that contains the format for the import file.
4. Click *Upload.*

Role Usage Import Template

Field Name	Definition	Example
System (Name)	Alphanumeric (20)	QF6
User (ID)	Alphanumeric (40)	Tchard1
First Name	Alphanumeric (50)	Tom
Last Name	Alphanumeric (50)	Chard
Role (Name)	Alphanumeric (100)	Z_AP_Payable
Execution Count	Numeric	Number of times that the role was used.
Last Executed	Date (MM/DD/YYYY)	08/27/2008
Expired	Numeric (1= expired, otherwise leave blank. Blank= not expired.)	Any value other than 1 indicates that the role is not expired.

6.1.3.3 Managing Role Assignment and Usage Data

A few details will help you manage the role usage data and ensure the desired data is being utilized by the user access review process.

- The role usage job appends the existing data in table.
- The ERM data populated by the role usage synchronization job or by the manual upload of role usage information is not the data reported in the ERM *User to Role Relationship Report*.

6.1.4 UAR Review Load Data job

Execute this job to retrieve user-to-role relationship and role usage data from ERM and create User Access Review requests. You execute the job in CUP by following the path *Configuration* > *Background Jobs* and selecting the task *UAR Review Load Data*.

To create User Access Review requests:

1. Go to *Configuration* tab > *Background Jobs.* The *Schedule Service* screen appears.
2. In the *Task Name* dropdown menu, select *UAR Review Load Data*.
3. In the *Description* field, enter a brief description.
4. In the *Schedule Type* dropdown menu, select the time you wish to schedule this job. The corresponding *Task Occurrence* or *Recurrence* pane appears.
   a. In the *Monthly Task Recurrence* pane, enter the *Time* and *Start Date*.
   b. For *Immediate* schedule type, click *Run*.

   For other schedule types (On Date, Daily, Weekly, Monthly, Quarterly, Yearly, and Other), you can *Activate* the service and/or *Save* the schedule.

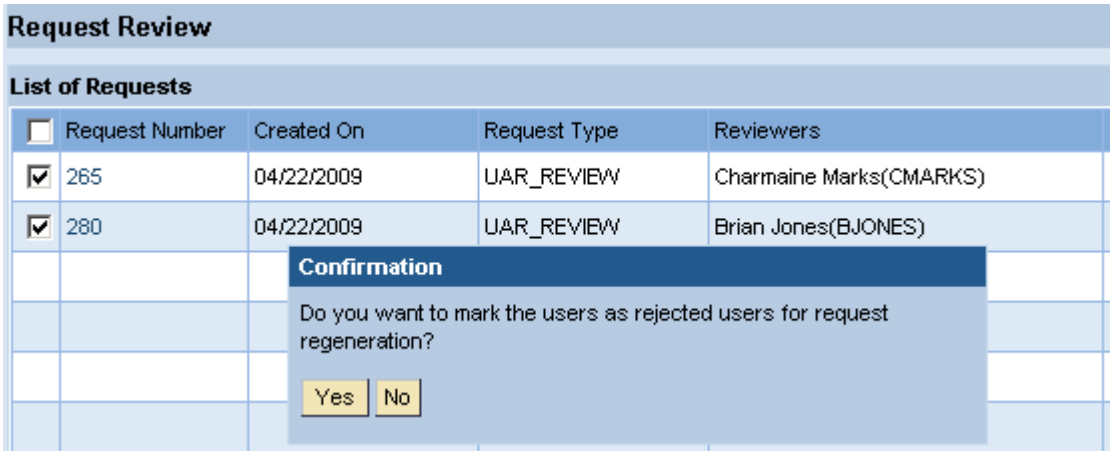
6.1.5 Admin Review

The administrator evaluates the requests to ensure completeness and accuracy of the request information prior to sending workflow items to reviewers. If the requests are incomplete or inaccurate, you

- *cancel the current UAR requests*
- *maintain user-to-manager relationships in the* User Details Data Source
- *generate new requests.*

To perform the admin review:

1. On the *Configuration* tab, navigate to *User Review* > *Request Review.* The search screen appears.
2. Search for requests and review the data to confirm accurate reviewer information.
3. To cancel an incorrect request, select a review request number and click the *Cancel Request(s)* button. If you choose to cancel a request, Access Control will ask you to indicate whether the users contained in the request(s) being cancelled should be marked as rejected users.



Yes: The review request is cancelled. All users in the request are considered *Rejected Users* and their requests are available in the *Manage Rejected Users* screen to be regenerated.

No: The review request is cancelled. All users in the request will only be included in another UAR request upon selection in execution of *UAR Review Load Data* job.

> **Tip**
> If you mistakenly choose to cancel a request and want the request to remain, select an item in the Configuration menu to exit the current menu option.

> **Tip**
> If you wish to evaluate the users and roles included on UAR requests, you may query the table VT_AE_RQD_UAR_ROLE.

6.1.6 UAR Review Update Workflow Job

After the *UAR Review Load Data* job has completed and you have performed Admin Review (if appropriate), you execute the *UAR Review Update Workflow* job to push the workflow tasks to the reviewers. In CUP, go to Configuration > Background Jobs and select the task *UAR Review Update Workflow.*

To generate workflow tasks for the user review:

1. Go to *Configuration* tab > *Background Jobs.* The *Schedule Service* screen appears.
2. In the *Task Name* dropdown menu, select *UAR Review Update Workflow*.
3. In the *Description* field, enter a brief description.
4. In the *Schedule Type* dropdown menu, select the time you wish to schedule this job. The corresponding *Task Occurrence* or *Recurrence* pane appears.
   a. In the Monthly Task Recurrence pane, enter the Time and Start Date.
   b. For *Immediate* schedule type, click *Run*.

6.1.7 Notifications

E-mail notifications are generated for reviewers with the next execution of the *Email Dispatcher* job. The UAR notification emails will contain a hyperlink to the CUP request.

6.2 UAR Request Review

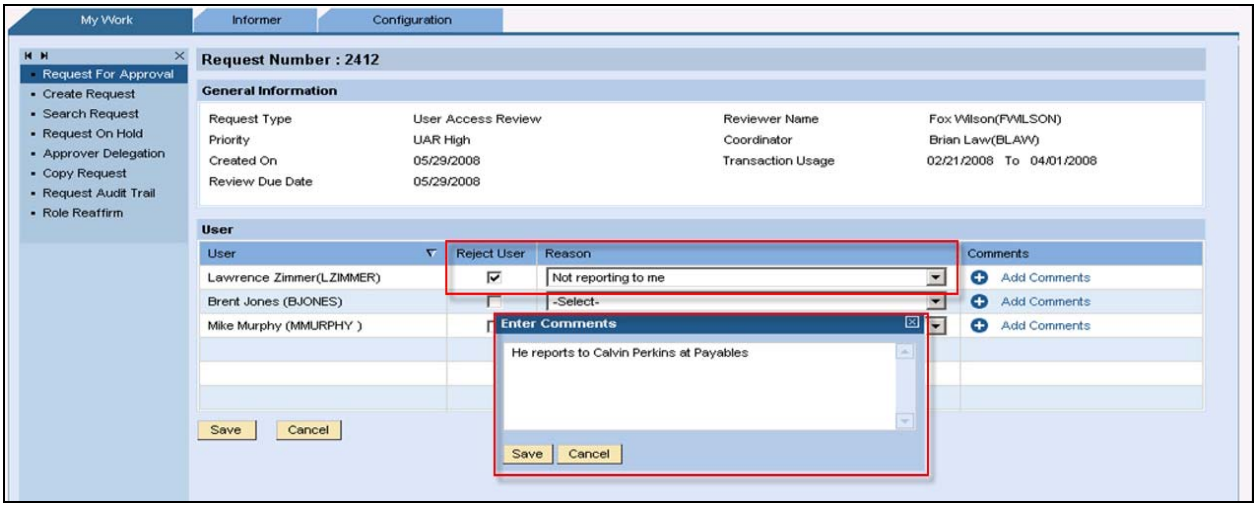
6.2.1 Reviewer Tasks

6.2.1.1 Rejecting Users

As of Support Package 06, the user's *Manage*r may reject users for whom they are no longer responsible during UAR approver review. Once rejected, users are able to be included on new requests. Rejected users are visible in the UAR History Report and the user Review Status Report. The *Reject User* option is not relevant for the Reviewer stage if the Reviewer is the Role Owner. The Role Owner review screen will not include the option to reject a user, but will include options to approve or remove the access.

