SAP GRC Access Control: Offline-Mode Risk Analysis

Applies to:

This document applies to the SAP GRC Access Control Suite. The document explains in detail how to use risk analysis and remediation **to perform offline-mode risk analysis** in SAP GRC Access Control.

Summary

Risk analysis may be performed in offline-mode. This process helps in detection of SOD violations in an ERP System without an online connection. Data from an ERP system is exported to files and may subsequently be imported into to GRC Access Control by using the data extractor utility.

Author: Alpesh Parmar, Aman Chuttani

Company: SAP

Created on: 22 January, 2008

Author Bio

Alpesh Parmar is a principal consultant at SAP's Regional Implementation Group for Governance, Risk, and Compliance. He is an expert in GRC Access Control and was instrumental in many successful Access Control ramp-up implementations. Before his current assignment Alpesh was part of the Access Control development team.

Aman Chuttani is a consultant at SAP's RIG for Governance, Risk and Compliance (GRC). He has gained extensive experience supporting SAP's customers in the implementation of SAP GRC Access Control.

Table of Contents

Introduction

Offline Mode Risk Analysis process is performed with the help of Risk Identification and Remediation (formerly known as Virsa Compliance Calibrator (CC)) module in SAP GRC Access Control Suite. This process helps in identifying SOD Violations in an ERP System remotely. The data from ERP system is exported to flat files and then it can be imported into the CC instance with the help of data extractor utility. It can also be used to remotely analyze an ERP system which may be present in a different ERP Landscape.

This process accounts some sub-processes which are to be followed in order, so that we can achieve a successful completion of a Remote Risk Assessment (RRA).

The various processes being followed in RRA process are

ERP Extraction

Generating Auth Objects and Text Objects For ERP

Generating User and Role Data for ERP

Configuring Risk Identification and Remediation

Uploading Auth objects and Text Objects

Rule Data upload

Rule Generation

Data Extraction Module

Extracting User Data

Extracting Role Data

Risk Analysis and Reports

Risk Analysis

Management Report Generation

Besides, one also has to keep a close watch on the Background Jobs Scheduled.

ERP Extraction

This is the foremost process which has to be followed in order to start the Offline Mode Risk Analysis process. This includes extracting the data from ERP system tables. This includes downloading ERP Authorization Objects, Users and Role Data from ERP tables. Please follow the following format while downloading the ERP data.

Generating Object Files

In Download Objects we will download ERP Authorization Objects and Description of the objects from ERP system. This is a one time process for a particular system.

Generating ERP Authorization Objects

Authorization Objects should be generated from the target ERP system with the following format. It is **recommended** that the downloaded data is stored as text files and should be tab-delimited files and records per file should be about 60000.

Field	Data Field Type	Field Size	Field Values	Sorting	Required	Description	Transformation Rules
ACTION	String	20	CAPS	Sorted Ascending, Sort Order 1	Yes	Action	
PERMISSION	String	10	CAPS	Sorted Ascending, Sort Order 2	Yes	Permission	
ACTVT	String	10	CAPS		Yes	Permission Object Field	
FROMVALUE	String	50	CAPS		Yes	Permission Object Field Value	
TOVALUE	String	50	CAPS		No	Permission Object Field Value	If this value does not exist for source system, leave blank.

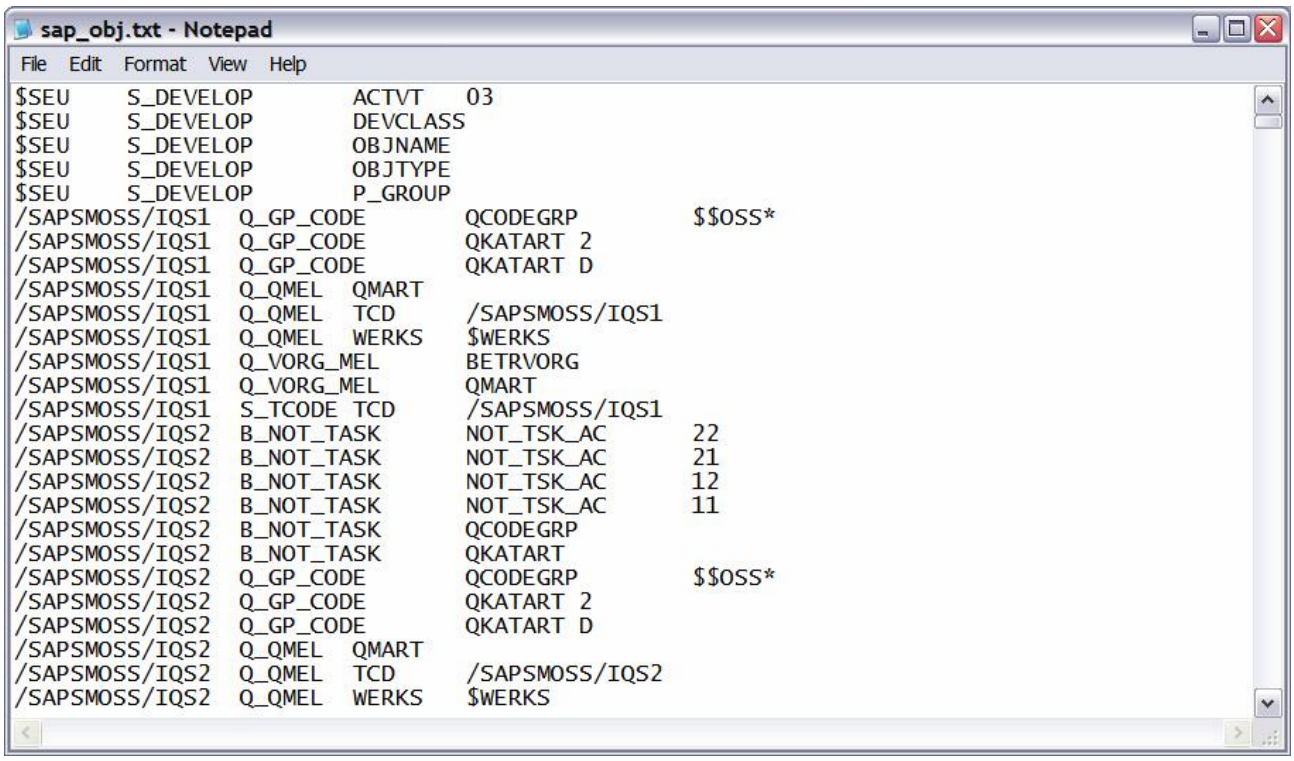
ACTION/TCODE

PERMISSION

ACTVT

FROMVALUE

TOVALUE



Generating ERP Description Objects

Authorization Description should be generated from the target ERP with the following format. It is **recommended** that the downloaded data is stored as text files and should be tab-delimited files and records per file should be about 60000.

Field	Data Field Type	Field Size	Field Values	Sorting	Required	Description	Transformation Rules
Leave Blank						Mandatory field, Required by load format	Leave Blank
"PRM"		3	CAPS			Hard code "PRM" as value for this field	Hard coded value PRM
Leave Blank						Mandatory field, Required by load format	Leave Blank
PERMISSION	String	50	CAPS		Yes	Permission	Sorted Ascending
"EN"		2	CAPS			Hard code "EN" as value for this field	Hard coded value EN
PERMISSION	String	<100			Yes	Permission	

DESCRIPTIONS						Description	

<blank>

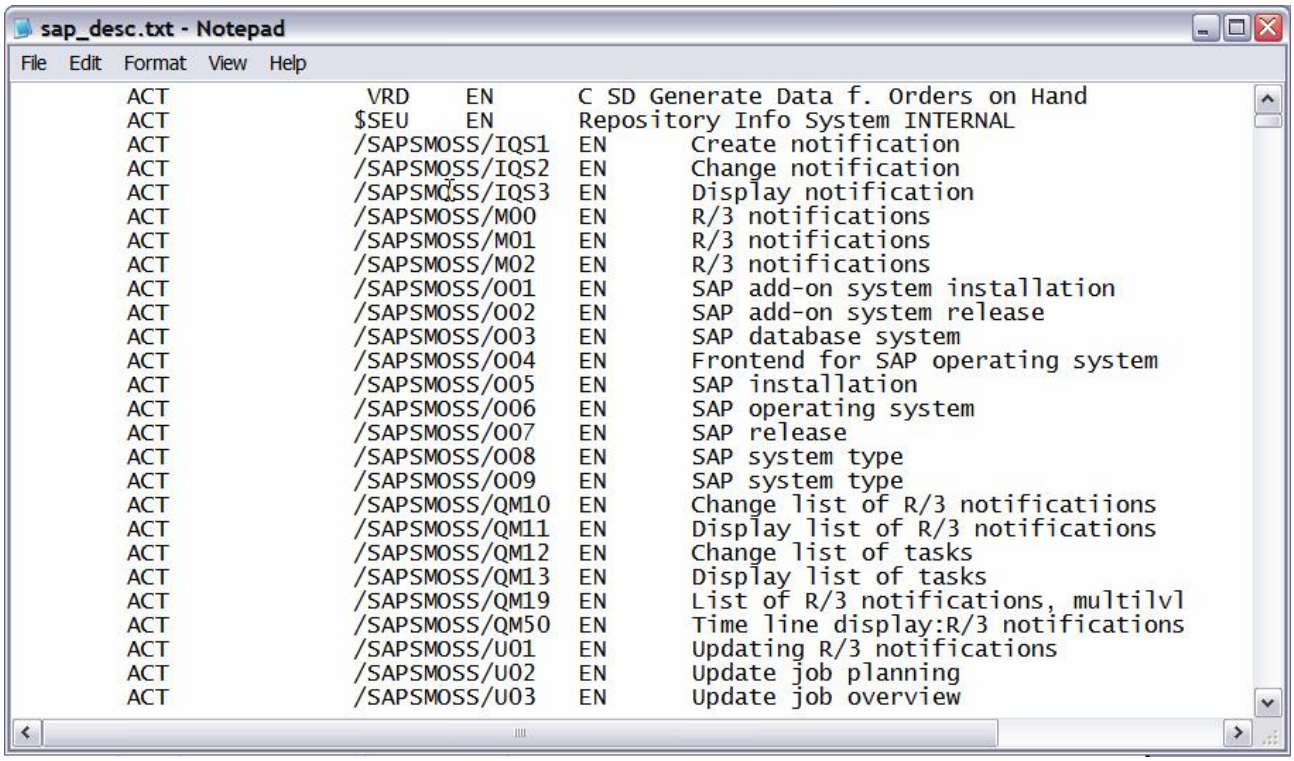
ERP Object Type

<blank>

ERP Object Key

ERP Object Language

ERP Object Text Description



Once the objects have been saved on the local system the next task will be to upload the objects onto the J2EE Application.

Extracting Data from ERP System

This process helps in retrieving data from the ERP system about the user and roles as well as their authorizations.

User Data Extraction

In User Data Extraction process we will be downloading user details, user actions and user permissions assigned to the user through roles from the back-end ERP system. Data will be downloaded into separate text files in the format mentioned below.

Extracting User Information

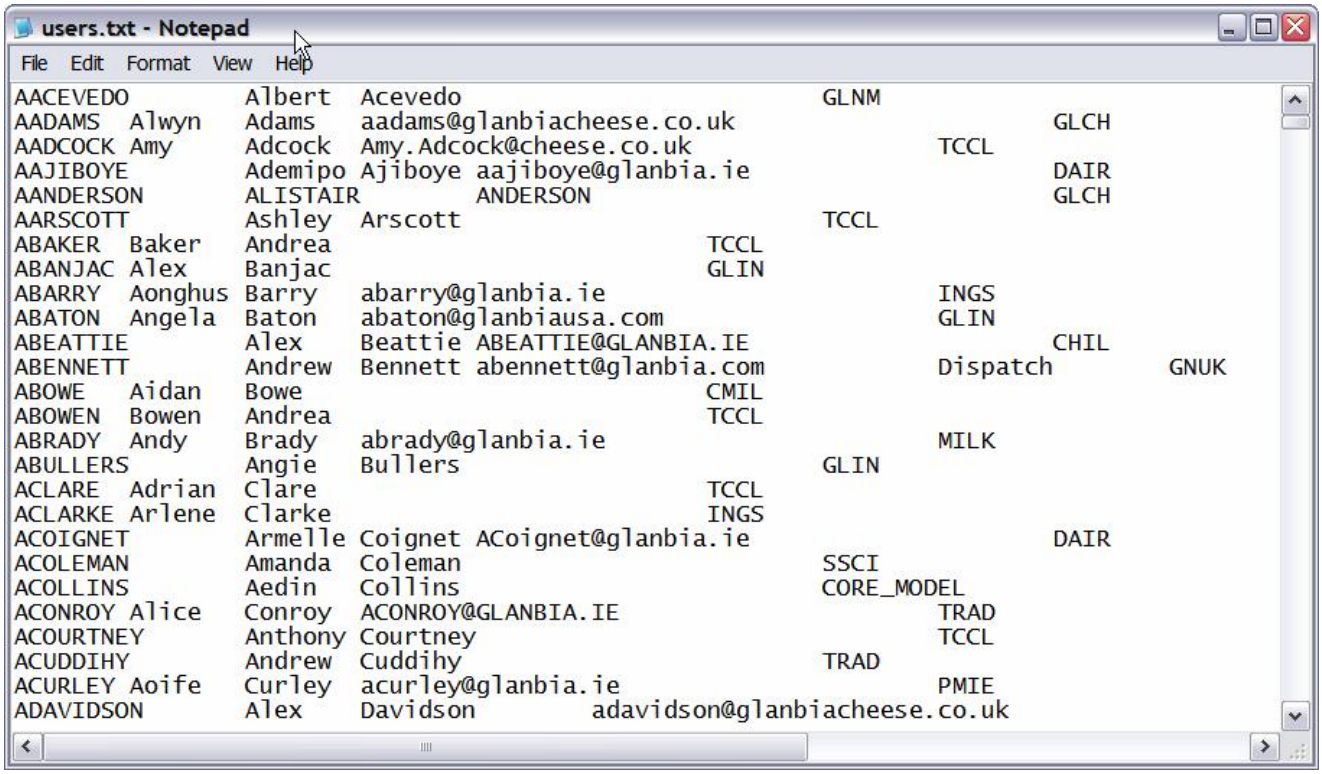
In User Extract we will download user information and should include the following information of the user.

Field	Data Field Type	Field Size	Field Values	Sorting	Required	Description	Transformation Rules
USREID	String	50	CAPS	Sorted Ascending	Yes	User ID	Unique records only
FNAME	String	50			Yes	First Name (if not available, repeat User ID field here)	
LNAME	String	50			Yes	Last Name (if not available, repeat User ID field here)	
EMAIL	String	250			No	Email address	
PHONE	String	40			No	Phone # - leave blank if not available	
DEPARTMENT	String	40			No	Department	
USERGROUP	String	20	CAPS		No	User Group - leave blank if not available	

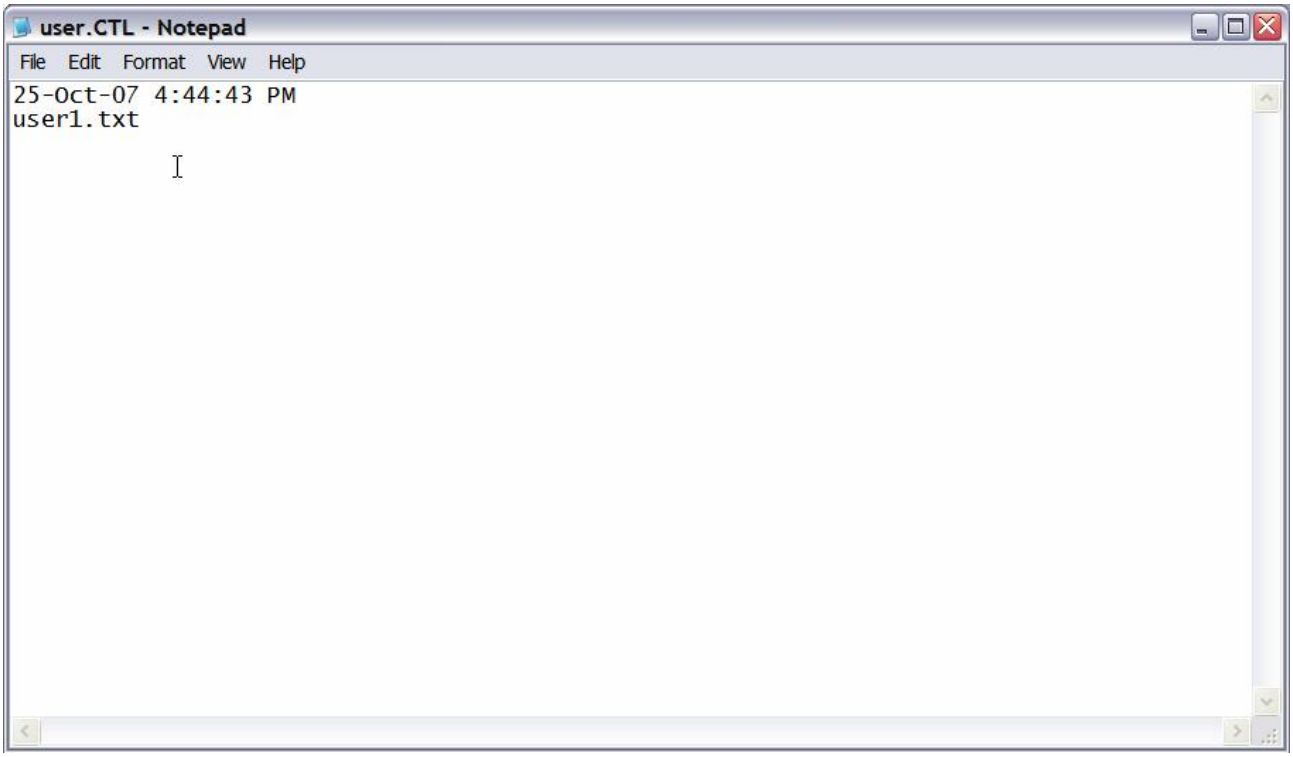
USERID - User ID with which users login to the system
FNAME - User First Name.
LNAME - User Last Name.
EMAIL - E-mail of the User
PHONE - Phone Number of User
DEPARMENT - Department of User.
USERGROUP - User Group of User.

Following are important points to be noted while downloading and formatting of User files:

“USERID” (User ID) field should be unique and should be “NOT NULL”.
There should not be any duplicate record in the file(s) (combination of all field columns in the file).
There should not be any blank records at the end of the file.



It is **recommended** that the downloaded data is stored as text files and should be tab-delimited files and records per file should be about 60000. Sometimes the extraction data can take up more than one file. Incase of multiple text files, we recommend customers to create a “Control (.CTL)” file having information of multiple text files. Following is a screen shot of control file having User files.



Extracting User Actions

In User Action Extract we will download actions assigned to users through roles and files should have following information of user actions.

Field	Data Field Type	Field Size	Field Values	Sorting	Required	Description	Transformation Rules
USERID	String	50	CAPS	Sorted Ascending, Sort Order 1	Yes	User ID	Unique record = The combination of (USERID / ROLES / TCODEFROM) has to be unique.
ROLES	String	49	CAPS	Sorted Ascending, Sort Order 2	Yes	Access Role Name	
ACTIONFROM	String	50	CAPS	Sorted Ascending, Sort Order 3	Yes	User Action	
ACTIONTO	String	50	CAPS		Yes	User Action, only applicable if User Action has range	If this value does not exist for source system, leave blank.

						From/To	
PROFILE	String	50	CAPS		Yes	Action Profile, if applicable. If not, repeat Role Name field.	If this value does not exist for source system, repeat ROLE field from column 2.
COMPOSITE ROLENAME	String	50	CAPS		No	Composite role name, leave blank if not available	If this value does not exist for source system, leave blank.

USERID - User ID with which users login to the system

ROLES - Roles/Responsibilities assigned to user

ACTIONFROM - Transactions/Actions from value assigned in each role

ACTIONTO - Transactions/Actions to value assigned in each role

PROFILE - Profile of associated Role.

COMPOSITE ROLENAME - Composite Role Name

Following are important points to be noted while downloading and formatting of User Action files:

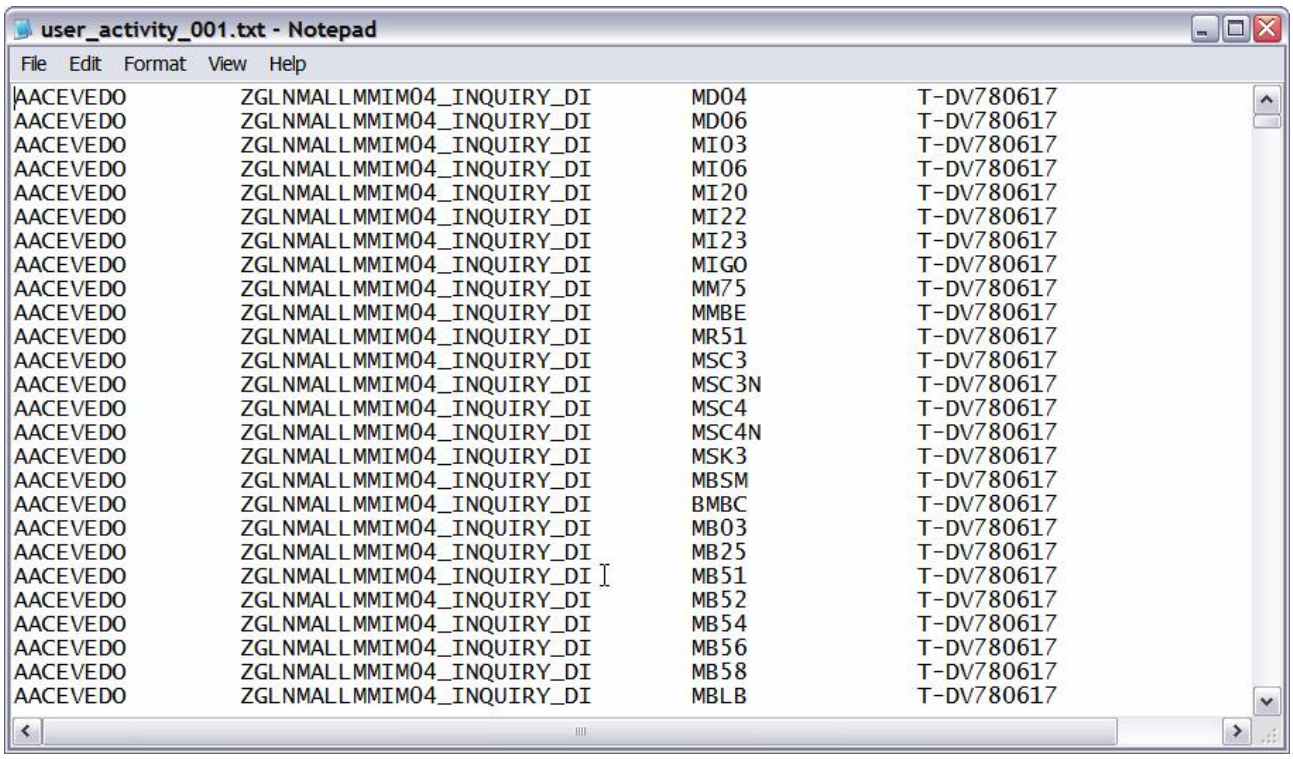
"USERID" (User ID) and "ROLES" (Role) fields can have multiple values but the combination of USERID/ROLE/ACTIONFROM/ACTIONTO (UserID/Role/ActionFrom/ActionTo) fields should be unique.

