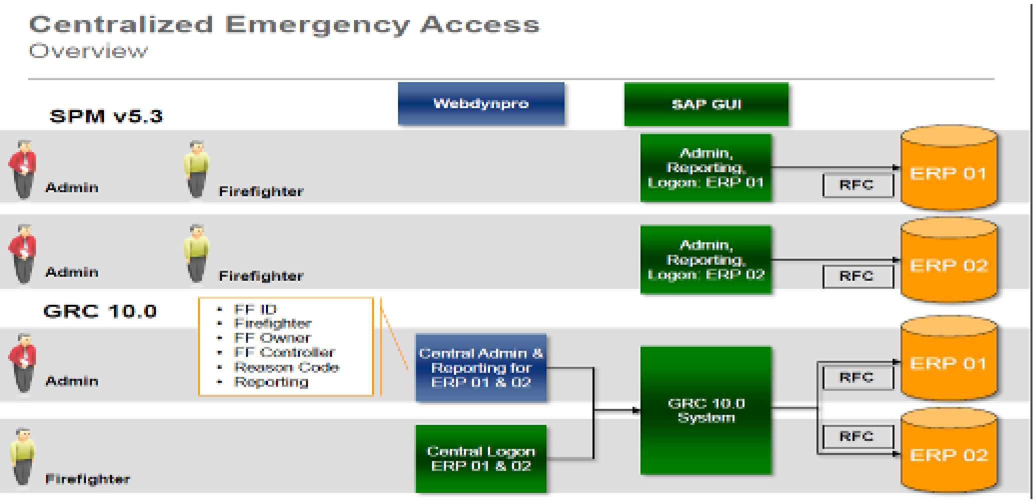
SAP GRC 10.0 – Super User Management

INTRODUCTION

Centralized Emergency Access: The purpose of Emergency Access Management is to allow users to take responsibility for tasks outside their normal job function. This component allows temporary access for users when assigned with solving a problem, giving them provisionally broad, but regulated access. This temporary access is monitored and recorded in this application.

New in 10.0

Access Control 10.0 has been enhanced in the area of Emergency Access Management with the ability to manage and utilize firefighting activities centrally from the Access Control 10.0 application. Also the log file can be distributed to controllers and owner via workflow for additional approval.



Feature and Benefits

- Simplified management and firefighting activities.
- Reduces repetitive assignments, easing administration.
- Improves log review efficiency by capturing previously undocumented activity.
- Improves log report navigation.
- Enables documented account of the controller's review.
- Administrators centrally manage firefighter assignments, controllers, and other master data.
- New options for group owners and controllers and improved provisioning.
- Firefighters centrally access their assignments.
- New ability for firefighters to update the activity log with unplanned firefighting tasks
- Access specific log reports from transaction report

- New workflow driven firefighter log report.
    - New categorization of firefighter access signifies criticality and drives workflow logic.

TERMINOLOGY

Firefighter: User requiring emergency access.

Firefighter ID: User ID with elevated privileges; it can only be accessed in the GRC server using transaction **GRAC_SPM**.

Firefighting: The act of using a firefighterID

Owner: User responsible for a firefighterID and the assignment of controllers and firefighters.

Controller: Reviews and approves (if necessary) the log files generated by a firefighter.

Configuration:

Activating BC Sets:

BC Set= Buisness Configuration settings which contains standard data for each component and the stnadard data is required to configure the components.

We can Use transaction SCPR20 to activate BC Sets.

Path: SPRO--> SAP Reference IMG--> Click on "Existing BC Sets"--> GRC--> General settings--> Key attributes--> Go-to--> Activate transaction--> activate

BC sets for EAM:

GRAC_SPM_CRITICALITY_LEVEL Criticality Level

Maintain connectors and connection types:

In this Customizing activity, you define connection types, which are then used while connecting to other systems.

Path: SPRO-->SAP Ref IMG--> GRC--> Common component settings--> Integration frame work--> Maintain connectors and connection types

Connection types:

EP	Enterprise Portal
FILE	File system for legacy extraction
LDAP	Ldap Connectors

LOCAL	Local Data Source
SAP	SAP System
SPML1	SPML1
SPML2	SPML2
WS	Web service

1. Define connector and maintain connection type
2. Define Connector group and assign respective SAP system into connector group.

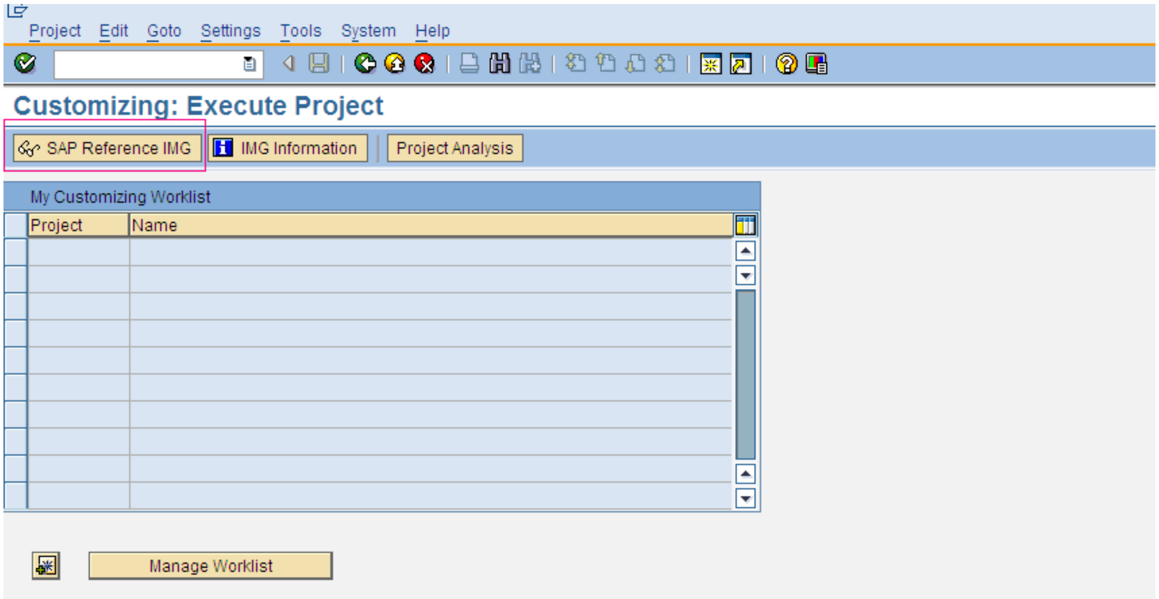
Maintain connection settings:

Integration scenarios:

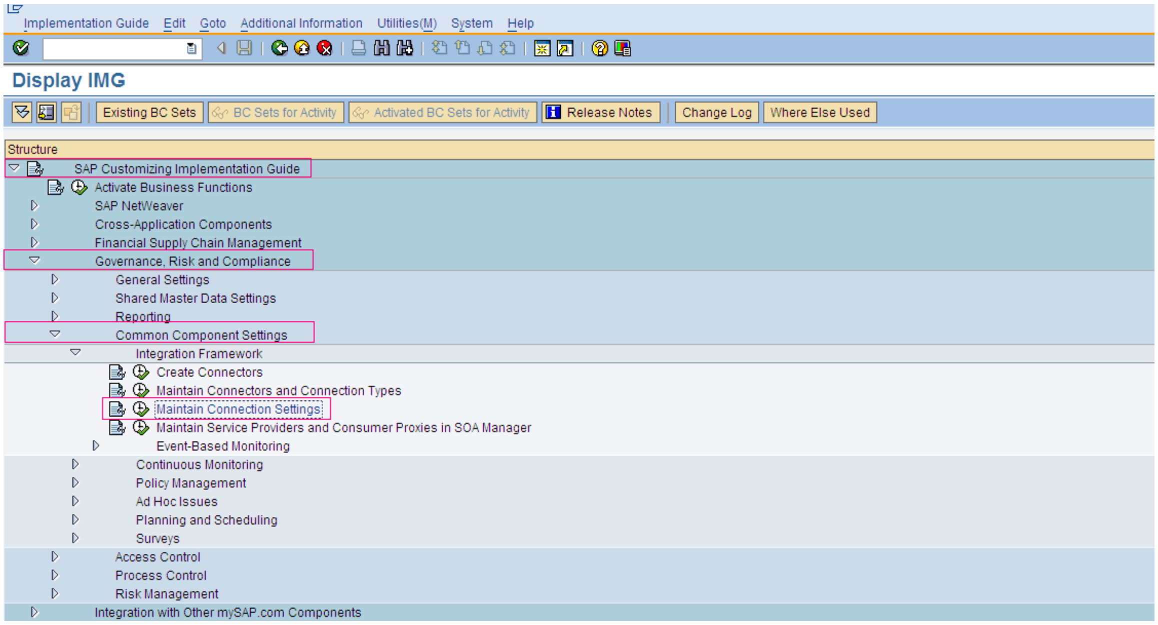
To create access requests it is required to have the SUPMG scenario linked to the connector, which is done via IMG in the GRC box:

Execute transaction SPRO =>Click on SAP Reference IMG

In this Customizing activity, you assign connectors to an integration scenario. The application uses the connectors to communicate with other systems in your landscape.