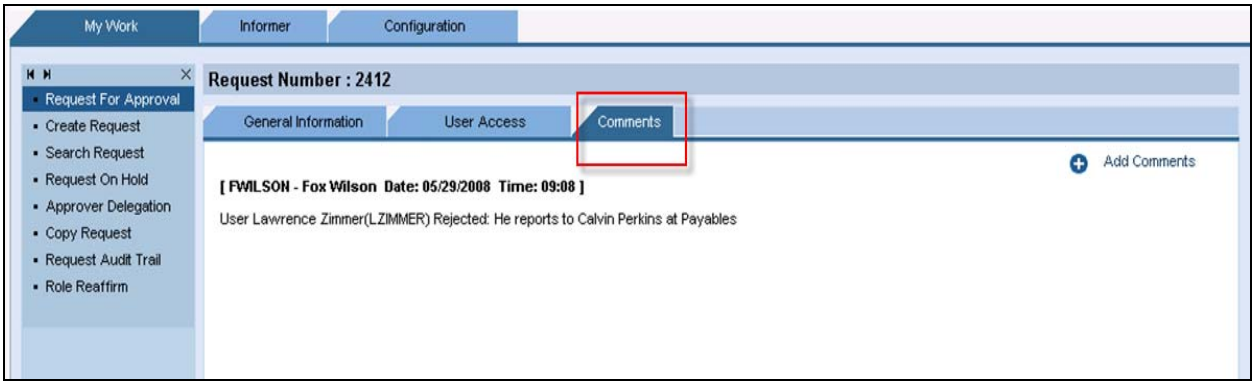
To reject users from UAR requests for which you are the *Reviewer (Manager):*

1. Go to *My Work* > *Request for Approval*.
2. Select a UAR request. Go to the *User Access* tab.
3. Click the *Reject User(s)* button.
4. The *User* pane appears and displays the list of users.
5. Click the *Reject User* checkbox next to the user you want to reject.

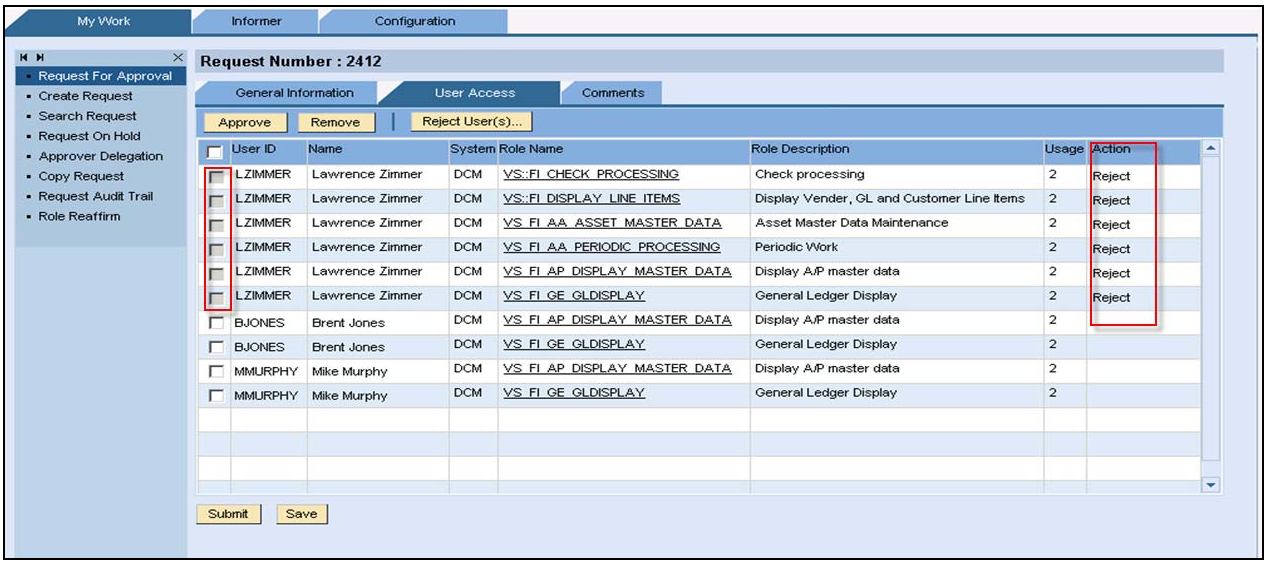


6. Click the *Reason* dropdown box and select a reason.
7. Click *Add Comments*, add a comment, and click *Save*.

   To view previous comments, go to the *Comments* tab. Comments are listed for each rejected user with a time stamp and a reviewer User ID.



8. On the *Request Number screen*, click *Save***.** The *User Access* tab is displayed.



On the *User Access* tab, all items for the rejected user are grayed and inactive, and the *Action* column displays *Reject***.** You can go back to the *Reject Use***r** screen and modify rejections prior to submitting the review request. Once you submit the request, the rejected items cannot be modified in a later stage. This applies even if the request is rerouted to another stage.

9. Click *Submit* to submit the request**.** Upon submission, the items marked for rejection will be visible in the *Manage Rejected Users* screen with the status *New*.

6.2.1.2 Approve / Request removal of access

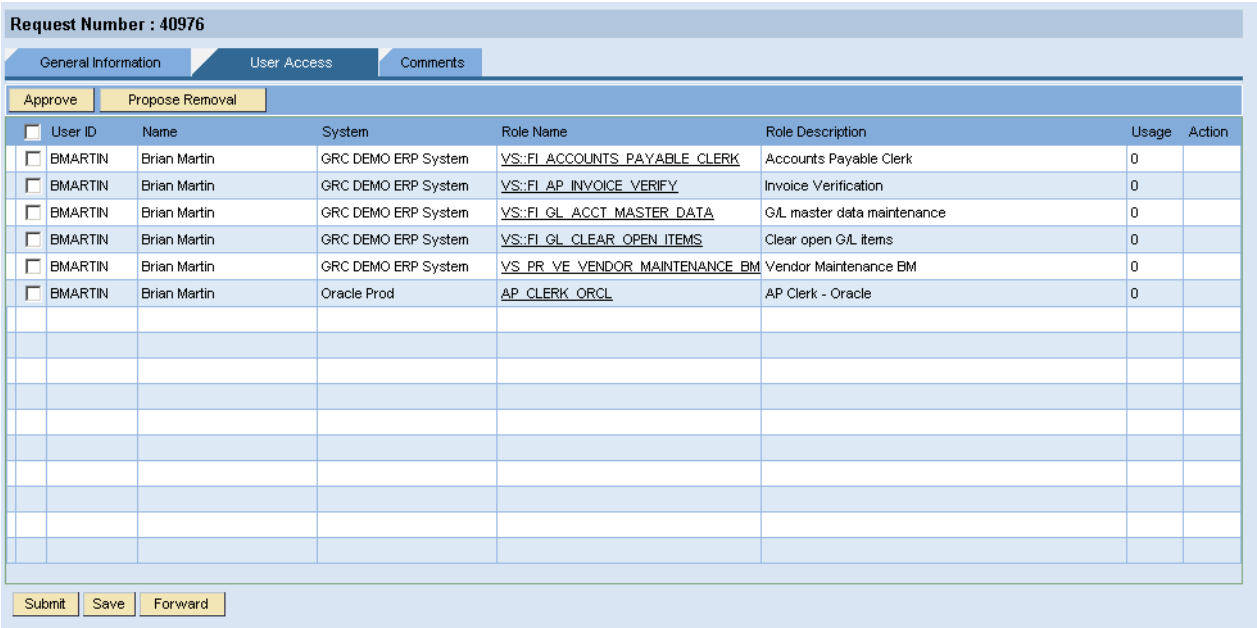
When the approver logs in to Access Control, the UAR requests for his approval will be in the *My Work* tab. The *User Name* column will be blank for UAR requests since there may be multiple users on each request.

