

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

Applies to:.....	1
Summary	1
Author Bio.....	1
Introduction.....	4
ERP Extraction.....	5
Generating Object Files	5
Generating ERP Authorization Objects.....	5
Generating ERP Description Objects.....	6
Extracting Data from ERP System	7
User Data Extraction	7
Role Data Extraction	15
Configuring Risk Identification and Remediation.....	21
Create a Connector	21
Upload Objects.....	23
Uploading Text Objects.....	23
Uploading Auth Objects.....	24
Rule Upload	25
Uploading Business Process	25
Uploading Functions	26
Uploading Function Authorizations	27
Uploading Rule Set	28
Uploading Risks' Details.....	29
Rule Generation	30
Additional Configuration.....	31
Data Upload.....	32
Uploading User Data	32
Users	32
User Actions	33
User Permissions	34
Extracting Data	34
Uploading Role Data.....	38
Roles	38
Role Actions.....	39
Role Permissions	40
Extracting Data	41
Risk Analysis and Reports.....	44
User Risk Analysis.....	44
Role Risk Analysis.....	45
Management Reports	48

<u>Background Jobs</u>	<u>50</u>
<u> Accessing Background Job's Status</u>	<u>50</u>
<u> Accessing the Logs</u>	<u>51</u>
<u> Accessing the Background Job Daemon.....</u>	<u>52</u>
<u> Accessing the Analysis Daemon.....</u>	<u>53</u>
<u>Copyright</u>	<u>54</u>

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

```

sap_obj.txt - Notepad
File Edit Format View Help
$SEU S_DEVELOP ACTVT 03
$SEU S_DEVELOP DEVCLASS
$SEU S_DEVELOP OBJNAME
$SEU S_DEVELOP OBJTYPE
$SEU S_DEVELOP P_GROUP
/SAPSMOSS/IQS1 Q_GP_CODE QCODEGRP $$OSS*
/SAPSMOSS/IQS1 Q_GP_CODE QKATART 2
/SAPSMOSS/IQS1 Q_GP_CODE QKATART D
/SAPSMOSS/IQS1 Q_QMEL QMART
/SAPSMOSS/IQS1 Q_QMEL TCD /SAPSMOSS/IQS1
/SAPSMOSS/IQS1 Q_QMEL WERKS $WERKS
/SAPSMOSS/IQS1 Q_VORG_MEL BETRVORG
/SAPSMOSS/IQS1 Q_VORG_MEL QMART
/SAPSMOSS/IQS1 S_TCODE TCD /SAPSMOSS/IQS1
/SAPSMOSS/IQS2 B_NOT_TASK NOT_TSK_AC 22
/SAPSMOSS/IQS2 B_NOT_TASK NOT_TSK_AC 21
/SAPSMOSS/IQS2 B_NOT_TASK NOT_TSK_AC 12
/SAPSMOSS/IQS2 B_NOT_TASK NOT_TSK_AC 11
/SAPSMOSS/IQS2 B_NOT_TASK QCODEGRP
/SAPSMOSS/IQS2 B_NOT_TASK QKATART
/SAPSMOSS/IQS2 Q_GP_CODE QCODEGRP $$OSS*
/SAPSMOSS/IQS2 Q_GP_CODE QKATART 2
/SAPSMOSS/IQS2 Q_GP_CODE QKATART D
/SAPSMOSS/IQS2 Q_QMEL QMART
/SAPSMOSS/IQS2 Q_QMEL TCD /SAPSMOSS/IQS2
/SAPSMOSS/IQS2 Q_QMEL WERKS $WERKS

```

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

```

File Edit Format View Help
ACT          VRD   EN    C SD Generate Data f. Orders on Hand
ACT          $SEU  EN    Repository Info System INTERNAL
ACT          /SAPSMOSS/IQS1 EN    Create notification
ACT          /SAPSMOSS/IQS2 EN    Change notification
ACT          /SAPSMOSS/IQS3 EN    Display notification
ACT          /SAPSMOSS/M00 EN    R/3 notifications
ACT          /SAPSMOSS/M01 EN    R/3 notifications
ACT          /SAPSMOSS/M02 EN    R/3 notifications
ACT          /SAPSMOSS/001 EN    SAP add-on system installation
ACT          /SAPSMOSS/002 EN    SAP add-on system release
ACT          /SAPSMOSS/003 EN    SAP database system
ACT          /SAPSMOSS/004 EN    Frontend for SAP operating system
ACT          /SAPSMOSS/005 EN    SAP installation
ACT          /SAPSMOSS/006 EN    SAP operating system
ACT          /SAPSMOSS/007 EN    SAP release
ACT          /SAPSMOSS/008 EN    SAP system type
ACT          /SAPSMOSS/009 EN    SAP system type
ACT          /SAPSMOSS/QM10 EN    Change list of R/3 notifications
ACT          /SAPSMOSS/QM11 EN    Display list of R/3 notifications
ACT          /SAPSMOSS/QM12 EN    Change list of tasks
ACT          /SAPSMOSS/QM13 EN    Display list of tasks
ACT          /SAPSMOSS/QM19 EN    List of R/3 notifications, multilvl
ACT          /SAPSMOSS/QM50 EN    Time line display:R/3 notifications
ACT          /SAPSMOSS/U01 EN    Updating R/3 notifications
ACT          /SAPSMOSS/U02 EN    Update job planning
ACT          /SAPSMOSS/U03 EN    Update job overview

```

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
 DEPARTMENT - 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).

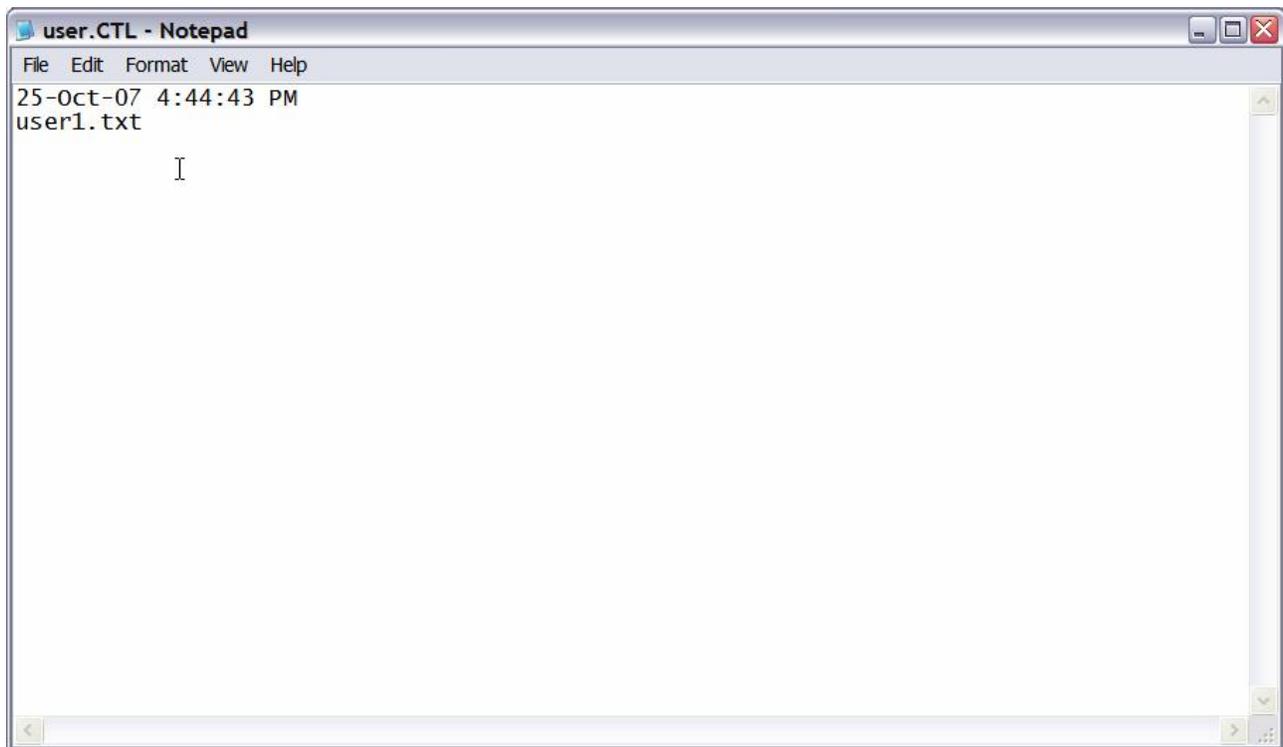
There should not be any blank records at the end of the file.

```

users.txt - Notepad
File Edit Format View Help
AACEVEDO      Albert  Acevedo      GLNM
AADAMS Alwyn  Adams  aadams@glanbiacheese.co.uk
AADCOCK Amy    Adcock  Amy.Adcock@cheese.co.uk      TCCL      GLCH
AAJIBOYE      Ademipo Ajiboye aajiboye@glanbia.ie        DAIR
AANDERSON     ALISTAIR ANDERSON      GLCH
AARSCOTT      Ashley Arscott      TCCL
ABAKER Baker  Andrea      TCCL
ABANJAC Alex   Banjac      GLIN
ABARRY Aonghus Barry  abarry@glanbia.ie          INGS
ABATON Angela Baton  abaton@glanbiausa.com      GLIN
ABEATTIE      Alex   Beattie  ABEATTIE@GLANBIA.IE      CHIL
ABENNETT      Andrew Bennett abennett@glanbia.com      Dispatch  GNUK
ABOWE Aidan  Bowe      CMIL
ABOWEN Bowen  Andrea      TCCL
ABRADY Andy   Brady  abrad@glanbia.ie          MILK
ABULLERS      Angie  Bullers     GLIN
ACLARE Adrian Clare      TCCL
ACLARKE Arlene Clarke     INGS
ACOIGNET      Armelle Coignet  ACoignet@glanbia.ie      DAIR
ACOLEMAN      Amanda Coleman     SSCI
ACOLLINS      Aedin  Collins     CORE_MODEL
ACONROY Alice  Conroy  ACONROY@GLANBIA.IE      TRAD
ACOURTNEY     Anthony Courtney    TCCL
ACUDDIHY      Andrew Cuddihy     TRAD
ACURLEY Aoife  Curley  acurley@glanbia.ie        PMIE
ADAVIDSON     Alex   Davidson  adavidson@glanbiacheese.co.uk

```

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. In case 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.