Expand SAP Customizing Implementation Guide =>Governance, Risk and Compliance => Common Component Settings => Execute Maintain Connection Settings

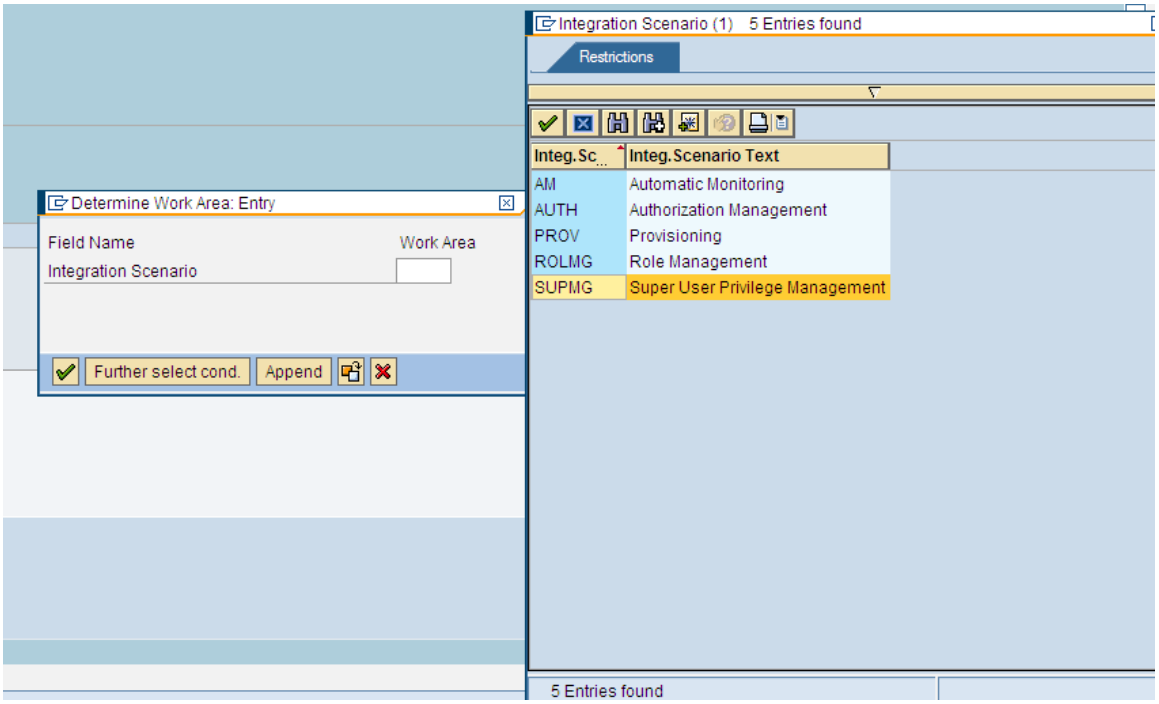

Implementation Guide Edit Goto Additional Information Utilities(M) System Help
Display IMG
Existing BC Sets
BC Sets for Activity
Activated BC Sets for Activity
Release Notes
Change Log
Where Else Used

Structure

- SAP Customizing Implementation Guide
  - Activate Business Functions
  - SAP NetWeaver
  - Cross-Application Components
  - Financial Supply Chain Management
  - Governance, Risk and Compliance
    - General Settings
    - Shared Master Data Settings
    - Reporting
    - Common Component Settings
      - Integration Framework
        - Create Connectors
        - Maintain Connectors and Connection Types
        - Maintain Connection Settings
        - Maintain Service Providers and Consumer Proxies in SOA Manager
        - Event-Based Monitoring
      - Continuous Monitoring
      - Policy Management
      - Ad Hoc Issues
      - Planning and Scheduling
      - Surveys
    - Access Control
    - Process Control
    - Risk Management
  - Integration with Other mySAP.com Components

Use: In this Customizing activity, you assign connectors to an integration scenario. The application uses the connectors to communicate with other systems in your landscape. For example, if you have an ERP integration scenario, you assign the connectors of the ERP systems to the integration scenario.

After execution, a pop-up appear prompting for Integration Scenario. We need to select the Integration Scenario as “SUPMG”.

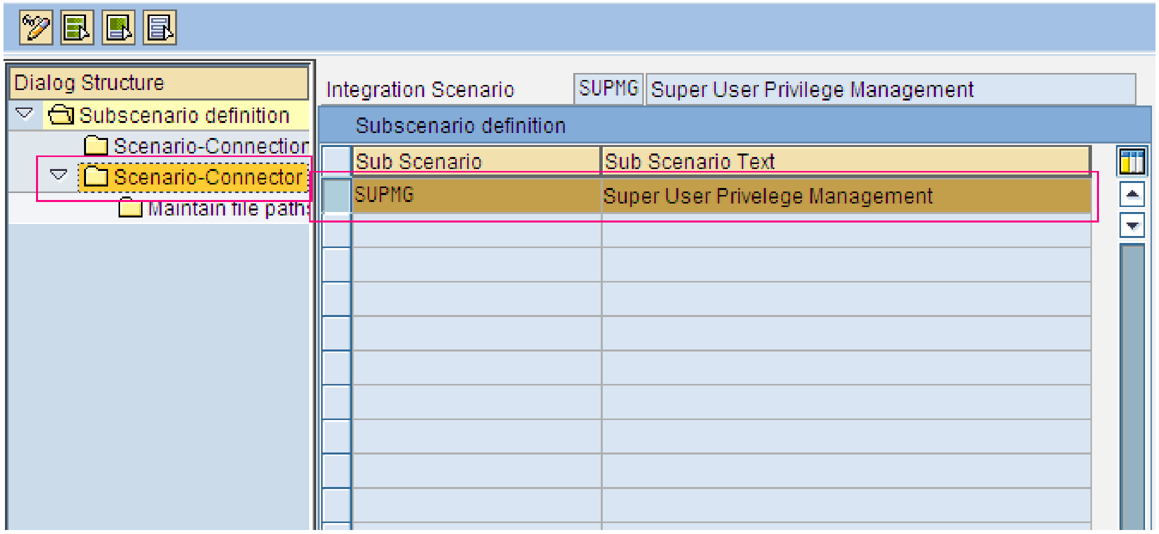

Determine Work Area: Entry
Further select cond.
Append
Integration Scenario (1) 5 Entries found
Restrictions

Field Name	Work Area
Integration Scenario	

Integ.Sc...	Integ.Scenario Text
AM	Automatic Monitoring
AUTH	Authorization Management
PROV	Provisioning
ROLMG	Role Management
SUPMG	Super User Privilege Management

5 Entries found

Below screen will appear. We then need to select the Sub Scenario SUPMG and double click on *Scenario-Connector Link*.

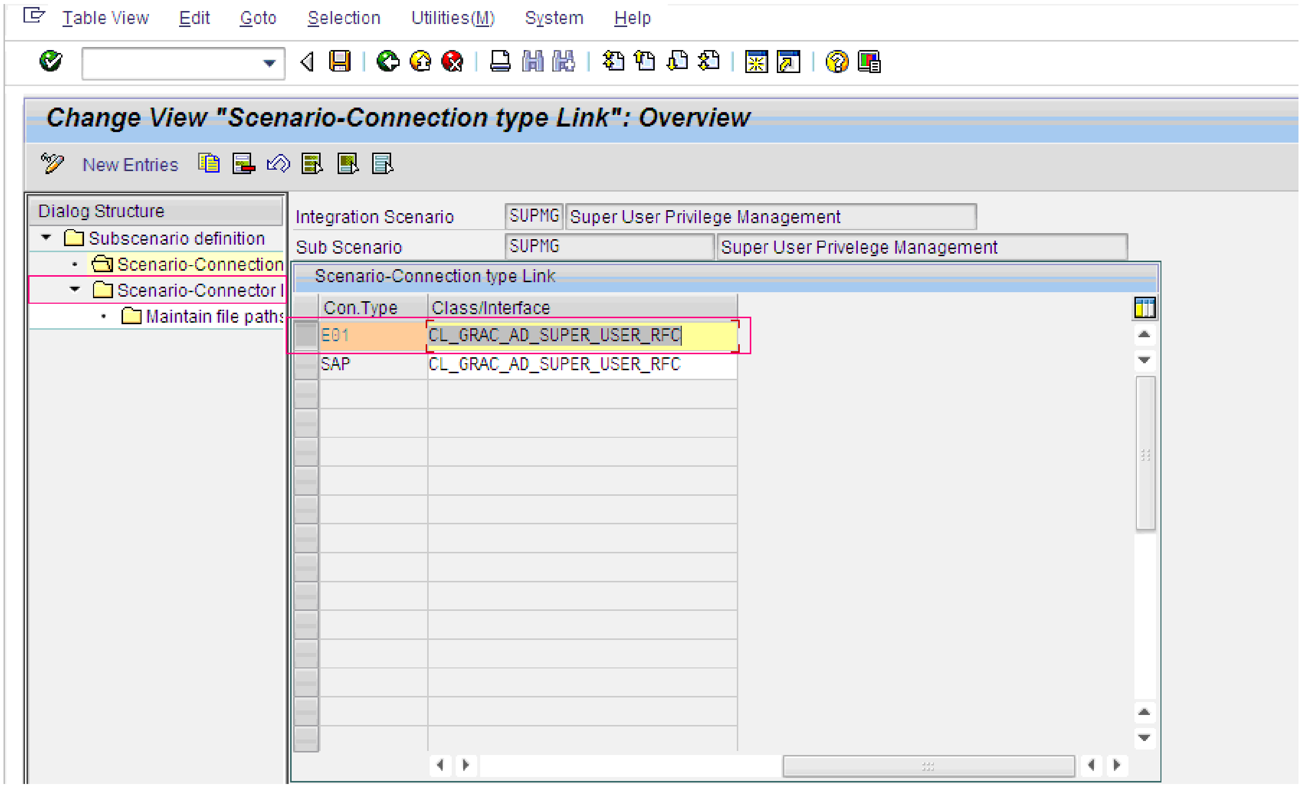


Integration Scenario SUPMG Super User Privilege Management

Subscenario definition

Sub Scenario	Sub Scenario Text
SUPMG	Super User Privelege Management

Below screen will appear:



Change View "Scenario-Connection type Link": Overview

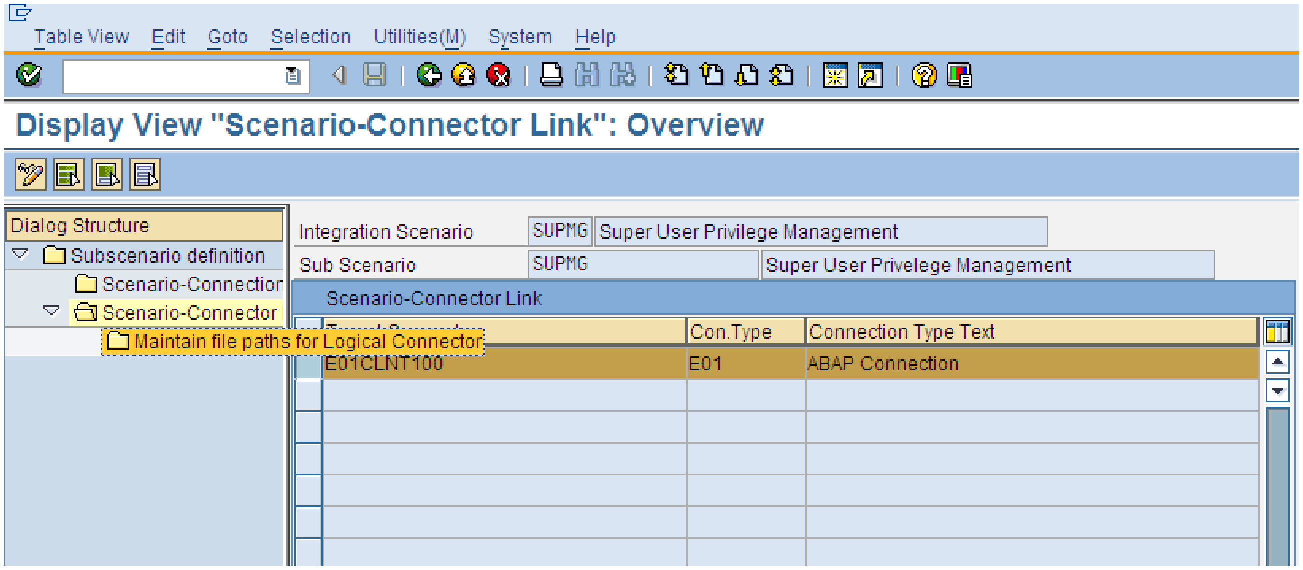
Integration Scenario SUPMG Super User Privilege Management

Sub Scenario SUPMG Super User Privelege Management

Scenario-Connection type Link

Con.Type	Class/Interface
E01	CL_GRAC_AD_SUPER_USER_RFC
SAP	CL_GRAC_AD_SUPER_USER_RFC

We then need to select the Con. Type E01 (as in this case) and double click on *Scenario-Connector Link*.