The *General Information* tab of the UAR request will indicate the Reviewer and the Coordinator. The *Transaction Usage* will display the date range of data collected by the *Role Usage Synchronization* job. The *From* date for transaction usage is determined by the last *Purge Usage*

job executed in Risk Analysis and Remediation. The *To* date is determined by the last *Role Usage Synchronization* job execution in ERM or by the manually uploaded data.

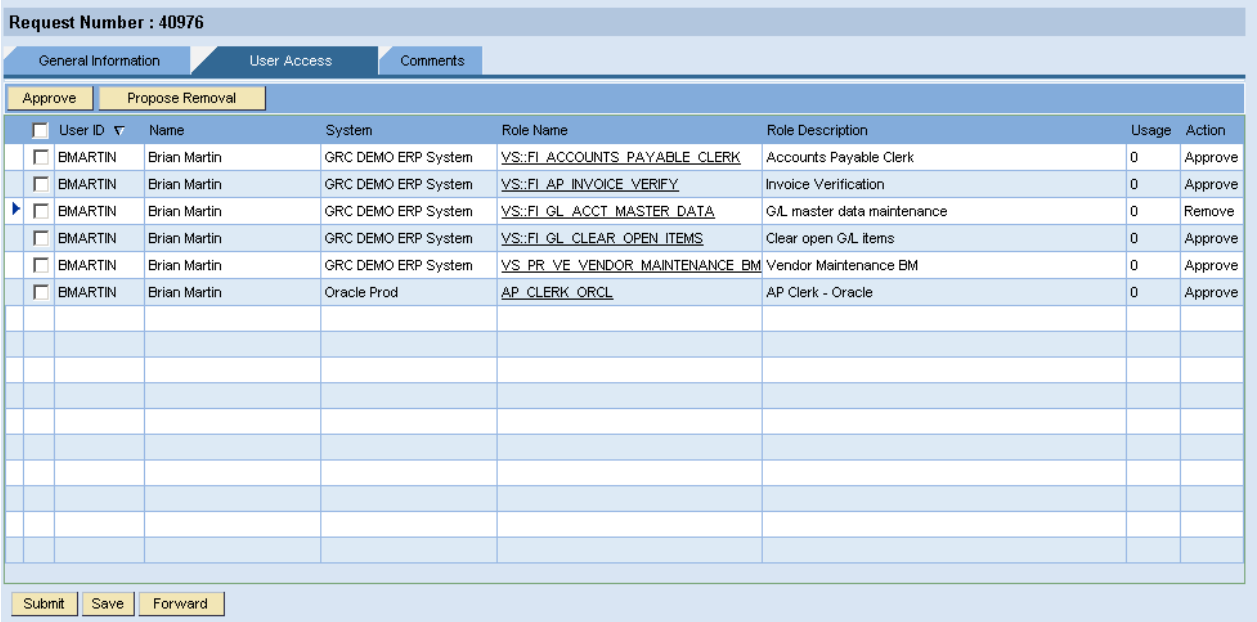
The *User* Access tab of the request will list the user being reviewed as well as the role and the usage information for the role. You may choose any column header to sort the request lines by that column.

Note: If you have selected items and decided an action, you should choose *Approve* or *Propose Removal* prior to sorting since sorting removes any selections that have not be updated in the *Action* column.



During the review of a user's access, you may view details of the role by selecting the role name in the request line item. The role details will be displayed and will include the actions currently defined in the role. Since the display of actions is real-time, the actions will not be displayed when the back-end system is unavailable.

The reviewer indicates which roles shall be retained and which shall be removed by selecting rows and choosing either *Approve* or *Propose Removal*. This causes the *Action* column to be updated. With each update of the action to be taken, the blue triangle denotes the item(s) just updated.



The reviewer may choose to *Save the* request multiple times to ensure work is saved in the request. The request will not be forwarded for the next action until the reviewer chooses *Submit* and then *Approve* to approve the recommendations for each request line item.

6.2.1.3 Submit Review

When all roles on the request have been reviewed and each row has been approved or marked for removal, the reviewer chooses *Submit* to complete his work. The request will continue to the next stage.

6.2.2 Managing Rejected Users

As of Support Package 06, the *Manage Rejected Users* process provides authorized users with the following functionality:

- Search for rejected users
- View search results and sort the results by user
- Generate review requests
- Cancel review request generation for those requests that have not been completed

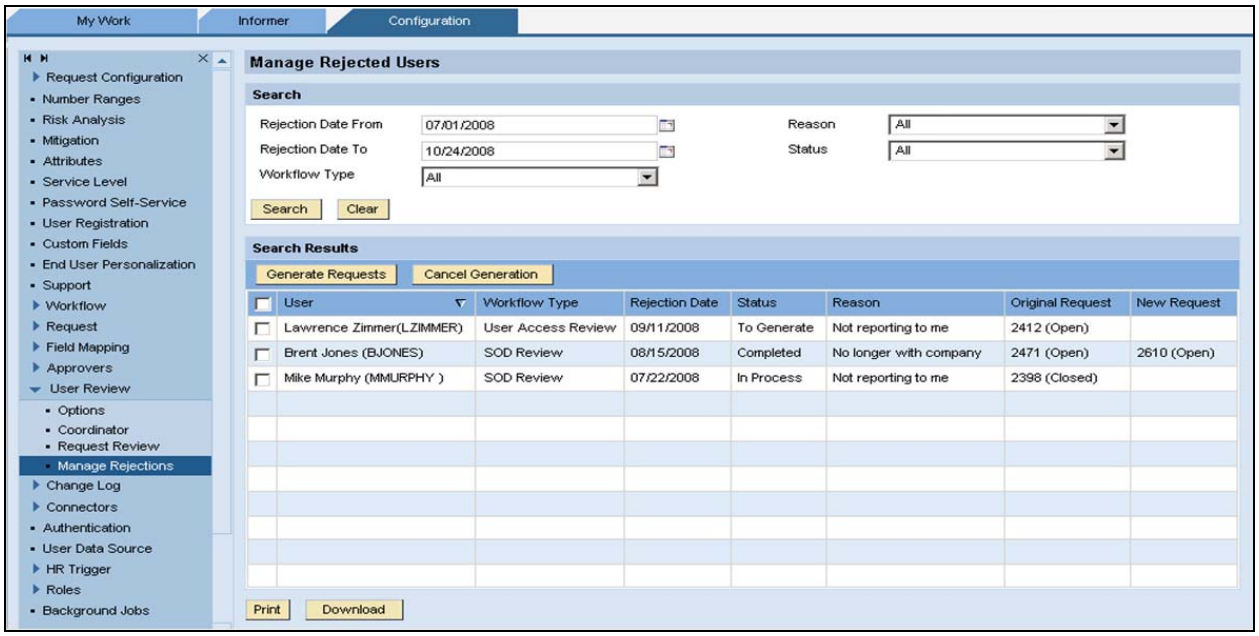
To access the screen, log on to *Configuration* > *User Review* > *Manage Rejections.*

6.2.2.1 Searching for Rejected Users

You can search using the following fields:

Field	Possible Values	Default Value
Rejection Date From	Any date	Current date
Rejection Date To	Any date	Current date
Note The *Rejection Date* is the date the rejected review request is submitted. If the reviewer rejects a request and only saves the request without submitting it, the user is not available on the screen above. For more information, see *Reviewer Rejects User in Request for Approval.*		
Workflow Type	• SOD Review • User Access Review	All
Reason	Any reason code for rejecting a user.	All
Status	• All • New • To Generate • In Process • Error • Completed	All

The rejected users resulting from the search are displayed.



The following columns are available:

Column	Description
User	You can sort the users by the User IDs.
Workflow Type	This column displays the related workflow type: SOD Review or User Access Review.
Rejection Date	This column displays the date the user is rejected.
Status	The following statuses are available: • **New** These are requests submitted by the reviewer. • **To Generate** The user is marked for re-generation, but the generation background job has not started. You can click **Cancel Generation** to cancel the request generation. • **In Process** The background generation job has started but has not completed. Requests with this status cannot be cancelled, because the background job has started. • **Error** The generation background job has encountered an error. • **Completed** The generation background job has completed. The new request number is updated.
Reason	This column displays the reason a user was rejected from the request.
Original Request	The column displays the original request number and request status for the rejected user.
New Request	The column displays the new request number and status for the rejected user.

