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
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.

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

**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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Field Type</th>
<th>Field Size</th>
<th>Field Values</th>
<th>Sorting</th>
<th>Required</th>
<th>Description</th>
<th>Transformation Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leave Blank</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Mandatory field, Required by load format</td>
<td>Leave Blank</td>
</tr>
<tr>
<td>&quot;PRM&quot;</td>
<td>String</td>
<td>3</td>
<td>CAPS</td>
<td></td>
<td></td>
<td>Hard code &quot;PRM&quot; as value for this field</td>
<td>Hard coded value PRM</td>
</tr>
<tr>
<td>Leave Blank</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Mandatory field, Required by load format</td>
<td>Leave Blank</td>
</tr>
<tr>
<td>PERMISSION</td>
<td>String</td>
<td>50</td>
<td>CAPS</td>
<td>Yes</td>
<td>Permission</td>
<td>Permission</td>
<td>Sorted Ascending</td>
</tr>
<tr>
<td>&quot;EN&quot;</td>
<td>String</td>
<td>2</td>
<td>CAPS</td>
<td></td>
<td></td>
<td>Hard code &quot;EN&quot; as value for this field</td>
<td>Hard coded value EN</td>
</tr>
<tr>
<td>PERMISSION</td>
<td>String</td>
<td>&lt;100</td>
<td></td>
<td>Yes</td>
<td>Permission</td>
<td>Permission</td>
<td></td>
</tr>
</tbody>
</table>
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.
<table>
<thead>
<tr>
<th>Field</th>
<th>Data Field Type</th>
<th>Field Size</th>
<th>Field Values</th>
<th>Sorting</th>
<th>Required</th>
<th>Description</th>
<th>Transformation Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>USREID</td>
<td>String</td>
<td>50</td>
<td>CAPS</td>
<td>Sorted Ascending</td>
<td>Yes</td>
<td>User ID</td>
<td>Unique records only</td>
</tr>
<tr>
<td>FNAME</td>
<td>String</td>
<td>50</td>
<td></td>
<td>Yes</td>
<td></td>
<td>First Name (if not available, repeat User ID field here)</td>
<td></td>
</tr>
<tr>
<td>LNAME</td>
<td>String</td>
<td>50</td>
<td></td>
<td>Yes</td>
<td></td>
<td>Last Name (if not available, repeat User ID field here)</td>
<td></td>
</tr>
<tr>
<td>EMAIL</td>
<td>String</td>
<td>250</td>
<td></td>
<td>No</td>
<td></td>
<td>Email address</td>
<td></td>
</tr>
<tr>
<td>PHONE</td>
<td>String</td>
<td>40</td>
<td></td>
<td>No</td>
<td></td>
<td>Phone # - leave blank if not available</td>
<td></td>
</tr>
<tr>
<td>DEPARTMENT</td>
<td>String</td>
<td>40</td>
<td></td>
<td>No</td>
<td></td>
<td>Department</td>
<td></td>
</tr>
<tr>
<td>USERGROUP</td>
<td>String</td>
<td>20</td>
<td>CAPS</td>
<td>No</td>
<td></td>
<td>User Group - leave blank if not available</td>
<td></td>
</tr>
</tbody>
</table>

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.
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.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Length</th>
<th>Case Sensitive</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROFILE</td>
<td>String</td>
<td>50</td>
<td>CAPS</td>
<td>Action Profile, if applicable. If not, repeat Role Name field.</td>
</tr>
<tr>
<td>COMPOSITE ROLENAME</td>
<td>String</td>
<td>50</td>
<td>No</td>
<td>Composite role name, leave blank if not available</td>
</tr>
</tbody>
</table>

**Important Notes for Downloading and Formatting:**

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

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Field Type</th>
<th>Field Size</th>
<th>Field Values</th>
<th>Sorting</th>
<th>Required</th>
<th>Description</th>
<th>Transformation Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>String</td>
<td>50</td>
<td>CAPS</td>
<td>Sorted Ascending</td>
<td>Yes</td>
<td>Access Role Name</td>
<td></td>
</tr>
<tr>
<td>Role description</td>
<td>String</td>
<td>100</td>
<td></td>
<td></td>
<td>Yes</td>
<td>Role Description</td>
<td></td>
</tr>
</tbody>
</table>

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. 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.
Extracting Role Action

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

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

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. 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 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.