Display View "Scenario-Connector Link": Overview

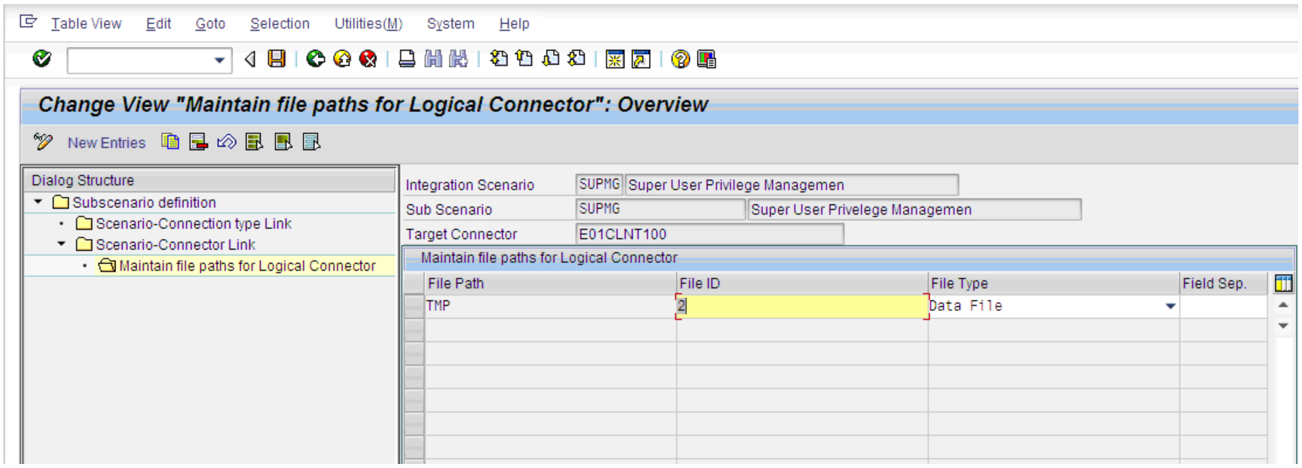
Dialog Structure
- Subscenario definition
  - Scenario-Connectior
  - Scenario-Connector
    - Maintain file paths for Logical Connector

Integration Scenario	SUPMG	Super User Privilege Management
Sub Scenario	SUPMG	Super User Privelege Management

Scenario-Connector Link

Target Connector	Con.Type	Connection Type Text
E01CLNT100	E01	ABAP Connection

Select Target Connector and double click on "*Maintain file paths for Logical Connector*". Below screen will display.



Change View "Maintain file paths for Logical Connector": Overview

Dialog Structure
- Subscenario definition
  - Scenario-Connection type Link
  - Scenario-Connector Link
    - Maintain file paths for Logical Connector

Integration Scenario	SUPMG	Super User Privilege Managemen
Sub Scenario	SUPMG	Super User Privelege Managemen
Target Connector	E01CLNT100	

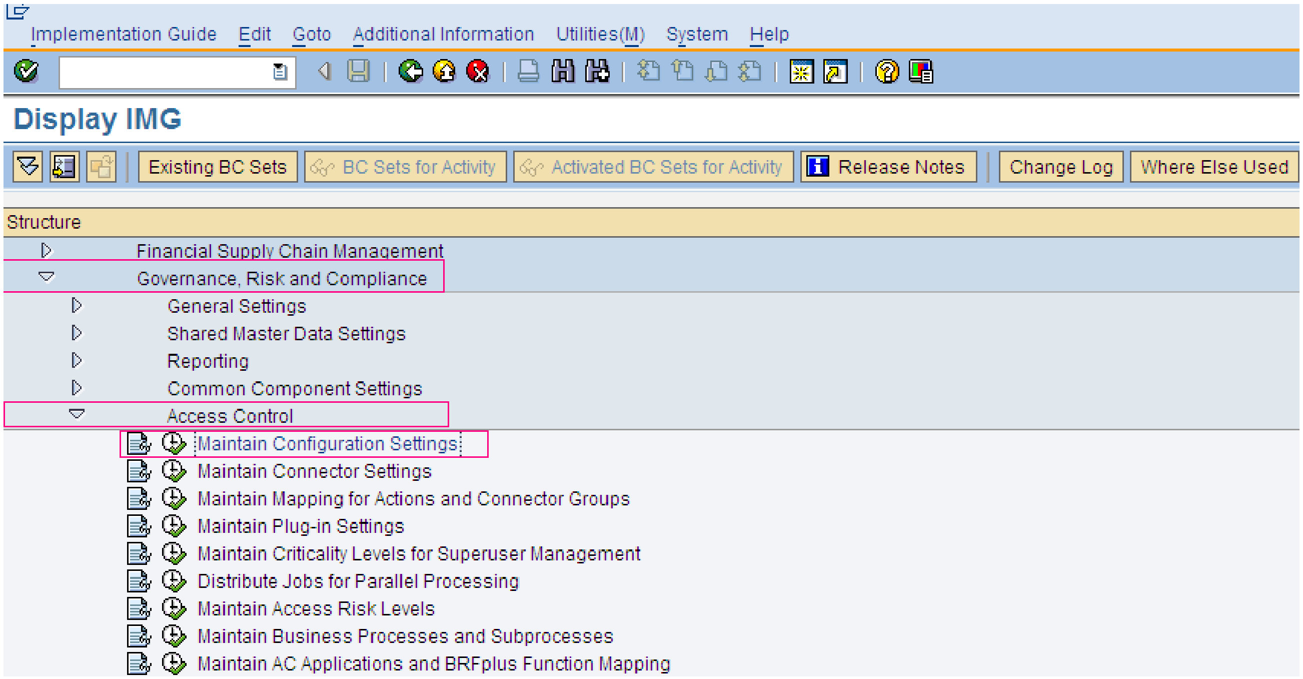
Maintain file paths for Logical Connector

File Path	File ID	File Type	Field Sep.
TMP	2	Data File	

We then need to maintain the above entries.

Once above activity is completed, we need to go back in SPRO screen and execute ***Maintain Configuration Settings.***

Governance, Risk and Compliance => Access Control => Execute Maintain Configuration Settings

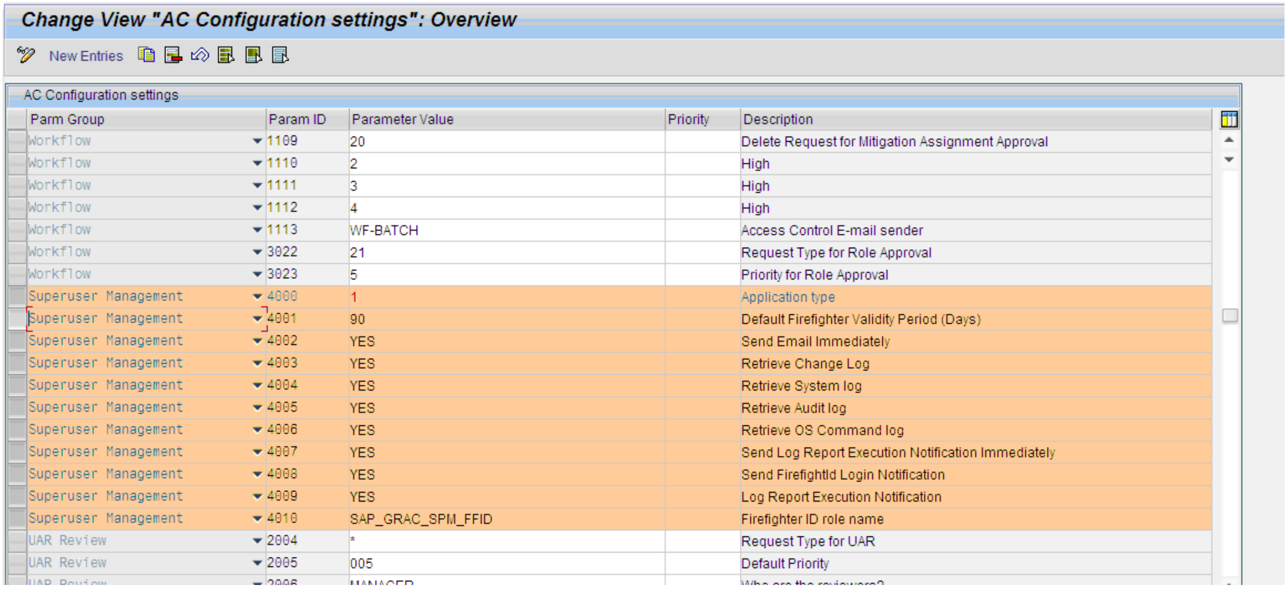


Display IMG

Structure

- Financial Supply Chain Management
- Governance, Risk and Compliance
  - General Settings
  - Shared Master Data Settings
  - Reporting
  - Common Component Settings
  - Access Control
    - Maintain Configuration Settings
    - Maintain Connector Settings
    - Maintain Mapping for Actions and Connector Groups
    - Maintain Plug-in Settings
    - Maintain Criticality Levels for Superuser Management
    - Distribute Jobs for Parallel Processing
    - Maintain Access Risk Levels
    - Maintain Business Processes and Subprocesses
    - Maintain AC Applications and BRFplus Function Mapping

Use: In this Customizing activity, you maintain the general configuration settings and parameters used in the access control application.