"ACTIONROM" (Action From) field value should be in ALL UPPERCASE.

If "ACTIONTO" value doesn't exist for source system, leave blank.

If "PROFILE" value doesn't exist for source system, repeat "ROLE" field.

If "COMPOSITE ROLENAME" value doesn't exist for source system, leave blank.



It is **recommended** that the downloaded data is stored as text files and should be tab-delimited files and records per file should be about 60000. Sometimes the extraction data can take up more than one file. Incase of multiple text files, we recommend customers to create a “Control (.CTL)” file having information of multiple text files. Following is a screen shot of control file having User Action files.

Extracting User Permissions

In User Permission Extract we will download permissions assigned to users through roles and files should have following information of user permissions.

Field	Data Field Type	Field Size	Field Values	Sorting	Required	Description	Transformation Rules
USERID	String	50	CAPS	Sorted Ascending, Sort Order 1	Yes	User ID	Unique record = The combination of colums 1 - 3 (USERID / ROLES / PERMISSION) has to be unique.
ROLE	String	49	CAPS	Sorted Ascending, Sort Order 2	Yes	Access Role Name	
PERMISSION	String	100	CAPS	Sorted Ascending, Sort Order 3	Yes	User Permission (Permission Object/Field), required if applicable	ACTION and PERMISSION fields using "||" with no space in between.
PRMGRP	String	20		Generate after sorting	Yes	Query generated numerical sequence (1++ counter per user)	Extractor/query generates this value. The value is generated after the data is sorted.
FROMVALUE	String	50	CAPS		Yes	Permission value	
TOVALUE	String	50	CAPS		Yes	Permission value, only applicable if User Action has range From/To	If this value does not exist for source system, leave blank.
PROFILE	String	50	CAPS		Yes	User Permission Profile, if applicable	If this value does not exist for source system, repeat ROLE field from column 2.
COMPOSITE ROLE	String	50			No	Composite role name, leave blank if not available	If this value does not exist for source system, leave blank.

USERID - User ID with which users login to the system.

ROLE - Roles/Responsibilities assigned to user.

PERMISSION - Permissions assigned in each role/responsibility.

PRMGRP - Permission group where permissions belong, a numeric sequence number.

FROMVALUE - Permission from value defined in role/responsibility.

TOVALUE - Permission to value defined in role/responsibility.

PROFILE - Profile of associated Role.

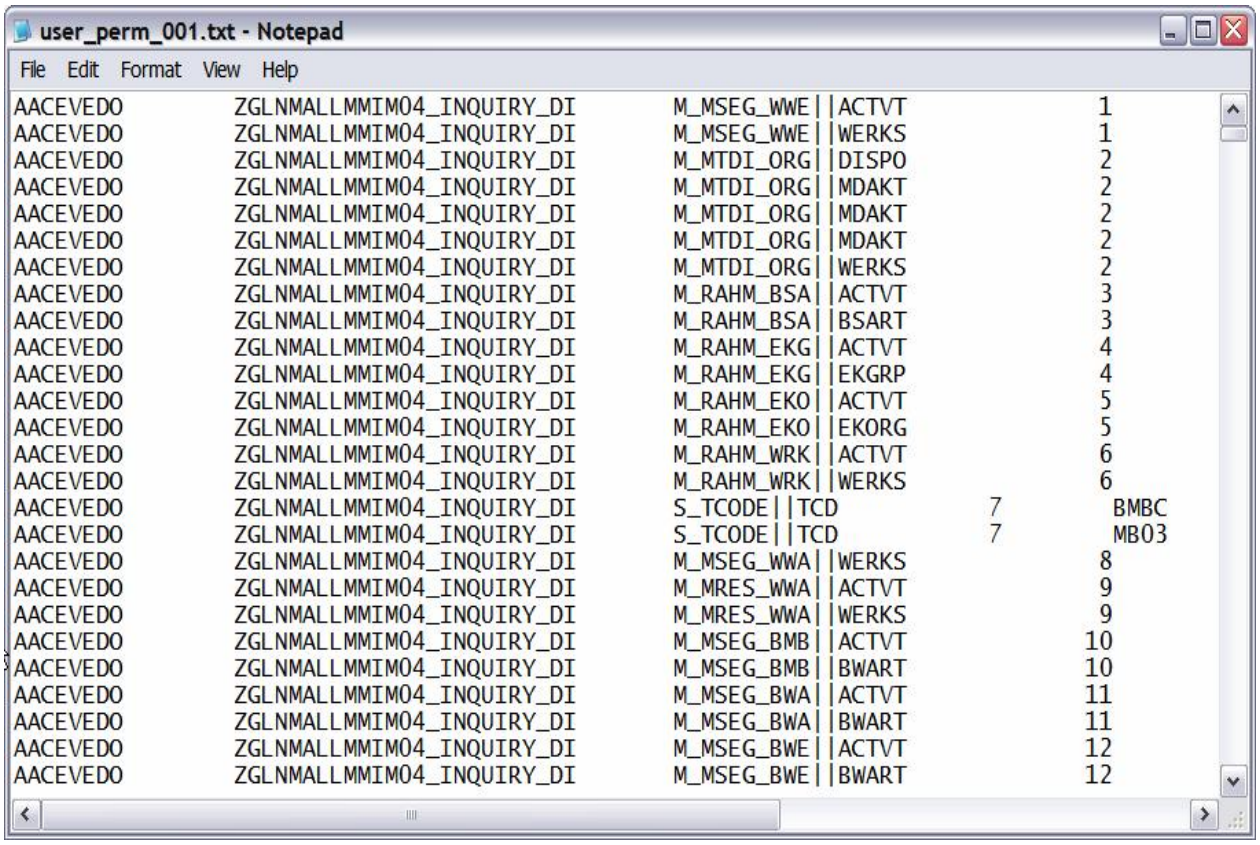
COMPOSITE ROLENAME - Composite Role Name.

Following are important points to be noted while downloading and formatting of User Permission files:

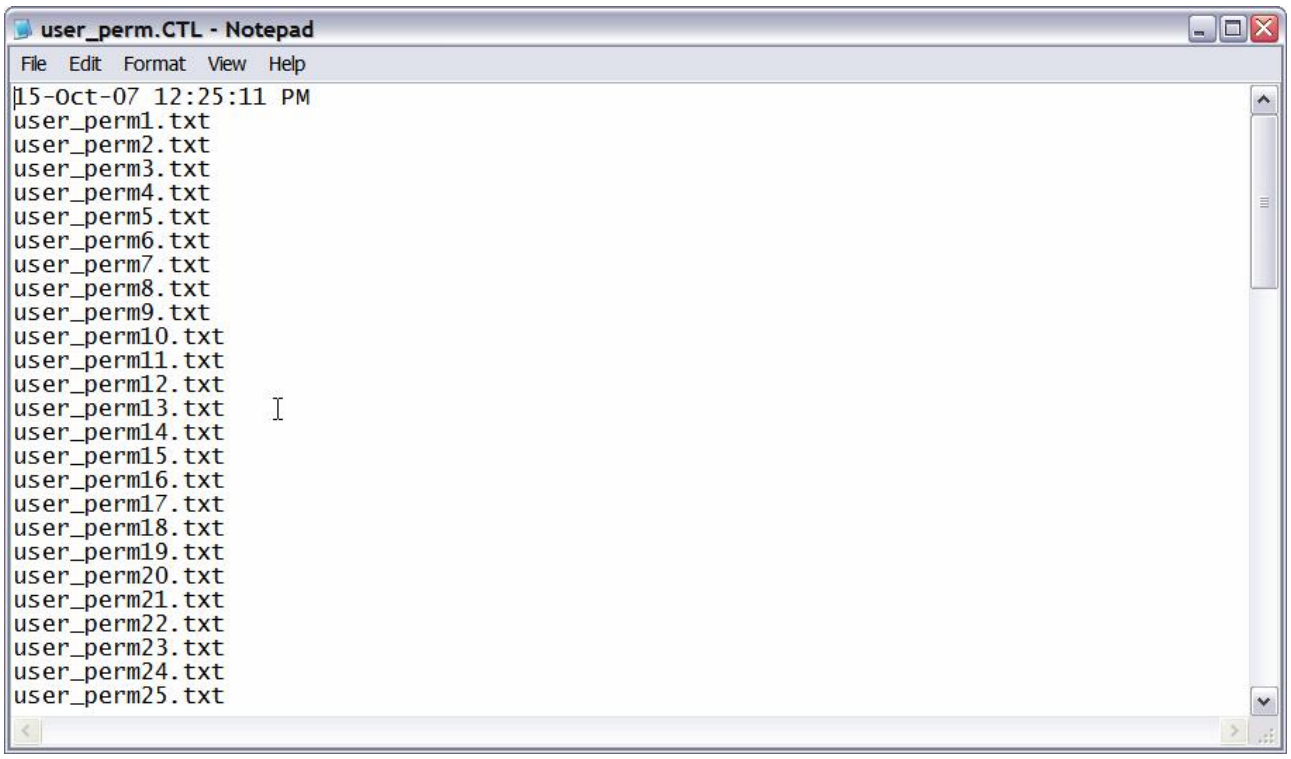
In the User Permission file, the “PERMISSION” field value must be joined with “||” separator. Unique record value based on combination of USERID, ROLE, PERMISSION, PRMGRP, FROMVALUE, and TOVALUE fields (User ID, Role, Permission, PRMGroup/SeqNo, From Value, and To Value).

In the User Permission file, “PRMGRP” field must be generated by the extractor in numerical sequence of “USERID” & “PERMISSION” combination. No duplicate of this combination is allowed.

“PERMISSION” and “FROMVALUE” field values should be in ALL UPPERCASE.



It is **recommended** that the downloaded data is stored as text files and should be tab-delimited files and records per file should be about 60000. Sometimes the extraction data can take up more than one file. Incase of multiple text files, we recommend customers to create a “Control (.CTL)” file having information of multiple text files. Following is a screen shot of control file having User Permission files.



Role Data Extraction

In Role Data Extraction process we will be downloading Role details, Role actions and Role permissions from the back-end ERP system. Data will be downloaded into separate text files in the format mentioned below.

Extracting Role Information

In Role Extract we will download role details and should include the following information of the role.

Field	Data Field Type	Field Size	Field Values	Sorting	Required	Description	Transformation Rules
Role	String	50	CAPS	Sorted Ascending	Yes	Access Role Name	
Role description	String	100			Yes	Role Description	

ROLE NAME - Role/Responsibility name.

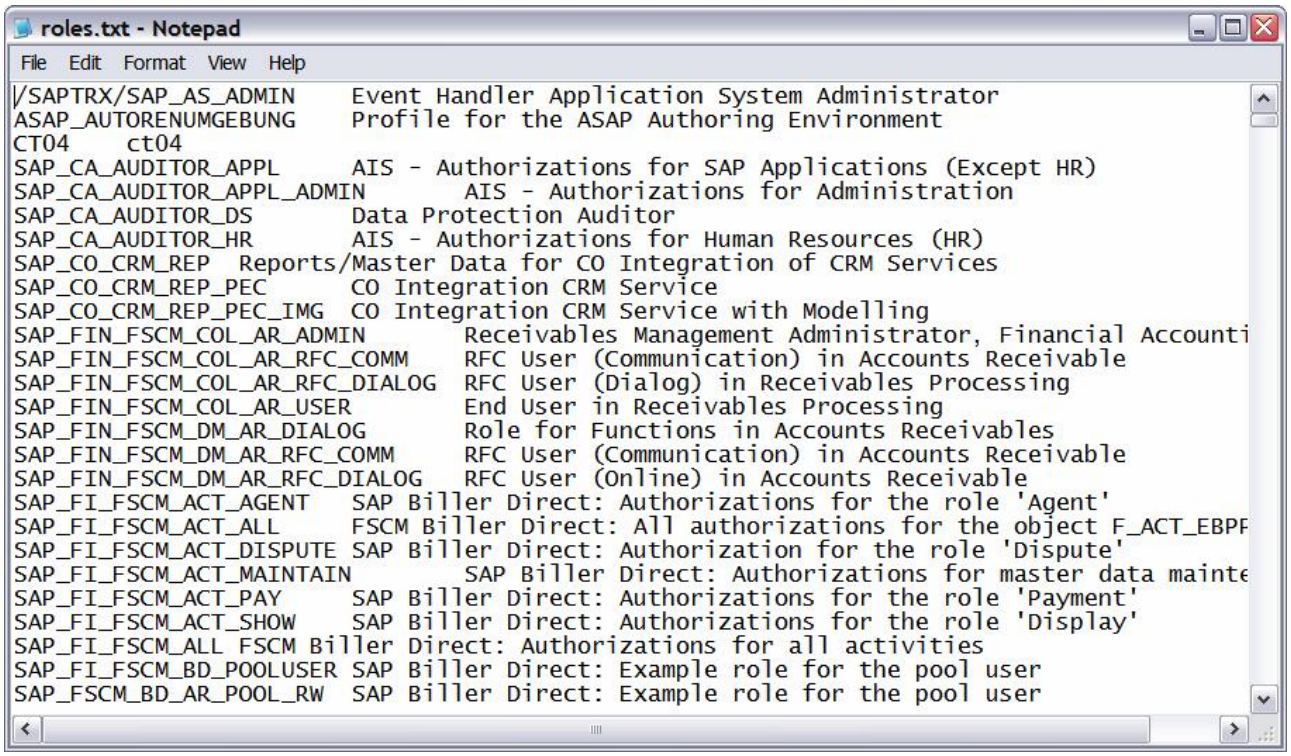
ROLE DESCRIPTION - Role/Responsibility Description.

Following are important points to be noted while downloading and formatting of Role files:

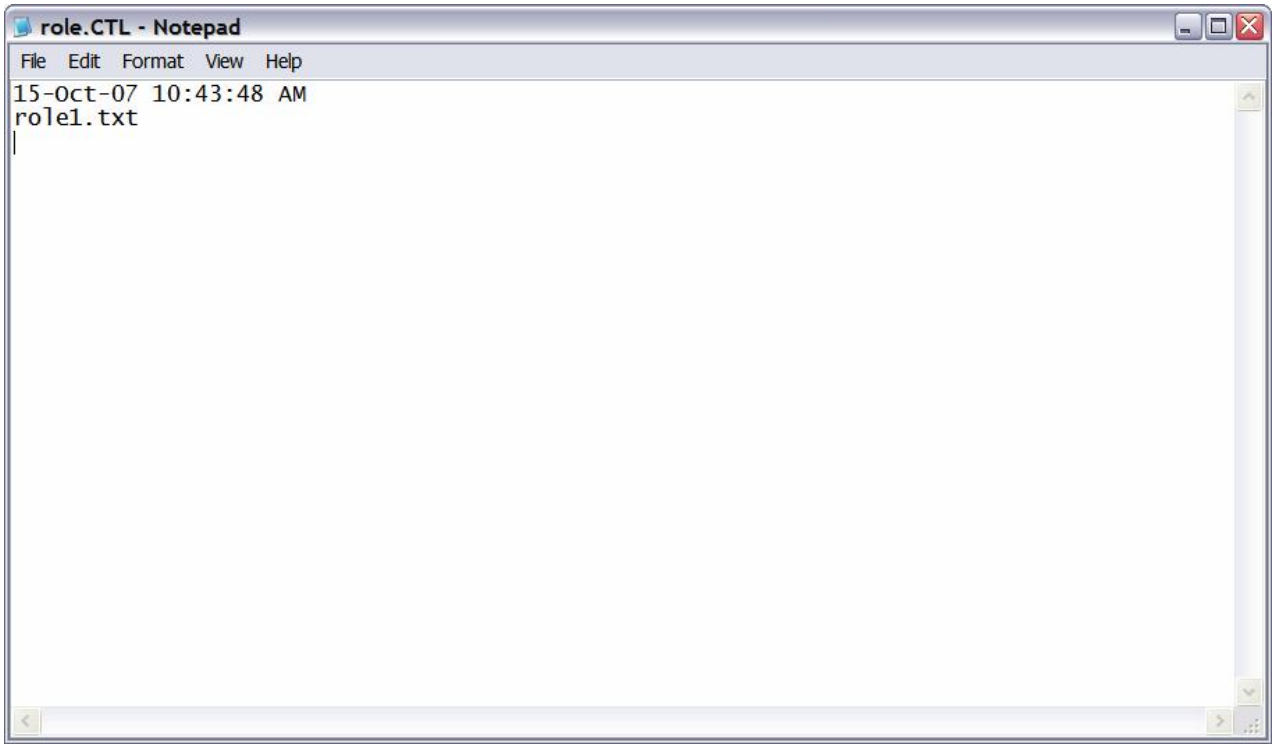
“ROLE NAME” (Role Name) field should be unique and should be “NOT NULL”.

There should not be any duplicate record in the file(s) (combination of all field columns in the file).

There should not be any blank records at the end of the file.



It is **recommended** that the downloaded data is stored as text files and should be tab-delimited files and records per file should be about 60000. Sometimes the extraction data can take up more than one file. Incase of multiple text files, we recommend customers to create a “Control (.CTL)” file having information of multiple text files. Following is a screen shot of control file having Role file.



Extracting Role Action

In Role Action Extract we will download actions assigned to Roles and files should have following information of role actions.

Field	Data Field Type	Field Size	Field Values	Sorting	Required	Description	Transformation Rules
ROLES	String	50	CAPS	Sorted Ascending, Sort Order 1	Yes	Role Name	
ACTIONFROM	String	50	CAPS	Sorted Ascending, Sort Order 2	Yes	Role Action	
ACTIONTO	String	50			No	Role Action	If this value does not exist for source system, leave blank.
PROFILE	String	50	CAPS		Yes	Security Profile	If this value does not exist for source system, repeat ROLE field from column 2.

ROLES - Role/Responsibility name.
TCODEFROM - Transaction/Action assigned to Role/Responsibility
TCODETO - Transaction/Action assigned to Role/Responsibility
PROFILE - Profile associated with Role

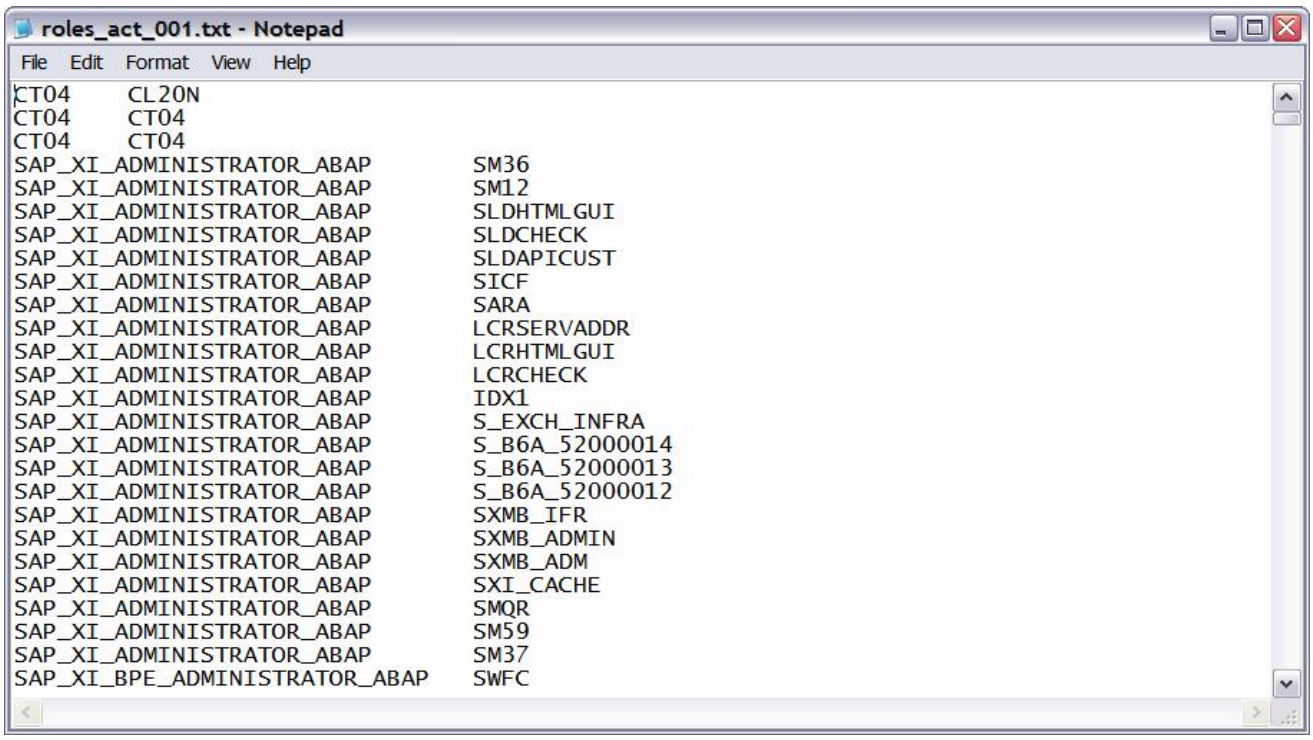
Following are important points to be noted while downloading and formatting of Role Action files:

“ROLES” (Role) field can have multiple values but the combination of ROLE/ACTIONFROM/ ACTIONTO (Role/ActionFrom/ActionTo) fields should be unique.