“ACTIONFROM” (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.

```

user_activity_001.txt - Notepad
File Edit Format View Help
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MD04      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MD06      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MI03      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MI06      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MI20      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MI22      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MI23      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MIGO      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MM75      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MMBE      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MR51      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MSC3      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MSC3N     T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MSC4      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MSC4N     T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MSK3      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MBSM      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      BMBC      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MB03      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MB25      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MB51      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MB52      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MB54      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MB56      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MB58      T-DV780617
AACEVEDO      ZGLNMALLMMIM04_INQUIRY_DI      MBLB      T-DV780617

```

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. In case 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.

```

user_act.CTL - Notepad
File Edit Format View Help
15-Oct-07 10:58:14 AM
user_act1.txt
user_act2.txt
user_act3.txt
user_act4.txt
user_act5.txt
user_act6.txt
user_act7.txt
user_act8.txt
user_act9.txt
user_act10.txt
user_act11.txt
user_act12.txt
user_act13.txt
user_act14.txt
user_act15.txt
user_act16.txt
user_act17.txt
user_act18.txt
user_act19.txt

```

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 columns 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:

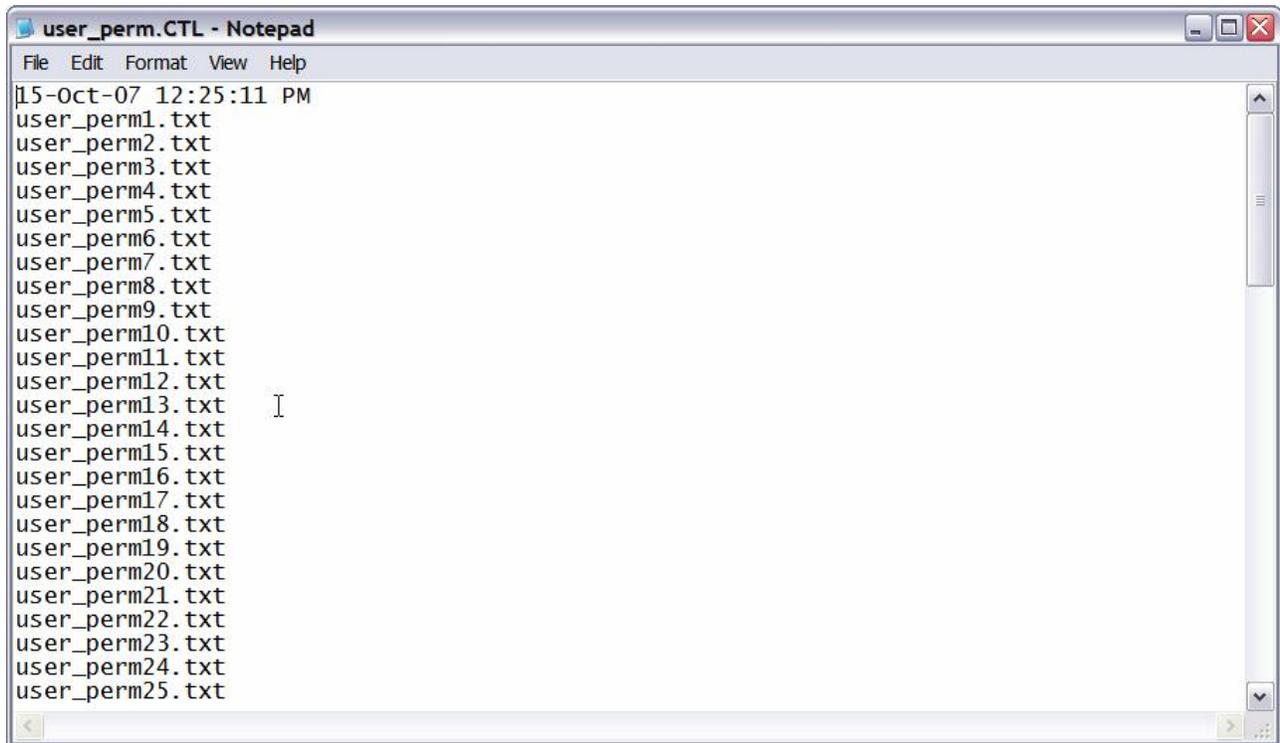
In the User Permission file, the "PERMISSION" field value must be joined with "|" separator. Unique record value based on combination of USERID, ROLE, PERMISSION, PRMGRP, FROMVALUE, and TOVALUE fields (User ID, Role, Permission, PRMGroup/SeqNo, From Value, and To Value).

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.

Role/Responsibility	Permission	PRMGRP	TOVALUE
ZGLNMALLMMIM04_INQUIRY_DI	M_MSEG_WWE ACTVT		1
ZGLNMALLMMIM04_INQUIRY_DI	M_MSEG_WWE WERKS		1
ZGLNMALLMMIM04_INQUIRY_DI	M_MTDI_ORG DISPO		2
ZGLNMALLMMIM04_INQUIRY_DI	M_MTDI_ORG MDAKT		2
ZGLNMALLMMIM04_INQUIRY_DI	M_MTDI_ORG MDAKT		2
ZGLNMALLMMIM04_INQUIRY_DI	M_MTDI_ORG MDAKT		2
ZGLNMALLMMIM04_INQUIRY_DI	M_MTDI_ORG WERKS		2
ZGLNMALLMMIM04_INQUIRY_DI	M_RAHM_BSA ACTVT		3
ZGLNMALLMMIM04_INQUIRY_DI	M_RAHM_BSA BSART		3
ZGLNMALLMMIM04_INQUIRY_DI	M_RAHM_EKG ACTVT		4
ZGLNMALLMMIM04_INQUIRY_DI	M_RAHM_EKG EKGRP		4
ZGLNMALLMMIM04_INQUIRY_DI	M_RAHM_EKO ACTVT		5
ZGLNMALLMMIM04_INQUIRY_DI	M_RAHM_EKO EKORG		5
ZGLNMALLMMIM04_INQUIRY_DI	M_RAHM_WRK ACTVT		6
ZGLNMALLMMIM04_INQUIRY_DI	M_RAHM_WRK WERKS		6
ZGLNMALLMMIM04_INQUIRY_DI	S_TCODE TCD	7	BMBC
ZGLNMALLMMIM04_INQUIRY_DI	S_TCODE TCD	7	MB03
ZGLNMALLMMIM04_INQUIRY_DI	M_MSEG_WWA WERKS		8
ZGLNMALLMMIM04_INQUIRY_DI	M_MRES_WWA ACTVT		9
ZGLNMALLMMIM04_INQUIRY_DI	M_MRES_WWA WERKS		9
ZGLNMALLMMIM04_INQUIRY_DI	M_MSEG_BMB ACTVT		10
ZGLNMALLMMIM04_INQUIRY_DI	M_MSEG_BMB BWART		10
ZGLNMALLMMIM04_INQUIRY_DI	M_MSEG_BWA ACTVT		11
ZGLNMALLMMIM04_INQUIRY_DI	M_MSEG_BWA BWART		11
ZGLNMALLMMIM04_INQUIRY_DI	M_MSEG_BWE ACTVT		12
ZGLNMALLMMIM04_INQUIRY_DI	M_MSEG_BWE BWART		12

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. In case 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.

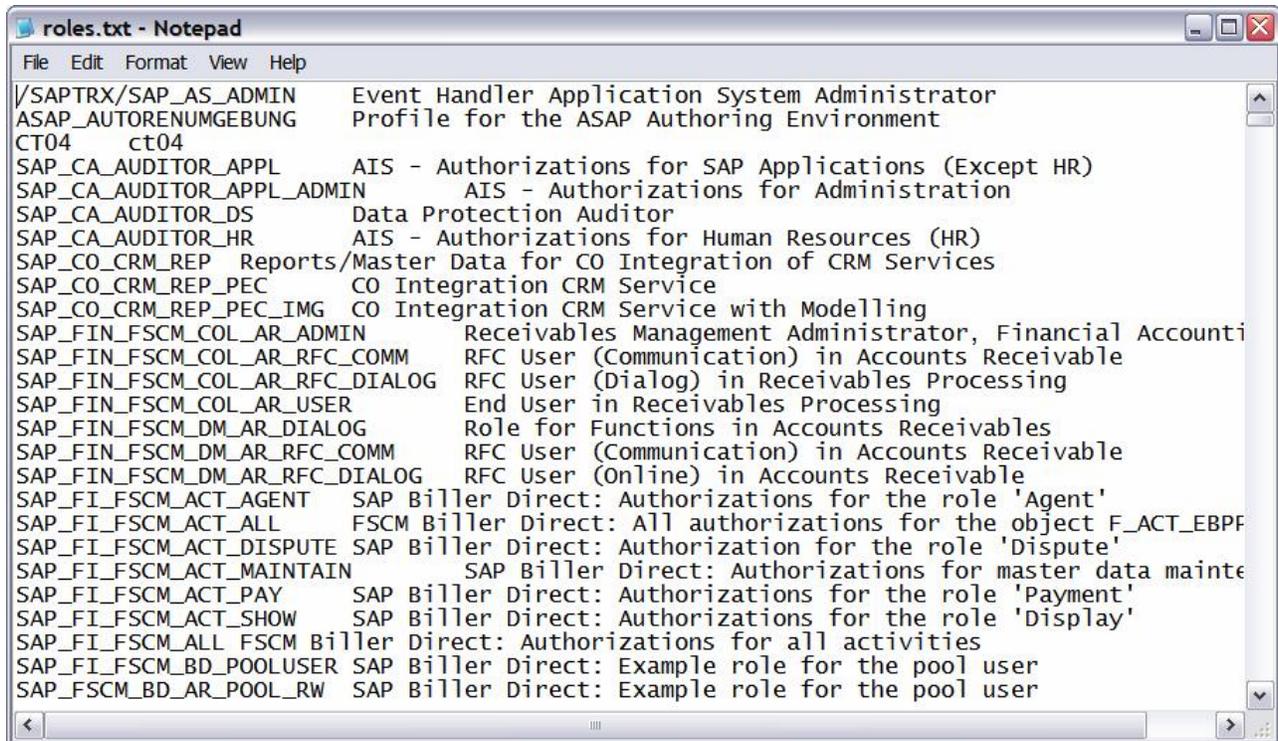
ROLE DESCRIPTION - Role/Responsibility Description.

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.

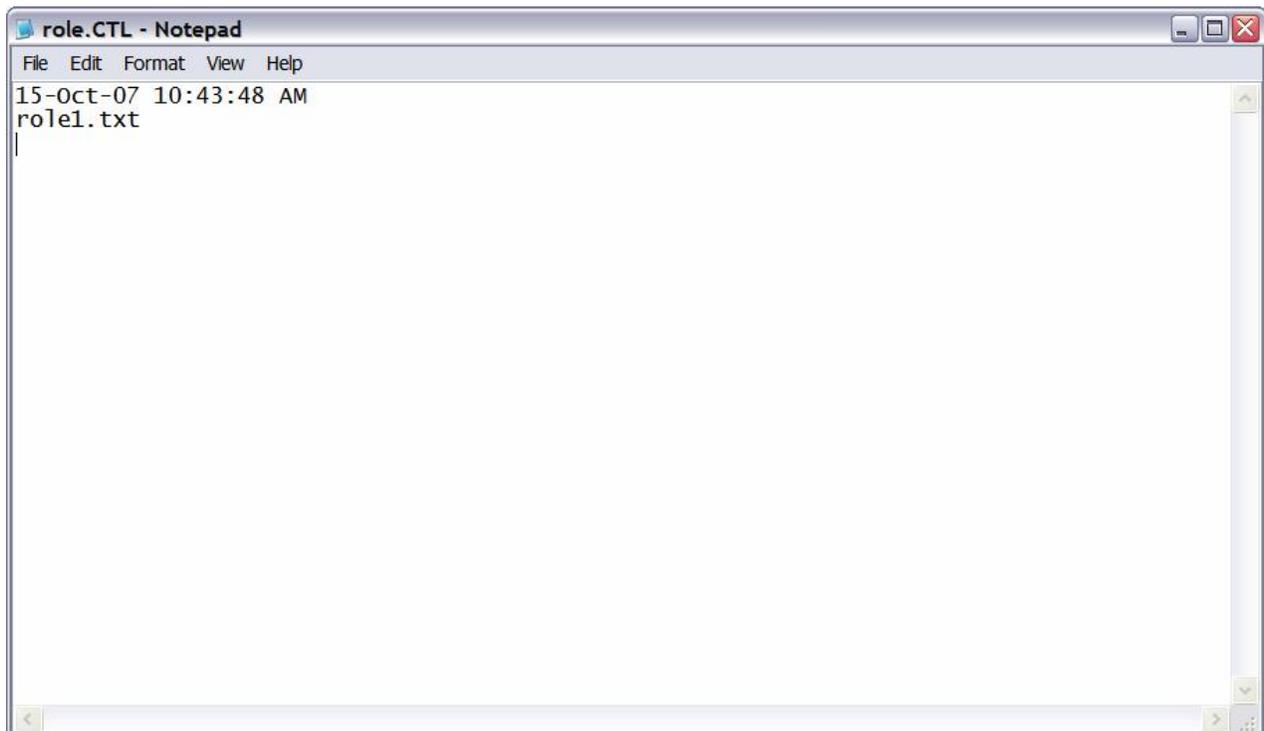


```

roles.txt - Notepad
File Edit Format View Help
/SAPTRX/SAP_AS_ADMIN      Event Handler Application System Administrator
ASAP_AUTORENUMGEBUNG     Profile for the ASAP Authoring Environment
CT04      ct04
SAP_CA_AUDITOR_APPL      AIS - Authorizations for SAP Applications (Except HR)
SAP_CA_AUDITOR_APPL_ADMIN  AIS - Authorizations for Administration
SAP_CA_AUDITOR_DS        Data Protection Auditor
SAP_CA_AUDITOR_HR        AIS - Authorizations for Human Resources (HR)
SAP_CO_CRM_REP            Reports/Master Data for CO Integration of CRM Services
SAP_CO_CRM_REP_PEC        CO Integration CRM Service
SAP_CO_CRM_REP_PEC_IMG    CO Integration CRM Service with Modelling
SAP_FIN_FSCM_COL_AR_ADMIN  Receivables Management Administrator, Financial Accounti
SAP_FIN_FSCM_COL_AR_RFC_COMM  RFC User (Communication) in Accounts Receivable
SAP_FIN_FSCM_COL_AR_RFC_DIALOG  RFC User (Dialog) in Receivables Processing
SAP_FIN_FSCM_COL_AR_USER    End User in Receivables Processing
SAP_FIN_FSCM_DM_AR_DIALOG    Role for Functions in Accounts Receivables
SAP_FIN_FSCM_DM_AR_RFC_COMM  RFC User (Communication) in Accounts Receivable
SAP_FIN_FSCM_DM_AR_RFC_DIALOG  RFC User (Online) in Accounts Receivable
SAP_FI_FSCM_ACT_AGENT        SAP Biller Direct: Authorizations for the role 'Agent'
SAP_FI_FSCM_ACT_ALL          FSCM Biller Direct: All authorizations for the object F_ACT_EBP
SAP_FI_FSCM_ACT_DISPUTE      SAP Biller Direct: Authorization for the role 'Dispute'
SAP_FI_FSCM_ACT_MAINTAIN      SAP Biller Direct: Authorizations for master data mainte
SAP_FI_FSCM_ACT_PAY          SAP Biller Direct: Authorizations for the role 'Payment'
SAP_FI_FSCM_ACT_SHOW         SAP Biller Direct: Authorizations for the role 'Display'
SAP_FI_FSCM_ALL              FSCM Biller Direct: Authorizations for all activities
SAP_FI_FSCM_BD_POOLUSER      SAP Biller Direct: Example role for the pool user
SAP_FSCM_BD_AR_POOL_RW       SAP Biller Direct: Example role for the pool user