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

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. 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.

```
<table>
<thead>
<tr>
<th>Create Connector</th>
</tr>
</thead>
<tbody>
<tr>
<td>System ID</td>
</tr>
<tr>
<td>System Name</td>
</tr>
<tr>
<td>System Type</td>
</tr>
<tr>
<td>Connection Type</td>
</tr>
<tr>
<td>Location</td>
</tr>
<tr>
<td>User ID</td>
</tr>
<tr>
<td>Password</td>
</tr>
</tbody>
</table>
```

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.

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 Foreground to upload the file.
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

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

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

![Function Authorization Screen](image)

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

![Risk Configuration Screen]

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:

<table>
<thead>
<tr>
<th>Risk Analysis - Default Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default report type for risk analysis</strong></td>
</tr>
<tr>
<td>This option sets the default Report Type when running a Risk Analysis.</td>
</tr>
<tr>
<td><strong>Default risk level for risk analysis</strong></td>
</tr>
<tr>
<td>This option sets the default Risk Level when running a Risk Analysis. The default value is ALL.</td>
</tr>
<tr>
<td><strong>Default user type for risk analysis</strong></td>
</tr>
<tr>
<td>This option sets the default User Type included when running a Risk Analysis. The default is All.</td>
</tr>
<tr>
<td><strong>Default rule set for risk analysis</strong></td>
</tr>
<tr>
<td>This option sets the default Rule Set included when running a Risk Analysis.</td>
</tr>
</tbody>
</table>

- **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.

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

![Create Data Extractor](image)

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

![Create Data Extractor](image)

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:

![Schedule Risk Analysis Background Job](image)

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.

<table>
<thead>
<tr>
<th>Background Daemon details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Daemon Iteration Interval (min)</td>
<td>1</td>
</tr>
<tr>
<td>Active</td>
<td>Running !!!</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Update Daemon details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Daemon Iteration Interval (min)</td>
<td>1</td>
</tr>
<tr>
<td>Active</td>
<td>Start</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Background Daemon execution details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Background Main Thread Initiated at Thu Jun 22 19:02:31 PDT 2006 and Active Status is true</td>
<td></td>
</tr>
<tr>
<td>-- Getting all the jobs Thu Jun 22 19:02:31 PDT 2006</td>
<td></td>
</tr>
<tr>
<td>-- Getting all the jobs Thu Jun 22 19:03:31 PDT 2006</td>
<td></td>
</tr>
<tr>
<td>-- Getting all the jobs Thu Jun 22 19:04:31 PDT 2006</td>
<td></td>
</tr>
<tr>
<td>-- Getting all the jobs Thu Jun 22 19:05:31 PDT 2006</td>
<td></td>
</tr>
<tr>
<td>-- Getting all the jobs Thu Jun 22 19:06:31 PDT 2006</td>
<td></td>
</tr>
<tr>
<td>-- Getting all the jobs Thu Jun 22 19:07:31 PDT 2006</td>
<td></td>
</tr>
<tr>
<td>-- Getting all the jobs Thu Jun 22 19:08:31 PDT 2006</td>
<td></td>
</tr>
<tr>
<td>-- Getting all the jobs Thu Jun 22 19:09:31 PDT 2006</td>
<td></td>
</tr>
</tbody>
</table>

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.

```
<table>
<thead>
<tr>
<th>Daemon ID</th>
<th>Status</th>
<th>Since</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>IDLE</td>
<td>Thursday, June 29, 2006 2:54:37 PM</td>
</tr>
<tr>
<td>1</td>
<td>IDLE</td>
<td>Thursday, June 29, 2006 2:54:39 PM</td>
</tr>
<tr>
<td>2</td>
<td>IDLE</td>
<td>Thursday, June 29, 2006 2:54:41 PM</td>
</tr>
<tr>
<td>3</td>
<td>IDLE</td>
<td>Thursday, June 29, 2006 2:54:43 PM</td>
</tr>
<tr>
<td>4</td>
<td>IDLE</td>
<td>Thursday, June 29, 2006 2:54:45 PM</td>
</tr>
<tr>
<td>5</td>
<td>IDLE</td>
<td>Thursday, June 29, 2006 2:54:47 PM</td>
</tr>
<tr>
<td>6</td>
<td>IDLE</td>
<td>Thursday, June 29, 2006 2:54:49 PM</td>
</tr>
<tr>
<td>7</td>
<td>IDLE</td>
<td>Thursday, June 29, 2006 2:54:51 PM</td>
</tr>
</tbody>
</table>
```

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.