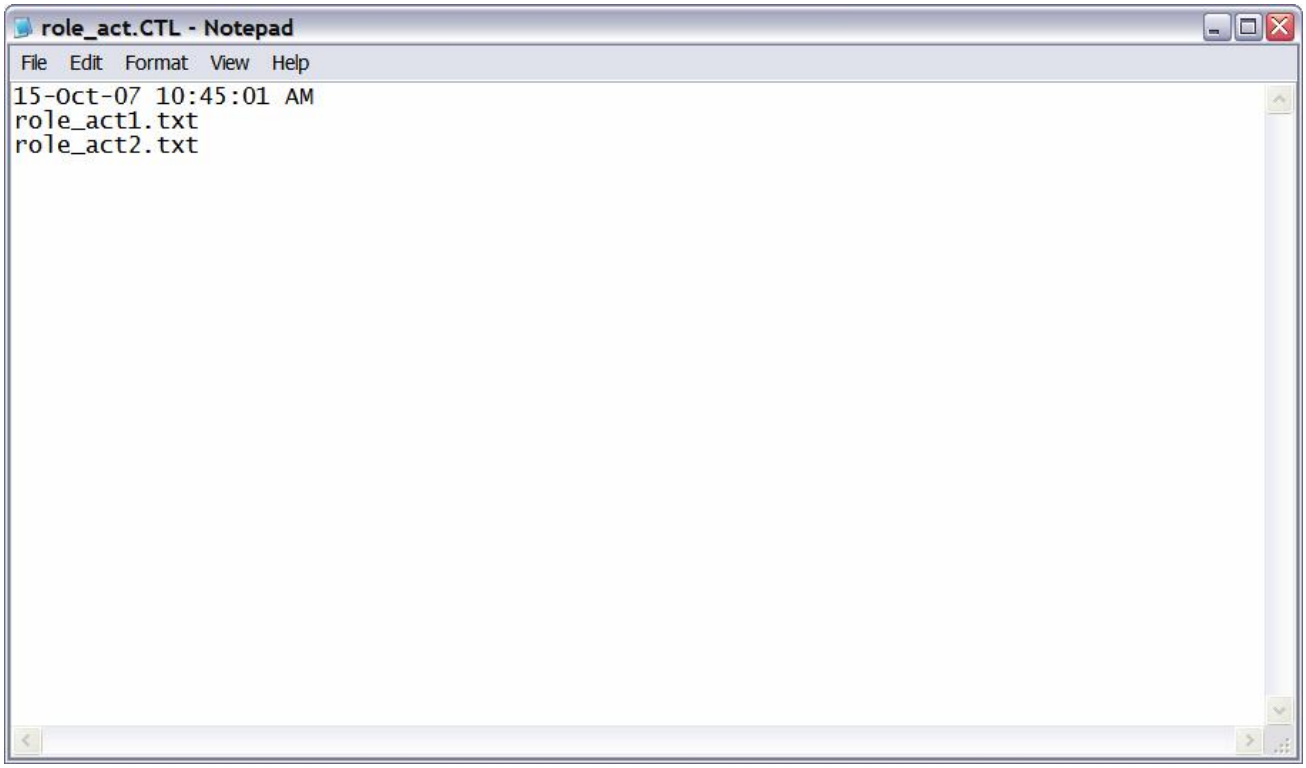
“ACTIONROM” (Action From) field value should be in ALL UPPERCASE.

If “ACTIONTO” value doesn’t exist for source system, leave blank.

If “PROFILE” value doesn’t exist for source system, repeat “ROLE” field.



It is **recommended** that the downloaded data is stored as text files and should be tab-delimited files and records per file should be about 60000. Sometimes the extraction data can take up more than one file. Incase of multiple text files, we recommend customers to create a “Control (.CTL)” file having information of multiple text files. Following is a screen shot of control file having Role Action files.



Extracting Role Permissions

In Role Permission Extract we will download permissions assigned to roles and files should have following information of role permissions.

Field	Data Field Type	Field Size	Field Values	Sorting	Required	Description	Transformation Rules
ROLE	String	50	CAPS	Sorted Ascending, Sort Order 1	Yes	Role Name	
PERMISSION	String	100	CAPS	Sorted Ascending, Sort Order 2		(Object/Field)	Concatenate ACTION and PERMISSION fields using "||" with no space in between.
PRMGRP	String	20		Generate after sorting		Query generated numerical sequence (1++ counter per role)	Extractor/query generates this value. The value is generated after the data is sorted.
FROMVALUE	String	50	CAPS		Yes	Permission value	
TOVALUE	String	50	CAPS		No	Permission value, only applicable if Permission has range From/To	If this value does not exist for source system, leave blank.
PROFILE	String	50	CAPS		Yes	Role Profile , if applicable	If this value does not exist for source system, repeat ROLE field from column 1.

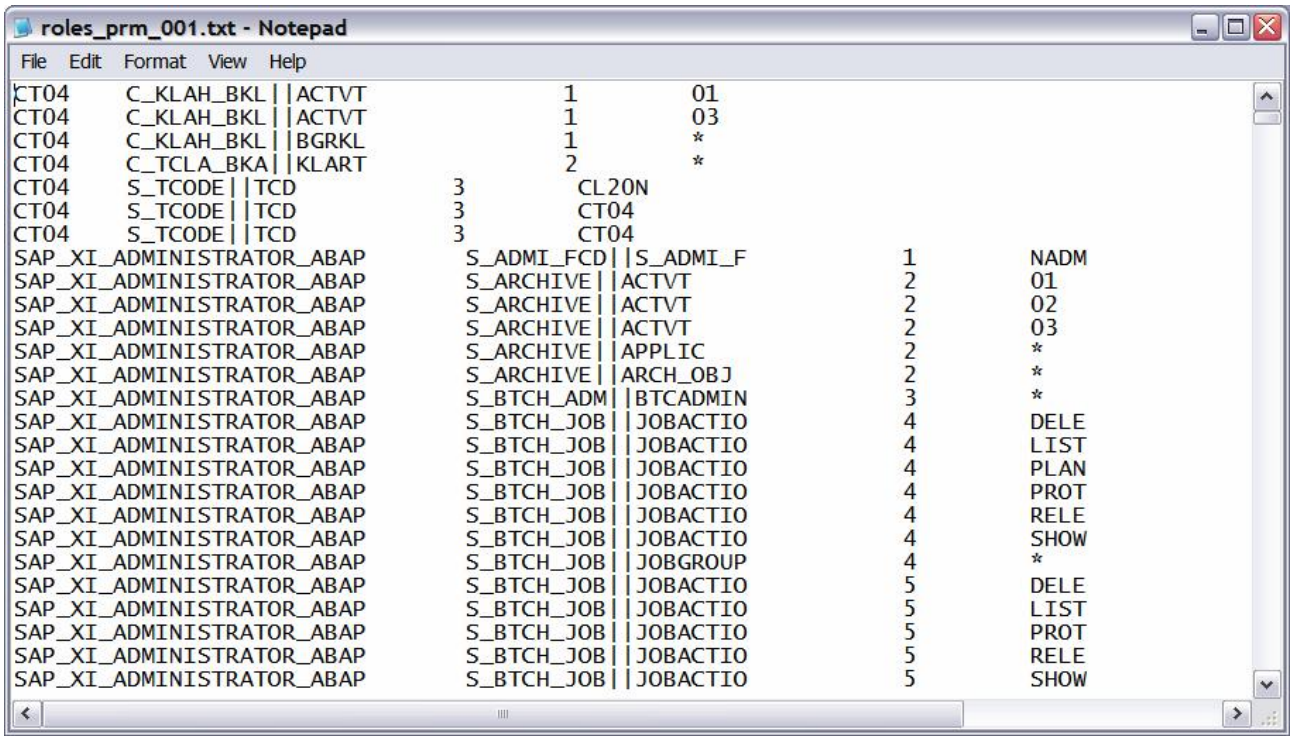
ROLES - Role/Responsibility name
PERMISSION - Permissions associated with Role/Responsibility
PRMGRP - Permission group where permissions belong, a numeric sequence number.
FROMVALUE - Permission from value in Role/Responsibility
TOVALUE - Permission to value in Role/Responsibility
PROFILE - Profile associated with Role.

Following are important points to be noted while downloading and formatting of Role Permission files:

In Role Permission file, the “PERMISSION” field value must be joined with “||” separator. Unique record value based on combination of ROLE, PERMISSION, PRMGRP, FROMVALUE, and TOVALUE fields (Role, Permission, PRMGroup/SeqNo, From Value, and To Value).

In Role Permission file, “PRMGRP” field must be generated by the extractor in numerical sequence of “USERID” & “PERMISSION” combination. No duplicate of this combination is allowed.

“PERMISSION” and “FROMVALUE” field values should be in ALL UPPERCASE.



It is **recommended** that the downloaded data is stored as text files and should be tab-delimited files and records per file should be about 60000. Sometimes the extraction data can take up more than one file. Incase of multiple text files, we recommend customers to create a “Control (.CTL)” file having information of multiple text files. Following is a screen shot of control file having Role Permission files.

Configuring Risk Identification and Remediation

Configuring of Risk Identification and Remediation needs to be done before uploading the data from backend system. Following are the detail steps that will walk you through configuring of Risk Identification and Remediation for RRA process.

Create a Connector

In this step we will be creating a connector to backend system. For RRA process we will be extracting data from flat files, so we select the connection type as “File – Local”.

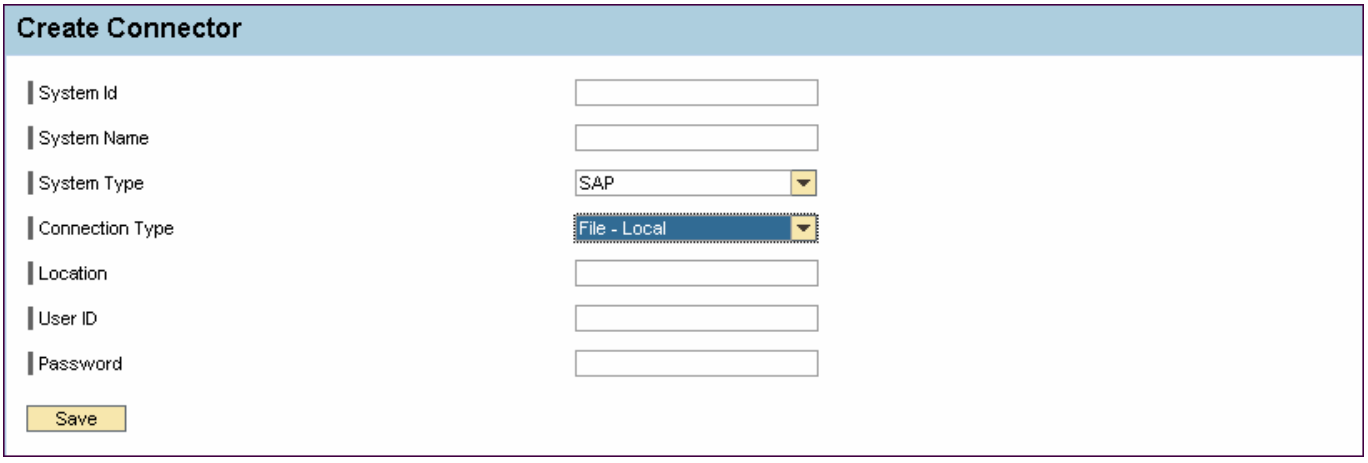
Log in to the server.

Click the Configuration Tab on top.

From left navigation menu, click ‘Connectors’.

Click Create.

The following screen will be displayed.



Enter the System ID, System Name.

Select the System type to be SAP.

Select the connection type to be File – Local.

Enter the location of the data files, user ID and password to access those files.

Upload Objects

In Upload Objects we will upload both Auth Objects and Text Objects that were downloaded during data extraction process.

Uploading Text Objects

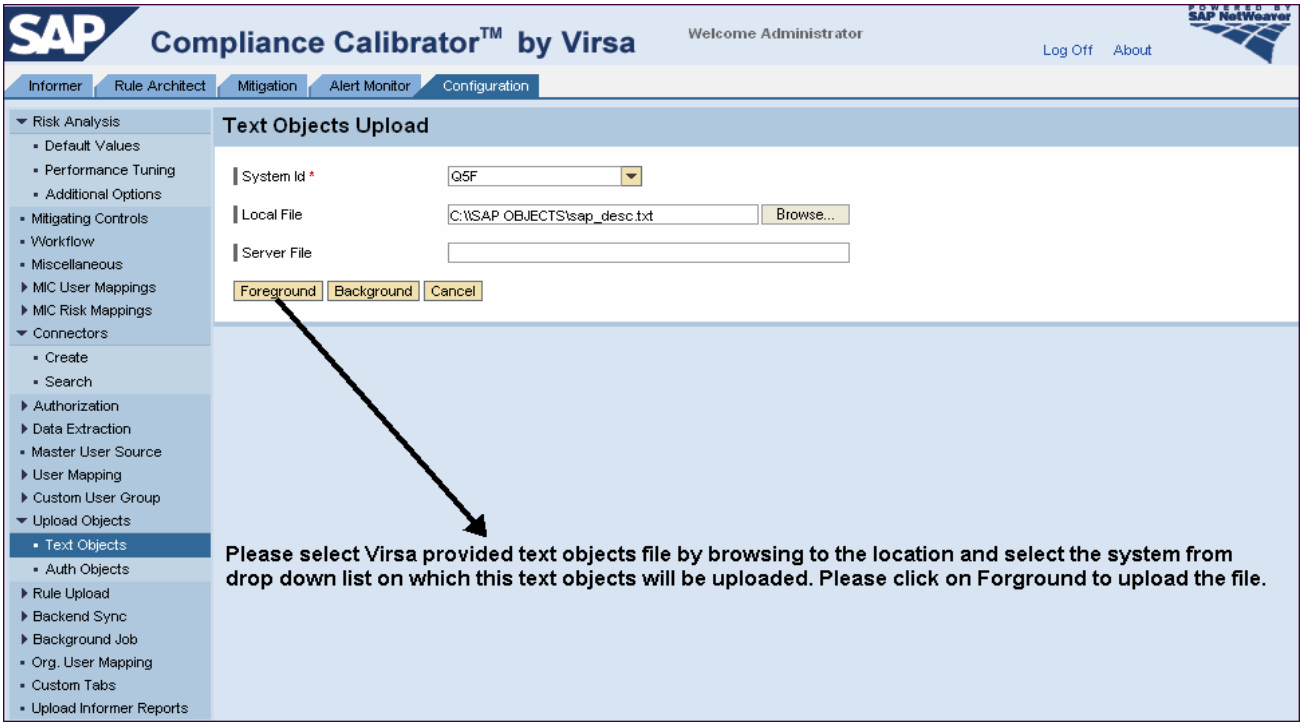
Log in to the server.

Click the Configuration Tab on top.

From left navigation menu, Click Upload Objects.

Click “Text Objects”

The following screen will be displayed



Enter the System ID. (These objects are system specific, hence for each system we have to upload the objects individually)

Enter the Location of the Files.

Click Foreground (Best Practice).

The status message of the upload will be displayed at the bottom of the screen.

Uploading Auth Objects

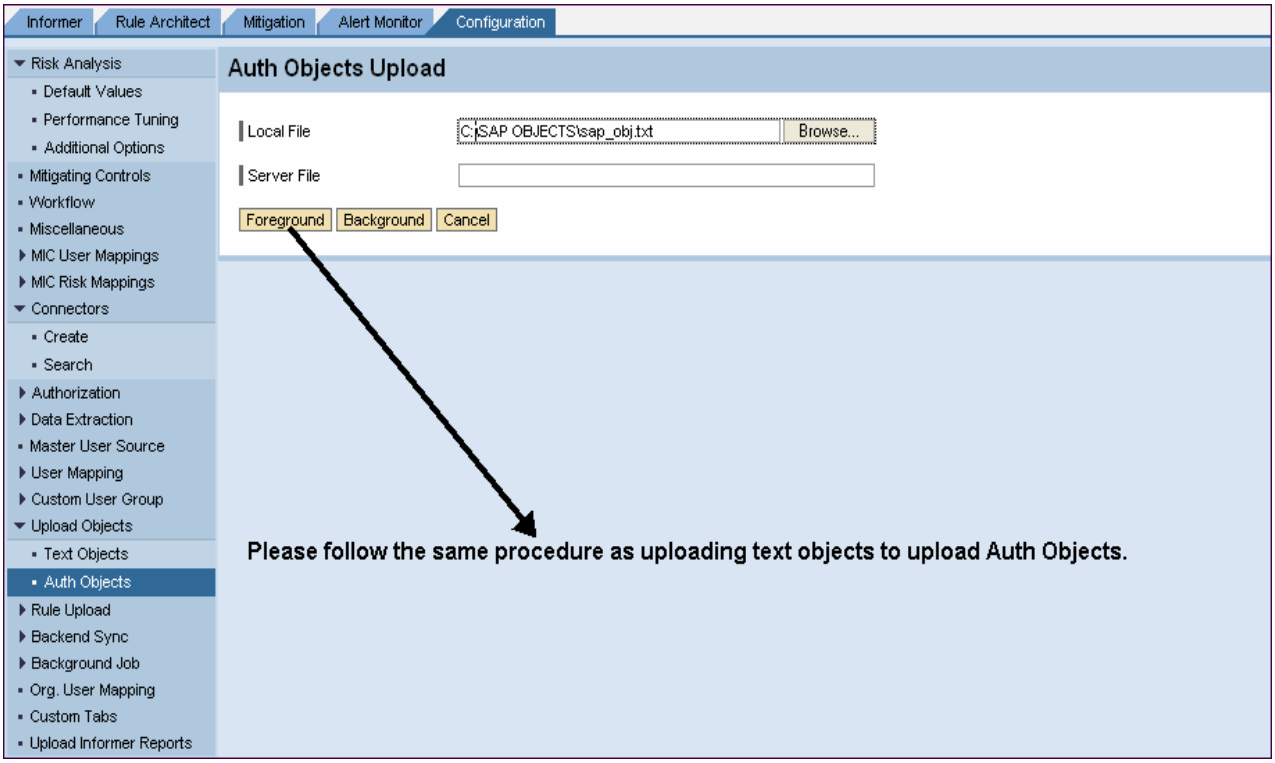
Log in to the server.

Click the Configuration Tab on top.

From left navigation menu, Click Upload Objects.

Click “Auth Objects”

The following screen will be displayed



Enter the System ID.

Enter the Location of the Files.

Click Foreground (Best Practice).

The status message of the upload will be displayed at the bottom of the screen.

Rule Upload

The SAP Best Practices are delivered with the Package which contains the files for rule generation. These files are to be uploaded in the sequence as mentioned below.

Uploading Business Process

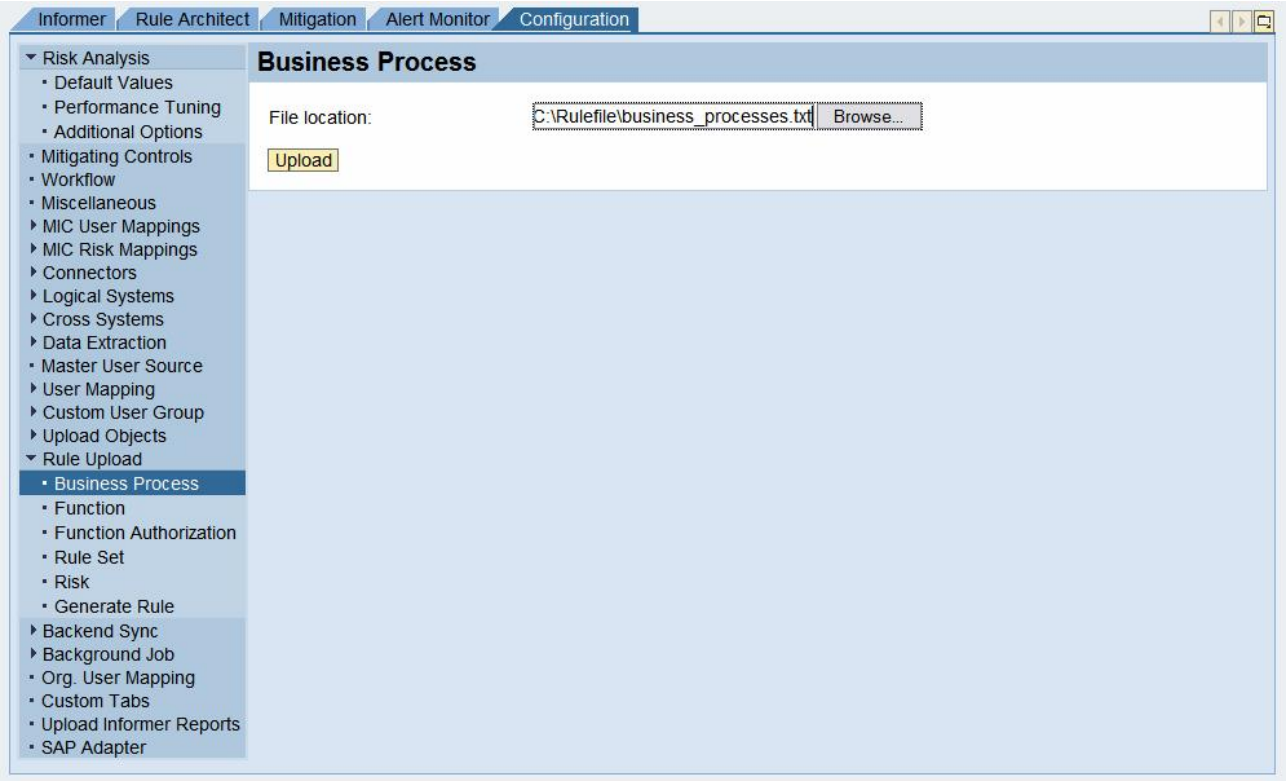
In this process we will upload various Business Processes that are associated with our data.

Click the Configuration Tab on top.

From left navigation menu, Click Rule Upload.

Click “Business Process”

The following screen will be displayed



Browse to the required file “business_processes.txt”.

Click Upload.

The Upload status will be displayed at the bottom of the screen.

Uploading Functions

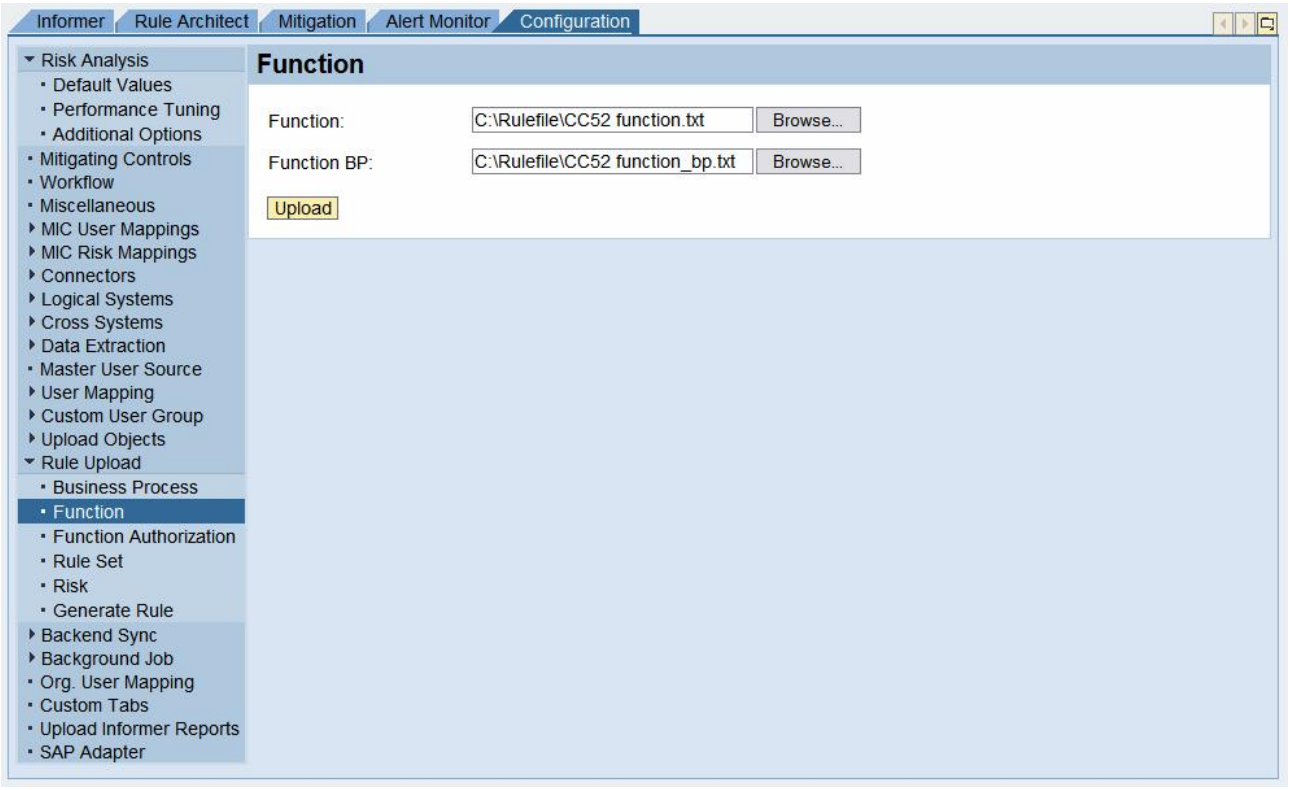
In this process we will upload various Functions that are associated with each Business Processes.