```

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. In case 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.



```

role.CTL - Notepad
File Edit Format View Help
15-Oct-07 10:43:48 AM
role1.txt

```

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.

“ACTIONFROM” (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.

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.

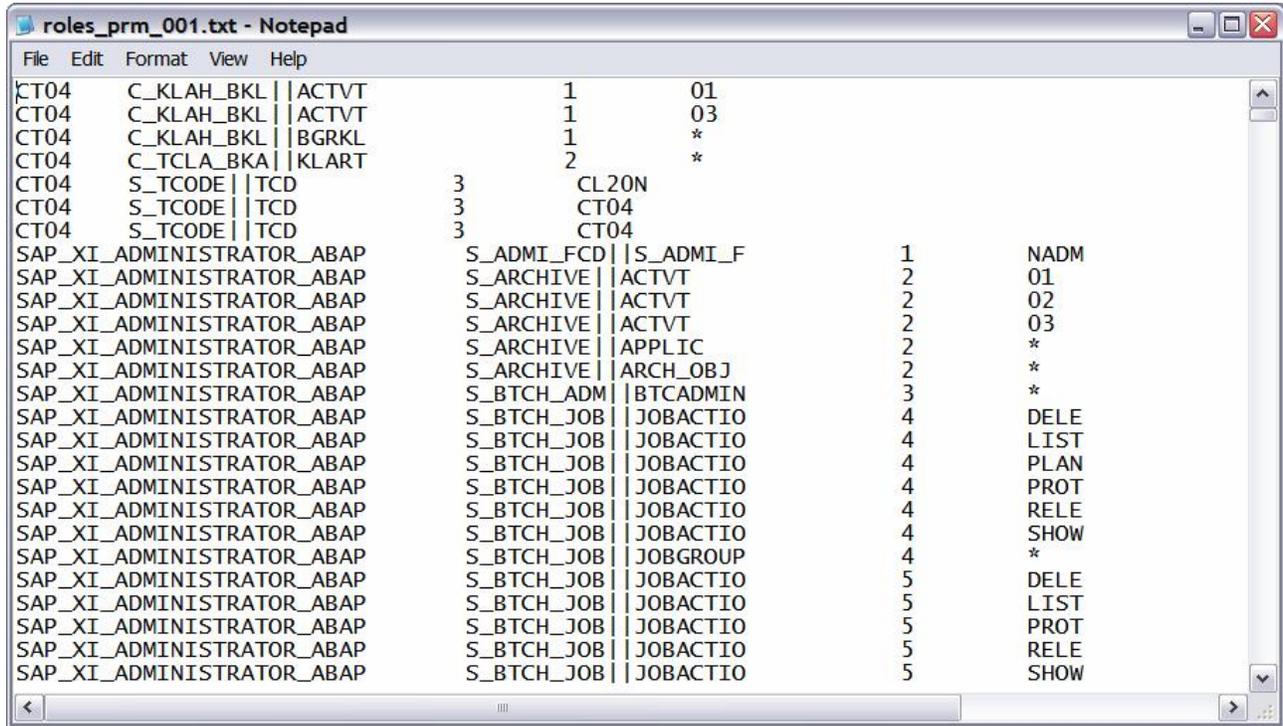
- ROLES - Role/Responsibility name
- PERMISSION - Permissions associated with Role/Responsibility
- PRMGRP - Permission group where permissions belong, a numeric sequence number.
- FROMVALUE - Permission from value in Role/Responsibility
- TOVALUE - Permission to value in Role/Responsibility
- PROFILE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

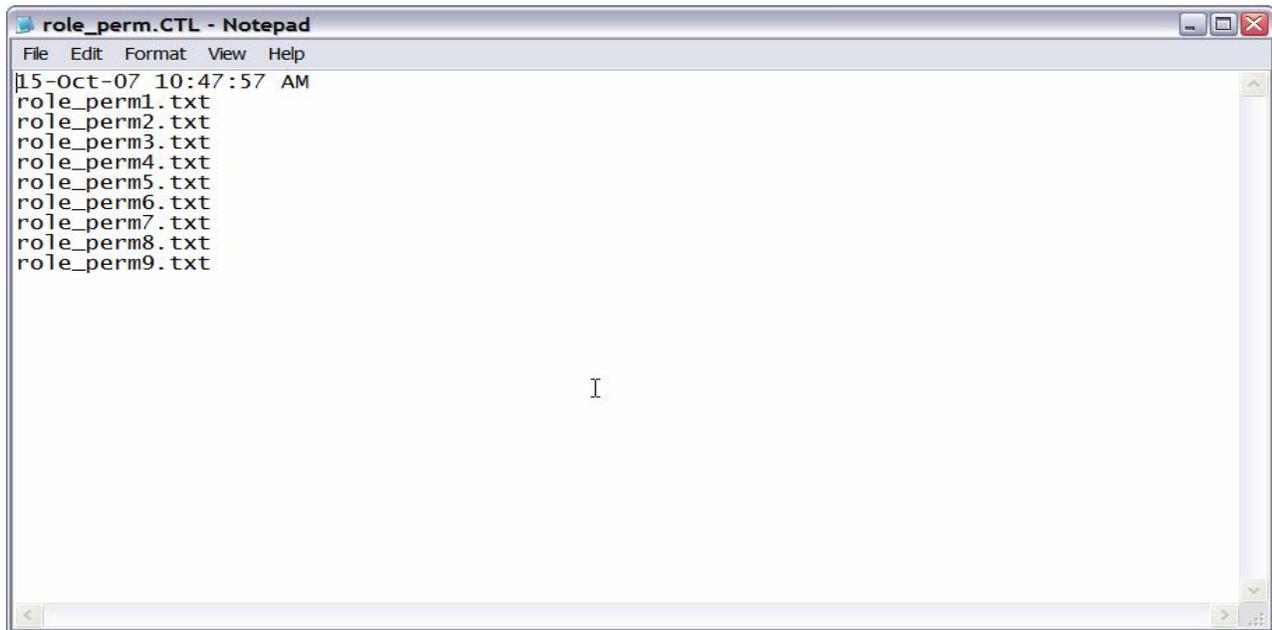


```

roles_prm_001.txt - Notepad
File Edit Format View Help
CT04 C_KLAH_BKL || ACTVT 1 01
CT04 C_KLAH_BKL || ACTVT 1 03
CT04 C_KLAH_BKL || BGRKL 1 *
CT04 C_TCLA_BKA || KLART 2 *
CT04 S_TCODE || TCD 3 CL20N
CT04 S_TCODE || TCD 3 CT04
CT04 S_TCODE || TCD 3 CT04
SAP_XI_ADMINISTRATOR_ABAP S_ADMI_FCD || S_ADMI_F 1 NADM
SAP_XI_ADMINISTRATOR_ABAP S_ARCHIVE || ACTVT 2 01
SAP_XI_ADMINISTRATOR_ABAP S_ARCHIVE || ACTVT 2 02
SAP_XI_ADMINISTRATOR_ABAP S_ARCHIVE || ACTVT 2 03
SAP_XI_ADMINISTRATOR_ABAP S_ARCHIVE || APPLIC 2 *
SAP_XI_ADMINISTRATOR_ABAP S_ARCHIVE || ARCH_OBJ 2 *
SAP_XI_ADMINISTRATOR_ABAP S_BTCH_ADM || BTCADMIN 3 *
SAP_XI_ADMINISTRATOR_ABAP S_BTCH_JOB || JOBACTIO 4 DELE
SAP_XI_ADMINISTRATOR_ABAP S_BTCH_JOB || JOBACTIO 4 LIST
SAP_XI_ADMINISTRATOR_ABAP S_BTCH_JOB || JOBACTIO 4 PLAN
SAP_XI_ADMINISTRATOR_ABAP S_BTCH_JOB || JOBACTIO 4 PROT
SAP_XI_ADMINISTRATOR_ABAP S_BTCH_JOB || JOBACTIO 4 RELE
SAP_XI_ADMINISTRATOR_ABAP S_BTCH_JOB || JOBACTIO 4 SHOW
SAP_XI_ADMINISTRATOR_ABAP S_BTCH_JOB || JOBACTIO 4 *
SAP_XI_ADMINISTRATOR_ABAP S_BTCH_JOB || JOBACTIO 5 DELE
SAP_XI_ADMINISTRATOR_ABAP S_BTCH_JOB || JOBACTIO 5 LIST
SAP_XI_ADMINISTRATOR_ABAP S_BTCH_JOB || JOBACTIO 5 PROT
SAP_XI_ADMINISTRATOR_ABAP S_BTCH_JOB || JOBACTIO 5 RELE
SAP_XI_ADMINISTRATOR_ABAP S_BTCH_JOB || JOBACTIO 5 SHOW

```

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. In case 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.