Change View "AC Configuration settings": Overview

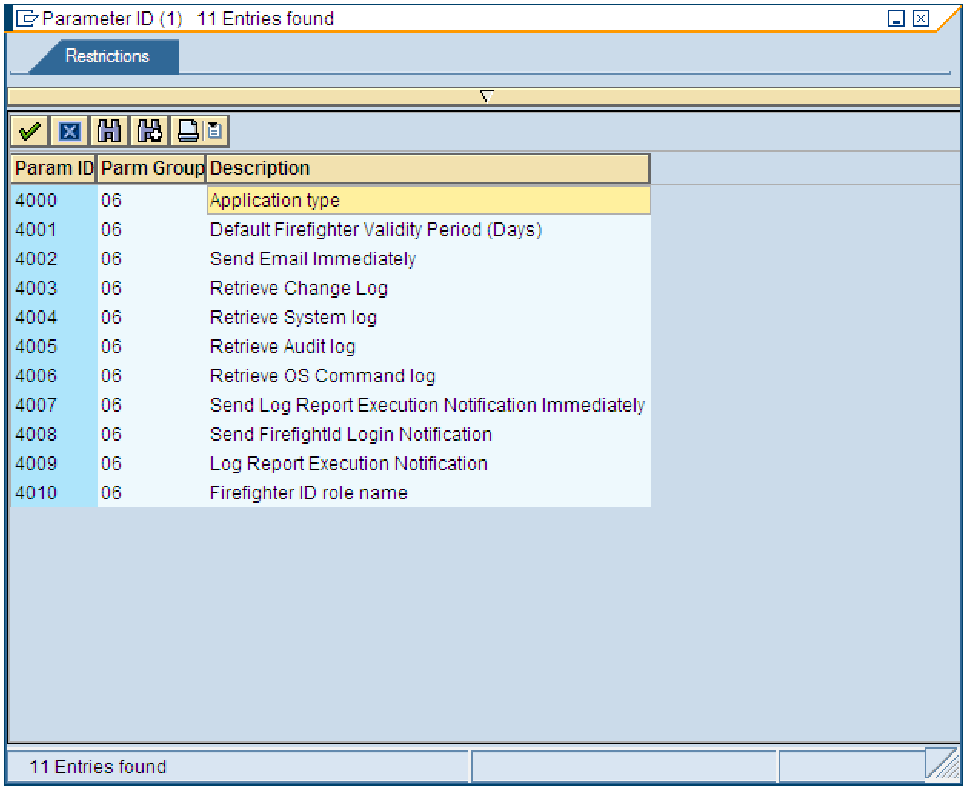
AC Configuration settings

Parm Group	Param ID	Parameter Value	Priority	Description
Workflow	1109	20		Delete Request for Mitigation Assignment Approval
Workflow	1110	2		High
Workflow	1111	3		High
Workflow	1112	4		High
Workflow	1113	WF-BATCH		Access Control E-mail sender
Workflow	3022	21		Request Type for Role Approval
Workflow	3023	5		Priority for Role Approval
Superuser Management	4000	1		Application type
Superuser Management	4001	90		Default Firefighter Validity Period (Days)
Superuser Management	4002	YES		Send Email Immediately
Superuser Management	4003	YES		Retrieve Change Log
Superuser Management	4004	YES		Retrieve System log
Superuser Management	4005	YES		Retrieve Audit log
Superuser Management	4006	YES		Retrieve OS Command log
Superuser Management	4007	YES		Send Log Report Execution Notification Immediately
Superuser Management	4008	YES		Send FirefightId Login Notification
Superuser Management	4009	YES		Log Report Execution Notification
Superuser Management	4010	SAP_GRAC_SPM_FFID		Firefighter ID role name
UAR Review	2004	*		Request Type for UAR
UAR Review	2005	005		Default Priority
UAR Review	2006	MANAGER		Who are the reviewers?

Here in the above screen, we need to select the *Parm Group* as “Superuser Management” and can configure below *Param Ids* accordingly.

To maintain the configuration settings:
1. Choose the New Entries pushbutton and select a parameter group from the dropdown list.
2. In the Parameter ID column, select a parameter ID for use with the parameter group. The short description appears on the right-hand side.

3. Select a Parameter Value from the dropdown list, or enter values in the field.
4. In the Priority field, enter a number for the priority.
5. Choose Save.



Param ID	Parm Group	Description
4000	06	Application type
4001	06	Default Firefighter Validity Period (Days)
4002	06	Send Email Immediately
4003	06	Retrieve Change Log
4004	06	Retrieve System log
4005	06	Retrieve Audit log
4006	06	Retrieve OS Command log
4007	06	Send Log Report Execution Notification Immediately
4008	06	Send FirefightId Login Notification
4009	06	Log Report Execution Notification
4010	06	Firefighter ID role name

11 Entries found

Below is the brief detail for the Param Ids for Super user Management:

Superuser Management 4000 Application type

You use this parameter to set the firefighting configuration:
Choose 1 for ID-based firefighting.
Choose 2 for Role-based firefighting.

Superuser Management 4001 Default Firefighter Validity Period (Days)

Set the default validity period (in days) of firefighter ID assignments to a firefighter.

Note: This is only the default period. You can override the validity period for each assignment as needed in the front-end.

Superuser Management 4002 Send E-mail Immediately

The application sends e-mail notifications to the controller.
Set the value to YES to send the e-mail notifications immediately.

Set the value to NO and the application sends notifications only when the user chooses the Update Firefighter Log button or runs the program GRAC_SPM_LOG_SYNC_UPDATE.
The Update Firefighter Log button is available on the Consolidated Log Report under Superuser Management Reports.

Superuser Management 4003 Retrieve Change Log

If set to YES then the application fetches the Change Log when the user chooses the Update Firefighter Log button or runs the program GRAC_SPM_LOG_SYNC_UPDATE.
The Update Firefighter Log button is available on the Consolidated Log Report under Superuser Management Reports.
Note: Plug-in system must have the O/S time and R/3 time zone matched for the logs to be properly collected. This is because STAD stores the logs in O/S files.

Superuser Management 4004 Retrieve System Log

If set to YES then the application fetches the System Log (debug changes) when the user chooses the Update Firefighter Log button or runs the program GRAC_SPM_LOG_SYNC_UPDATE.
The Update Firefighter Log button is available on the Consolidated Log Report under Superuser Management Reports.

Superuser Management 4005 Retrieve Audit Log

If set to YES then the application fetches the audit (security) logs when the user chooses the Update Firefighter Log button or runs the program GRAC_SPM_LOG_SYNC_UPDATE.
The Update Firefighter Log button is available on the Consolidated Log Report under Superuser Management Reports.
Note: You can activate Audit Logs using the transaction SM19.

Superuser Management 4006 Retrieve O/S Command Log

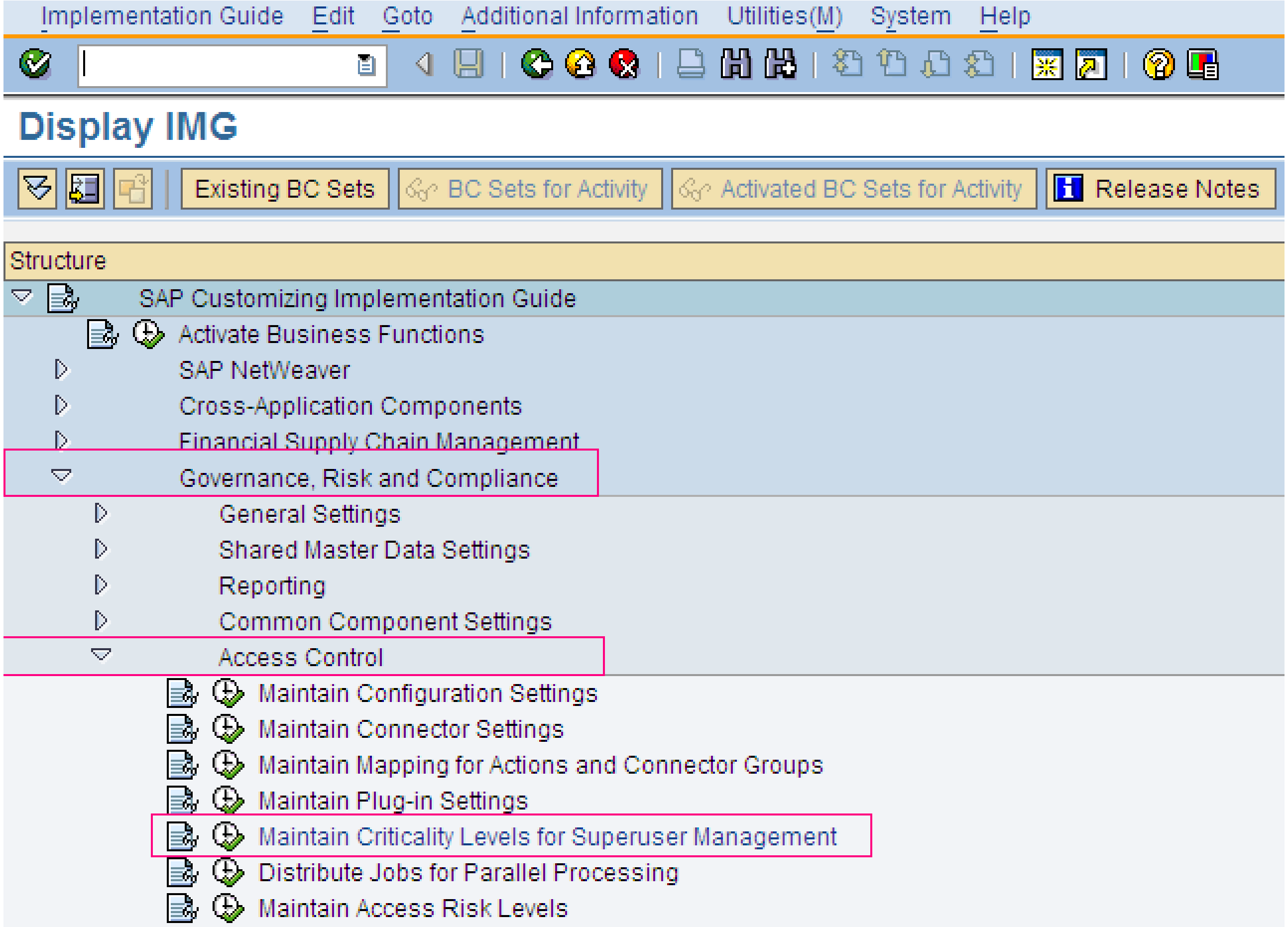
If set to YES then the application fetches the O/S Command Log when the user chooses the Update Firefighter Log button or runs the program GRAC_SPM_LOG_SYNC_UPDATE. The O/S Command Log tracks information when O/S commands (SM49) are created, changed, or executed.
The Update Firefighter Log button is available on the Consolidated Log Report under Superuser Management Reports.