6.2.2.2 Selecting Users for UAR Request Generation

Select user names from the *User* column and click *Generate Requests*. This action *marks* the user to be included on a new UAR request when the *UAR Review Process Rejected* background job is executed.

Recommendation

Before generating requests for the rejected users, make sure the users have the correct reviewer information. This will prevent incorrect information entering the request cycle again.

Example
If the reviewer information is stored in an LDAP data source and is incorrect, it must be updated in the LDAP data source so that new requests are generated with the correct reviewer name.

If the admin review option is set to *Yes*, the administrator can choose to modify the reviewer/coordinator information to correct the reviewer information. As of SP06, a request per user is generated for users without a manager in the data source when the *Reviewer* is set as the *Manager.*

6.2.2.3 Cancelling Request Generation

To cancel the request generation, select users from the *Users* column and click *Cancel Generation*.

You can choose to cancel a request generation. You can cancel the request generation for all users whose request status is *To Generate*. Once the request status is *In Process*, the background job has started and the request cannot be cancelled.

6.2.2.4 Generation New Requests for Rejected Users

To generate new requests for marked users:

1. *Go to* Configuration *tab* > Background Jobs. The Schedule Service screen appears.
2. In the *Task Name* dropdown menu, select *UAR Review Process Rejected*.
3. In the *Description* field, enter a brief description.
4. In the *Schedule Type* dropdown menu, select the time you wish to schedule this job. The corresponding *Task Occurrence* or *Recurrence* pane appears.
   a. In the Monthly Task Recurrence pane, enter the Time and Start Date.
   b. For *Immediate* schedule type, click *Run*.

6.2.3 Reminders

Reminders are sent as determined by configuration when the UAR request reviewers do not complete the review by the time specified. No change to the request or users occurs at reminder generation.

6.2.4 Escalation

Escalation will occur when a reviewer has not completed his review by the time specified in configuration. The escalation may include deactivating a user, de-provisioning roles and/or forwarding to the next stage.

6.2.5 Administrator Actions

Persons assigned the AE_Admin role can perform many actions for UAR requests. These actions include:

Specify reviewers during Admin Review

Modify Coordinators

Cancel requests

Indicate action to be taken for a user(s) on a UAR request (retain or remove access)

Forward a request to a new reviewer

6.3 Managing the Review Process – UAR Status Report

The *User Review Status Report* allows you to monitor UAR requests to ensure that the process is completed in a timely manner. This report will be very useful to coordinators or other persons overseeing the review process. You reach the User Access Review Status Report in CUP by navigating to the *Informer > Analysis View > Analytical Reports > User Review Status Report.* (This report was introduced in Support Package 05.)

6.3.1 User Review Status Report Purpose

The status report can be used to monitor the review process. It can be useful to administrators, coordinators, and management. Please note that a stage of a review is not considered complete until the reviewer has submitted the request.

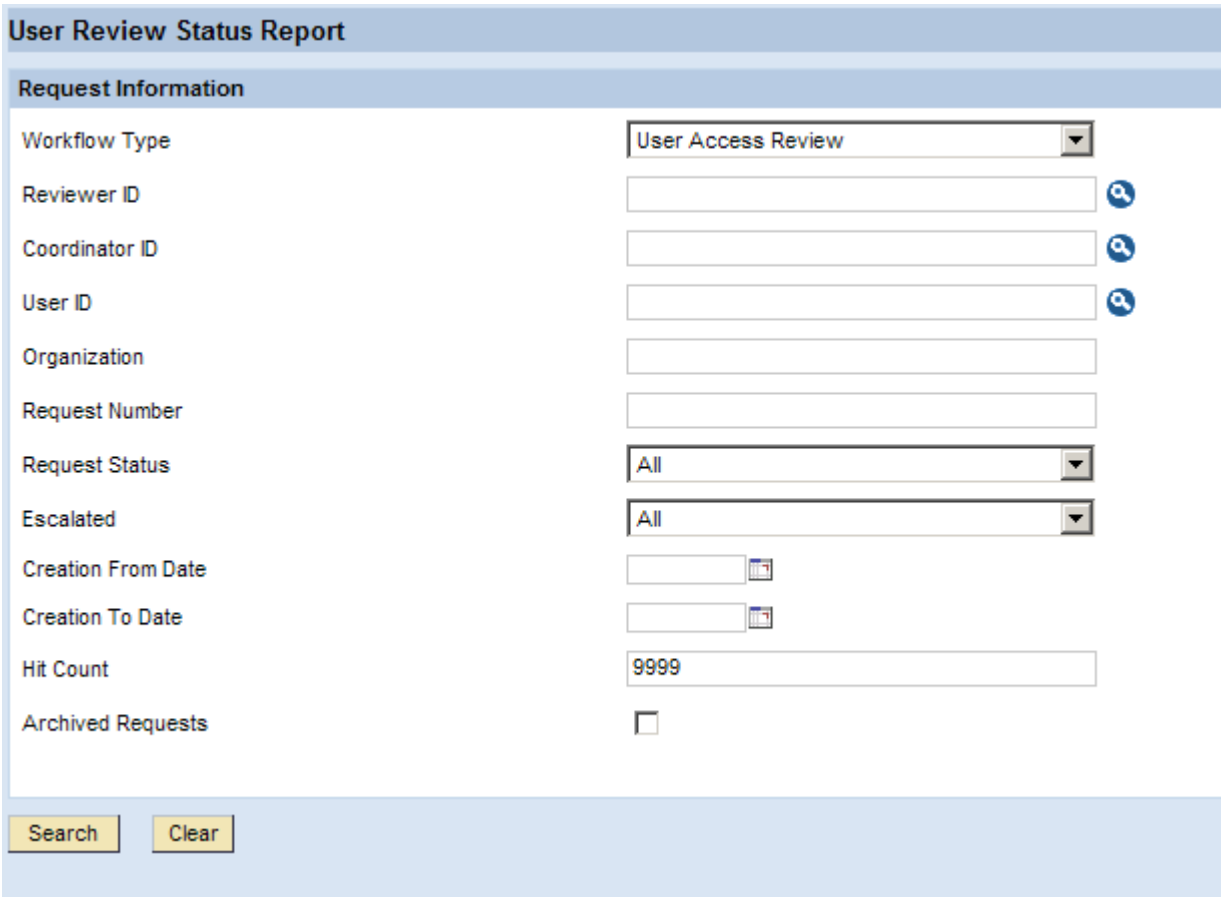
The User Access Review Status Report:

- Displays all requests, both complete and incomplete.
- Displays the detailed status of the request by user.
- Can be printed.

6.3.2 Selection Criteria

Shown below is the selection screen for the *User Review Status Report.*

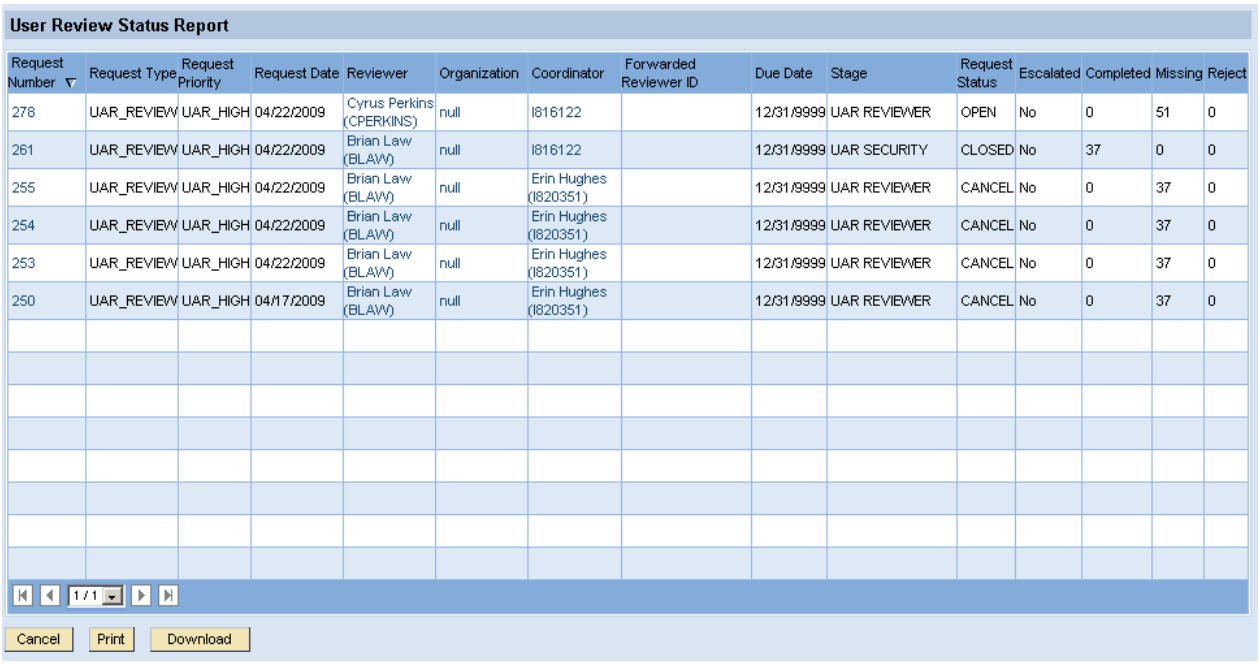
Select *Workflow Type* of *User Access Review.* You may filter results by other criteria, such as coordinator, reviewer, organization, or request status.