Create Connector

System Id	<input type="text"/>
System Name	<input type="text"/>
System Type	SAP ▼
Connection Type	File - Local ▼
Location	<input type="text"/>
User ID	<input type="text"/>
Password	<input type="text"/>
<input type="button" value="Save"/>	

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

The screenshot shows the 'Text Objects Upload' screen in the SAP Compliance Calibrator by Virsa application. The interface includes a navigation menu on the left with 'Upload Objects' selected, and a main content area with the following elements:

- System Id ***: A dropdown menu with 'Q5F' selected.
- Local File**: A text input field containing 'C:\SAP OBJECTS\sap_desc.txt' and a 'Browse...' button.
- Server File**: An empty text input field.
- Buttons**: 'Foreground', 'Background', and 'Cancel' buttons.

A black arrow points from the 'Foreground' button to the following instruction:

Please select Virsa provided text objects file by browsing to the location and select the system from drop down list on which this text objects will be uploaded. Please click on Forground to upload the file.

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

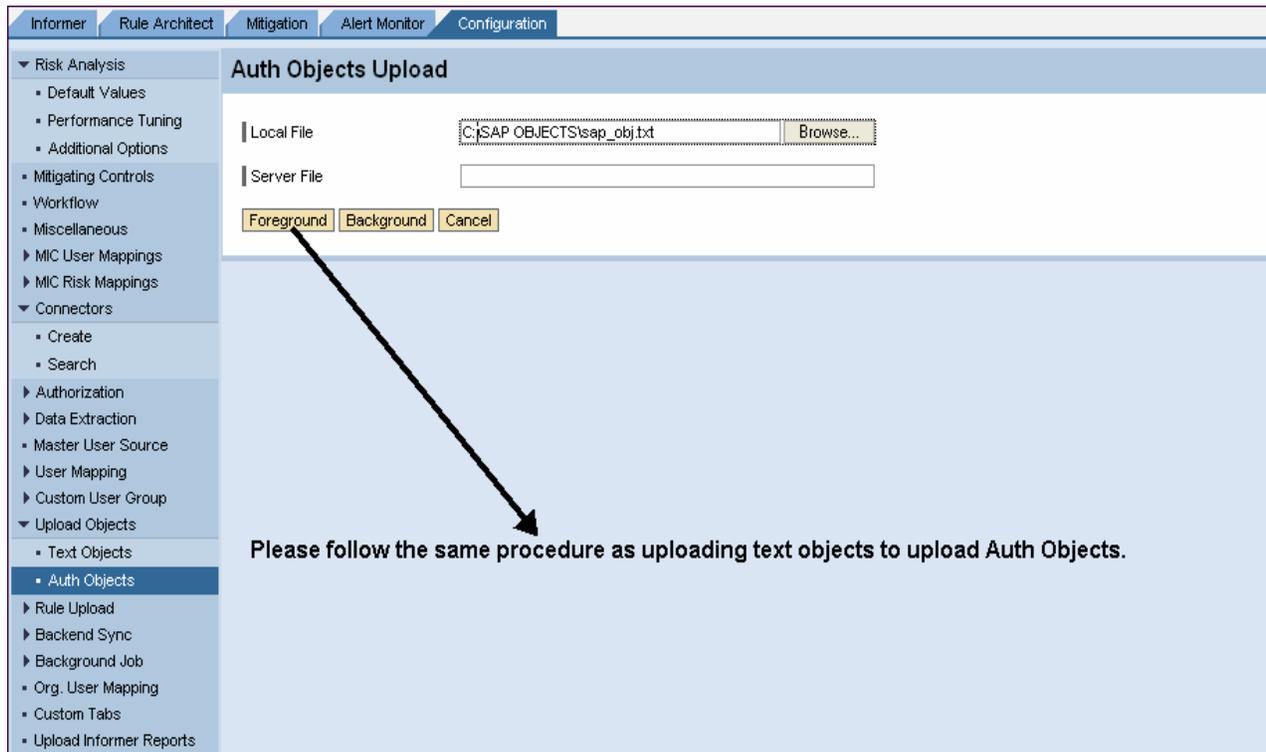
Log in to the server.

Click the Configuration Tab on top.

From left navigation menu, Click Upload Objects.

Click “Auth Objects”

The following screen will be displayed



The screenshot displays the 'Auth Objects Upload' configuration screen. The left-hand navigation menu is expanded to show 'Auth Objects' under the 'Upload Objects' category. The main content area features two input sections: 'Local File' with a text box containing 'C:\SAP OBJECTS\sap_obj.txt' and a 'Browse...' button, and 'Server File' with an empty text box. Below these are three buttons: 'Foreground', 'Background', and 'Cancel'. A black arrow points from the 'Foreground' button to a text message at the bottom of the screen: 'Please follow the same procedure as uploading text objects to upload Auth Objects.'

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

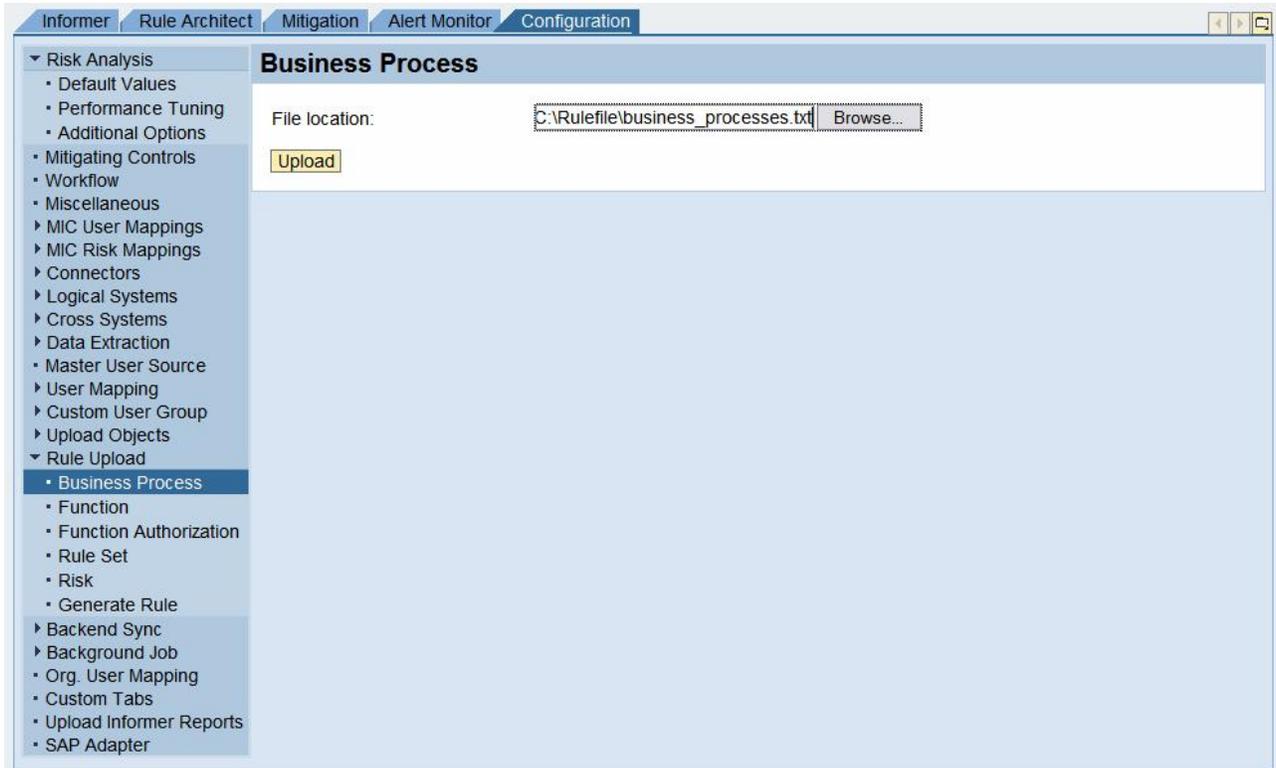
In this process we will upload various Business Processes that are associated with our data.

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



The screenshot shows the SAP GRC Configuration interface. The top navigation bar includes tabs for Informer, Rule Architect, Mitigation, Alert Monitor, and Configuration. The left navigation menu is expanded to show the 'Rule Upload' section, with 'Function' selected. The main content area is titled 'Function' and contains two input fields: 'Function:' with the value 'C:\Rulefile\CC52 function.txt' and 'Function BP:' with the value 'C:\Rulefile\CC52 function_bp.txt'. Each field has a 'Browse...' button next to it. Below the input fields is an 'Upload' button.

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

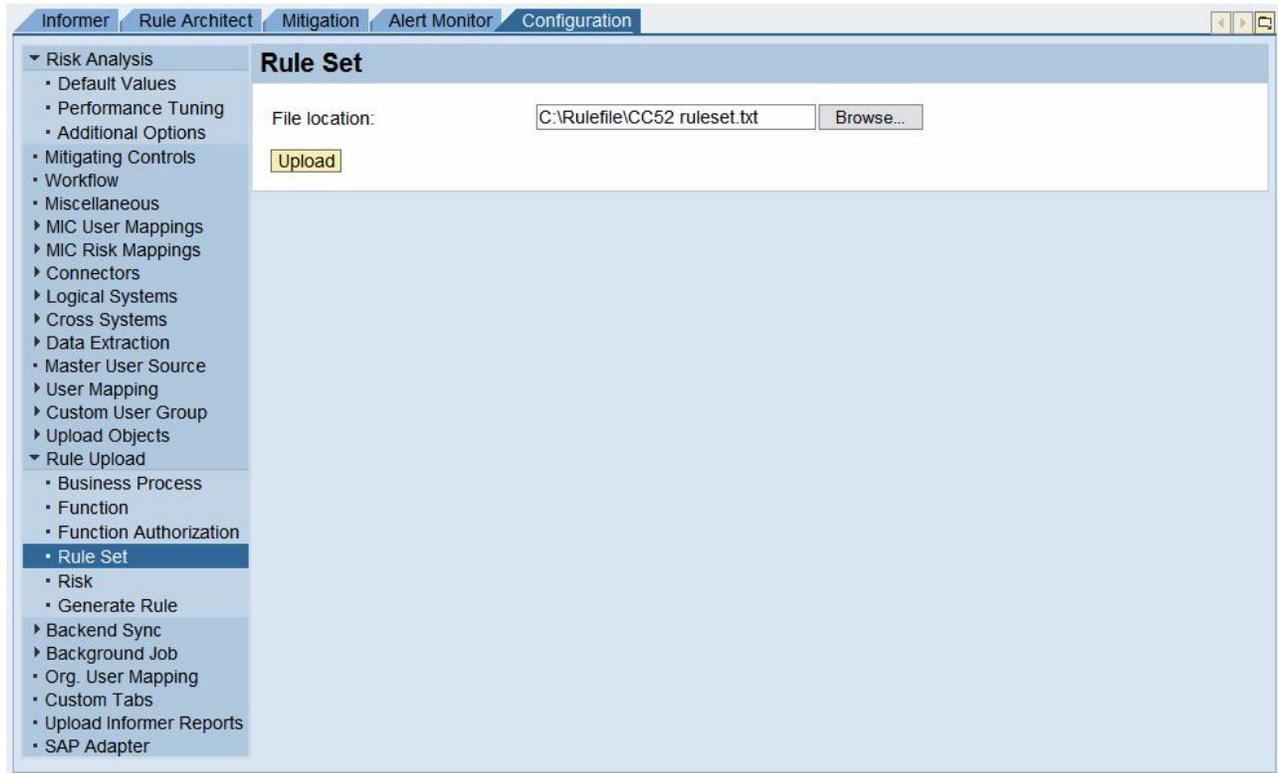
In this process we will upload various Rule set that will define Segregation of Duties (SoD).

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

The screenshot shows the SAP GRC Configuration interface. The top navigation bar includes tabs for Informer, Rule Architect, Mitigation, Alert Monitor, and Configuration. The left navigation menu is expanded to show the 'Rule Upload' section, with 'Risk' selected. The main content area is titled 'Risk' and contains three input fields for file selection: 'Risk' (C:\Rulefile\CC52 risks.txt), 'Risk Description' (C:\Rulefile\CC52 risks_desc.txt), and 'Rule Set Mapping' (C:\Rulefile\CC52 ruleset.txt). Each field has a 'Browse...' button. Below the input fields is an 'Upload' button.