Click the Configuration Tab on top.

From left navigation menu, Click Rule Upload.

Click Function.

The following screen will be displayed



Browse to required files.

Click Upload.

The Upload status will be displayed at the bottom of the screen.

Uploading Function Authorizations

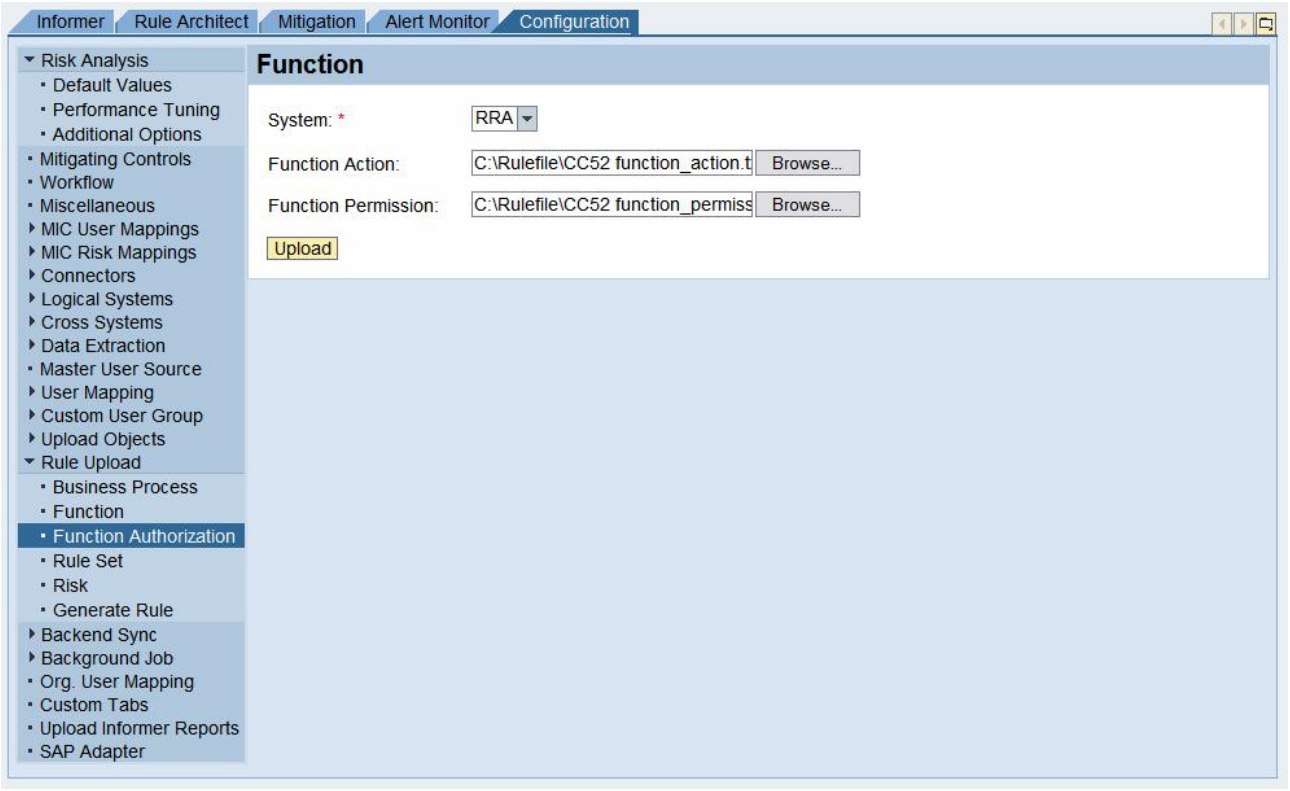
In this process we will upload various Function Actions and Function Permissions associated with each system. For our RRA process we will upload all Function Actions and Function Permissions files.

Click the Configuration Tab on top.

From left navigation menu, Click Rule Upload.

Click Function Authorization.

The following screen will be displayed



Browse to required files. (These objects are system specific, hence for each system we have to upload the objects individually)

Click Upload.

The Upload status will be displayed at the bottom of the screen.

Uploading Rule Set

In this process we will upload various Rule set that will define Segregation of Duties (SoD).

Click the Configuration Tab on top.

From left navigation menu, Click Rule Upload.

Click Rule Set.

The following screen will be displayed

Browse to required file.

Click Upload.

The Upload status will be displayed at the bottom of the screen.

Uploading Risks' Details

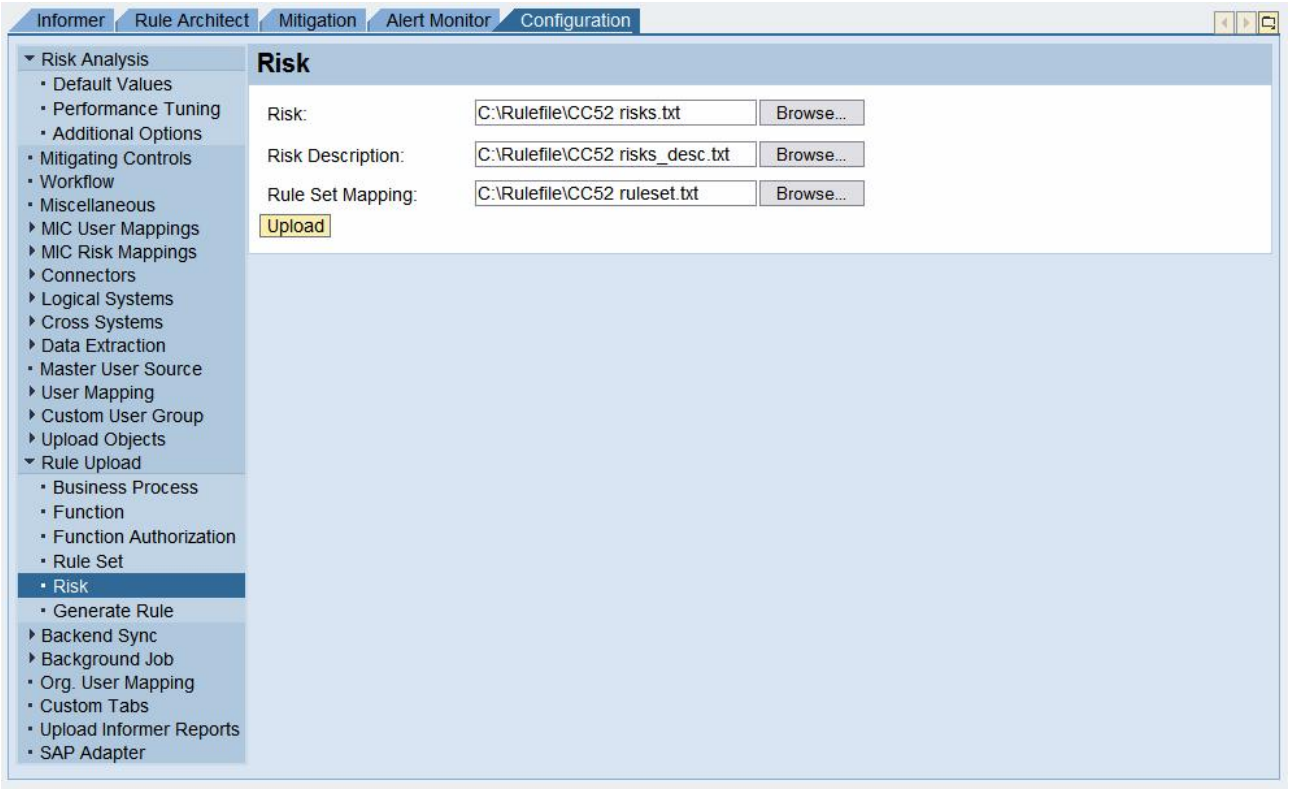
In this process we will upload pre-defined Risks, Risk Descriptions and mapping of these Risks to respective Rule set.

Click the Configuration Tab on top.

From left navigation menu, Click Rule Upload.

Click Risk.

The following screen will be displayed



Browse to required files.

Click Upload.

The Upload status will be displayed at the bottom of the screen.

Rule Generation

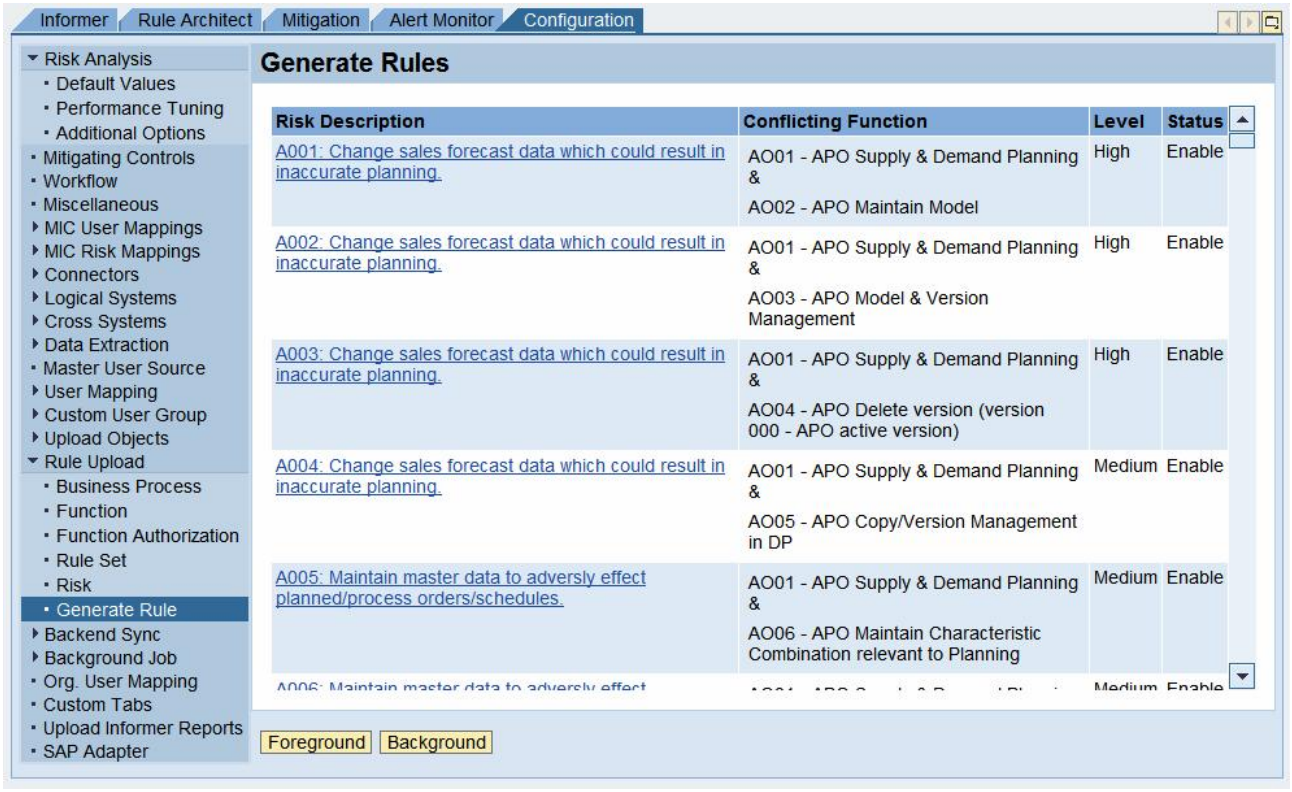
In this process we will generate the Rules that were uploaded in previous steps.

Click the Configuration Tab on top.

From left navigation menu, Click Rule Upload.

Click Generate Rule.

The following screen will be displayed



Click Foreground.

The Rule Generation status will be displayed on the screen.

Additional Configuration

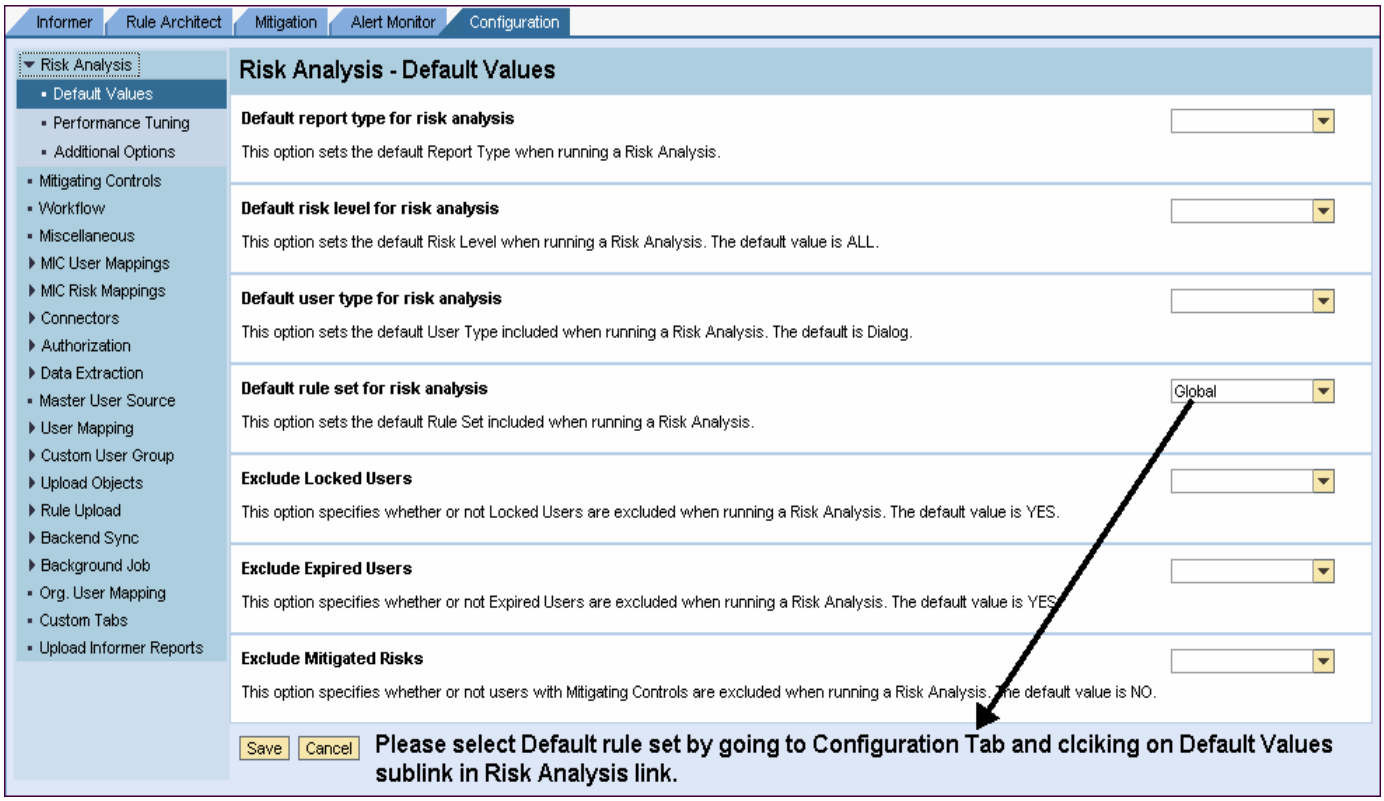
One final step of configuring Compliance Calibrator is making “Global” rule set as Default rule set for risk analysis.

Click the Configuration Tab on top.

From left navigation menu, Click Risk Analysis.

Click Default Values.

The following screen will be displayed



Change the Default Rule Set to GLOBAL

Click Save

Data Upload

Uploading User Data

Uploading of User Data includes uploading of Users, User Actions and User permissions that were downloaded in data extraction process earlier. Before scheduling a data upload we need to define Data Extractor. Following are detail steps to create a Data Extractor for User Upload.

Users

Click the Configuration Tab on top.

From left navigation menu, Click Data Extraction.

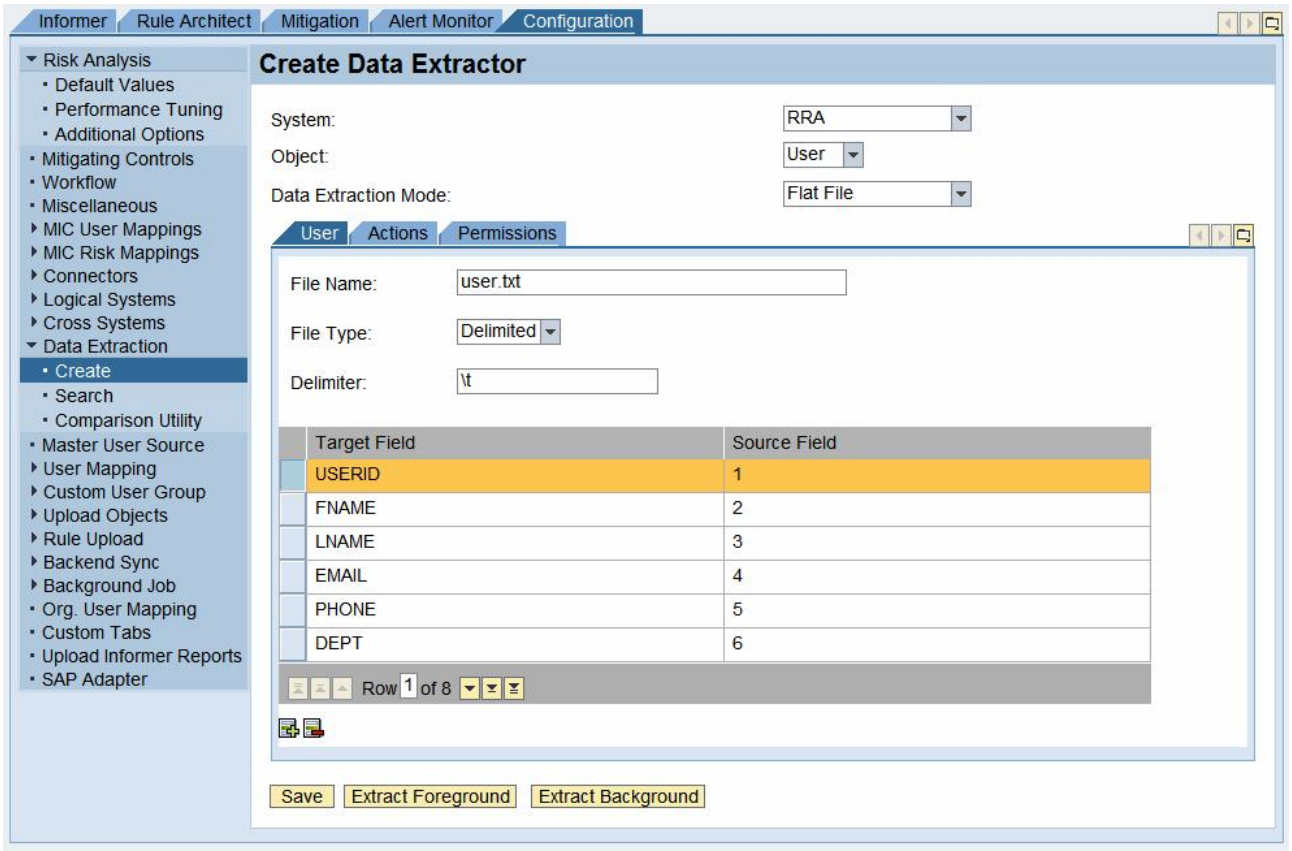
Click Create.

Select the System ID

Select the Object type as User.

Select Data Extraction Mode as Flat File.

The following screen will be displayed

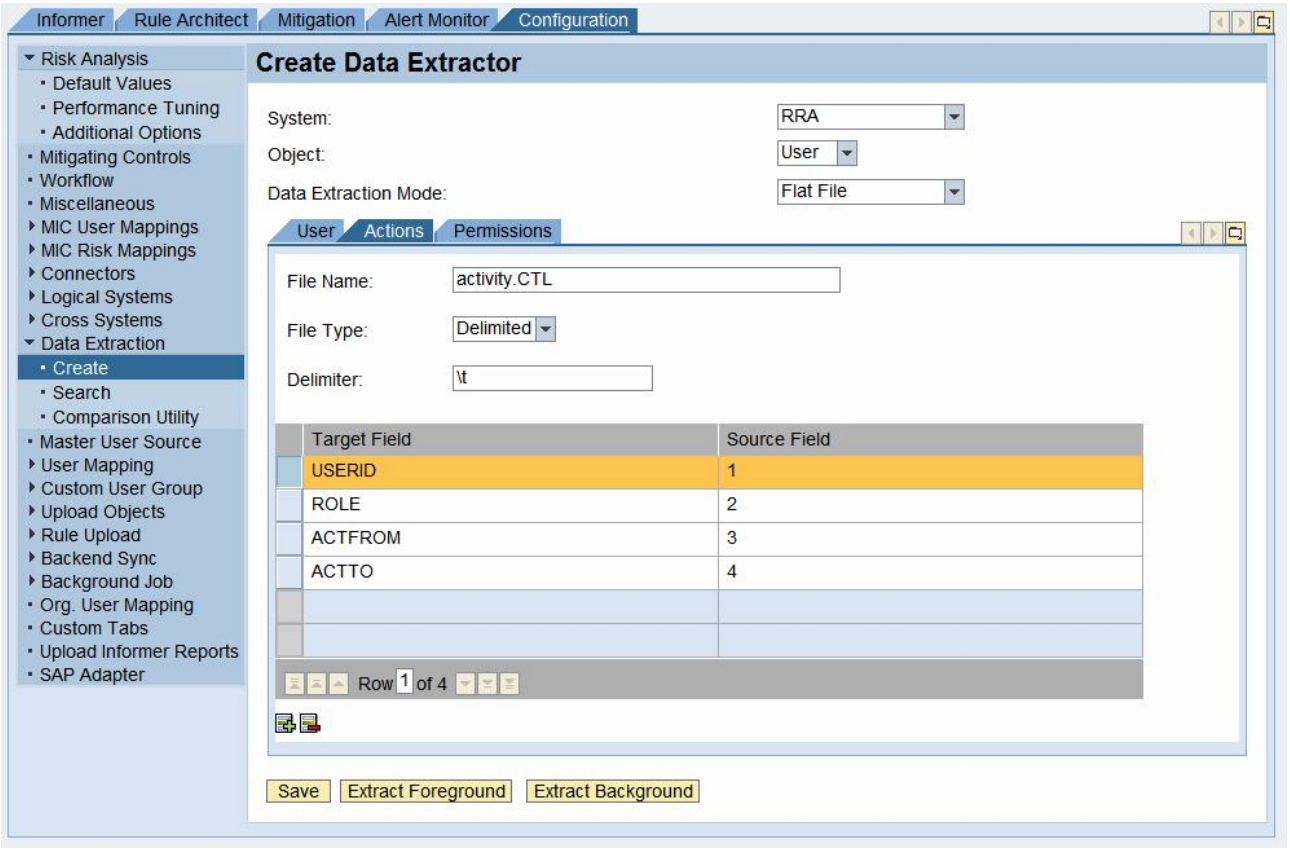


Enter the file name for user data.