Note: Putting a “0” instead of the 9999 Hit Count will return all requests that meet your criteria.

6.3.3 Output

This is an example of the report output screen. You can see the current *Stage*, the number of items *Completed* in the request, *Reviewer,* and other helpful information.



User Review Status Report

Request Number	Request Type	Request Priority	Request Date	Reviewer	Organization	Coordinator	Forwarded Reviewer ID	Due Date	Stage	Request Status	Escalated	Completed	Missing	Reject
278	UAR_REVIEW	UAR_HIGH	04/22/2009	Cyrus Perkins (CPERKINS)	null	I816122		12/31/9999	UAR REVIEWER	OPEN	No	0	51	0
261	UAR_REVIEW	UAR_HIGH	04/22/2009	Brian Law (BLAW)	null	I816122		12/31/9999	UAR SECURITY	CLOSED	No	37	0	0
255	UAR_REVIEW	UAR_HIGH	04/22/2009	Brian Law (BLAW)	null	Erin Hughes (I820351)		12/31/9999	UAR REVIEWER	CANCEL	No	0	37	0
254	UAR_REVIEW	UAR_HIGH	04/22/2009	Brian Law (BLAW)	null	Erin Hughes (I820351)		12/31/9999	UAR REVIEWER	CANCEL	No	0	37	0
253	UAR_REVIEW	UAR_HIGH	04/22/2009	Brian Law (BLAW)	null	Erin Hughes (I820351)		12/31/9999	UAR REVIEWER	CANCEL	No	0	37	0
250	UAR_REVIEW	UAR_HIGH	04/17/2009	Brian Law (BLAW)	null	Erin Hughes (I820351)		12/31/9999	UAR REVIEWER	CANCEL	No	0	37	0

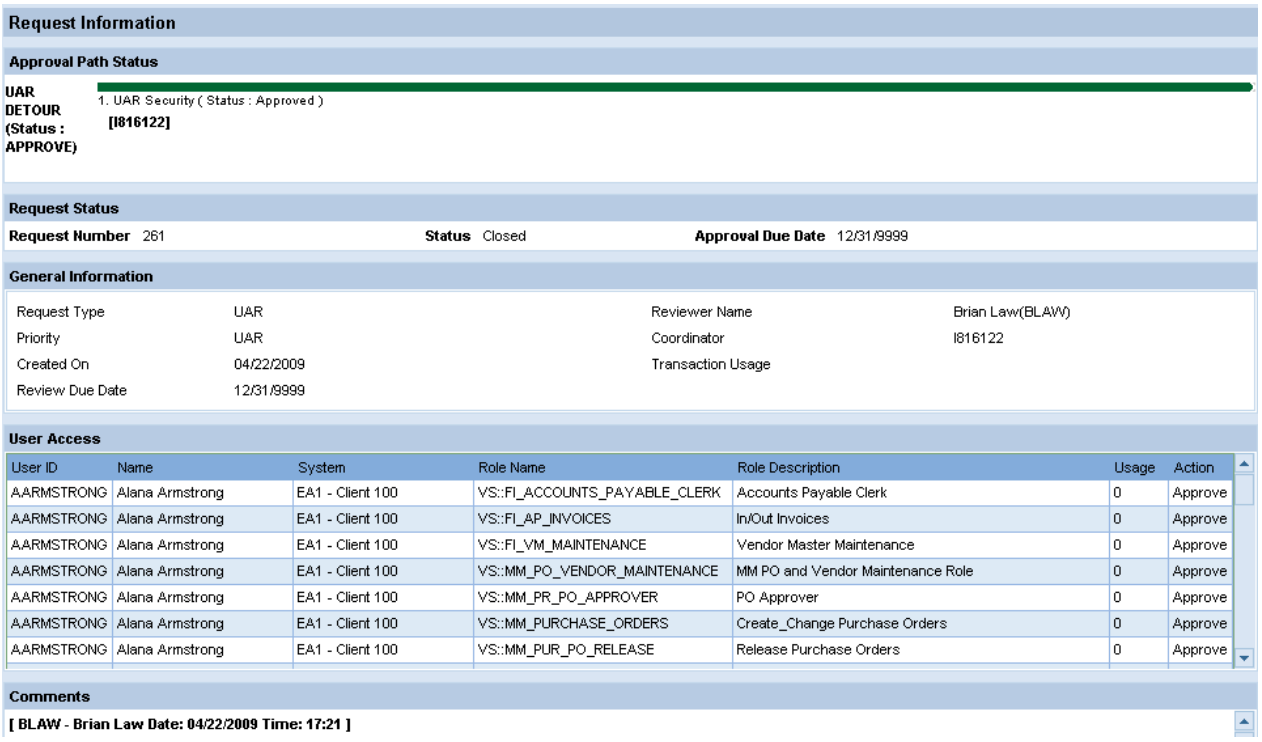
1 / 1

Cancel Print Download

6.3.3.1 Request Details

You can use the hyperlinks for *Request Number* to view the request. Using the scroll bar in the *User Access* pane allows you to scroll through the line items of the request and view the action indicated for each line.

- If the user is rejected and the review request is saved or submitted, all the line items for the user will have *Action* as **Reject**.
- If the request is escalated at any stage of the workflow, all line items in the request will have *Escalated* as **Yes**.



Request Information

Approval Path Status

UAR DETOUR (Status : APPROVE)

1. UAR Security (Status : Approved)
[I816122]

Request Status

Request Number 261 **Status** Closed **Approval Due Date** 12/31/9999

General Information

Request Type	UAR	Reviewer Name	Brian Law(BLAW)
Priority	UAR	Coordinator	I816122
Created On	04/22/2009	Transaction Usage	
Review Due Date	12/31/9999		

User Access

User ID	Name	System	Role Name	Role Description	Usage	Action
AARMSTRONG	Alana Armstrong	EA1 - Client 100	VS::FI_ACCOUNTS_PAYABLE_CLERK	Accounts Payable Clerk	0	Approve
AARMSTRONG	Alana Armstrong	EA1 - Client 100	VS::FI_AP_INVOICES	In/Out Invoices	0	Approve
AARMSTRONG	Alana Armstrong	EA1 - Client 100	VS::FI_VM_MAINTENANCE	Vendor Master Maintenance	0	Approve
AARMSTRONG	Alana Armstrong	EA1 - Client 100	VS::MM_PO_VENDOR_MAINTENANCE	MM PO and Vendor Maintenance Role	0	Approve
AARMSTRONG	Alana Armstrong	EA1 - Client 100	VS::MM_PR_PO_APPROVER	PO Approver	0	Approve
AARMSTRONG	Alana Armstrong	EA1 - Client 100	VS::MM_PURCHASE_ORDERS	Create_Change Purchase Orders	0	Approve
AARMSTRONG	Alana Armstrong	EA1 - Client 100	VS::MM_PUR_PO_RELEASE	Release Purchase Orders	0	Approve

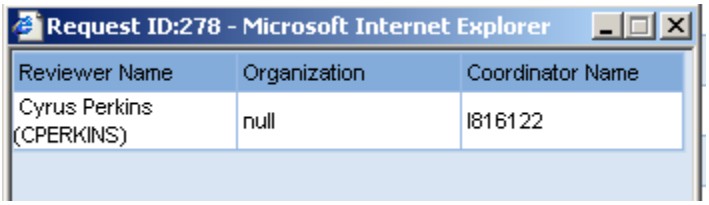
Comments

[BLAW - Brian Law Date: 04/22/2009 Time: 17:21]

Choose *Cancel* to return to the report output.