Superuser Management 4007 Send Log Report Execution Notification Immediately

The application can send log reports controllers. The application sends the notifications as e-mails or workflow items based on the configuration of the controllers.
Set the value to YES and the application sends notifications when the user chooses the Update Firefighter Log button or runs the program GRAC_SPM_LOG_SYNC_UPDATE.
The Update Firefighter Log button is available on the Consolidated Log Report under Superuser Management Reports.

Set the value to NO and the application only collects the logs when the user chooses the Update Firefighter Log button or runs the GRAC_SPM_LOG_SYNC_UPDATE program. The application sends the e-mail notifications when the G
RAC_SPM_WORKFLOW_SYNC program is run.

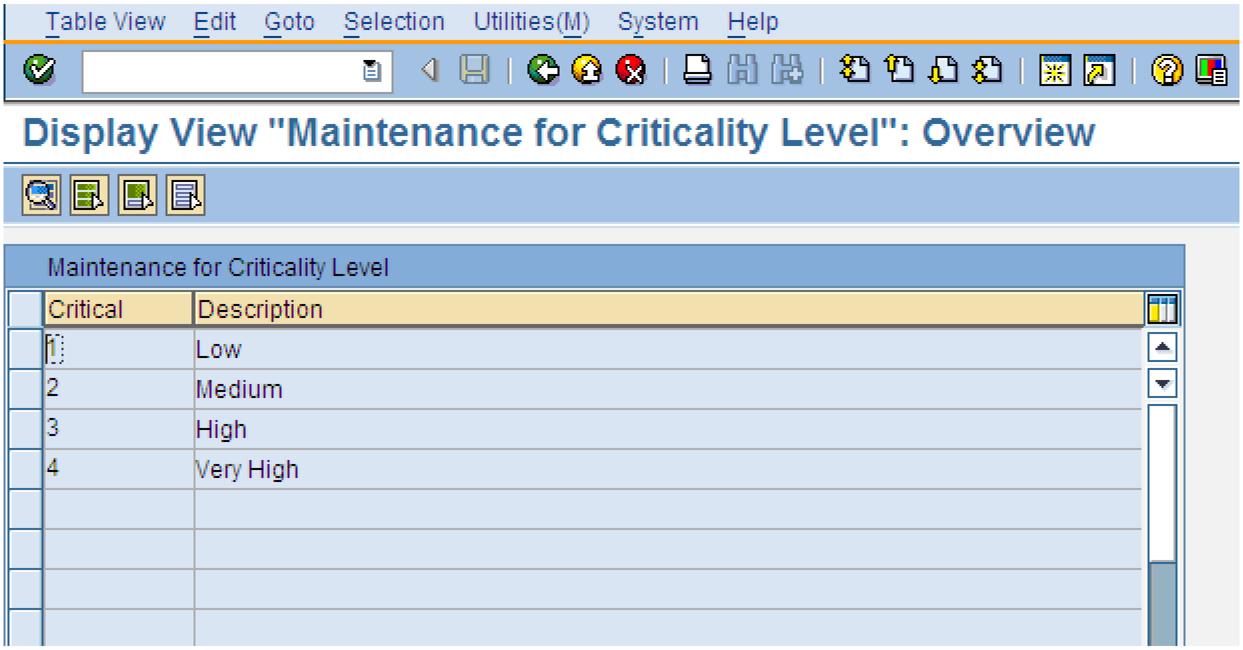
After configuring we need to go back to SPRO IMG and select **Maintain Criticality Levels for Superuser Management**



- SAP Customizing Implementation Guide
  - Activate Business Functions
  - SAP NetWeaver
  - Cross-Application Components
  - Financial Supply Chain Management
  - Governance, Risk and Compliance
    - General Settings
    - Shared Master Data Settings
    - Reporting
    - Common Component Settings
    - Access Control
      - Maintain Configuration Settings
      - Maintain Connector Settings
      - Maintain Mapping for Actions and Connector Groups
      - Maintain Plug-in Settings
      - Maintain Criticality Levels for Superuser Management
      - Distribute Jobs for Parallel Processing
      - Maintain Access Risk Levels

In this Customizing activity, you can specify the criticality level for the access control application.

To maintain the criticality levels:
1. Choose the New Entries pushbutton, and then enter a number between 1 and 99 to define the criticality level.
2. In the Short Description column, enter a user-defined description.
3. Save the entry.



Display View "Maintenance for Criticality Level": Overview

Maintenance for Criticality Level

Critical	Description
1	Low
2	Medium
3	High
4	Very High

At this point of time, configuration part has been completed. Now we need to maintain the Owner and Controller for the FF Ids.

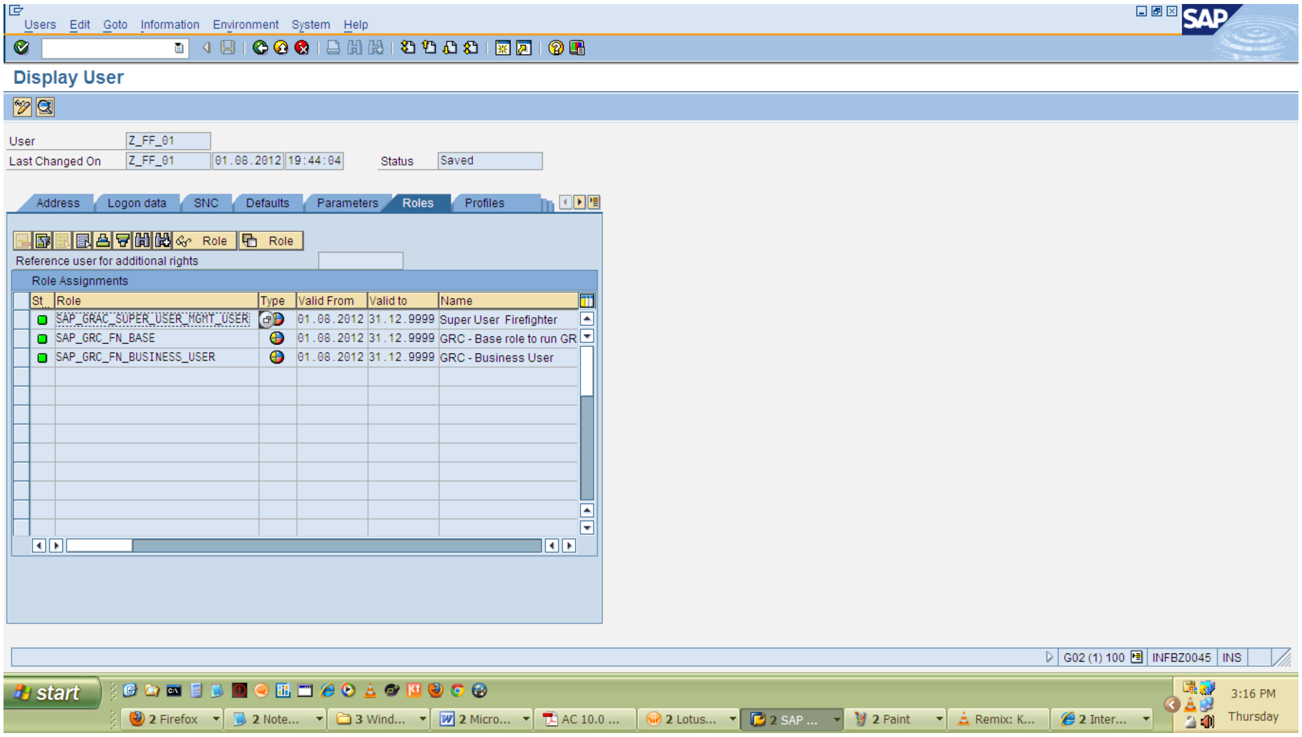
Firstly we need to create the Owner and Controller in the GRC box and FireFighter Ids in the R/3 box.
Here in this case **Z_OWNER** is Owner with the role assignment SAP_GRAC_SUPER_USER_MGMT_OWNER.

Z_CNTLR is Controller with the role assignment SAP_GRAC_SUPER_USER_MGMT_CNTLR.

Z_FF_01 is the FireFighter with role assignment SAP_GRAC_SUPER_USER_MGMT_USER, SAP_GRC_FN_BASE, SAP_GRC_FN_BUSINESS_USER.

ZECC_F_ID_01 is the FireFighter Id which we have created in **R/3 Box.**

Refer below screenshots for the above mentioned users.