User Actions

Click the Actions tab.

The following screen will be displayed

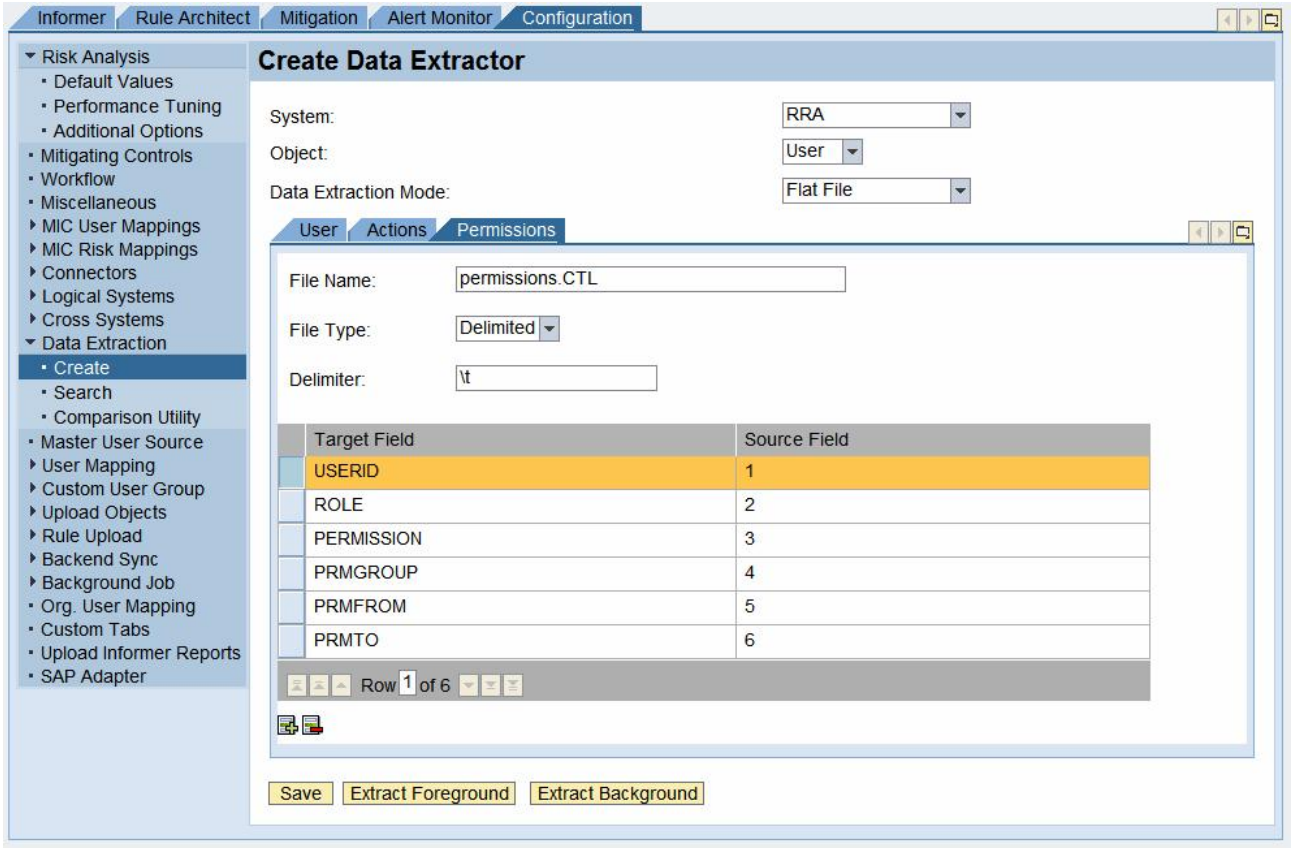


Enter the file name for user activity data.

User Permissions

Click the Permissions tab.

The following screen will be displayed



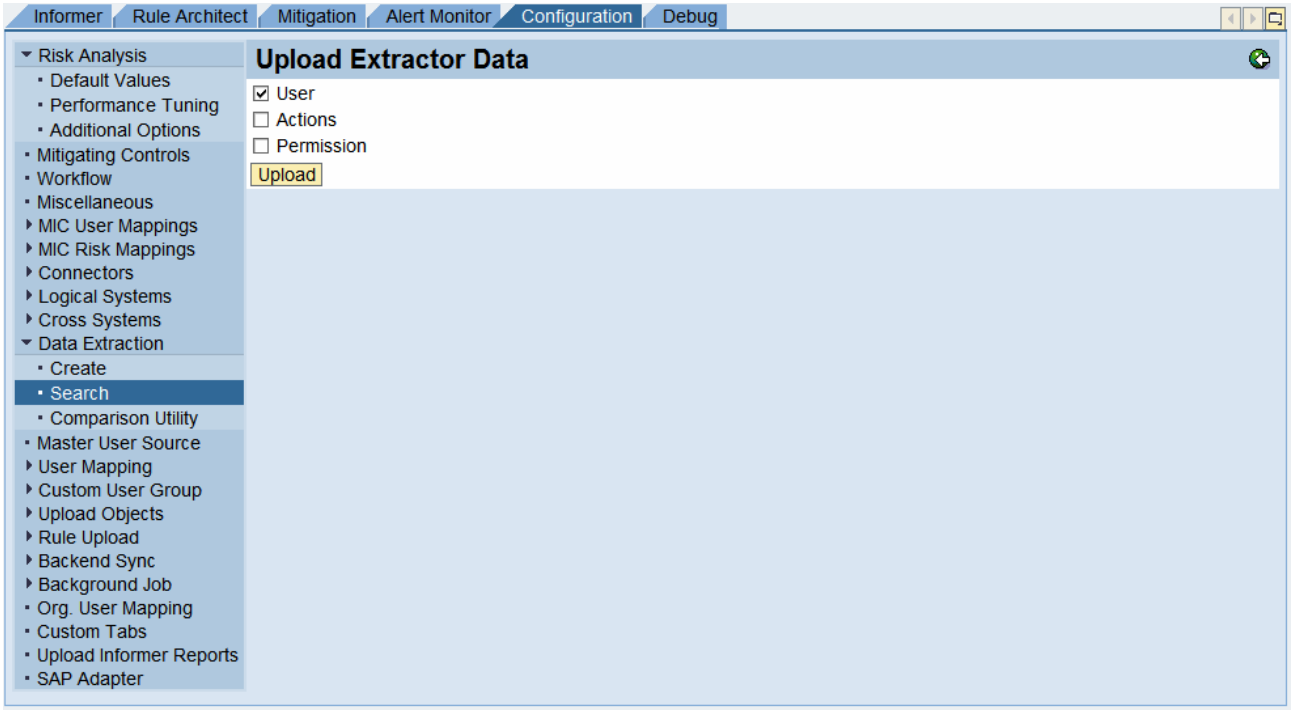
Enter the file name for user permission data.

Extracting Data

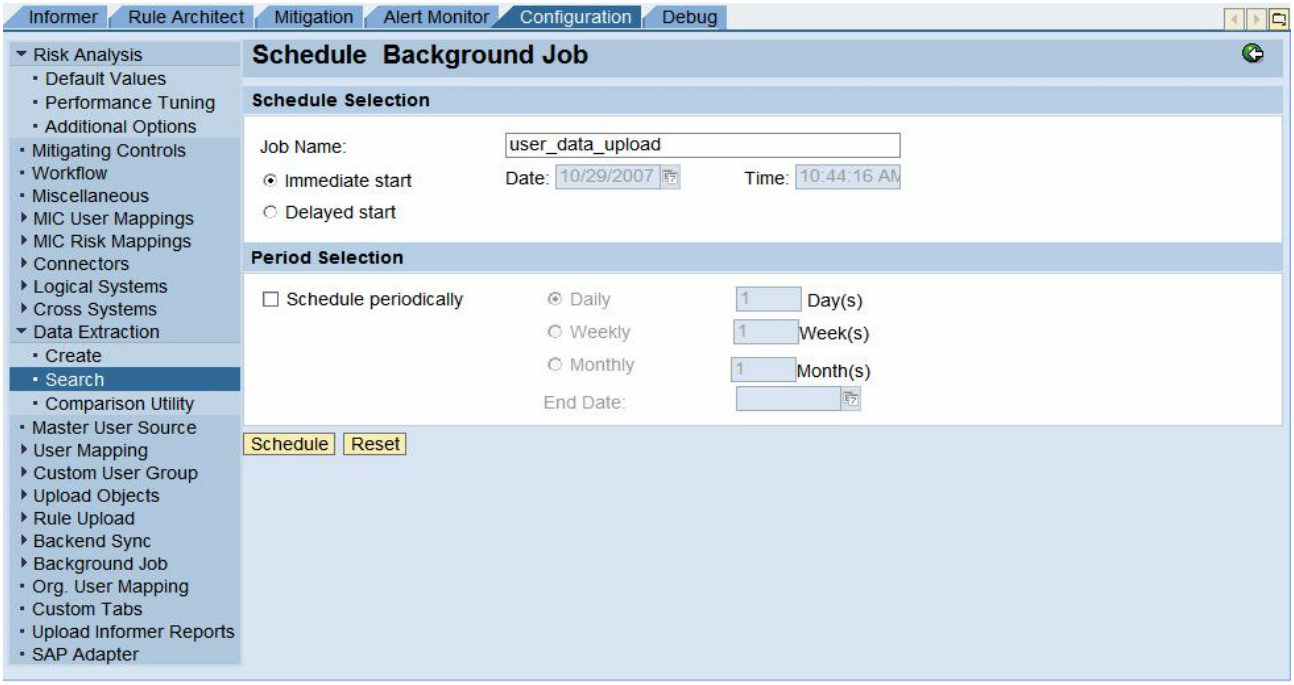
Click the Save Button.

Click Extract Background.

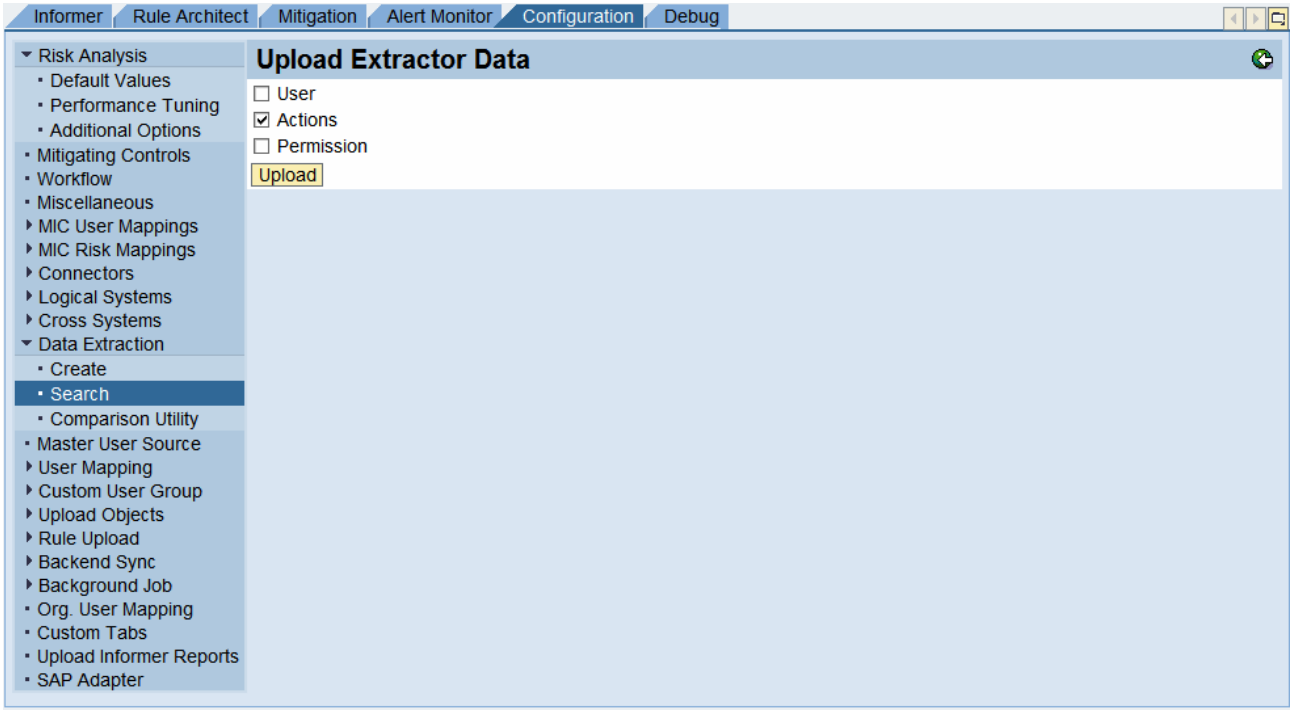
The following screen will be displayed. It is always **recommended** that during data extraction we should extract data from files individually.



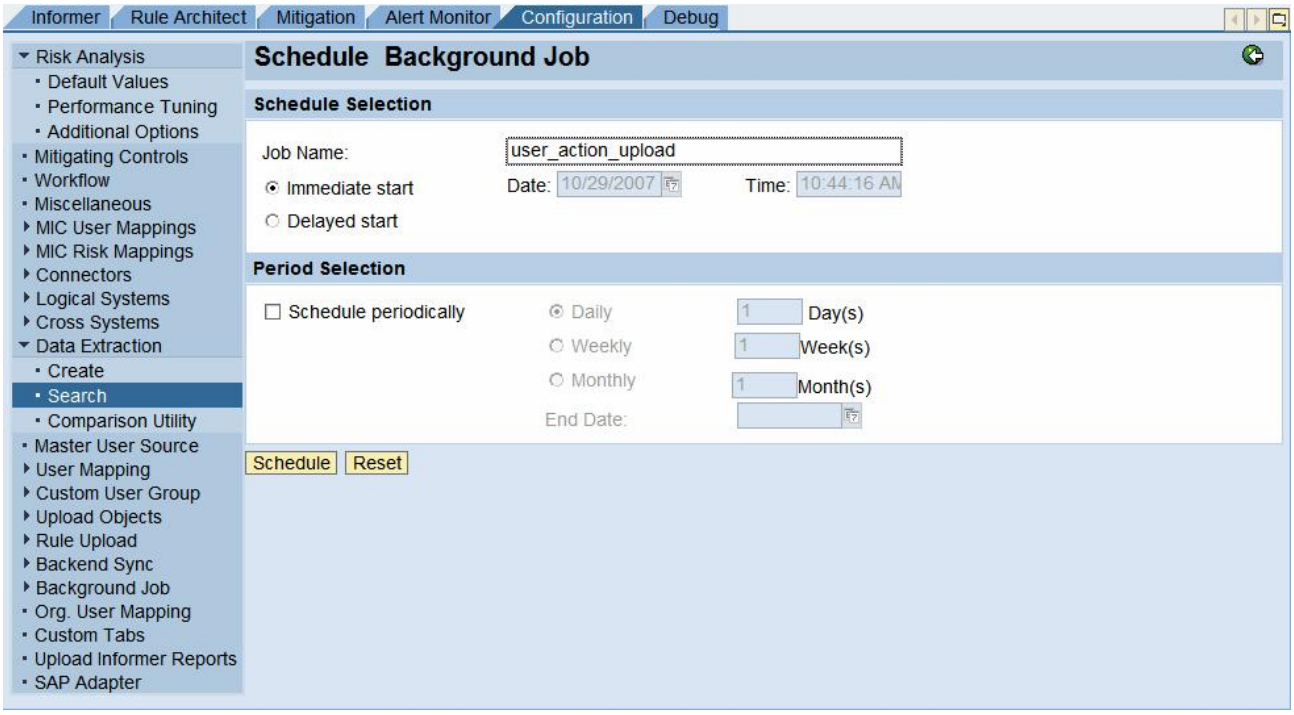
After selecting appropriate checkbox, click **Upload** to schedule Background Job for User upload. The following screens will be displayed. Enter the Job name and Click Schedule.



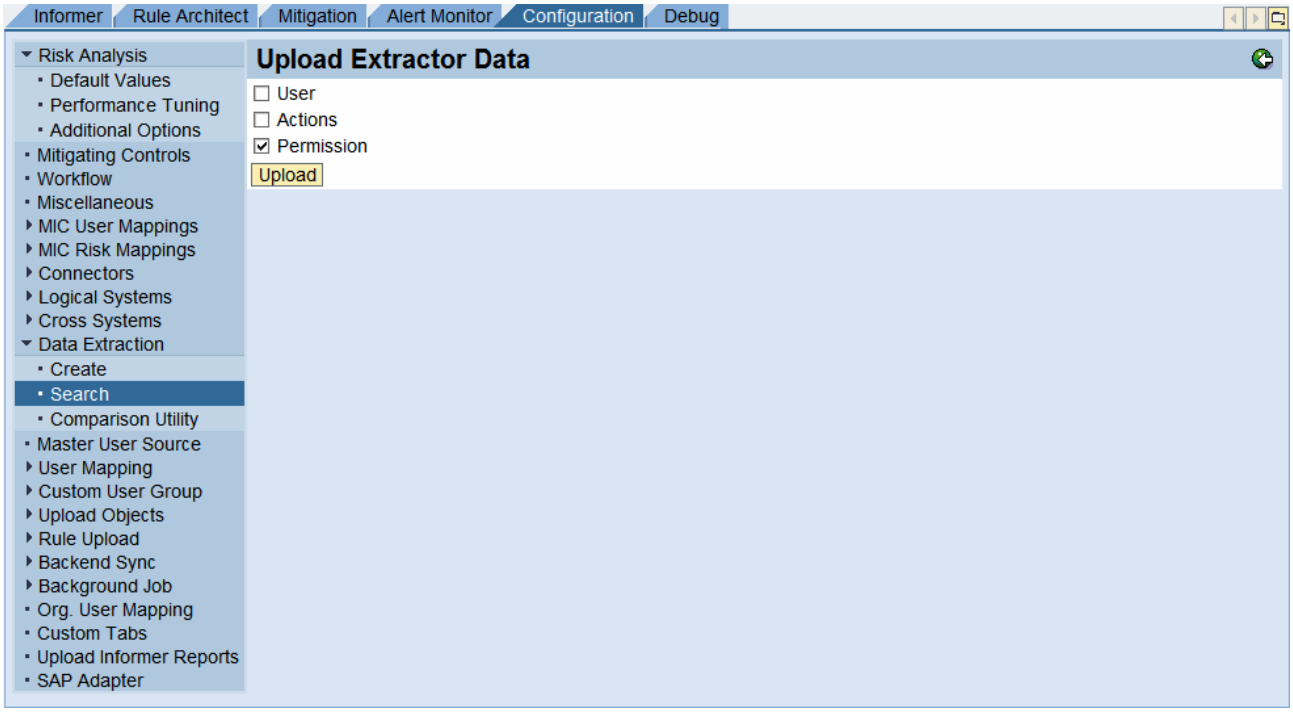
Repeat the same Upload process for User Actions.



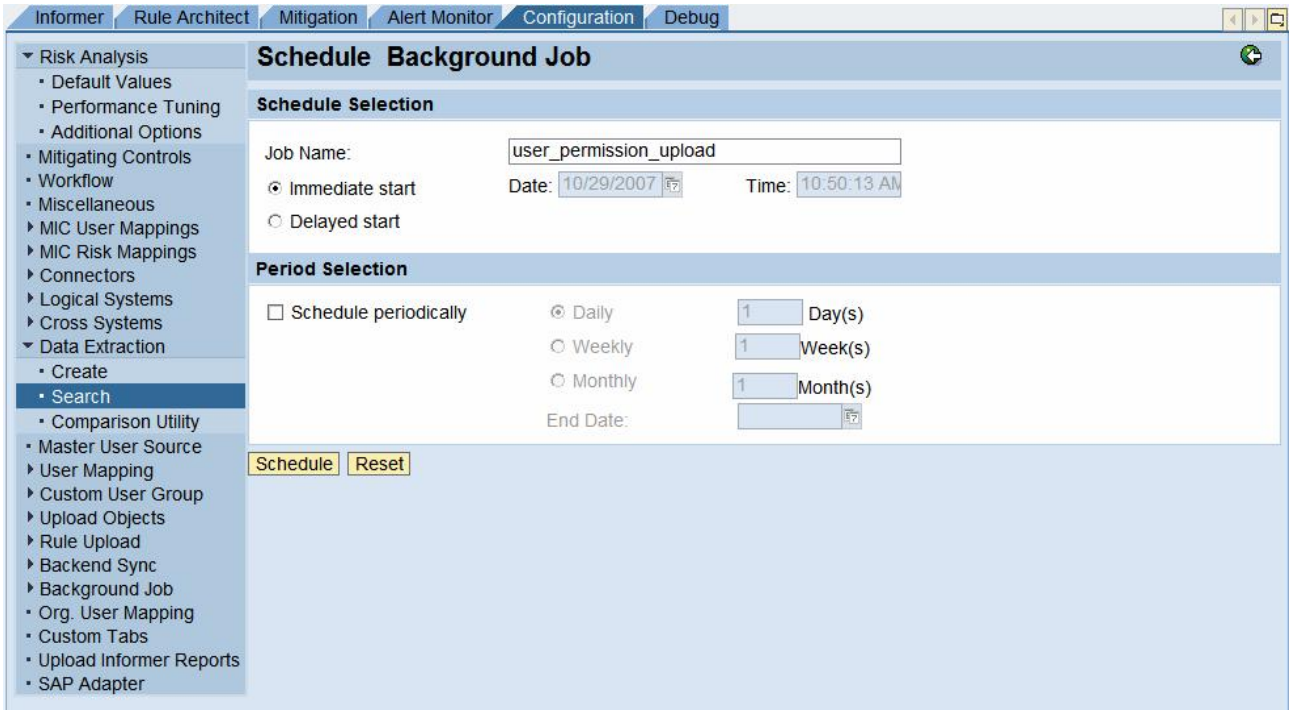
After selecting appropriate checkbox, click **Upload** to schedule Background Job for User Action upload. The following screens will be displayed. Enter the Job name and Click Schedule.