6.3.3.2 Reviewer Details

You can use the hyperlinks for *Reviewer, Organization,* or *Coordinator to* view details of the reviewer.



Request ID:278 - Microsoft Internet Explorer

Reviewer Name	Organization	Coordinator Name
Cyrus Perkins (CPERKINS)	null	I816122

7. Audit/Reporting

The User Access Review process provides helpful information for requests or items on requests that are complete. The *User Access Review History Report* shows the actions taken for requests in the user review process. The audit trail of a request shows the detail of the activity taken for the request.

7.1 UAR History Report

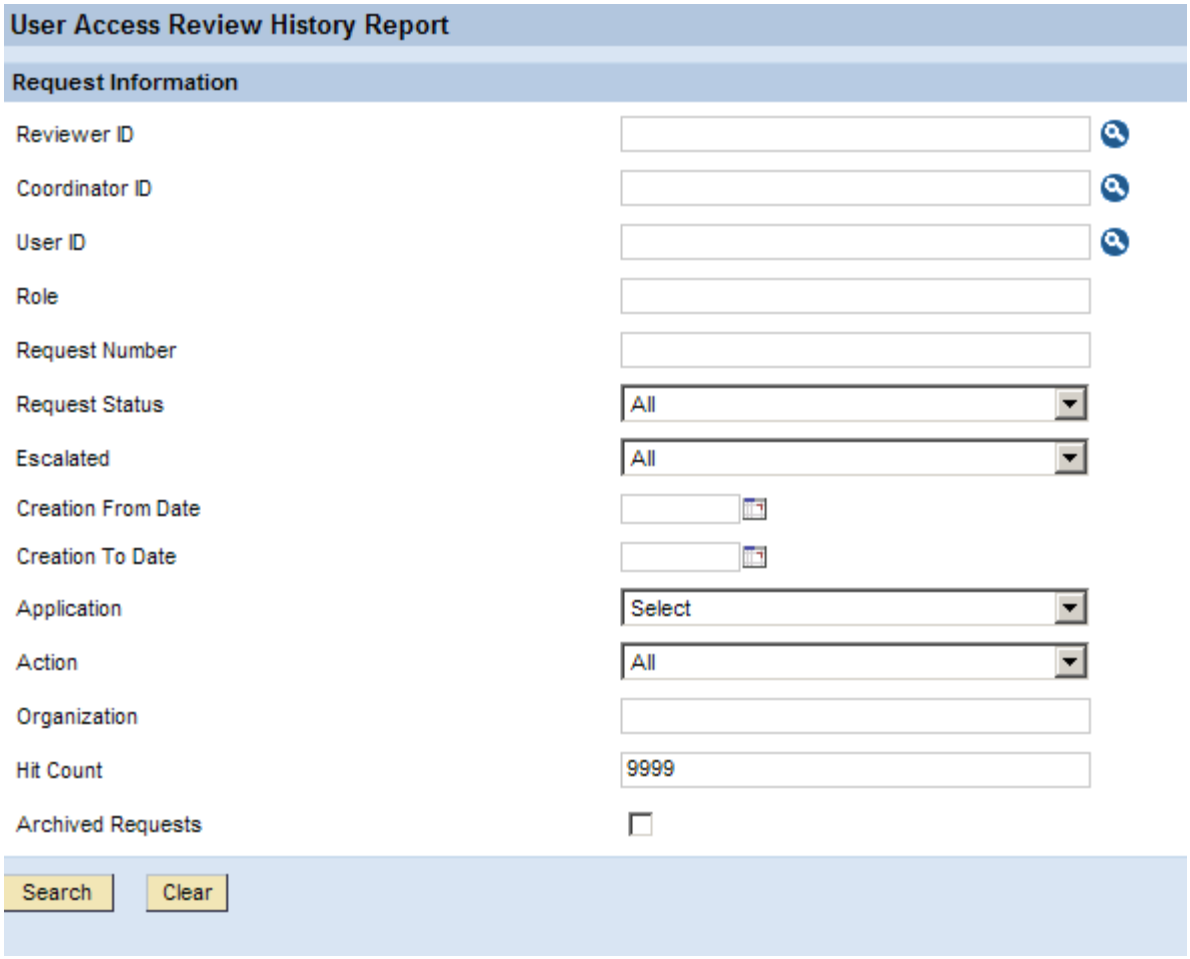
Navigate to *Informer > Analysis View > Analytical Reports > User Access Review History Report.*

7.1.1 Purpose

This report shows the history of activity for UAR requests. This is most helpful after a portion of the review process or the entire review process is complete.

7.1.2 Selection Criteria

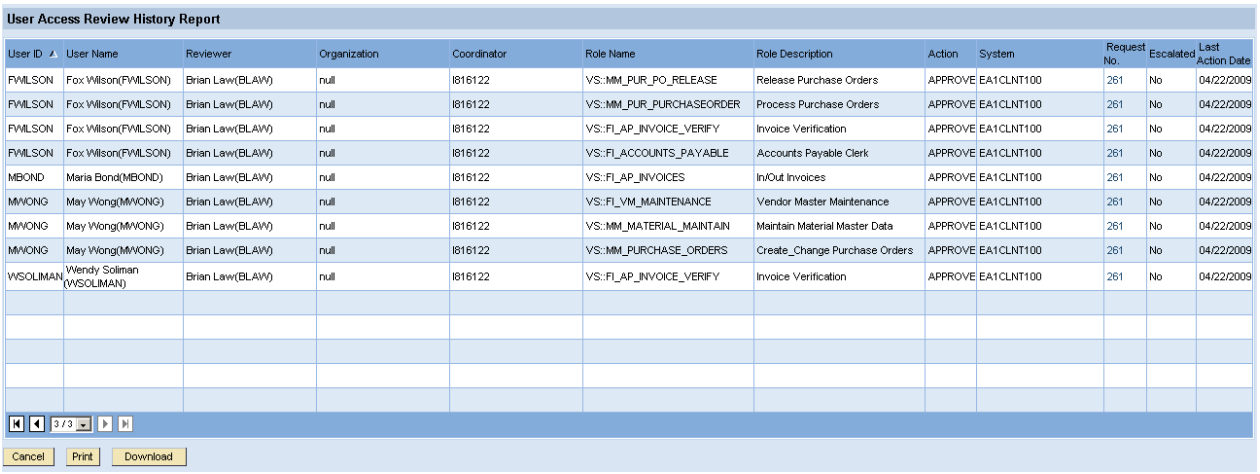
Shown below is the selection screen for the User Access Review History Report. You may filter the requests by multiple criteria, including coordinator and status. You may also filter the report to show only rejected items by choosing the Action of Reject.



Note: Putting a “0” instead of the 9999 Hit Count will produce ALL requests.

7.1.3 Output

Shown below is an example of the report output. You may sort the columns by clicking the column header.