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

The screenshot shows the SAP GRC Configuration interface. The left navigation menu is expanded to 'Rule Upload' > 'Generate Rule'. The main area displays a table titled 'Generate Rules' with the following data:

Risk Description	Conflicting Function	Level	Status
A001: Change sales forecast data which could result in inaccurate planning.	AO01 - APO Supply & Demand Planning & AO02 - APO Maintain Model	High	Enable
A002: Change sales forecast data which could result in inaccurate planning.	AO01 - APO Supply & Demand Planning & AO03 - APO Model & Version Management	High	Enable
A003: Change sales forecast data which could result in inaccurate planning.	AO01 - APO Supply & Demand Planning & AO04 - APO Delete version (version 000 - APO active version)	High	Enable
A004: Change sales forecast data which could result in inaccurate planning.	AO01 - APO Supply & Demand Planning & AO05 - APO Copy/Version Management in DP	Medium	Enable
A005: Maintain master data to adversely effect planned/process orders/schedules.	AO01 - APO Supply & Demand Planning & AO06 - APO Maintain Characteristic Combination relevant to Planning	Medium	Enable
A006: Maintain master data to adversely effect	AO01 - APO Supply & Demand Planning & AO06 - APO Maintain Characteristic Combination relevant to Planning	Medium	Enable

At the bottom of the table, there are two buttons: 'Foreground' and 'Background'.

Click Foreground.

The Rule Generation status will be displayed on the screen.

Additional Configuration

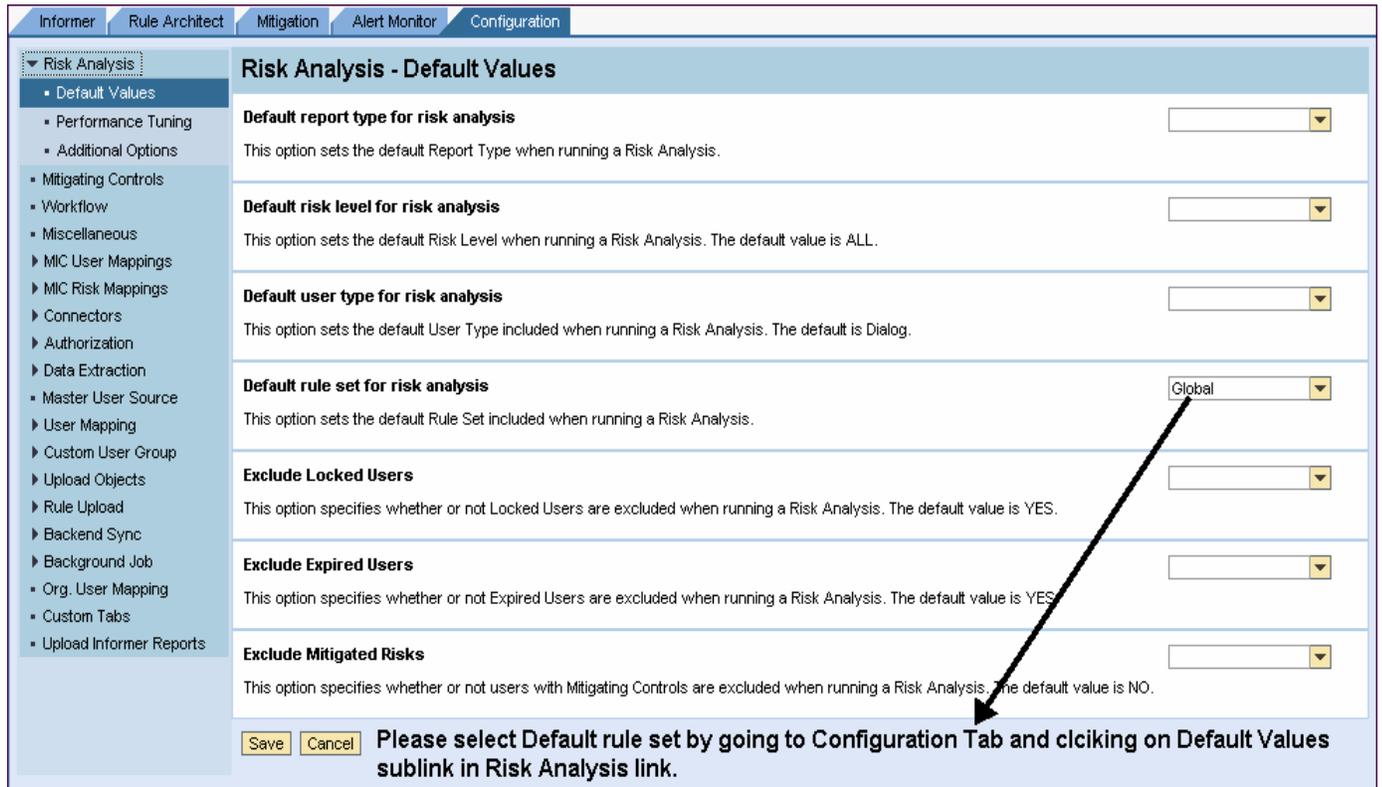
One final step of configuring Compliance Calibrator is making “Global” rule set as Default rule set for risk analysis.

Click the Configuration Tab on top.

From left navigation menu, Click Risk Analysis.

Click Default Values.

The following screen will be displayed



The screenshot shows the 'Risk Analysis - Default Values' configuration page. The left navigation menu is expanded to 'Risk Analysis' > 'Default Values'. The main content area contains several configuration options, each with a dropdown menu:

- Default report type for risk analysis**: This option sets the default Report Type when running a Risk Analysis.
- Default risk level for risk analysis**: This option sets the default Risk Level when running a Risk Analysis. The default value is ALL.
- Default user type for risk analysis**: This option sets the default User Type included when running a Risk Analysis. The default is Dialog.
- Default rule set for risk analysis**: This option sets the default Rule Set included when running a Risk Analysis. The dropdown is currently set to 'Global'.
- Exclude Locked Users**: This option specifies whether or not Locked Users are excluded when running a Risk Analysis. The default value is YES.
- Exclude Expired Users**: This option specifies whether or not Expired Users are excluded when running a Risk Analysis. The default value is YES.
- Exclude Mitigated Risks**: This option specifies whether or not users with Mitigating Controls are excluded when running a Risk Analysis. The default value is NO.

At the bottom of the page, there are 'Save' and 'Cancel' buttons. A red box highlights the 'Save' button and contains the text: **Please select Default rule set by going to Configuration Tab and clicking on Default Values sublink in Risk Analysis link.** A red arrow points from this text to the 'Default rule set for risk analysis' dropdown menu.

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

The screenshot displays the 'Create Data Extractor' configuration window. The 'System' is set to 'RRA', the 'Object' is 'User', and the 'Data Extraction Mode' is 'Flat File'. The 'User' tab is selected, showing a 'File Name' of 'user.txt', 'File Type' as 'Delimited', and a 'Delimiter' of '\t'. A table below maps target fields to source fields:

Target Field	Source Field
USERID	1
FNAME	2
LNAME	3
EMAIL	4
PHONE	5
DEPT	6

At the bottom of the window, there are three buttons: 'Save', 'Extract Foreground', and 'Extract Background'.

Enter the file name for user data.

User Actions

Click the Actions tab.

The following screen will be displayed

The screenshot shows the 'Create Data Extractor' configuration window in SAP GRC. The 'Configuration' tab is active, and the 'Actions' sub-tab is selected. The configuration includes the following fields and options:

- System:** RRA
- Object:** User
- Data Extraction Mode:** Flat File
- File Name:** activity.CTL
- File Type:** Delimited
- Delimiter:** \t

A table below these fields maps target fields to source fields:

Target Field	Source Field
USERID	1
ROLE	2
ACTFROM	3
ACTTO	4

At the bottom of the window, there are three buttons: 'Save', 'Extract Foreground', and 'Extract Background'. The status bar indicates 'Row 1 of 4'.

Enter the file name for user activity data.

User Permissions

Click the Permissions tab.

The following screen will be displayed

Create Data Extractor

System: RRA
 Object: User
 Data Extraction Mode: Flat File

User Actions Permissions

File Name: permissions.CTL
 File Type: Delimited
 Delimiter: \t

Target Field	Source Field
USERID	1
ROLE	2
PERMISSION	3
PRMGROUP	4
PRMFROM	5
PRMTO	6

Row 1 of 6

Save Extract Foreground Extract Background

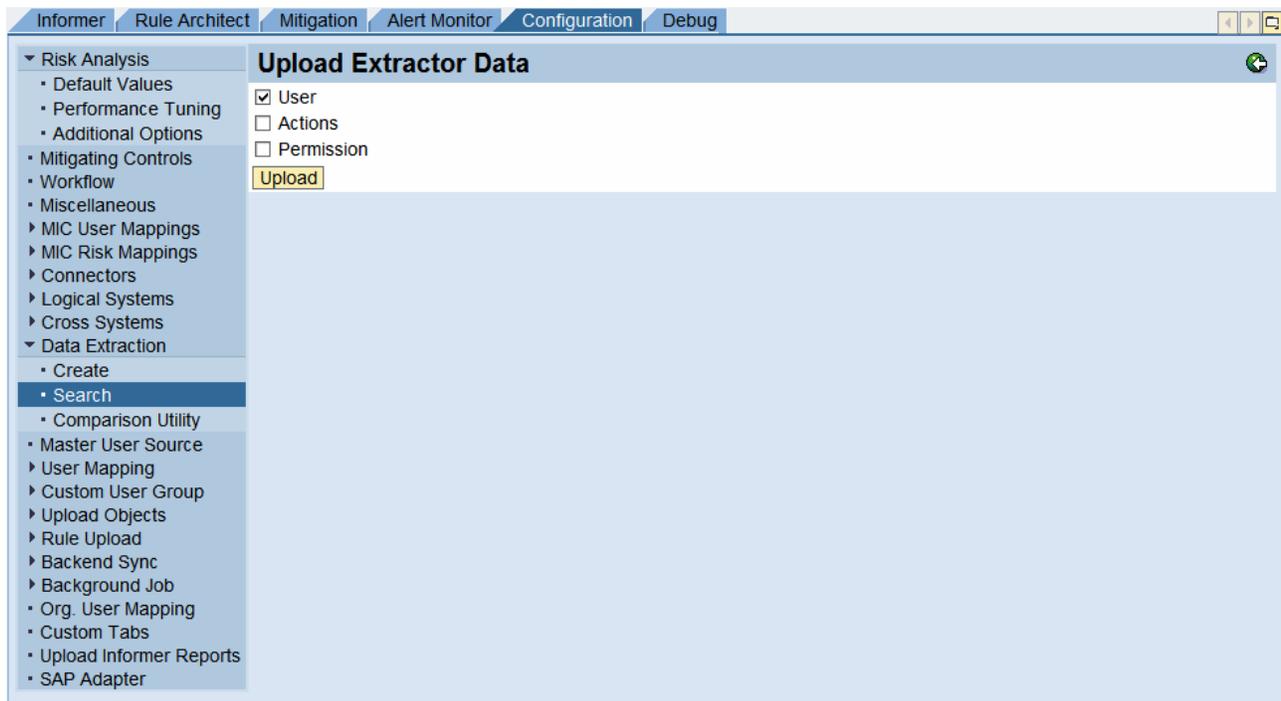
Enter the file name for user permission data.