Repeat the same Upload process for User Permissions.



After selecting appropriate checkbox, click **Upload** to schedule Background Job for User Permission upload. The following screens will be displayed. Enter the Job name and Click Schedule.



The Background job for data extraction will be scheduled.

Uploading Role Data

Uploading of Role Data includes uploading of Roles, Role Actions and Role permissions that were downloaded in data extraction process earlier. Before scheduling a data upload we need to define Data Extractor. Following are detail steps to create a Data Extractor for Role Upload.

Roles

Click the Configuration Tab on top.

From left navigation menu, Click Data Extraction.

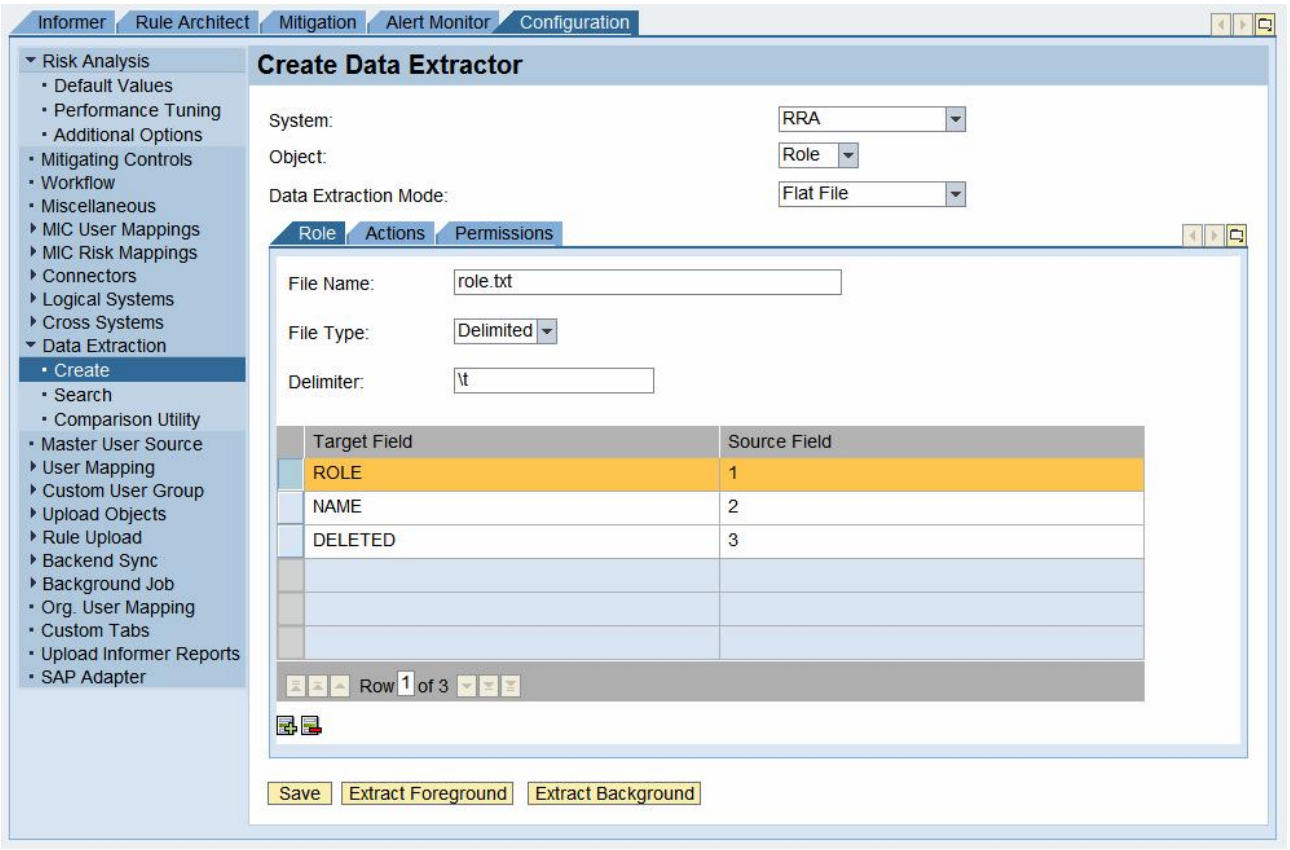
Click Create.

Select the System ID

Select the Object type as Role.

Select Data Extraction Mode as Flat File.

The following screen will be displayed

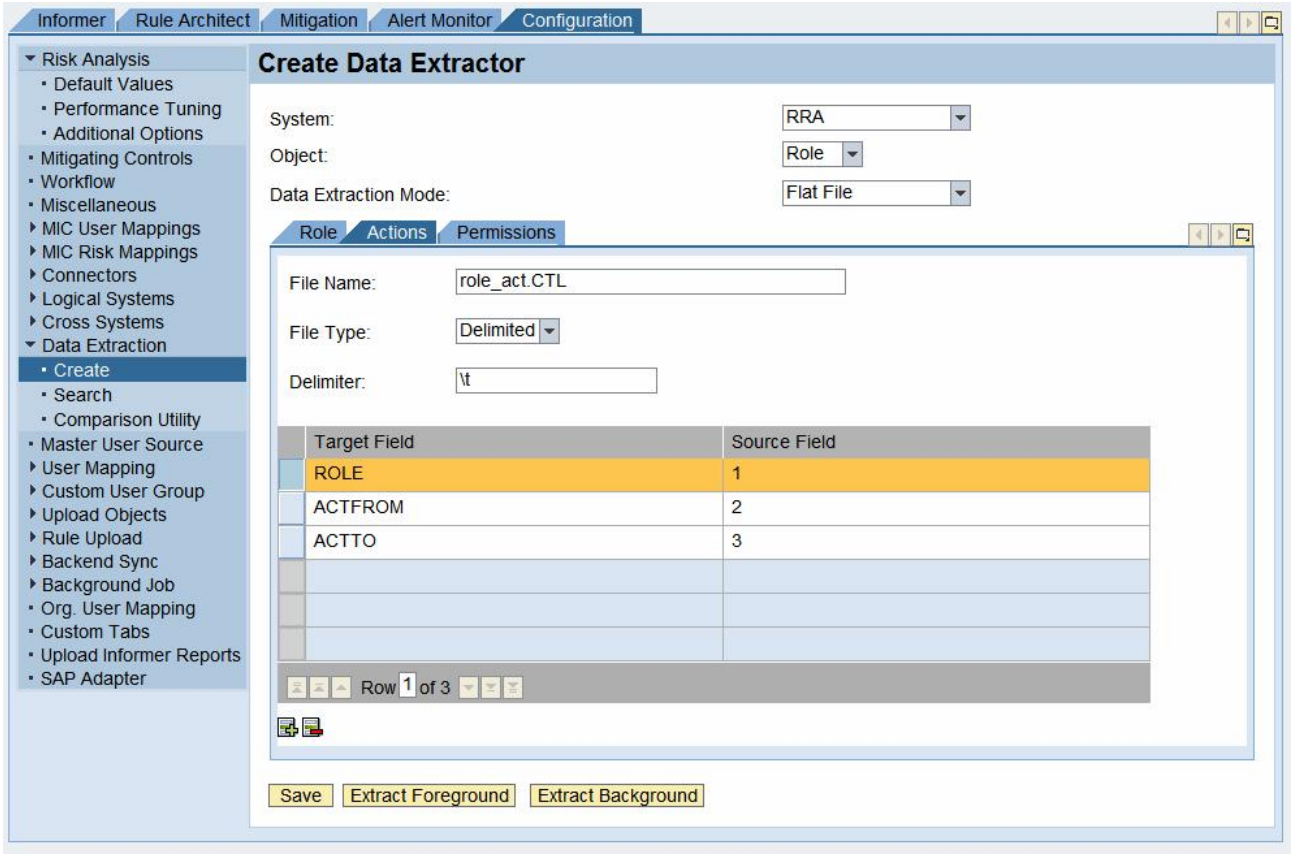


Enter the file name for role data.

Role Actions

Click the Actions tab.

The following screen will be displayed

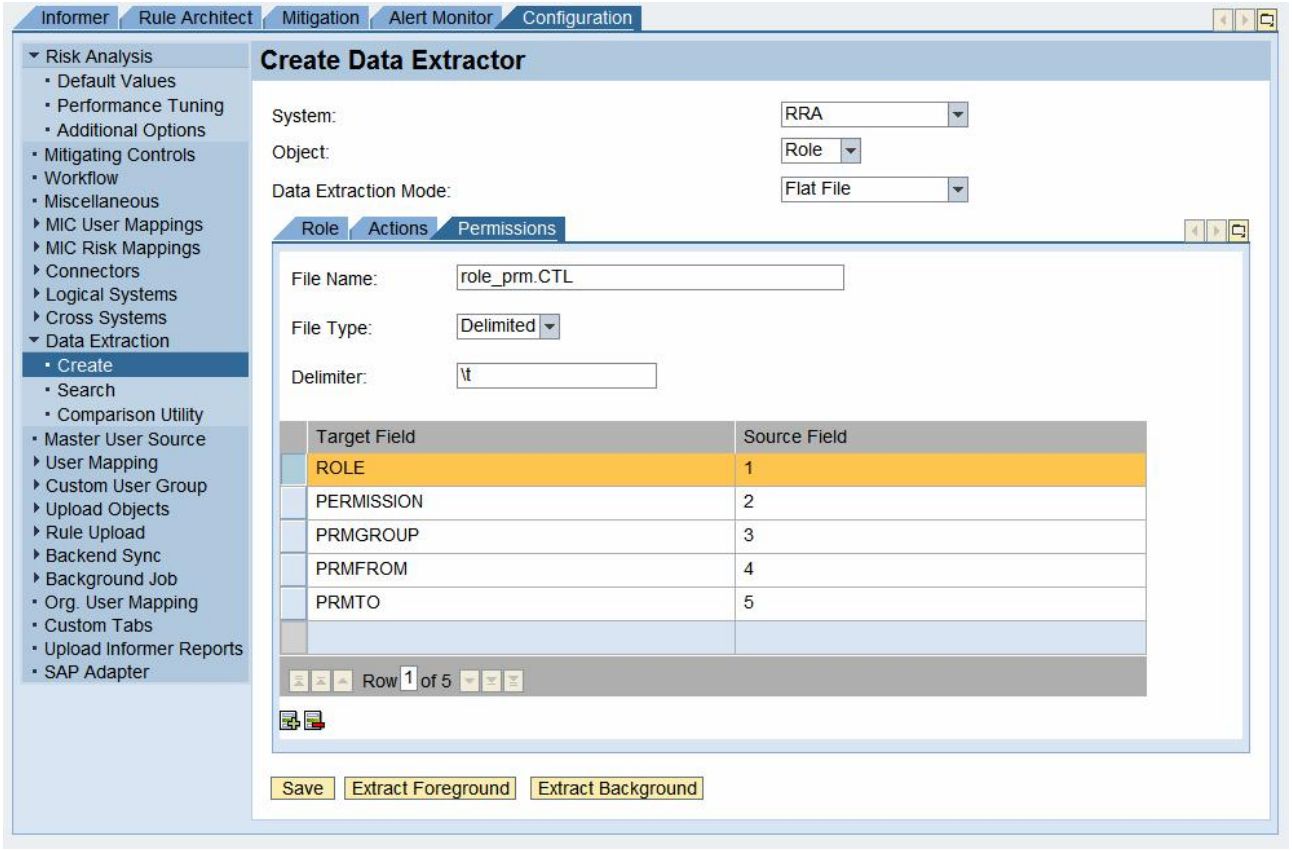


Enter the file name for role activity data.

Role Permissions

Click the Permissions tab.

The following screen will be displayed



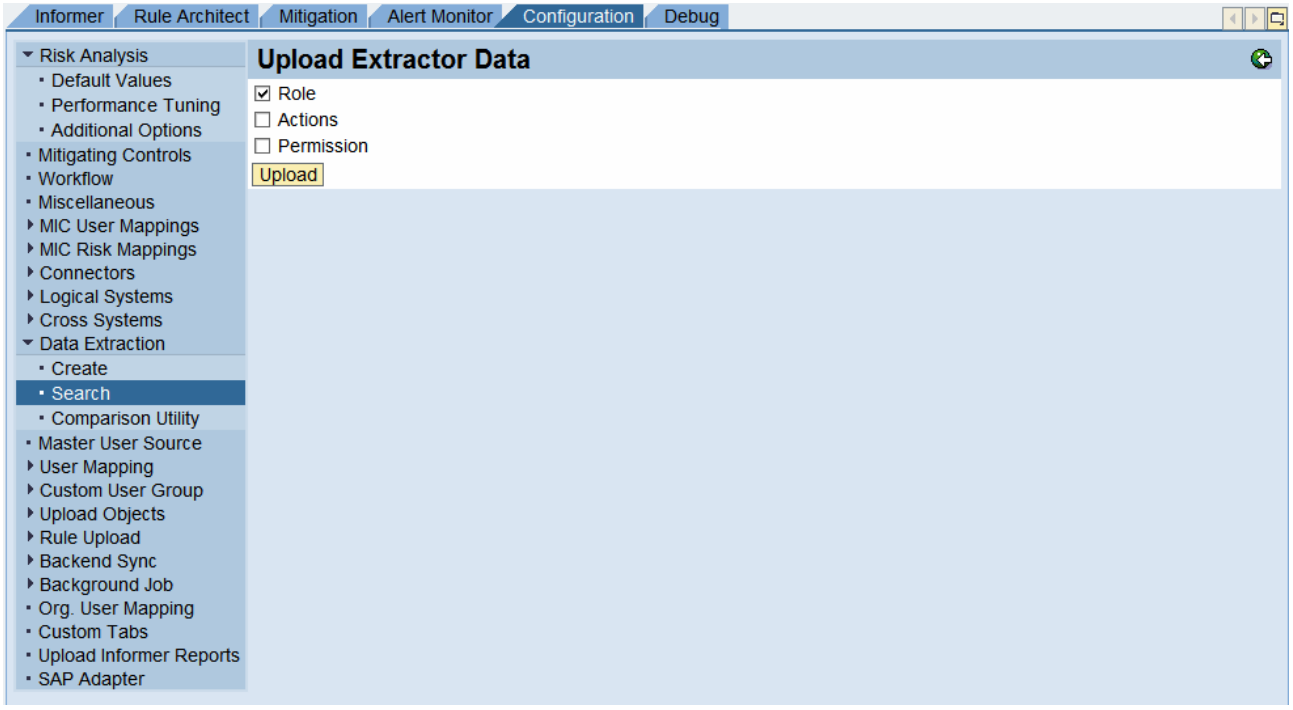
Enter the file name for role permission data.

Extracting Data

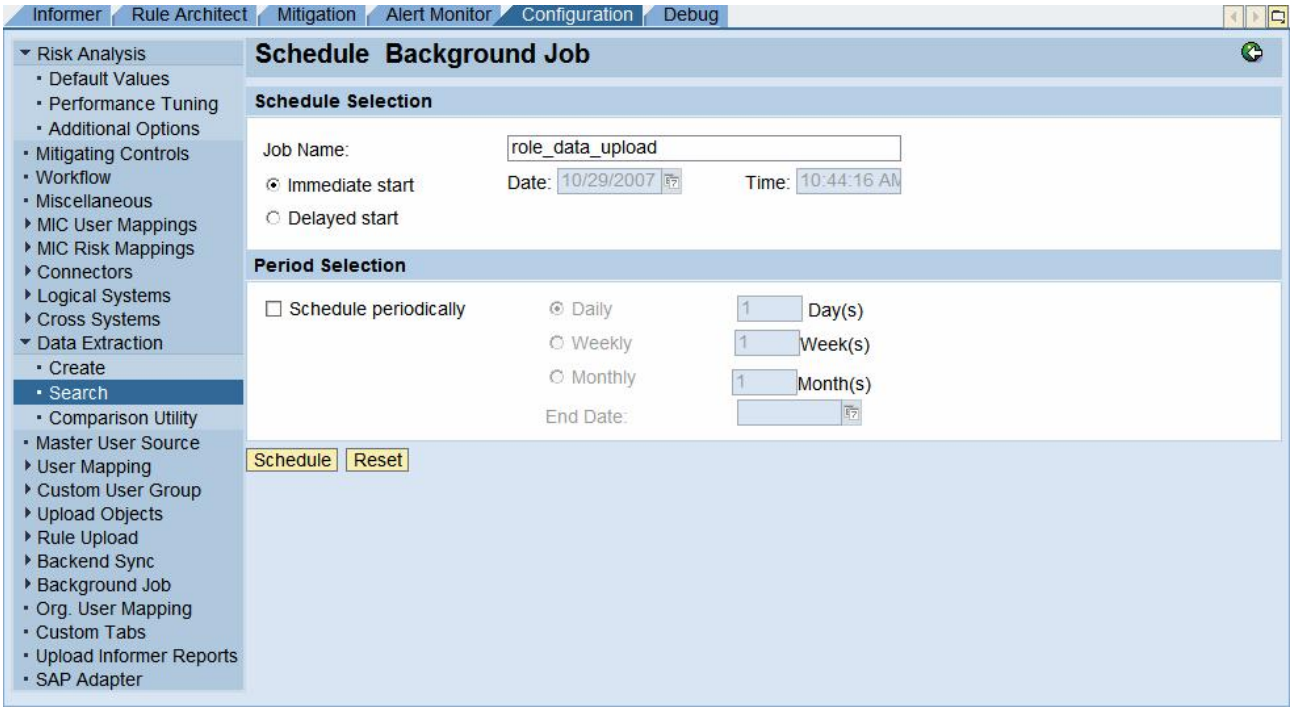
Click the Save Button.

Click Extract Background.

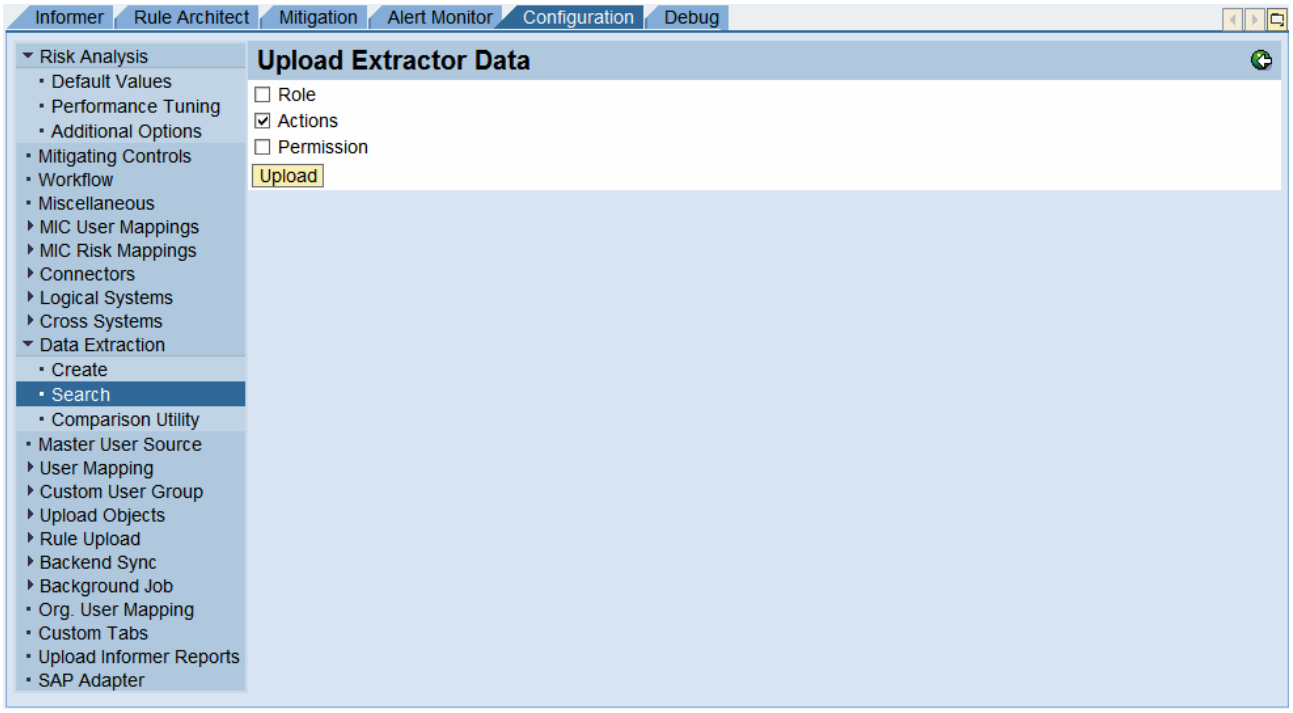
The following screen will be displayed. It is always **recommended** that during data extraction we should extract data from files individually.



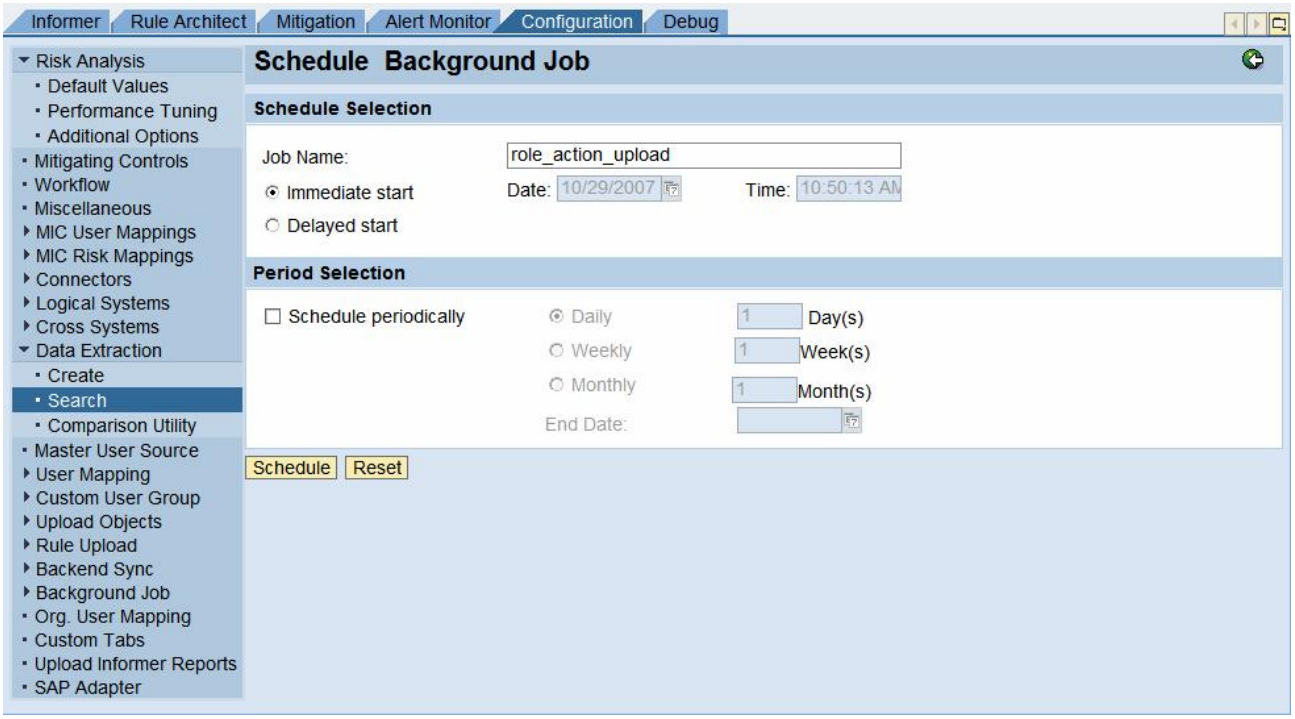
After selecting appropriate checkbox, click **Upload** to schedule Background Job for Role Upload. The following screens will be displayed. Enter the Job name and Click Schedule.