User Access Review History Report

User ID	User Name	Reviewer	Organization	Coordinator	Role Name	Role Description	Action	System	Request No.	Escalated	Last Action Date
FWILSON	Fox Wilson(FWILSON)	Brian Law(BLAW)	null	I816122	VS::MM_PUR_PO_RELEASE	Release Purchase Orders	APPROVE	EA1CLNT100	261	No	04/22/2009
FWILSON	Fox Wilson(FWILSON)	Brian Law(BLAW)	null	I816122	VS::MM_PUR_PURCHASEORDER	Process Purchase Orders	APPROVE	EA1CLNT100	261	No	04/22/2009
FWILSON	Fox Wilson(FWILSON)	Brian Law(BLAW)	null	I816122	VS::FI_AP_INVOICE_VERIFY	Invoice Verification	APPROVE	EA1CLNT100	261	No	04/22/2009
FWILSON	Fox Wilson(FWILSON)	Brian Law(BLAW)	null	I816122	VS::FI_ACCOUNTS_PAYABLE	Accounts Payable Clerk	APPROVE	EA1CLNT100	261	No	04/22/2009
MBOND	Maria Bond(MBOND)	Brian Law(BLAW)	null	I816122	VS::FI_AP_INVOICES	In/Out Invoices	APPROVE	EA1CLNT100	261	No	04/22/2009
MWONG	May Wong(MWONG)	Brian Law(BLAW)	null	I816122	VS::FI_VM_MAINTENANCE	Vendor Master Maintenance	APPROVE	EA1CLNT100	261	No	04/22/2009
MWONG	May Wong(MWONG)	Brian Law(BLAW)	null	I816122	VS::MM_MATERIAL_MAINTAIN	Maintain Material Master Data	APPROVE	EA1CLNT100	261	No	04/22/2009
MWONG	May Wong(MWONG)	Brian Law(BLAW)	null	I816122	VS::MM_PURCHASE_ORDERS	Create_Change Purchase Orders	APPROVE	EA1CLNT100	261	No	04/22/2009
WSOLIMAN	Wendy Soliman (WSOLIMAN)	Brian Law(BLAW)	null	I816122	VS::FI_AP_INVOICE_VERIFY	Invoice Verification	APPROVE	EA1CLNT100	261	No	04/22/2009

3 / 3

Cancel Print Download

7.1.3.1 Request Details

You can use the hyperlinks for *Request Number* to view the request. Using the scroll bar in the *User Access* pane allows you to scroll through the line items of the request and view the action indicated for each line.

- If the user is rejected and the review request is saved or submitted, all the line items for the user will have *Action* as **Reject**.
- If the request is escalated at any stage of the workflow, all line items in the request will have *Escalated* as **Yes**.

Choose *Cancel* to return to the report output.

7.2 Request Audit Trail

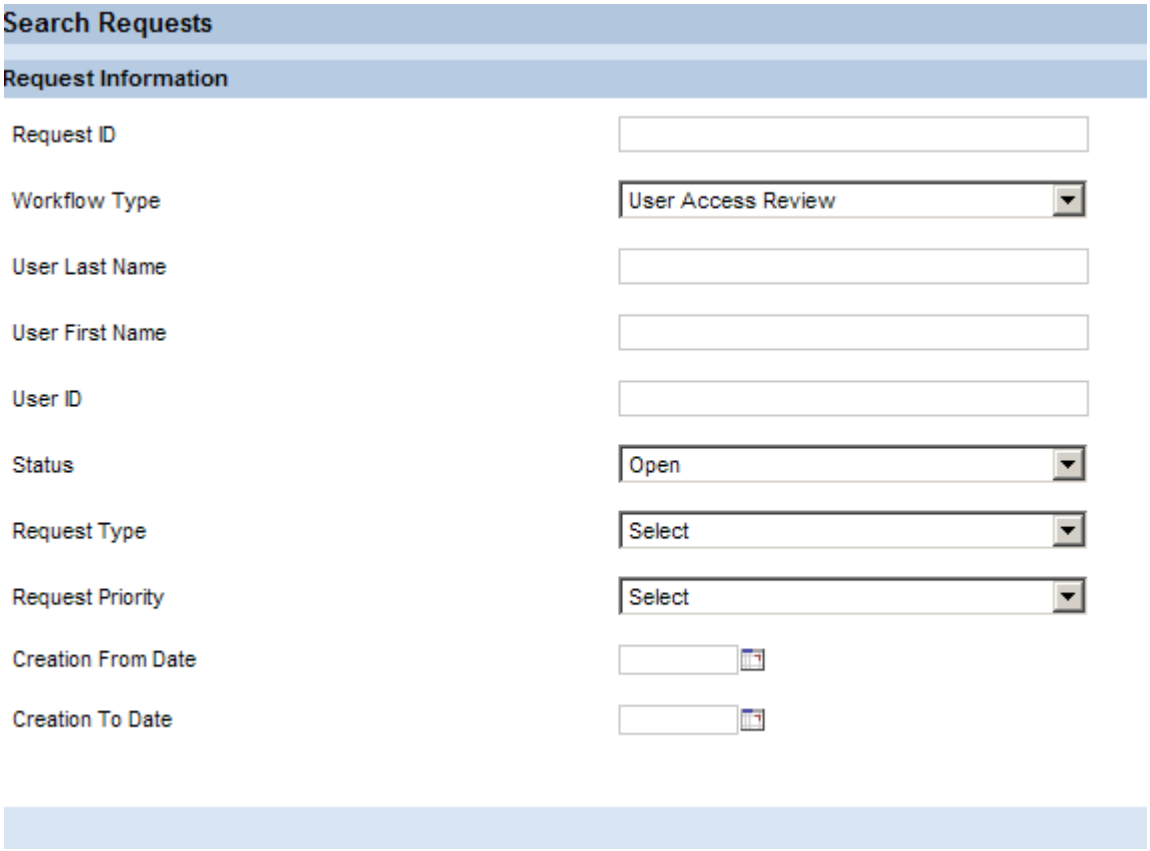
You can view the audit trail of a particular request to see the detailed activity in the life of the request. Navigate to *My Work → Request Audit Trail*

7.2.1 Purpose

This information is very helpful to internal or external auditors. It is also helpful to member of the review team when investigating specific roles or users.