Extracting Data

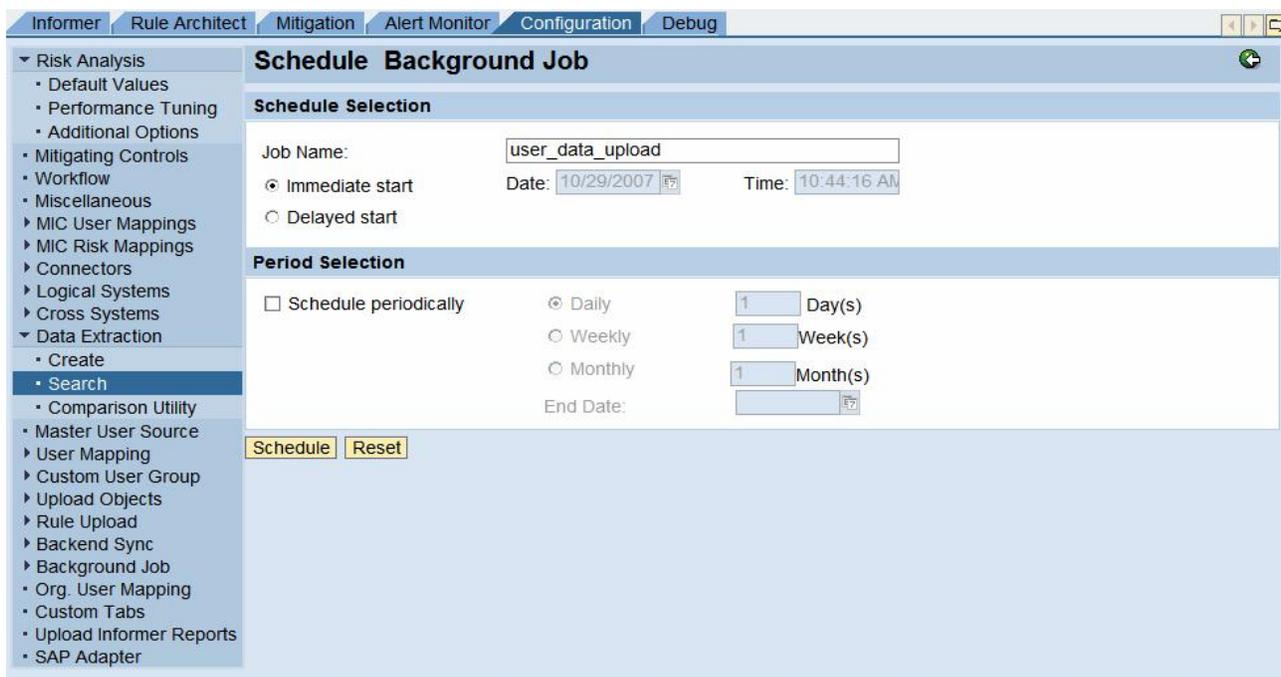
Click the Save Button.

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.

The screenshot shows the SAP GRC Configuration console. The top navigation bar includes 'Informer', 'Rule Architect', 'Mitigation', 'Alert Monitor', 'Configuration', and 'Debug'. The left sidebar is expanded to 'Data Extraction' > 'Search'. The main content area is titled 'Upload Extractor Data' and contains three checkboxes: 'User' (unchecked), 'Actions' (checked), and 'Permission' (unchecked). Below these is a yellow 'Upload' button.

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.

The screenshot shows the 'Schedule Background Job' screen. The left sidebar is the same as the previous screenshot. The main content area is titled 'Schedule Background Job'. It has a 'Job Name' field containing 'user_action_upload'. Under 'Schedule Selection', 'Immediate start' is selected with a date of '10/29/2007' and a time of '10:44:16 AM'. Under 'Period Selection', 'Daily' is selected with a frequency of '1 Day(s)'. There are 'Schedule' and 'Reset' buttons at the bottom.

Repeat the same Upload process for User Permissions.

The screenshot shows the SAP GRC configuration interface. The top navigation bar includes 'Informer', 'Rule Architect', 'Mitigation', 'Alert Monitor', 'Configuration', and 'Debug'. The left sidebar contains a tree view with the following items: Risk Analysis (expanded), Default Values, Performance Tuning, Additional Options, Mitigating Controls, Workflow, Miscellaneous, MIC User Mappings, MIC Risk Mappings, Connectors, Logical Systems, Cross Systems, Data Extraction (expanded), Create, Search (selected), Comparison Utility, Master User Source, User Mapping, Custom User Group, Upload Objects, Rule Upload, Backend Sync, Background Job, Org. User Mapping, Custom Tabs, Upload Informer Reports, and SAP Adapter. The main content area is titled 'Upload Extractor Data' and contains three checkboxes: 'User' (unchecked), 'Actions' (unchecked), and 'Permission' (checked). Below these checkboxes is an 'Upload' button.

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 screenshot shows the SAP GRC configuration interface. The top navigation bar includes 'Informer', 'Rule Architect', 'Mitigation', 'Alert Monitor', 'Configuration', and 'Debug'. The left sidebar contains a tree view with the following items: Risk Analysis (expanded), Default Values, Performance Tuning, Additional Options, Mitigating Controls, Workflow, Miscellaneous, MIC User Mappings, MIC Risk Mappings, Connectors, Logical Systems, Cross Systems, Data Extraction (expanded), Create, Search (selected), Comparison Utility, Master User Source, User Mapping, Custom User Group, Upload Objects, Rule Upload, Backend Sync, Background Job, Org. User Mapping, Custom Tabs, Upload Informer Reports, and SAP Adapter. The main content area is titled 'Schedule Background Job' and contains a 'Schedule Selection' section with 'Job Name' set to 'user_permission_upload', 'Immediate start' selected, 'Date' set to '10/29/2007', and 'Time' set to '10:50:13 AM'. Below this is a 'Period Selection' section with 'Daily' selected and '1' day(s) specified. 'Schedule' and 'Reset' buttons are at the bottom.

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

Create Data Extractor

System: RRA
Object: Role
Data Extraction Mode: Flat File

File Name: role.txt
File Type: Delimited
Delimiter: \t

Target Field	Source Field
ROLE	1
NAME	2
DELETED	3

Row 1 of 3

Save Extract Foreground Extract Background

Enter the file name for role data.

Role Actions

Click the Actions tab.

The following screen will be displayed

The screenshot shows the 'Create Data Extractor' configuration window in SAP GRC. The 'Configuration' tab is active, and the 'Actions' sub-tab is selected. The main configuration area includes:

- System:** RRA
- Object:** Role
- Data Extraction Mode:** Flat File
- File Name:** role_act.CTL
- File Type:** Delimited
- Delimiter:** \t

A table below these fields maps target fields to source fields:

Target Field	Source Field
ROLE	1
ACTFROM	2
ACTTO	3

At the bottom of the configuration area, there are three buttons: 'Save', 'Extract Foreground', and 'Extract Background'. The status bar indicates 'Row 1 of 3'.

Enter the file name for role activity data.

Role Permissions

Click the Permissions tab.

The following screen will be displayed

The screenshot shows the 'Create Data Extractor' configuration window in SAP GRC. The 'Permissions' tab is selected, displaying a table with the following data:

Target Field	Source Field
ROLE	1
PERMISSION	2
PRMGROUP	3
PRMFROM	4
PRMTO	5

Other configuration details include: System: RRA, Object: Role, Data Extraction Mode: Flat File, File Name: role_prm.CTL, File Type: Delimited, and Delimiter: \t. The interface also includes a navigation pane on the left and buttons for Save, Extract Foreground, and Extract Background at the bottom.

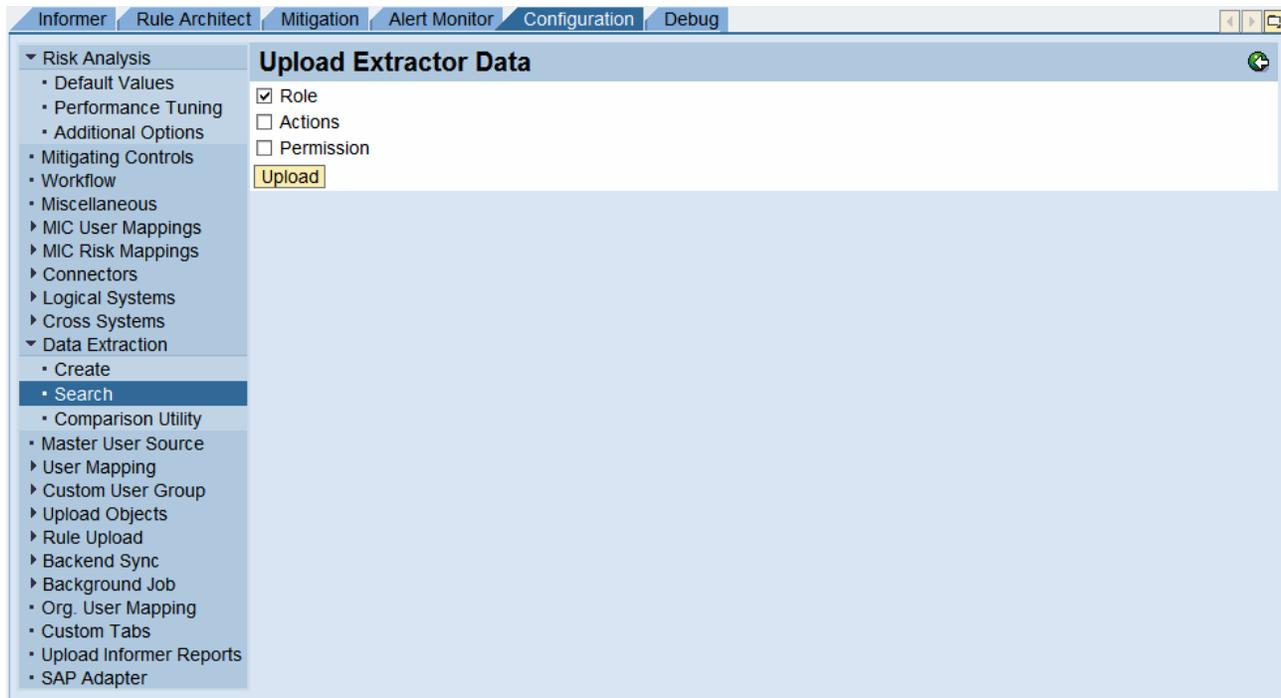
Enter the file name for role permission data.

Extracting Data

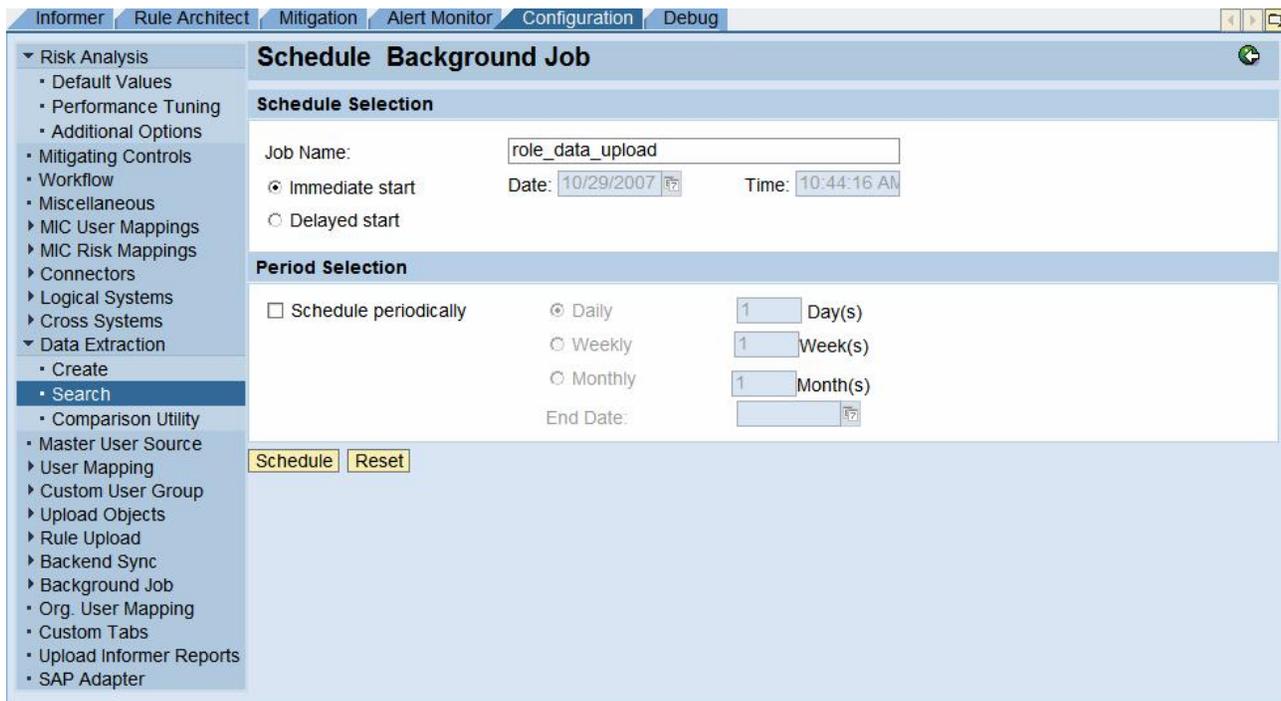
Click the Save Button.