Display User

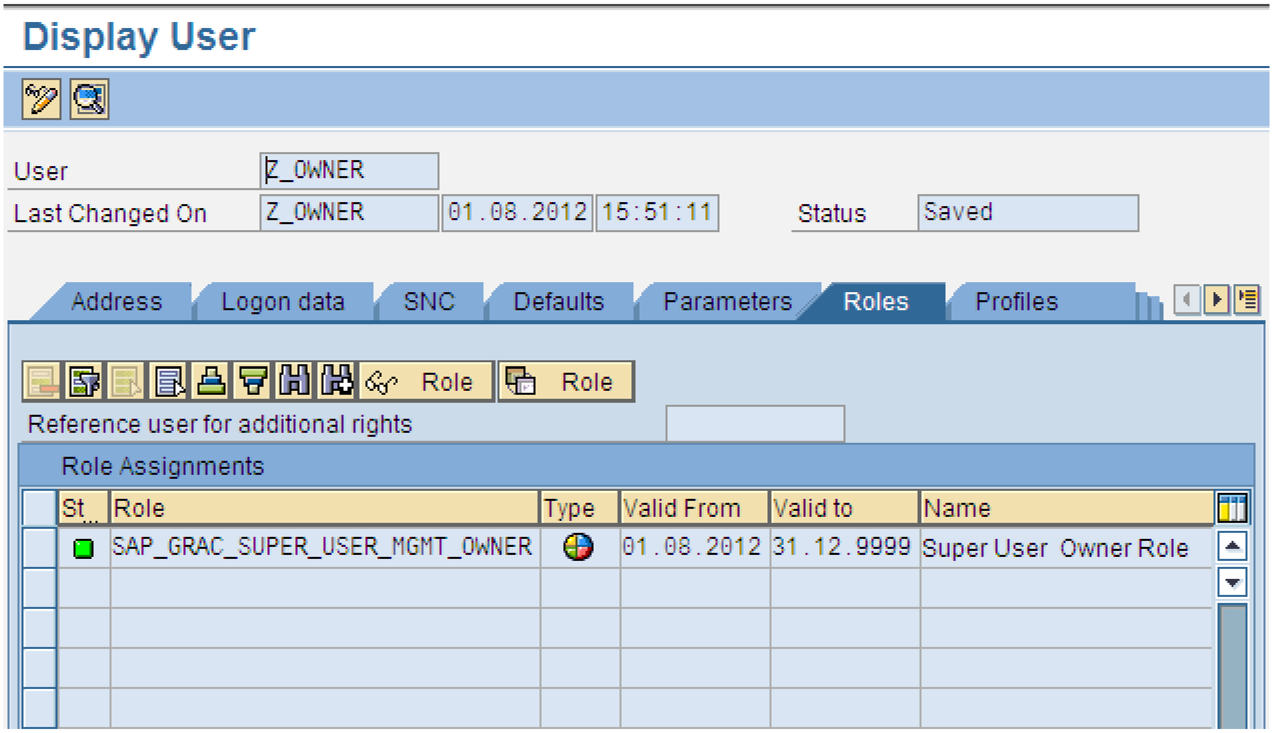
User Z_FF_01

Last Changed On Z_FF_01 01.08.2012 19:44:04 Status Saved

Reference user for additional rights

Role Assignments

St	Role	Type	Valid From	Valid to	Name
🟩	SAP_GRAC_SUPER_USER_MGMT_USER		01.08.2012	31.12.9999	Super User Firefighter
🟩	SAP_GRC_FN_BASE		01.08.2012	31.12.9999	GRC - Base role to run GR
🟩	SAP_GRC_FN_BUSINESS_USER		01.08.2012	31.12.9999	GRC - Business User



Display User

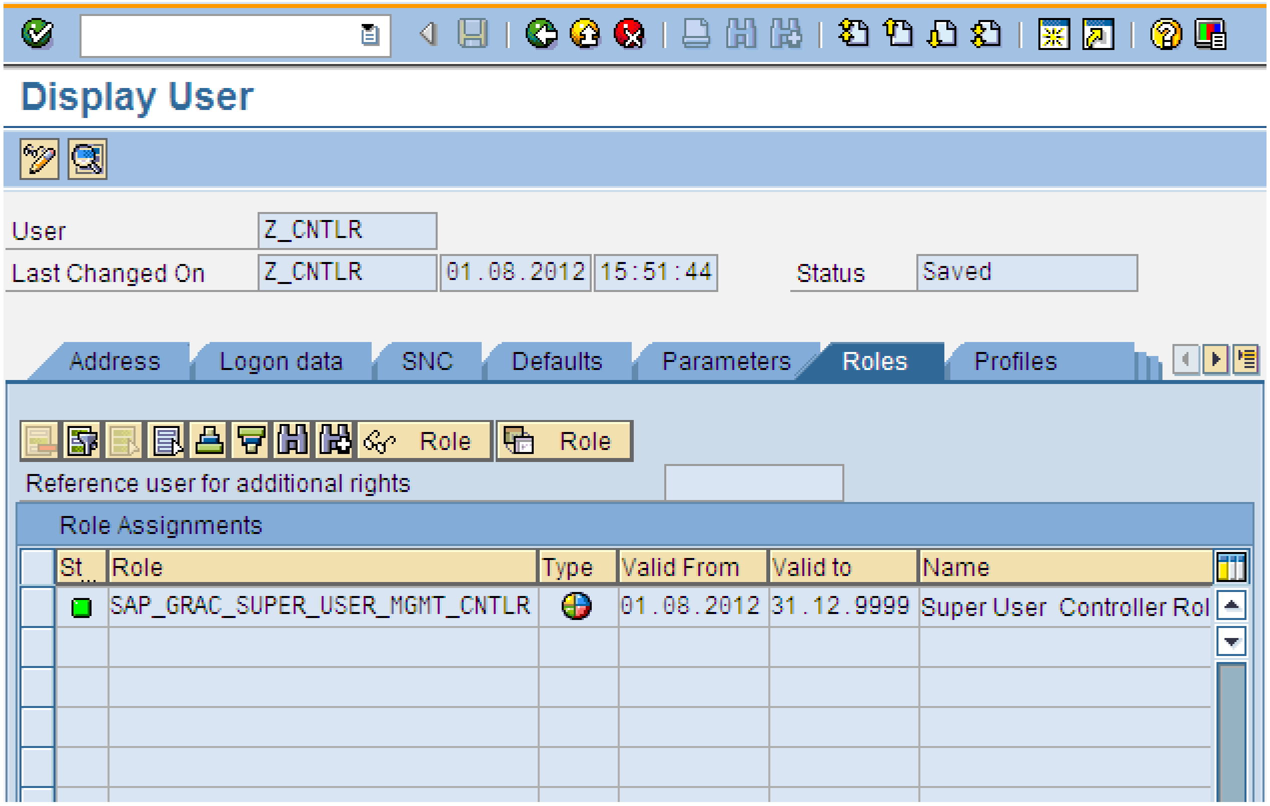
User Z_OWNER

Last Changed On Z_OWNER 01.08.2012 15:51:11 Status Saved

Reference user for additional rights

Role Assignments

St	Role	Type	Valid From	Valid to	Name
🟩	SAP_GRAC_SUPER_USER_MGMT_OWNER		01.08.2012	31.12.9999	Super User Owner Role



Display User

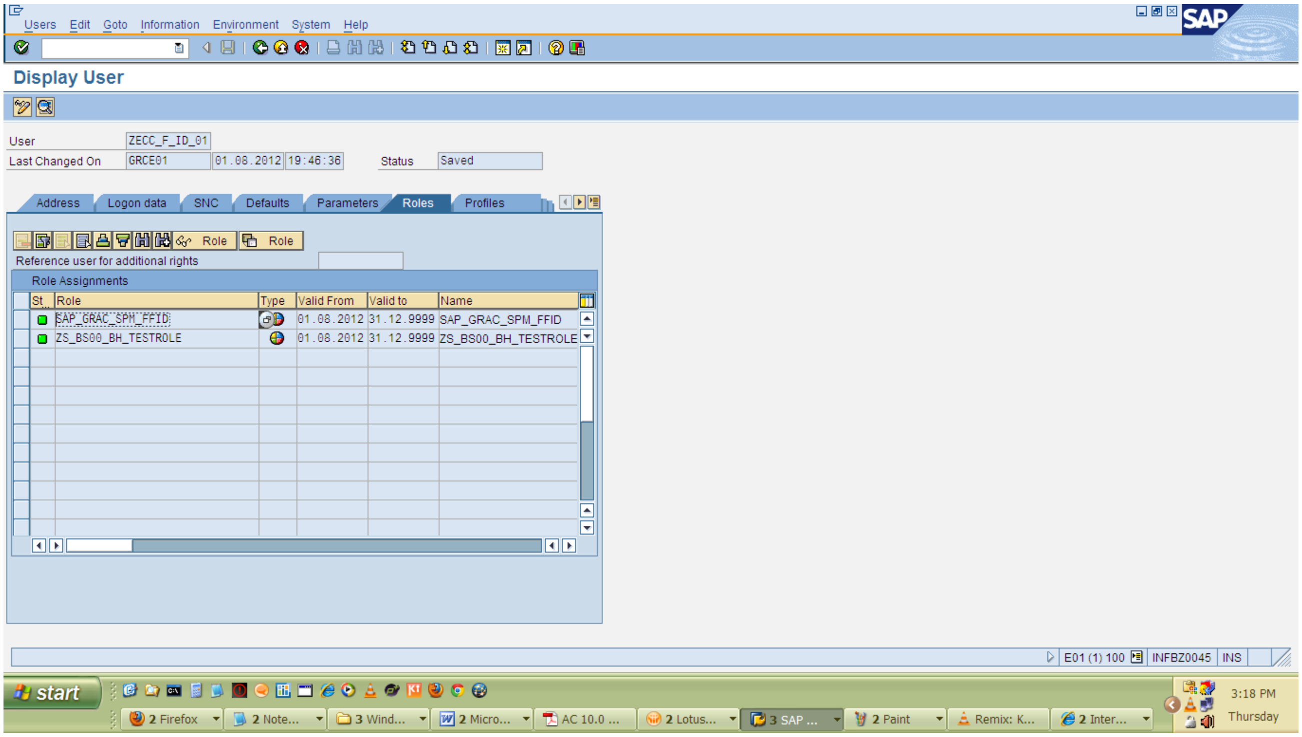
User Z_CNTLR

Last Changed On Z_CNTLR 01.08.2012 15:51:44 Status Saved

Reference user for additional rights

Role Assignments

St...	Role	Type	Valid From	Valid to	Name
🟩	SAP_GRAC_SUPER_USER_MGMT_CNTLR		01.08.2012	31.12.9999	Super User Controller Rol



Display User

User ZECC_F_ID_01

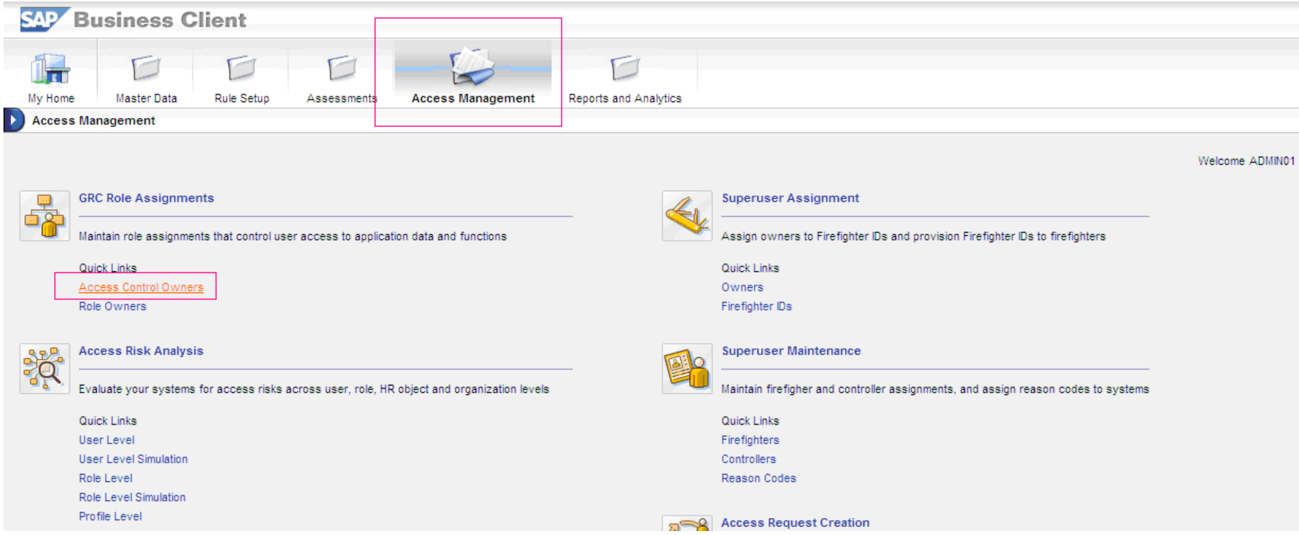
Last Changed On GRCE01 01.08.2012 19:46:36 Status Saved