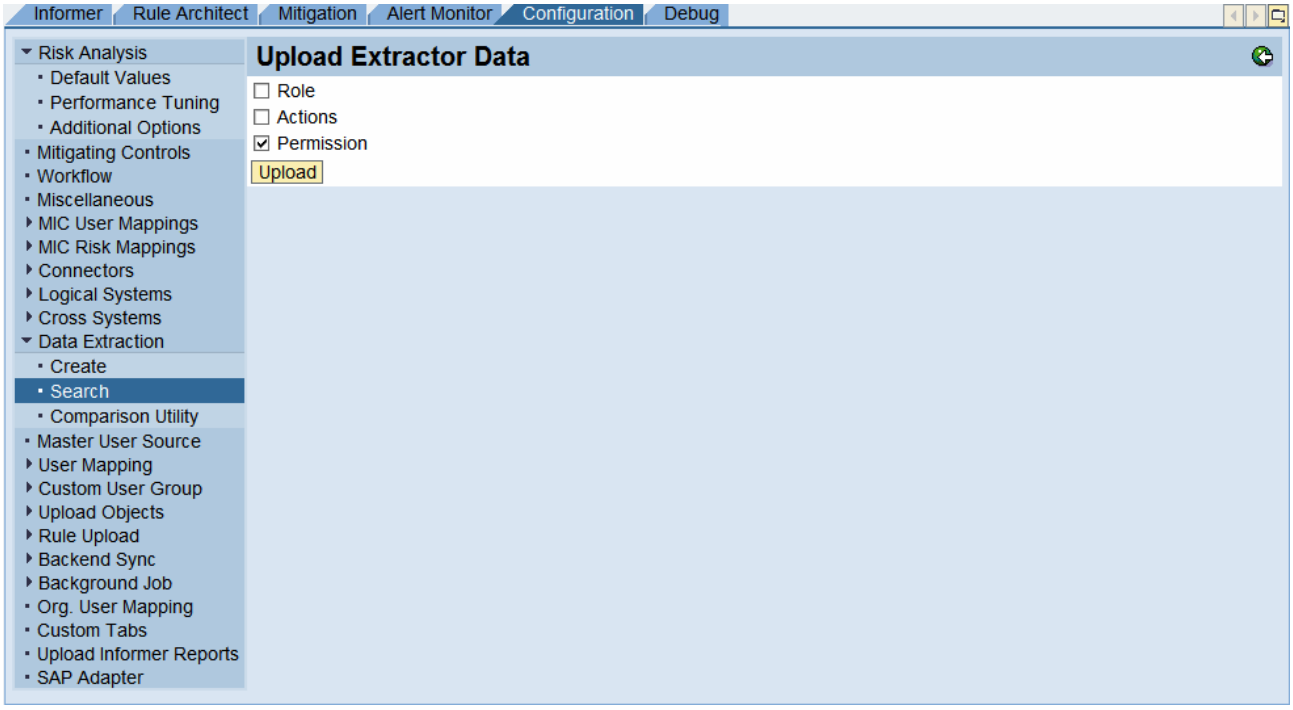
Repeat the same Upload process for Role Actions.



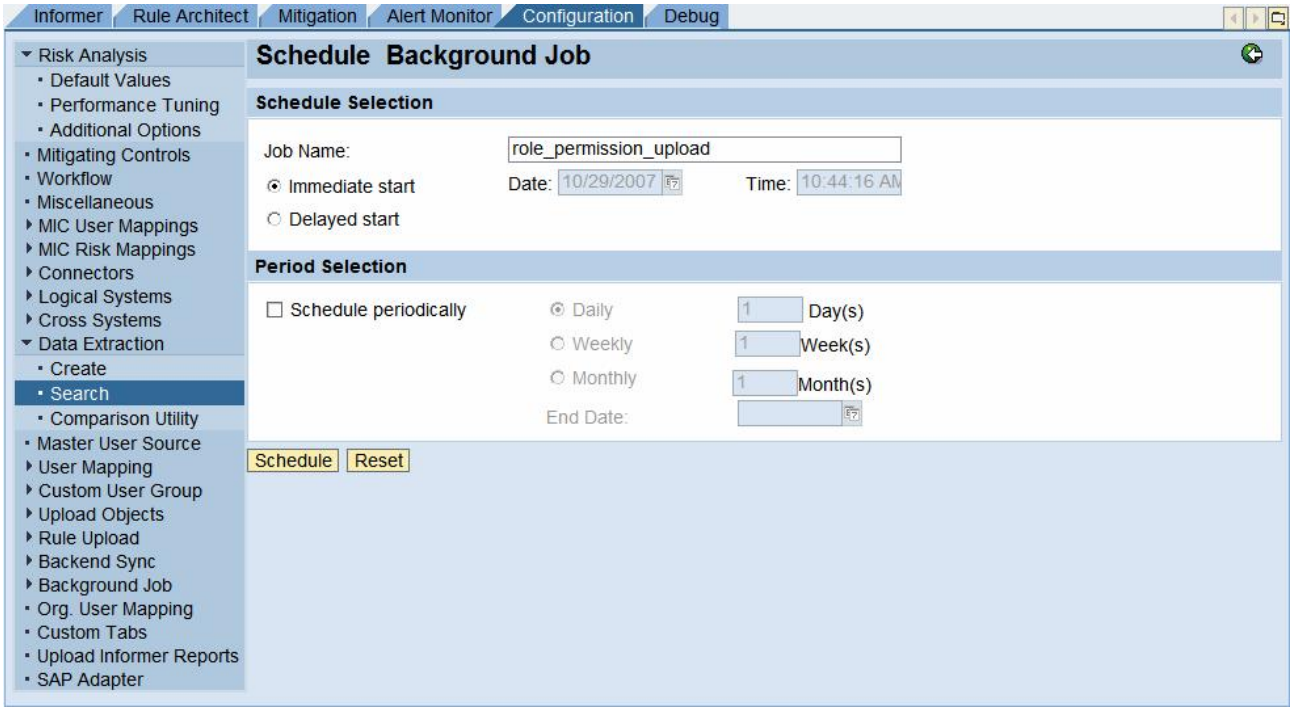
After selecting appropriate checkbox, click **Upload** to schedule Background Job. The following screens will be displayed. Enter the Job name and Click Schedule.



Repeat the same Upload process for Role Permissions.



After selecting appropriate checkbox, click **Upload** to schedule Background Job for Role Permissions upload. The following screens will be displayed. Enter the Job name and Click Schedule.



The Background job for data extraction will be scheduled.

Risk Analysis and Reports

Once User and Role data is uploaded into Risk Identification and Remediation, SOD analysis will be run against the set of rules defined in the system. Once the SOD analysis is done, management reports will be generated against the analyzed data. Following are detail steps to run risk analysis on the data extracted.

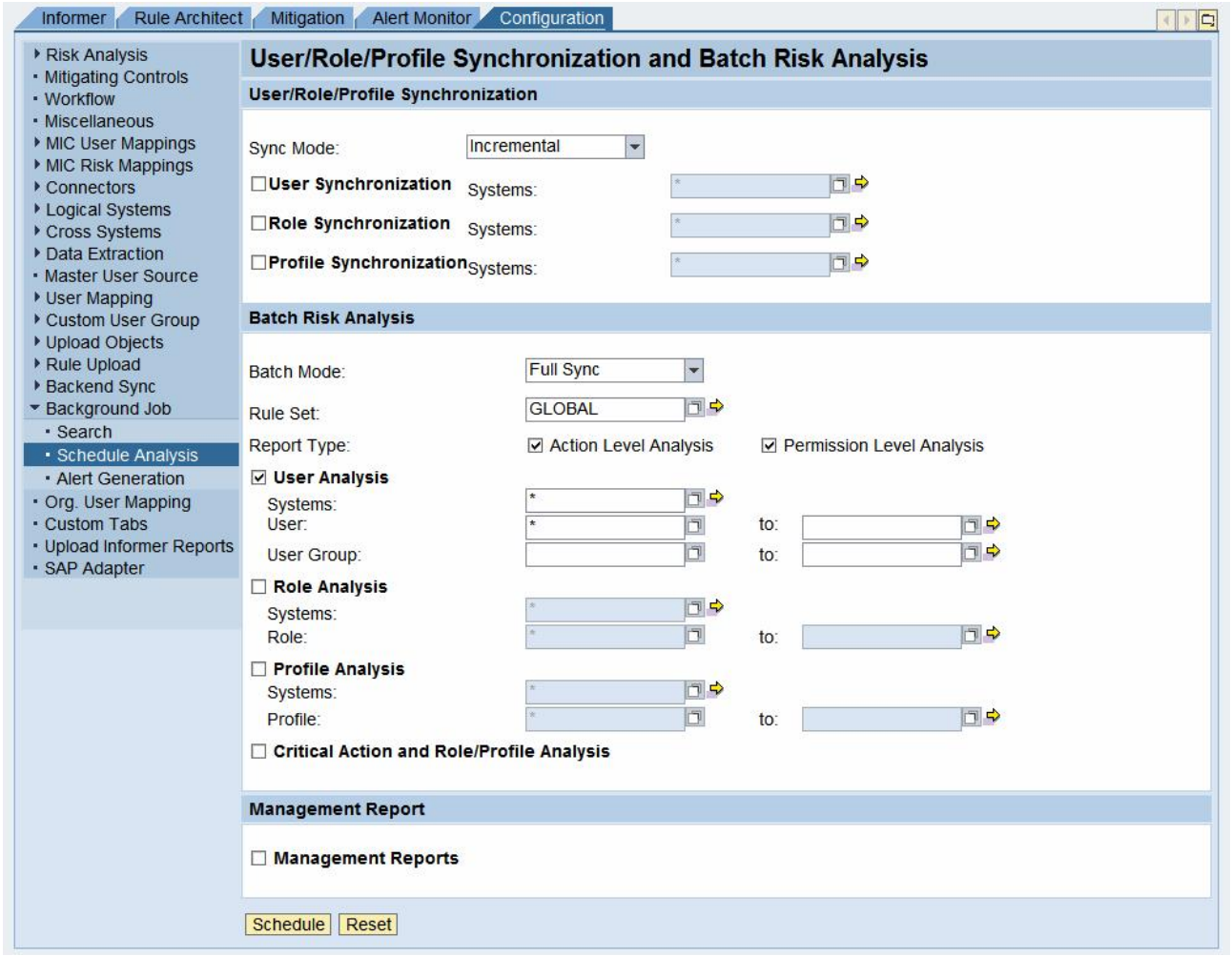
User Risk Analysis

Click the Configuration Tab on top.

From left navigation menu, Click Background Job.

Click Schedule Analysis.

The following screen will be displayed.



Go to Batch Risk Analysis

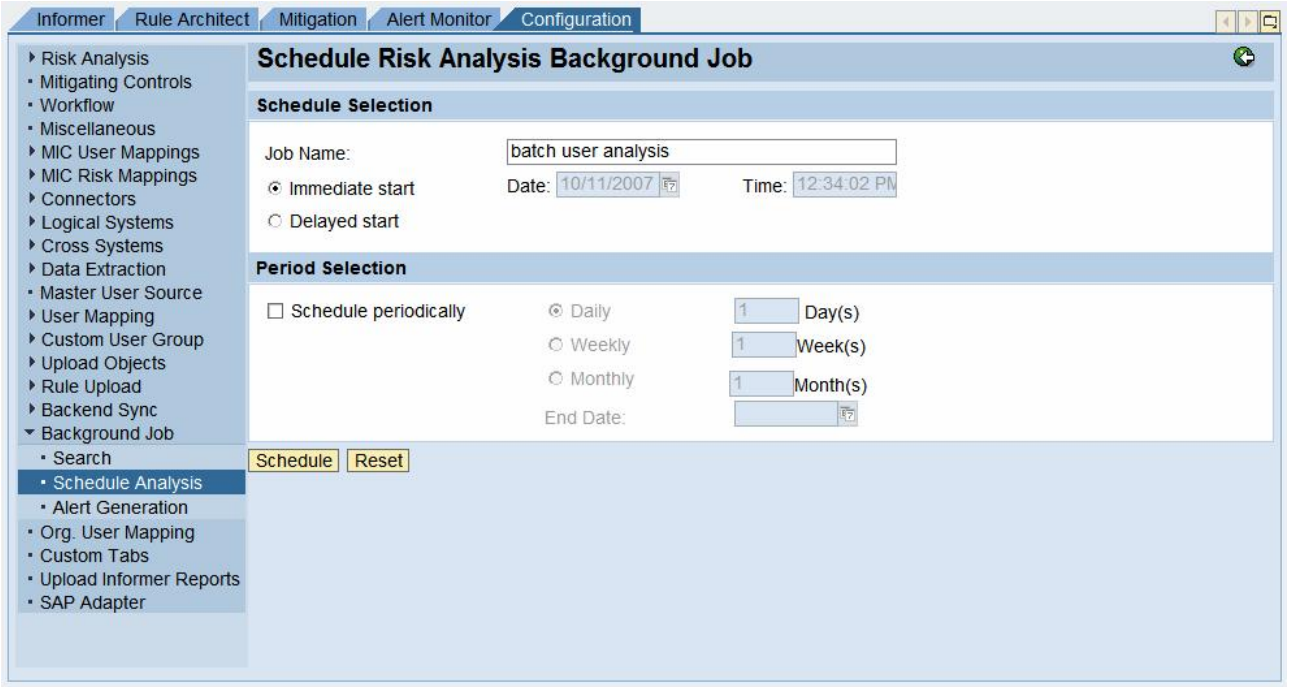
Select Batch Mode as Full Sync

Select Required Report Type.

Check User Analysis.

Click Schedule.

The following screen will be displayed



Click Schedule and User Risk Analysis Background job will be scheduled.

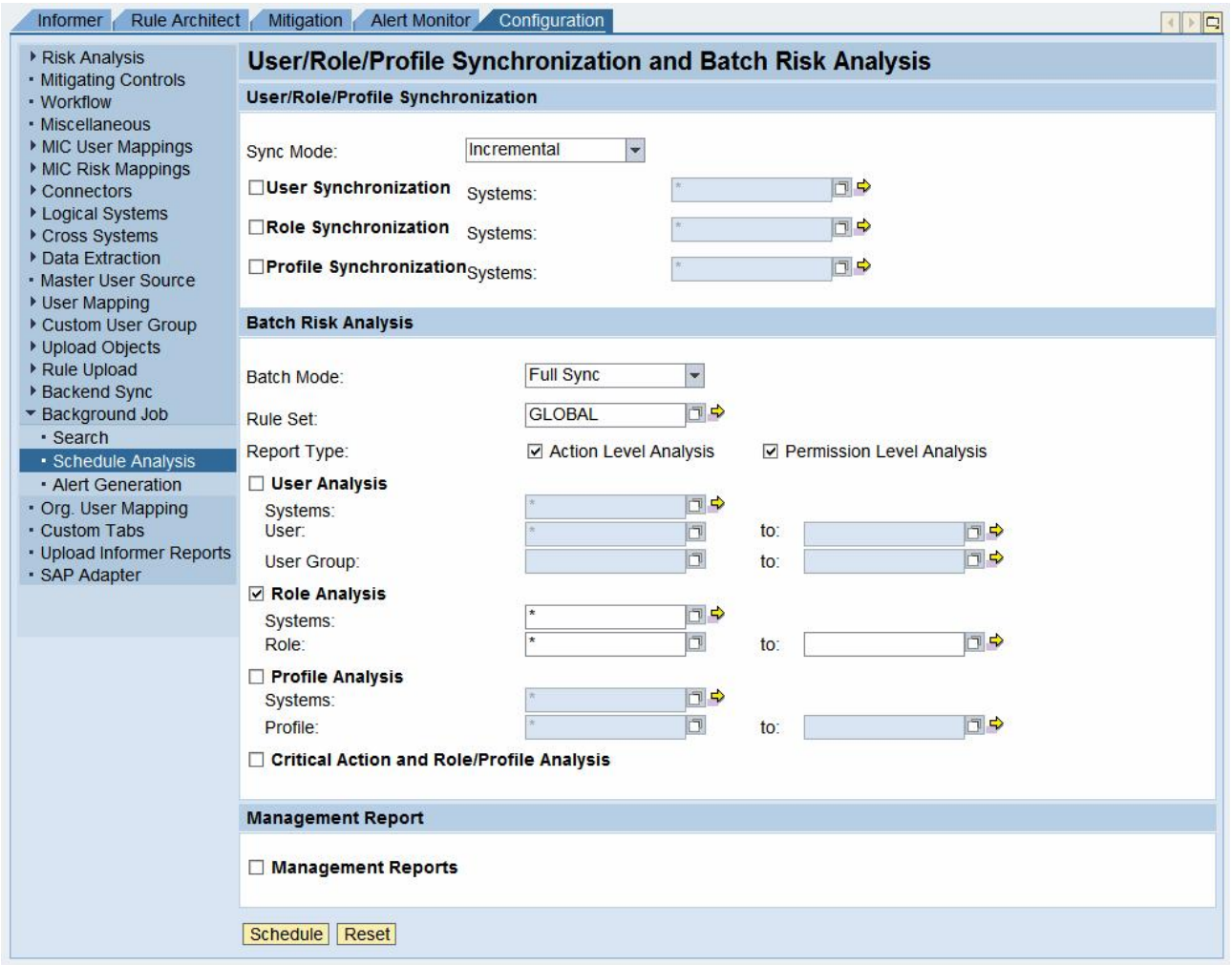
Role Risk Analysis

Click the Configuration Tab on top.

From left navigation menu, Click Background Job.

Click Schedule Analysis.

The following screen will be displayed.



Go to Batch Risk Analysis

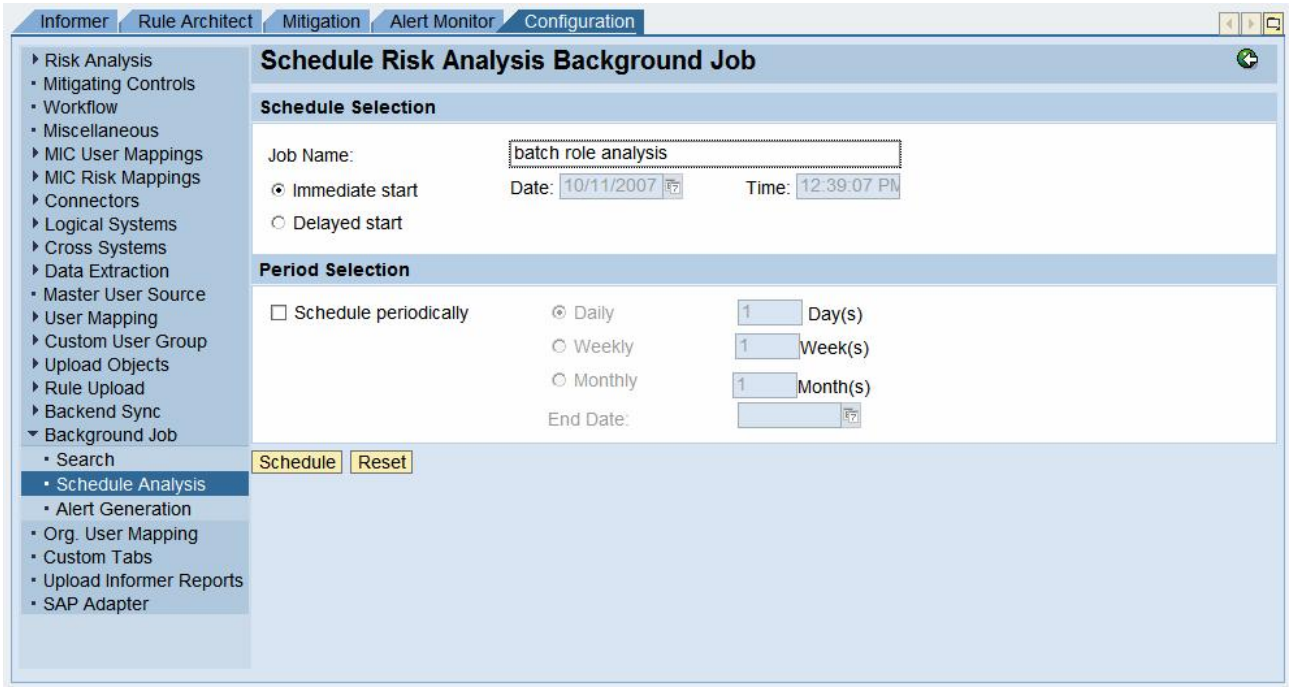
Select Batch Mode as Full Sync

Select Required Report Type.

Check Role Analysis.

Click Schedule.