Click Extract Background.

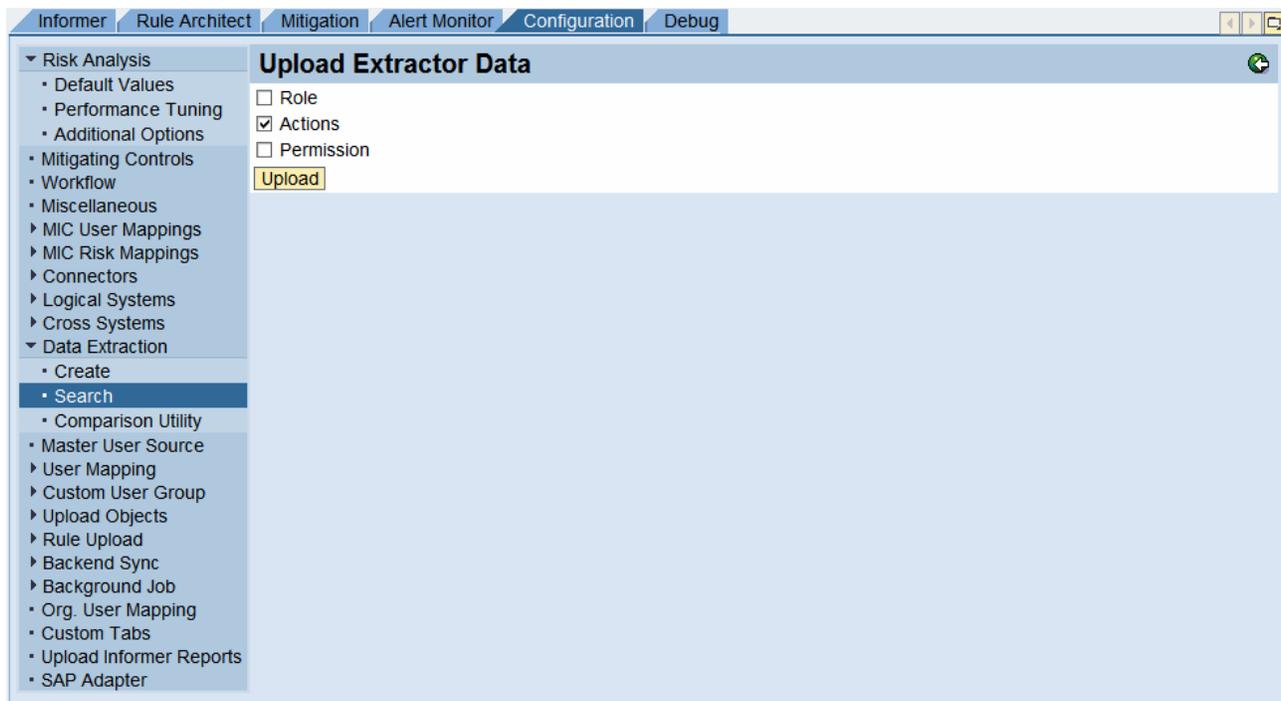
The following screen will be displayed. It is always **recommended** that during data extraction we should extract data from files individually.



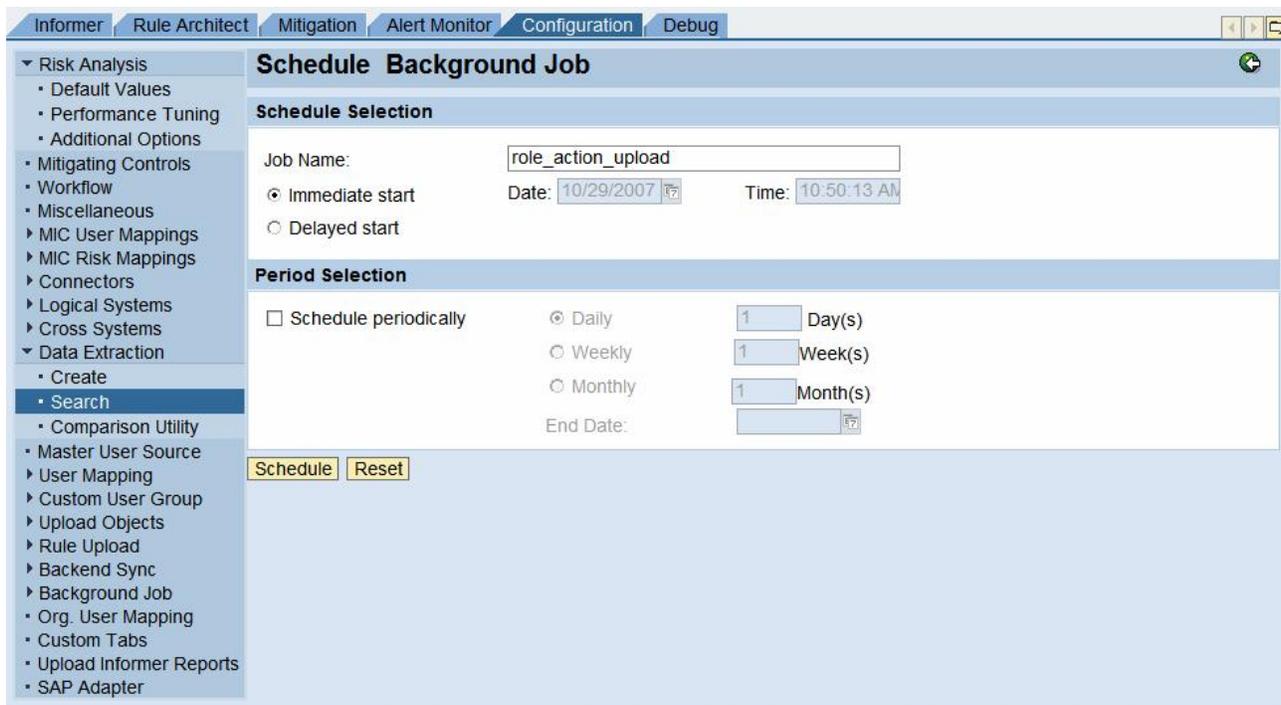
After selecting appropriate checkbox, click **Upload** to schedule Background Job for Role Upload. The following screens will be displayed. Enter the Job name and Click Schedule.



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.

The screenshot shows the SAP GRC interface with the 'Configuration' tab selected. The left sidebar contains a tree view with the following items: Risk Analysis (Default Values, Performance Tuning, Additional Options), Mitigating Controls (Workflow, Miscellaneous, MIC User Mappings, MIC Risk Mappings, Connectors, Logical Systems, Cross Systems), Data Extraction (Create, Search), Comparison Utility, Master User Source, User Mapping, Custom User Group, Upload Objects, Rule Upload, Backend Sync, Background Job, Org. User Mapping, Custom Tabs, Upload Informer Reports, and SAP Adapter. The 'Search' item is highlighted. The main content area is titled 'Upload Extractor Data' and contains three checkboxes: 'Role' (unchecked), 'Actions' (unchecked), and 'Permission' (checked). Below the checkboxes is an 'Upload' button.

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 screenshot shows the SAP GRC interface with the 'Configuration' tab selected. The left sidebar is the same as the previous screenshot. The main content area is titled 'Schedule Background Job' and contains the following fields and options: 'Job Name' (role_permission_upload), 'Date' (10/29/2007), and 'Time' (10:44:16 AM). There are two radio buttons: 'Immediate start' (selected) and 'Delayed start'. Below that is a section for 'Period Selection' with three radio buttons: 'Schedule periodically' (unchecked), 'Daily' (selected), and 'Weekly' (unchecked). There are also input fields for '1 Day(s)', '1 Week(s)', and '1 Month(s)'. An 'End Date' field is also present. At the bottom are 'Schedule' and 'Reset' buttons.

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.

The screenshot shows the 'Configuration' tab in the SAP GRC interface. The left navigation menu is expanded to 'Background Job' > 'Schedule Analysis'. The main content area is titled 'User/Role/Profile Synchronization and Batch Risk Analysis' and is divided into several sections:

- User/Role/Profile Synchronization:** Sync Mode is set to 'Incremental'. There are three sections for synchronization:
 - User Synchronization** Systems: *
 - Role Synchronization** Systems: *
 - Profile Synchronization** Systems: *
- Batch Risk Analysis:** Batch Mode is set to 'Full Sync'. Rule Set is 'GLOBAL'. Report Type has checkboxes for 'Action Level Analysis' (checked) and 'Permission Level Analysis' (checked).
 - User Analysis:** Systems: *, User: *, User Group: [] to: []
 - Role Analysis:** Systems: *, Role: [] to: []
 - Profile Analysis:** Systems: *, Profile: [] to: []
 - Critical Action and Role/Profile Analysis**
- Management Report:** **Management Reports**

At the bottom of the configuration area, there are 'Schedule' and 'Reset' buttons.

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

The screenshot shows the 'Configuration' tab in the SAP GRC interface. The left navigation pane is expanded to 'Background Job' > 'Schedule Analysis'. The main content area is titled 'Schedule Risk Analysis Background Job' and contains the following fields and options:

- Schedule Selection:**
 - Job Name:
 - Immediate start Date: Time:
 - Delayed start
- Period Selection:**
 - Schedule periodically
 - Daily Day(s)
 - Weekly Week(s)
 - Monthly Month(s)
 - End Date:

At the bottom of the configuration area, there are two buttons: 'Schedule' and 'Reset'.

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.

[Informer](#) | [Rule Architect](#) | [Mitigation](#) | [Alert Monitor](#) | [Configuration](#)

User/Role/Profile Synchronization and Batch Risk Analysis

User/Role/Profile Synchronization

Sync Mode:

User Synchronization Systems:

Role Synchronization Systems:

Profile Synchronization Systems:

Batch Risk Analysis

Batch Mode:

Rule Set:

Report Type: Action Level Analysis Permission Level Analysis

User Analysis

Systems: to:

User: to:

User Group: to:

Role Analysis

Systems: to:

Role: to:

Profile Analysis

Systems: to:

Profile: to:

Critical Action and Role/Profile Analysis

Management Report

Management Reports

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

The screenshot shows the 'Schedule Risk Analysis Background Job' configuration screen. The left sidebar contains a navigation tree with the following items: Risk Analysis, Mitigating Controls, Workflow, Miscellaneous, MIC User Mappings, MIC Risk Mappings, Connectors, Logical Systems, Cross Systems, Data Extraction, Master User Source, User Mapping, Custom User Group, Rule Upload, Backend Sync, Background Job (expanded), Search, Schedule Analysis (highlighted), Alert Generation, Org. User Mapping, Custom Tabs, Upload Informer Reports, and SAP Adapter. The main content area is titled 'Schedule Risk Analysis Background Job' and includes a 'Schedule Selection' section with a 'Job Name' field containing 'batch role analysis', an 'Immediate start' radio button selected, a 'Date' field with '10/11/2007', and a 'Time' field with '12:39:07 PM'. Below this is a 'Period Selection' section with a 'Schedule periodically' checkbox, 'Daily' radio button selected, and input fields for '1' Day(s), '1' Week(s), and '1' Month(s). An 'End Date' field is also present. At the bottom of the form are 'Schedule' and 'Reset' buttons.