Reference user for additional rights

Role Assignments

St...	Role	Type	Valid From	Valid to	Name
🟩	SAP_GRAC_SPM_FFID		01.08.2012	31.12.9999	SAP_GRAC_SPM_FFID
🟩	ZS_BS00_BH_TESTROLE		01.08.2012	31.12.9999	ZS_BS00_BH_TESTROLE

Execute t-code NWBC in GRC box and then click on SAP_GRC_NWBC. You will be redirected to the portal as below screen:



GRC Role Assignments

Maintain role assignments that control user access to application data and functions

Quick Links
Access Control Owners
Role Owners

Superuser Assignment

Assign owners to Firefighter IDs and provision Firefighter IDs to firefighters

Quick Links
Owners
Firefighter IDs

Access Risk Analysis

Evaluate your systems for access risks across user, role, HR object and organization levels

Quick Links
User Level
User Level Simulation
Role Level
Role Level Simulation
Profile Level

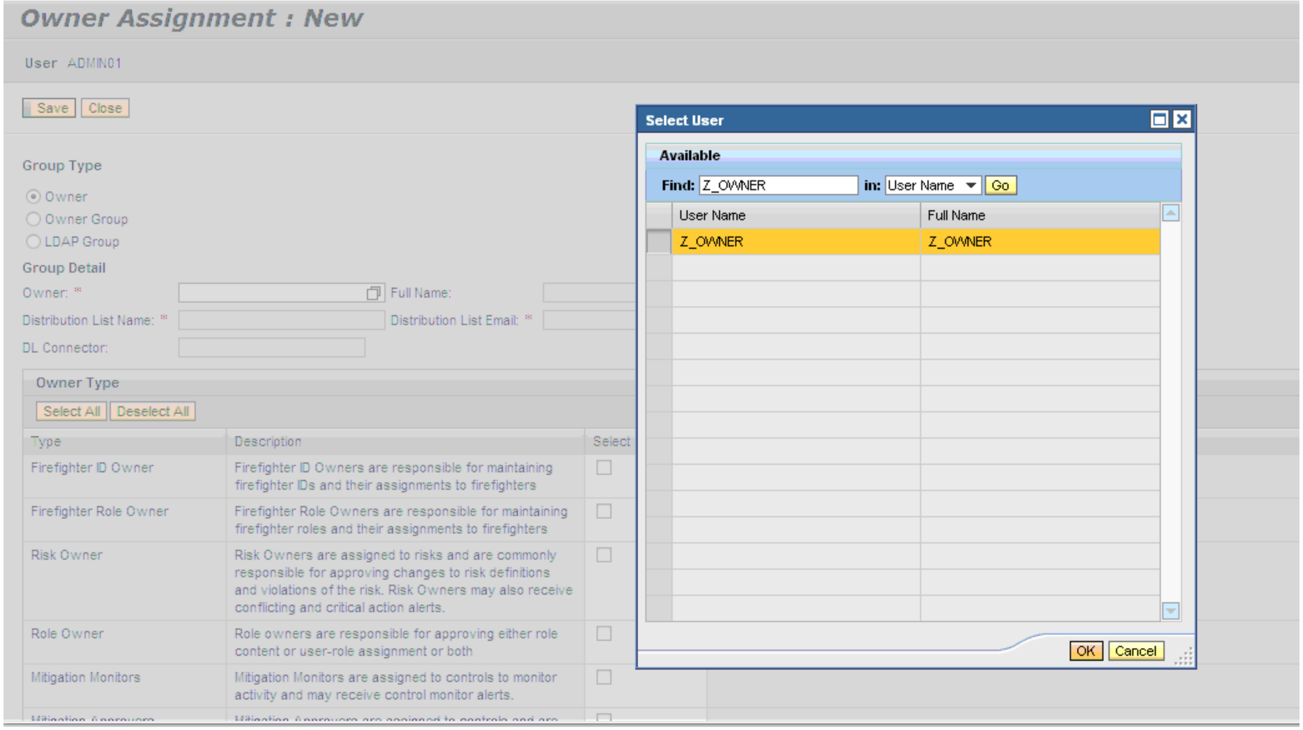
Superuser Maintenance

Maintain firefigher and controller assignments, and assign reason codes to systems

Quick Links
Firefighters
Controllers
Reason Codes

Access Request Creation

Now click over Access Management and select Access Control Owners. Click create for FireFighter Owner.



Owner Assignment : New

User ADMIN01

Group Type

● Owner
○ Owner Group
○ LDAP Group

Group Detail

Owner: *
Full Name:
Distribution List Name: *
Distribution List Email: *
DL Connector:

Owner Type

Type	Description	Select
Firefighter ID Owner	Firefighter ID Owners are responsible for maintaining firefighter IDs and their assignments to firefighters	□
Firefighter Role Owner	Firefighter Role Owners are responsible for maintaining firefighter roles and their assignments to firefighters	□
Risk Owner	Risk Owners are assigned to risks and are commonly responsible for approving changes to risk definitions and violations of the risk. Risk Owners may also receive conflicting and critical action alerts.	□
Role Owner	Role owners are responsible for approving either role content or user-role assignment or both	□
Mitigation Monitors	Mitigation Monitors are assigned to controls to monitor activity and may receive control monitor alerts.	□

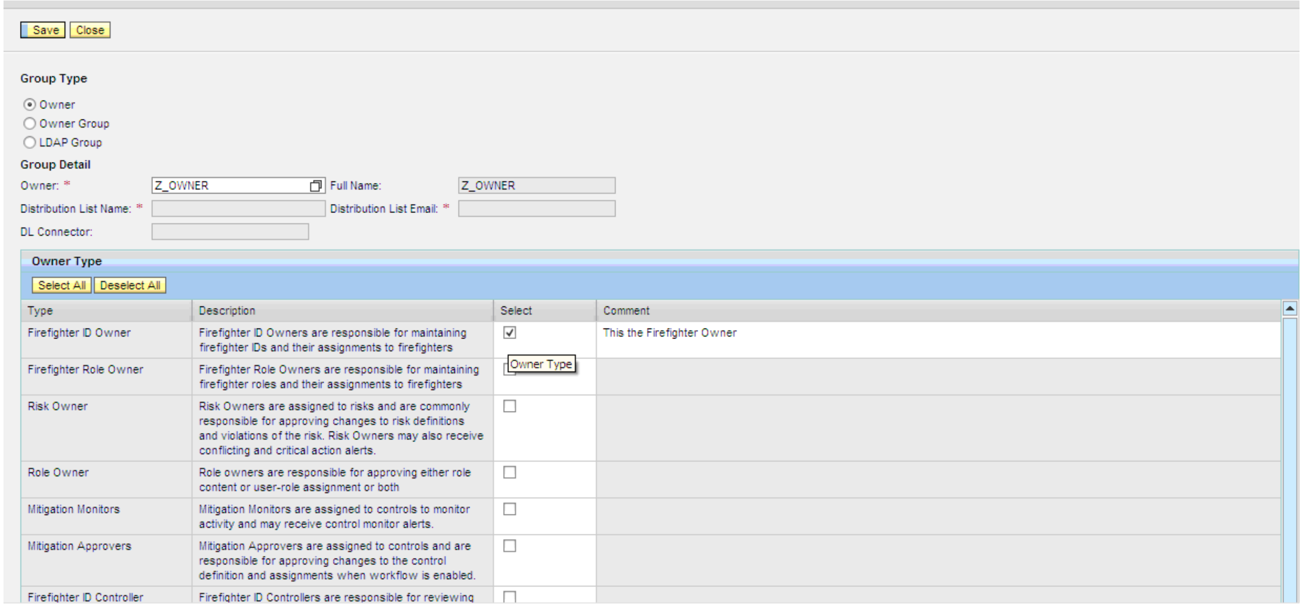
Select User

Available

Find: Z_OWNER in: User Name

User Name	Full Name
Z_OWNER	Z_OWNER

Select FF Owner which you have created in the GRC box and click on OK.