The following screen will be displayed



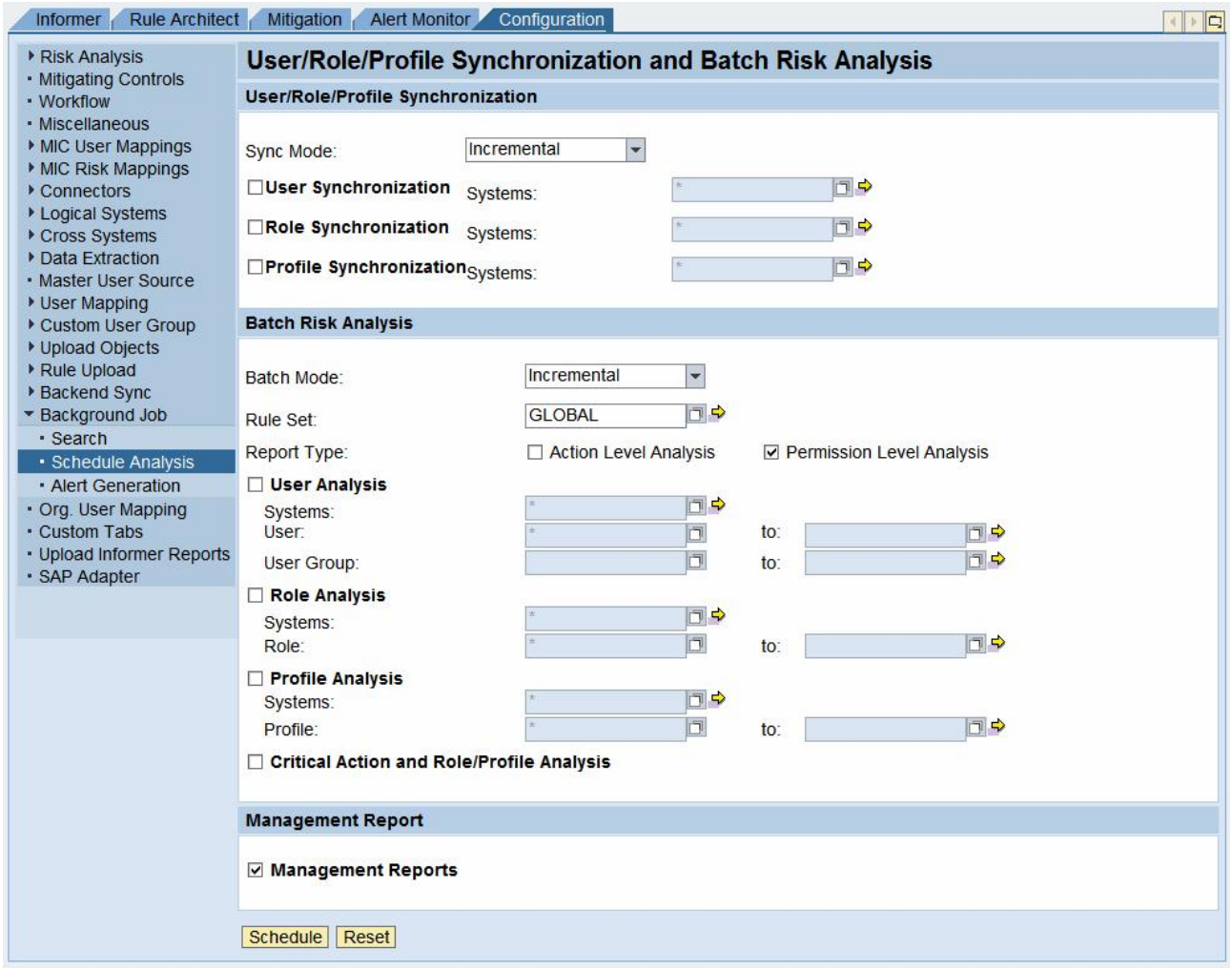
Click Schedule and Role Risk Analysis Background job will be scheduled.

Management Reports

Management report will provide overall information on how many risks exists in the system associated with different Business Processes and provides a graphical view of this report. Management report should be scheduled once the Risk Analysis is done for User and Role data.

Click Schedule Analysis.

The following screen will be displayed.

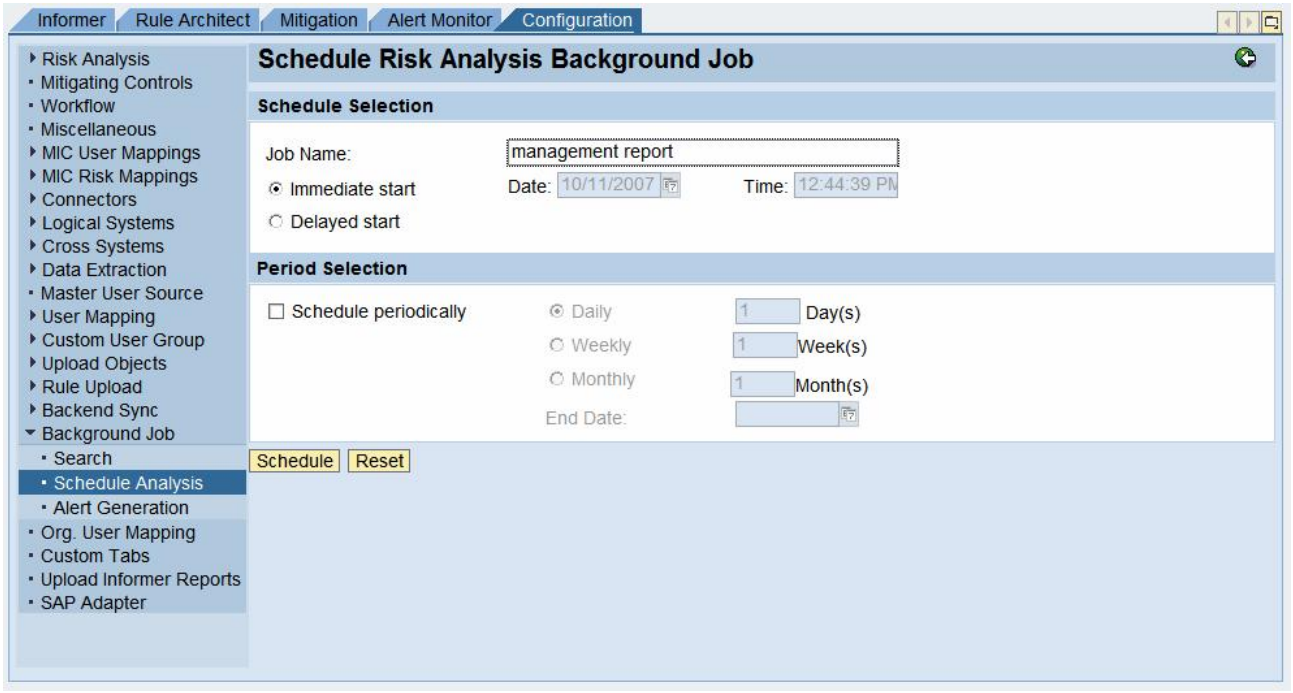


Go to Management Report.

Check Management Report.

Click Schedule.

The following screen will be displayed



Click Schedule and Management Report Background job will be scheduled.

Background Jobs

Status of all the background jobs scheduled can be easy accessed from the Configuration Tab.

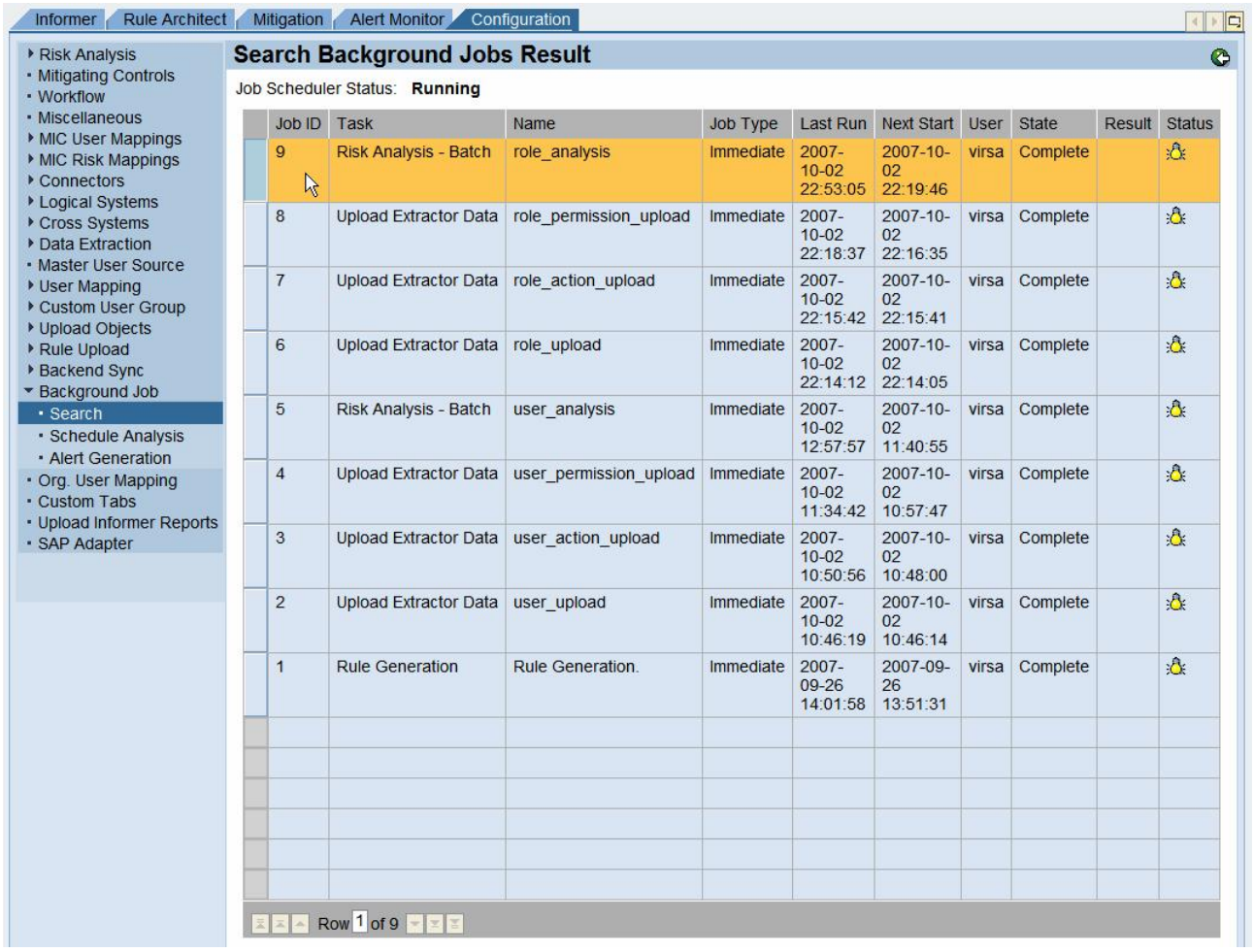
Accessing Background Job's Status

Click the Configuration Tab on top.

From left navigation menu, Click Background Job.

Click Search.

Click the Search button and following screen will be displayed.



We can see the latest status of the background jobs from the **State** column in the report.

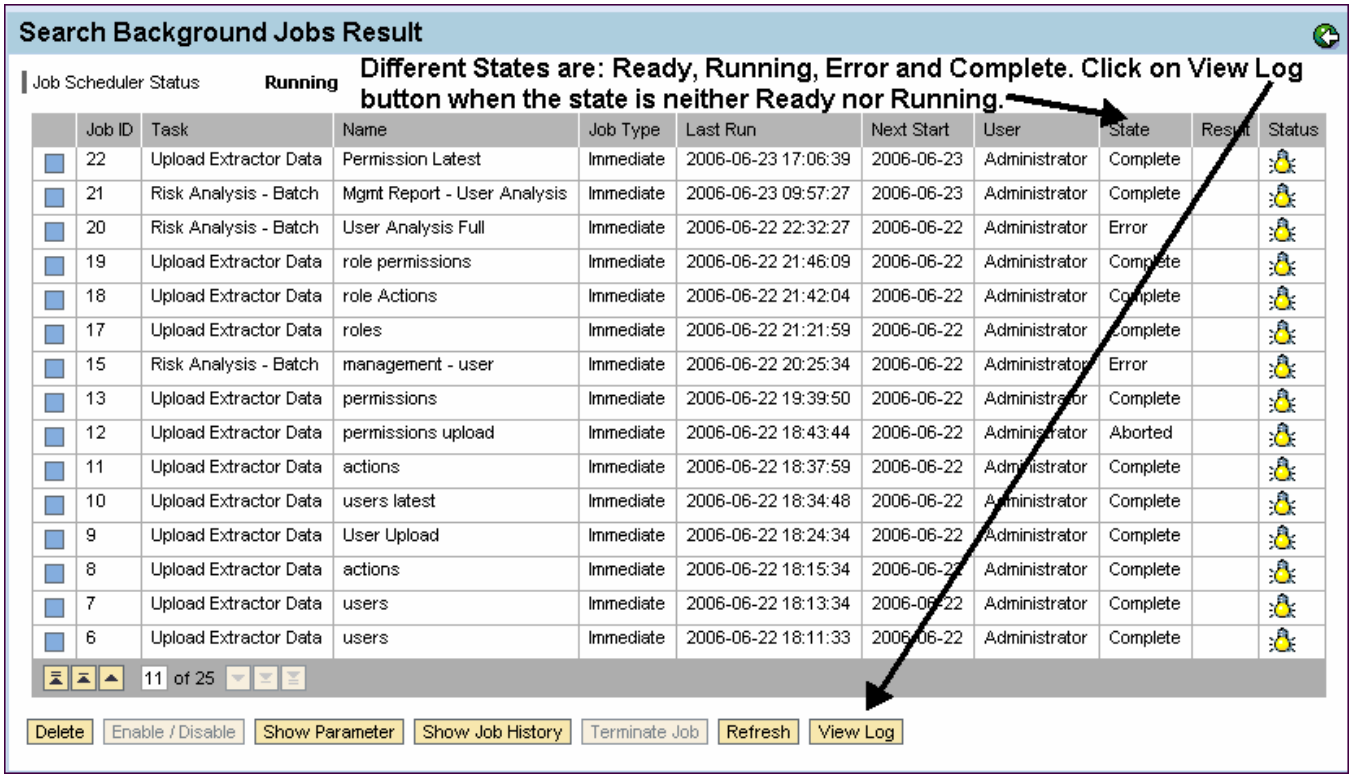
Accessing the Logs

Click the Configuration Tab on top.

From left navigation menu, Click Background Job.

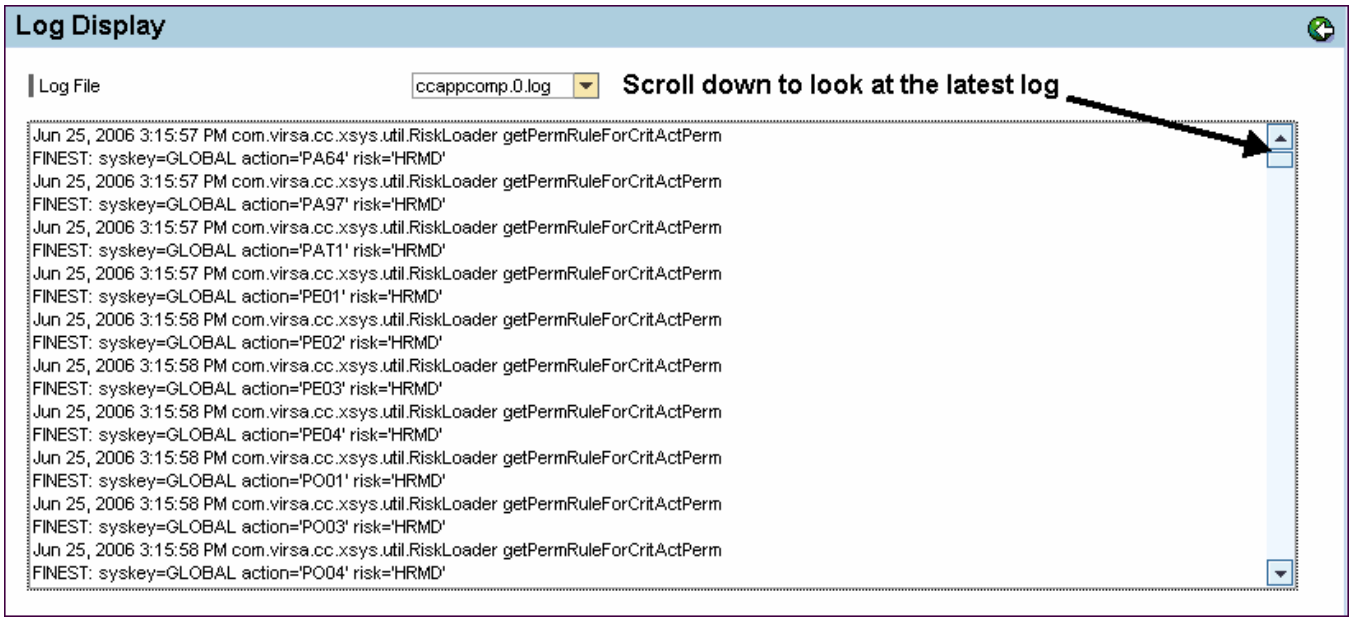
Click Search.

Click the Search button and following screen will be displayed.



To access the logs, Click View Log.

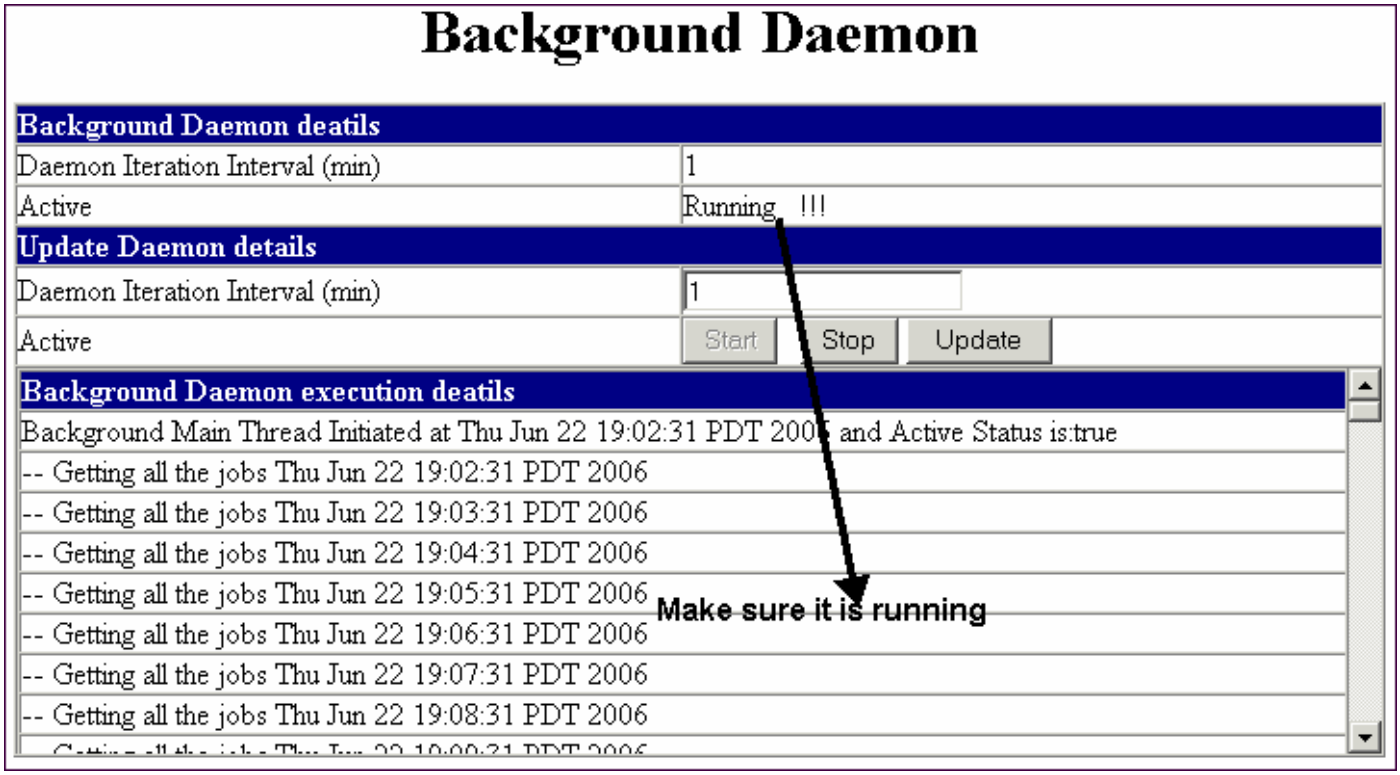
The following screen will be displayed.



Accessing the Background Job Daemon

The background job daemon resides on the URL http://<server_ip>:<port_id>/virsa/CCBgStatus.jsp

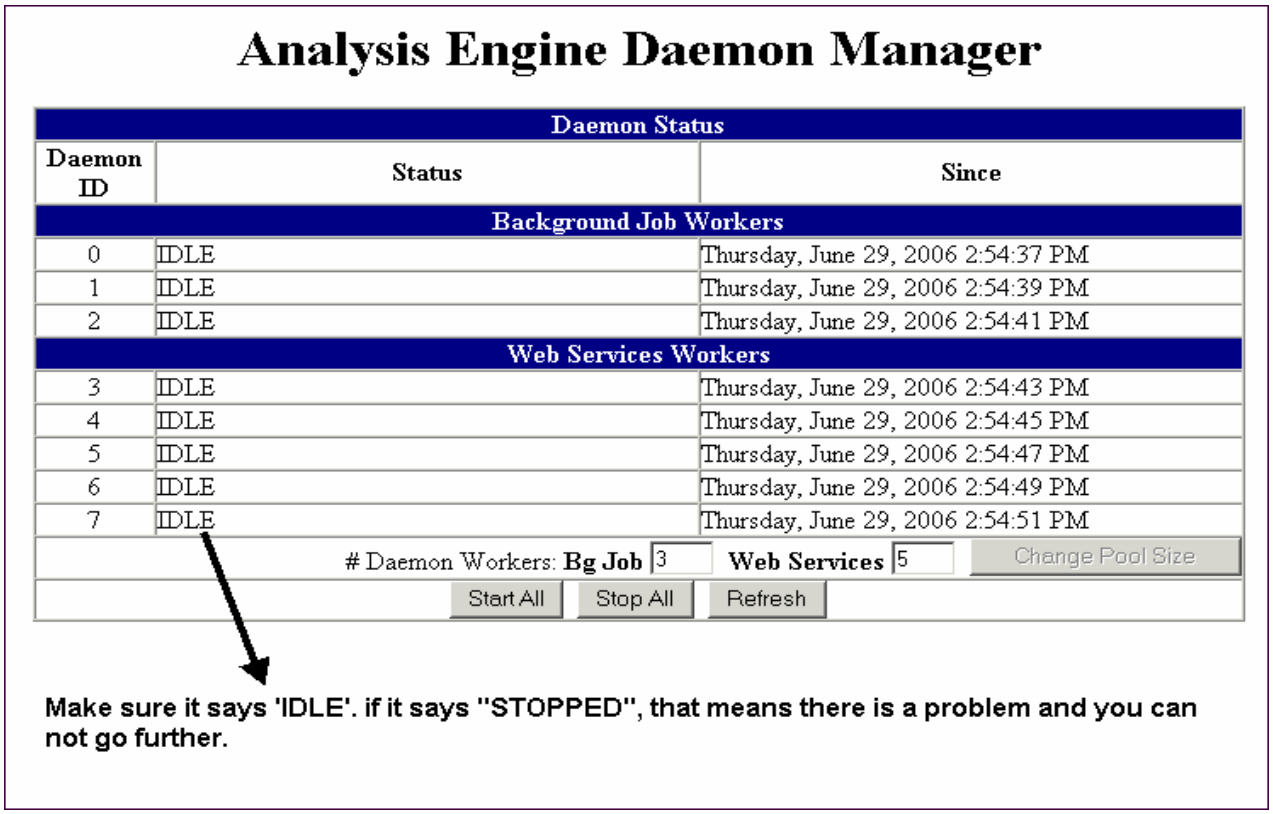
The Background daemon displays the status as follows.



Accessing the Analysis Daemon

The risk analysis daemon resides on the URL http://<server_ip>:<port_id>/virsa/CCADStatus.jsp

The Analysis daemon displays the status as follows.



Copyright