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.

The screenshot shows the SAP GRC Configuration interface. The left sidebar contains a navigation tree with the following items: Risk Analysis, Mitigating Controls, Workflow, Miscellaneous, MIC User Mappings, MIC Risk Mappings, Connectors, Logical Systems, Cross Systems, Data Extraction, Master User Source, User Mapping, Custom User Group, Upload Objects, Rule Upload, Backend Sync, Background Job, Search, Schedule Analysis (highlighted), Alert Generation, Org. User Mapping, Custom Tabs, Upload Informer Reports, and SAP Adapter. The main content area is titled "User/Role/Profile Synchronization and Batch Risk Analysis" and is divided into three sections:

- User/Role/Profile Synchronization:** Sync Mode is set to "Incremental". There are three checkboxes for "User Synchronization", "Role Synchronization", and "Profile Synchronization", each with a "Systems:" field and a selection icon.
- Batch Risk Analysis:** Batch Mode is set to "Incremental". Rule Set is "GLOBAL". Report Type has checkboxes for "Action Level Analysis" (unchecked) and "Permission Level Analysis" (checked). There are three checkboxes for "User Analysis", "Role Analysis", and "Profile Analysis". Each has "Systems:" and "to:" fields with selection icons. "Critical Action and Role/Profile Analysis" is also unchecked.
- Management Report:** A checkbox for "Management Reports" is checked.

At the bottom of the configuration area, there are "Schedule" and "Reset" buttons.

Go to Management Report.

Check Management Report.

Click Schedule.

The following screen will be displayed

The screenshot shows the 'Schedule Risk Analysis Background Job' configuration screen in SAP GRC. The interface includes a navigation menu on the left and a main configuration area on the right. The main area is titled 'Schedule Risk Analysis Background Job' and contains the following sections:

- Schedule Selection:** Job Name: management report; Start: Immediate start (selected) with Date: 10/11/2007 and Time: 12:44:39 PM; Delayed start (unselected).
- Period Selection:** Schedule periodically (unselected); Frequency: Daily (selected) with 1 Day(s); Weekly (unselected) with 1 Week(s); Monthly (unselected) with 1 Month(s); End Date: (empty).

At the bottom of the configuration area, there are 'Schedule' and 'Reset' buttons. The left navigation menu includes categories like Risk Analysis, Mitigating Controls, Workflow, and Background Job, with 'Schedule Analysis' currently selected.

Click Schedule and Management Report Background job will be scheduled.

Background Jobs

Status of all the background jobs scheduled can be easily 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.

Job Scheduler Status: **Running**

Job ID	Task	Name	Job Type	Last Run	Next Start	User	State	Result	Status
9	Risk Analysis - Batch	role_analysis	Immediate	2007-10-02 22:53:05	2007-10-02 22:19:46	virsa	Complete		
8	Upload Extractor Data	role_permission_upload	Immediate	2007-10-02 22:18:37	2007-10-02 22:16:35	virsa	Complete		
7	Upload Extractor Data	role_action_upload	Immediate	2007-10-02 22:15:42	2007-10-02 22:15:41	virsa	Complete		
6	Upload Extractor Data	role_upload	Immediate	2007-10-02 22:14:12	2007-10-02 22:14:05	virsa	Complete		
5	Risk Analysis - Batch	user_analysis	Immediate	2007-10-02 12:57:57	2007-10-02 11:40:55	virsa	Complete		
4	Upload Extractor Data	user_permission_upload	Immediate	2007-10-02 11:34:42	2007-10-02 10:57:47	virsa	Complete		
3	Upload Extractor Data	user_action_upload	Immediate	2007-10-02 10:50:56	2007-10-02 10:48:00	virsa	Complete		
2	Upload Extractor Data	user_upload	Immediate	2007-10-02 10:46:19	2007-10-02 10:46:14	virsa	Complete		
1	Rule Generation	Rule Generation.	Immediate	2007-09-26 14:01:58	2007-09-26 13:51:31	virsa	Complete		

Row 1 of 9

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.

Search Background Jobs Result

Job Scheduler Status: **Running** Different States are: Ready, Running, Error and Complete. Click on View Log button when the state is neither Ready nor Running.

Job ID	Task	Name	Job Type	Last Run	Next Start	User	State	Result	Status
22	Upload Extractor Data	Permission Latest	Immediate	2006-06-23 17:06:39	2006-06-23	Administrator	Complete		
21	Risk Analysis - Batch	Mgmt Report - User Analysis	Immediate	2006-06-23 09:57:27	2006-06-23	Administrator	Complete		
20	Risk Analysis - Batch	User Analysis Full	Immediate	2006-06-22 22:32:27	2006-06-22	Administrator	Error		
19	Upload Extractor Data	role permissions	Immediate	2006-06-22 21:46:09	2006-06-22	Administrator	Complete		
18	Upload Extractor Data	role Actions	Immediate	2006-06-22 21:42:04	2006-06-22	Administrator	Complete		
17	Upload Extractor Data	roles	Immediate	2006-06-22 21:21:59	2006-06-22	Administrator	Complete		
15	Risk Analysis - Batch	management - user	Immediate	2006-06-22 20:25:34	2006-06-22	Administrator	Error		
13	Upload Extractor Data	permissions	Immediate	2006-06-22 19:39:50	2006-06-22	Administrator	Complete		
12	Upload Extractor Data	permissions upload	Immediate	2006-06-22 18:43:44	2006-06-22	Administrator	Aborted		
11	Upload Extractor Data	actions	Immediate	2006-06-22 18:37:59	2006-06-22	Administrator	Complete		
10	Upload Extractor Data	users latest	Immediate	2006-06-22 18:34:48	2006-06-22	Administrator	Complete		
9	Upload Extractor Data	User Upload	Immediate	2006-06-22 18:24:34	2006-06-22	Administrator	Complete		
8	Upload Extractor Data	actions	Immediate	2006-06-22 18:15:34	2006-06-22	Administrator	Complete		
7	Upload Extractor Data	users	Immediate	2006-06-22 18:13:34	2006-06-22	Administrator	Complete		
6	Upload Extractor Data	users	Immediate	2006-06-22 18:11:33	2006-06-22	Administrator	Complete		

11 of 25

To access the logs, Click View Log.

The following screen will be displayed.

Log Display

Log File: Scroll down to look at the latest log

```

Jun 25, 2006 3:15:57 PM com.virsa.cc.xsys.util.RiskLoader getPermRuleForCritActPerm
FINEST: syskey=GLOBAL action='PA64' risk='HRMD'
Jun 25, 2006 3:15:57 PM com.virsa.cc.xsys.util.RiskLoader getPermRuleForCritActPerm
FINEST: syskey=GLOBAL action='PA97' risk='HRMD'
Jun 25, 2006 3:15:57 PM com.virsa.cc.xsys.util.RiskLoader getPermRuleForCritActPerm
FINEST: syskey=GLOBAL action='PAT1' risk='HRMD'
Jun 25, 2006 3:15:57 PM com.virsa.cc.xsys.util.RiskLoader getPermRuleForCritActPerm
FINEST: syskey=GLOBAL action='PE01' risk='HRMD'
Jun 25, 2006 3:15:58 PM com.virsa.cc.xsys.util.RiskLoader getPermRuleForCritActPerm
FINEST: syskey=GLOBAL action='PE02' risk='HRMD'
Jun 25, 2006 3:15:58 PM com.virsa.cc.xsys.util.RiskLoader getPermRuleForCritActPerm
FINEST: syskey=GLOBAL action='PE03' risk='HRMD'
Jun 25, 2006 3:15:58 PM com.virsa.cc.xsys.util.RiskLoader getPermRuleForCritActPerm
FINEST: syskey=GLOBAL action='PE04' risk='HRMD'
Jun 25, 2006 3:15:58 PM com.virsa.cc.xsys.util.RiskLoader getPermRuleForCritActPerm
FINEST: syskey=GLOBAL action='PO01' risk='HRMD'
Jun 25, 2006 3:15:58 PM com.virsa.cc.xsys.util.RiskLoader getPermRuleForCritActPerm
FINEST: syskey=GLOBAL action='PO03' risk='HRMD'
Jun 25, 2006 3:15:58 PM com.virsa.cc.xsys.util.RiskLoader getPermRuleForCritActPerm
FINEST: syskey=GLOBAL action='PO04' risk='HRMD'

```

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.

Background Daemon

Background Daemon details	
Daemon Iteration Interval (min)	1
Active	Running !!!
Update Daemon details	
Daemon Iteration Interval (min)	<input type="text" value="1"/>
Active	<input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Update"/>
Background Daemon execution details	
Background Main Thread Initiated at Thu Jun 22 19:02:31 PDT 2006 and Active Status is:true	
-- Getting all the jobs Thu Jun 22 19:02:31 PDT 2006	
-- Getting all the jobs Thu Jun 22 19:03:31 PDT 2006	
-- Getting all the jobs Thu Jun 22 19:04:31 PDT 2006	
-- Getting all the jobs Thu Jun 22 19:05:31 PDT 2006	
-- Getting all the jobs Thu Jun 22 19:06:31 PDT 2006	
-- Getting all the jobs Thu Jun 22 19:07:31 PDT 2006	
-- Getting all the jobs Thu Jun 22 19:08:31 PDT 2006	
-- Getting all the jobs Thu Jun 22 19:09:31 PDT 2006	

Make sure it is running

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.

Analysis Engine Daemon Manager

Daemon Status		
Daemon ID	Status	Since
Background Job Workers		
0	IDLE	Thursday, June 29, 2006 2:54:37 PM
1	IDLE	Thursday, June 29, 2006 2:54:39 PM
2	IDLE	Thursday, June 29, 2006 2:54:41 PM
Web Services Workers		
3	IDLE	Thursday, June 29, 2006 2:54:43 PM
4	IDLE	Thursday, June 29, 2006 2:54:45 PM
5	IDLE	Thursday, June 29, 2006 2:54:47 PM
6	IDLE	Thursday, June 29, 2006 2:54:49 PM
7	IDLE	Thursday, June 29, 2006 2:54:51 PM
# Daemon Workers: Bg Job <input type="text" value="3"/> Web Services <input type="text" value="5"/> Change Pool Size		
<input type="button" value="Start All"/> <input type="button" value="Stop All"/> <input type="button" value="Refresh"/>		


Make sure it says 'IDLE'. if it says "STOPPED", that means there is a problem and you can not go further.

Copyright

© Copyright 2007 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, Informix, i5/OS, POWER, POWER5, OpenPower and PowerPC are trademarks or registered trademarks of IBM Corporation.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

MaxDB is a trademark of MySQL AB, Sweden.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

These materials are provided "as is" without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

SAP shall not be liable for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials.

SAP does not warrant the accuracy or completeness of the information, text, graphics, links or other items contained within these materials. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third party web pages nor provide any warranty whatsoever relating to third party web pages.

Any software coding and/or code lines/strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, except if such damages were caused by SAP intentionally or grossly negligent.