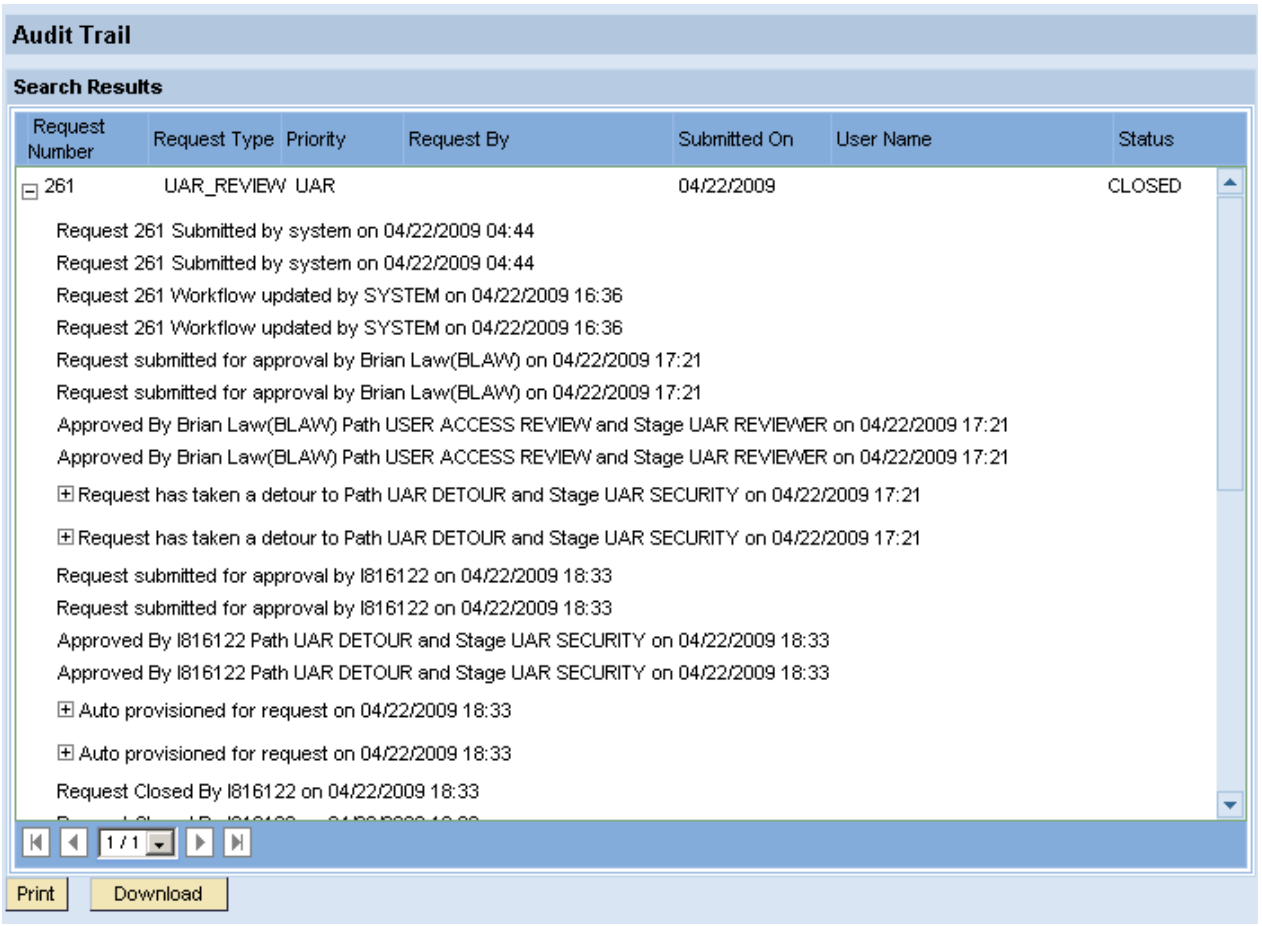
7.2.2 Selection Criteria

Shown below is the selection screen for searching requests. You may enter a specific request ID or choose Workflow Type of User Access Review. You may filter results by other criteria, such as coordinator, reviewer, organization, or request status.



7.2.3 Output

The *Audit Trail* shows the history of the report from request creation through closure. It may be printed or downloaded.



8. Appendix – CUP Role Import/Export Template

8.1 Procedure

You can download a spreadsheet (.xls) template to your local system to use for importing roles. After downloading the spreadsheet, populate the fields with your own roles, and then import the information.

Recommendation

SAP strongly recommends that you edit the downloaded template with your additional roles. Use the data format of the values represented in the dummy role. However, you must delete the dummy role in the template before using it. Do not modify the sheet name and header names.

Business process, sub process, functional area, company, and system must exist in Compliant User Provisioning before the roles can be successfully uploaded. If they do not exist, attempting to import them fails. These attributes are added through the *Roles* > *Attributes* screen.

To download the role import template:

1. Click *Download Template,* and then click *Save* to save the template to your system.

   Be sure to save the template in a location where it is for you to find later.

2. Open the template, and enter values for the roles you want to import.

   For more information, see Role Import/Export Template Details.

3. Save and close the template with the new information.

Now you can import the role information. For more information on importing roles, see Importing Roles.

8.2 Role Import/Export Template Details

The following table describes the items in the import template spreadsheet.

Role Import Template Spreadsheet			
Role Import Column	**Description**	**Mandatory**	**Case-Sensitive**
Connector Type	Name of the Connector Type. Only one connector type is allowed.	Yes	Yes – upper case letters
RoleName	Technical name of the role.	Yes	Yes
Type	Select *Single* or *Composite*. Only one value is allowed.	Yes	No
Last Reaffirm Date	Date of the role's last reaffirm. Required format is MM/DD/YY.	Yes	MM/DD/YY
System	Technical name of the system in which the role resides. System must exist as a connector. List as many systems as you want, separated by commas.	Yes – at least one system is required	Yes – upper case letters

Role Import Template Spreadsheet			
Role Import Column	**Description**	**Mandatory**	**Case-Sensitive**
RoleApprover	User ID of the role's approvers. Several role approvers might be included, separated by commas. Alternate approvers follow the approver and are separated by a pipe symbol (|). Lead Approver designation follows the alternate approver separated by a pipe symbol (|). Format: Roleappr|alternative|Y,roleapprover|alternate Example: WONG|BLAW|Y,CPERKINS MWONG is the role approver, BLAW is MWONG's alternate approver, and MWONG is the Lead Approver. CPERKINS is the second role approver, no alternate and is not the lead approver.	No	No
Functional Area	Functional area of the role. This is the technical name of the functional area, and it must expire in the system before the role is uploaded successfully. Several functional areas are permitted, separated by commas.	Yes – at least one functional area is required	Yes
Company	Company associated with the role. This is the technical name of the company, and it must expire in the system before the role is uploaded successfully. Several companies are permitted, separated by commas	Yes – at least one Company is required	Yes
RoleProfileIndicator	Options are either *Role* or *Profile*.	Yes	No
Responsibilityid	This field is no longer used as part of Compliant User Provisioning but it remains in the template for backward compatibility. It is a number used to represent the responsibility ID. Enter zero if not using this functionality.	Yes – use a zero if not using this functionality	N/A
Comments Mandatory	Options are *Yes* or *No*.	Yes	Yes – use upper case letters *Yes* or mixed *Yes*.

Role Import Template Spreadsheet			
Role Import Column	**Description**	**Mandatory**	**Case-Sensitive**
ParentRoleOwner	This field is no longer used as part of Compliant User Provisioning but it remains in the template for backward compatibility. Options are *Yes* or *No*. Select *No,* if not using this functionality.	Yes Choose No if not using this functionality	No
Description_de	German short description. Required only if your users want to use Access Control in German.	No	No
DetailDescription_de	German detail. Required only if your users want to use Access Control in German.	No	No
Description_hu	Hungarian short description. Required only if your users want to use Access Control in Hungarian.	No	No
DetailDescription_hu	Hungarian detail description. Required only if your users want to use Access Control in Hungarian.	No	No
Description_ja	Japanese short description. Required only if your users want to use Access Control in Japanese.	No	No
DetailDescription_ja	Japanese detail description. Required only if your users want to use Access Control in Japanese.	No	No
Description_it	Italian short description. Required only if your users want to use Access Control in Italian.	No	No
DetailDescription_it	Italian detail description. Required only if your users want to use Access Control in Italian.	No	No
Description_ es	Spanish short description. Required only if your users want to use Access Control in Spanish.	No	No
DetailDescription_es	Spanish detail description. Required only if your users want to use Access Control in Spanish.	No	No

Role Import Template Spreadsheet			
Role Import Column	**Description**	**Mandatory**	**Case-Sensitive**
Description_pt	Portuguese short description. Required only if your users want to use Access Control in Portuguese.	No	No
DetailDescription_pt	Portuguese detail description. Required only if your users want to use Access Control in Portuguese.	No	No
Description_en	English short description. Required only if your users want to use Access Control in English.	No	No
DetailDescription_en	English detail description. Required only if your users want to use Access Control in English.	No	No
Description_fr	French short description. Required only if your users want to use Access Control in French.	No	No
DetailDescription_fr	French detail description. Required only if your users want to use Access Control in French.	No	No
BusinessProcess	The technical name of the business process. It must exist in the system before the role is uploaded successfully. Only one business process is allowed per role.	Yes	Yes – use upper case letters
SubProcess	The technical name of the sub process. It must exist in the system and be assigned to the business process listed in the *Business Process* column on this spreadsheet before the role is uploaded successfully. Only one sub process is allowed per role.	Yes	Yes – use upper case letters
CriticalLevel	Options are *Critical*, *High*, *Medium*, and *Low*.	Yes	No – Suggest using mixed-case letters as displayed in the description column
ReaffirmPeriod	The number of months that a role needs to be reaffirmed. For example, enter a reaffirm period of one year or 12 months as **12**.	Yes	N/A – enter a number

Role Import Template Spreadsheet			
Role Import Column	**Description**	**Mandatory**	**Case-Sensitive**
Custom Attributes (Custom Fields for the Role)	This column contains all custom role attributes for the role.	No	N/A
Verification Training System	This column contains all system names for your verification/training system.	No	Yes, use upper case letters

For more information, or for information on changing existing CUP roles with the spreadsheet, see the *AC 5.3 Configuration Guide.*

9. Related Content

Access Control 5.3 Configuration Guide

Access Control 5.3 Security Guide

Access Control 5.3 Application Help

Access Control 5.3 SP06 Supplemental Note 1292484

10. Feedback

Your feedback regarding this document is important to us. Please send comments to the following email address. GRC_CAO_Access_Control@sap.com

11.Copyright