Group Type

● Owner
○ Owner Group
○ LDAP Group

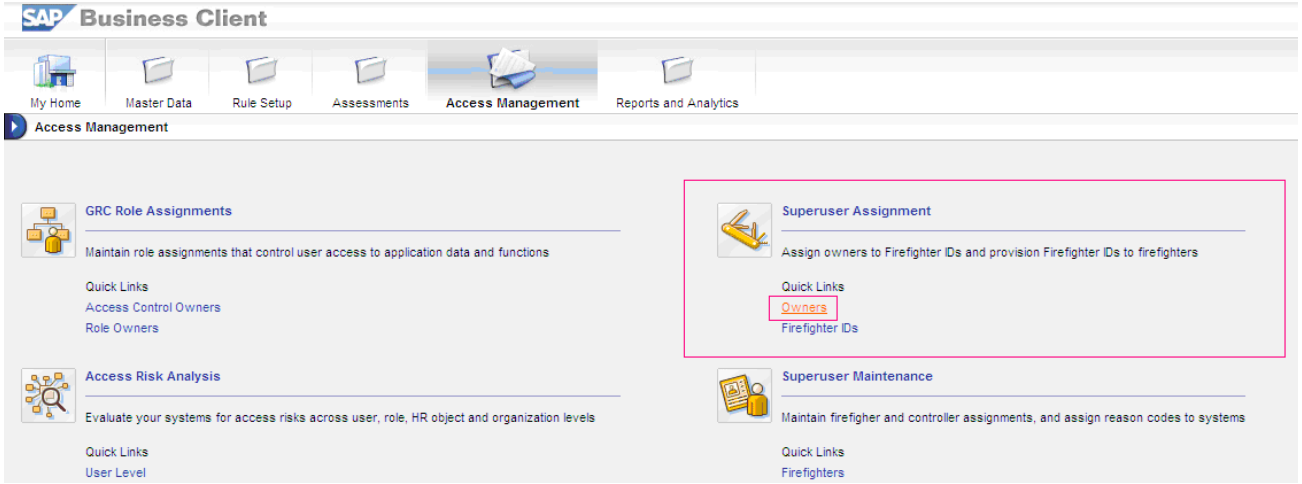
Group Detail

Owner: *	Z_OWNER	Full Name:	Z_OWNER
Distribution List Name: *		Distribution List Email: *	
DL Connector:			

Owner Type

Type	Description	Select	Comment
Firefighter ID Owner	Firefighter ID Owners are responsible for maintaining firefighter IDs and their assignments to firefighters	☑	This the Firefighter Owner
Firefighter Role Owner	Firefighter Role Owners are responsible for maintaining firefighter roles and their assignments to firefighters	□ Owner Type	
Risk Owner	Risk Owners are assigned to risks and are commonly responsible for approving changes to risk definitions and violations of the risk. Risk Owners may also receive conflicting and critical action alerts.	□	
Role Owner	Role owners are responsible for approving either role content or user-role assignment or both	□	
Mitigation Monitors	Mitigation Monitors are assigned to controls to monitor activity and may receive control monitor alerts.	□	
Mitigation Approvers	Mitigation Approvers are assigned to controls and are responsible for approving changes to the control definition and assignments when workflow is enabled.	□	
Firefighter ID Controller	Firefighter ID Controllers are responsible for reviewing	□	

Put your comments if any under FF Id Owner.
We then need to select the Owners under Super User Assignment.



GRC Role Assignments

Maintain role assignments that control user access to application data and functions

Quick Links
Access Control Owners
Role Owners

Superuser Assignment

Assign owners to Firefighter IDs and provision Firefighter IDs to firefighters

Quick Links
Owners
Firefighter IDs

Access Risk Analysis

Evaluate your systems for access risks across user, role, HR object and organization levels

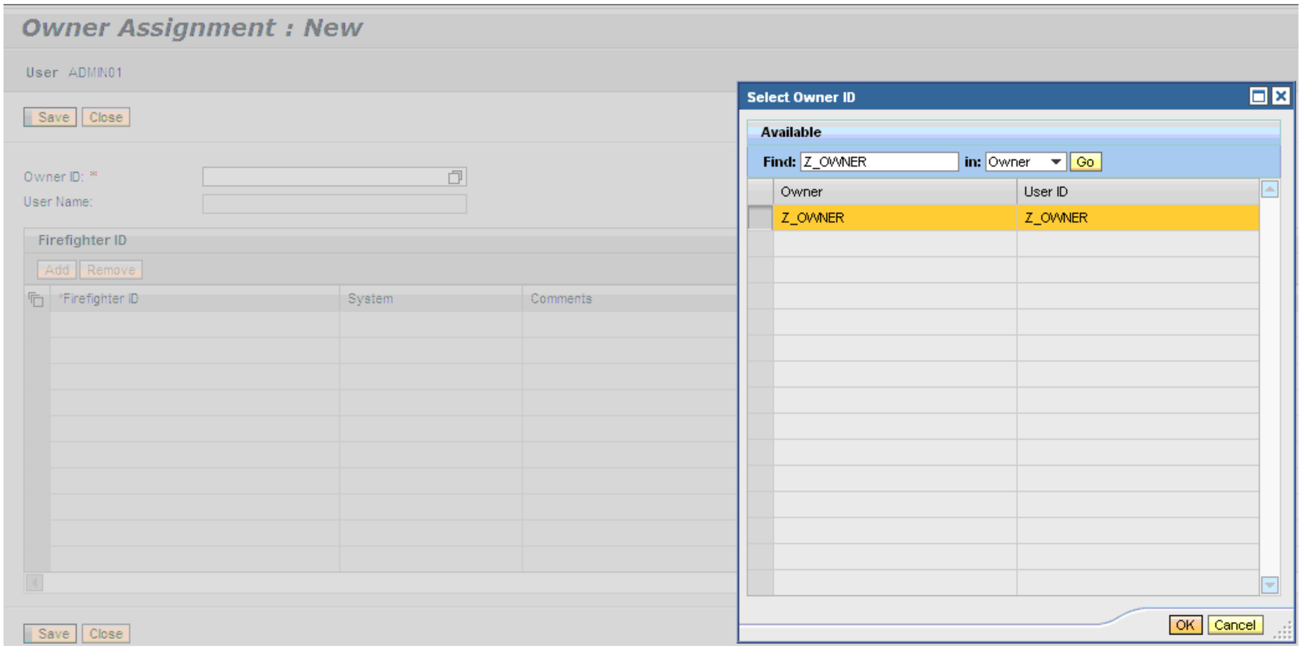
Quick Links
User Level

Superuser Maintenance

Maintain firefigher and controller assignments, and assign reason codes to systems

Quick Links
Firefighters

We then need to click on Assign in order to assign the Owner to the FF Id.
Select the Owner.



Owner Assignment : New

User ADMIN01

Owner ID: *

User Name:

Firefighter ID

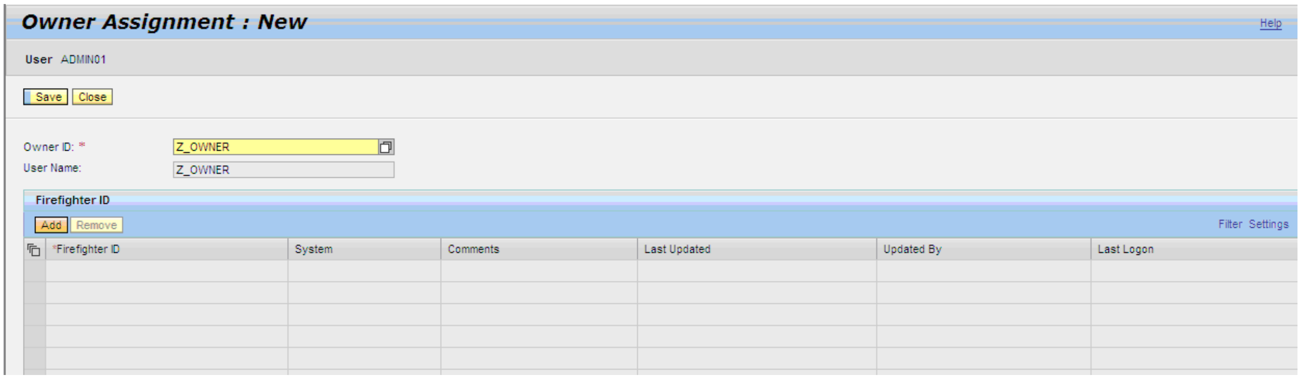
*Firefighter ID	System	Comments

Select Owner ID

Available

Find: Z_OWNER in: Owner

Owner	User ID
Z_OWNER	Z_OWNER



Owner Assignment : New

User ADMIN01

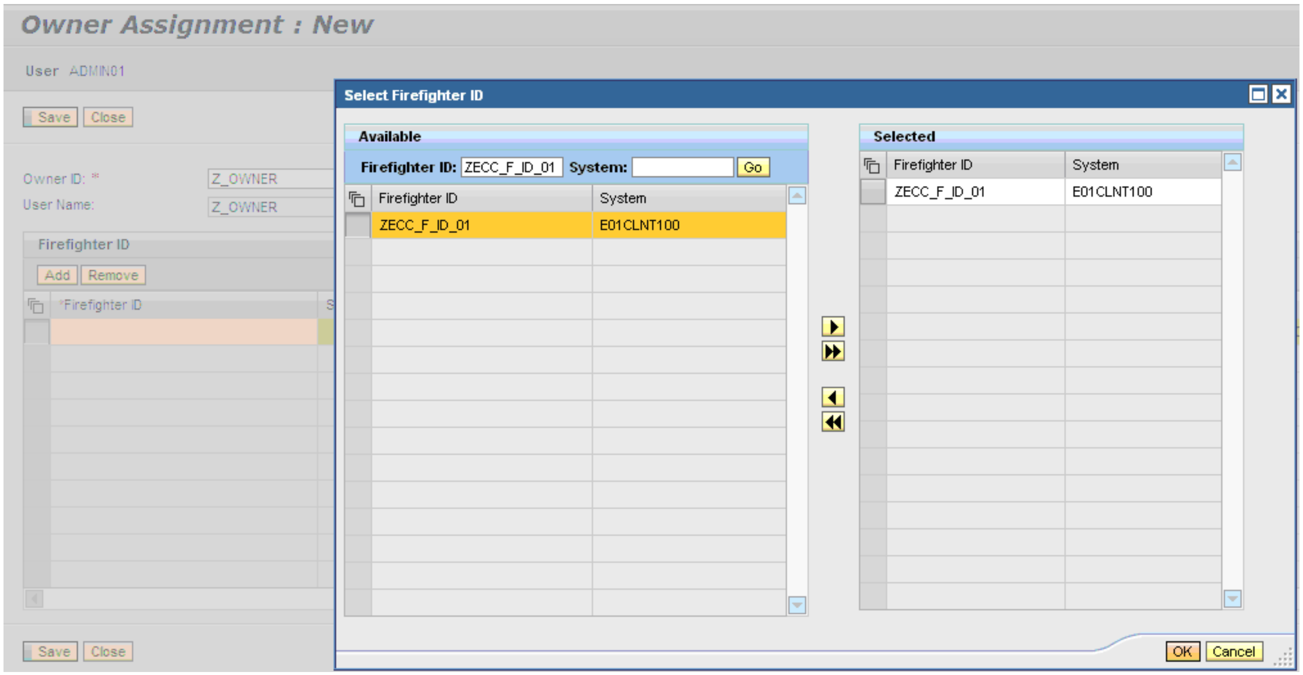
Owner ID: * Z_OWNER

User Name: Z_OWNER

Firefighter ID

*Firefighter ID	System	Comments	Last Updated	Updated By	Last Logon

Find the FF Id which we have created in the R/3 box.



Owner ID: * Z_OWNER

User Name: Z_OWNER

Firefighter ID: ZECC_F_ID_01 System:

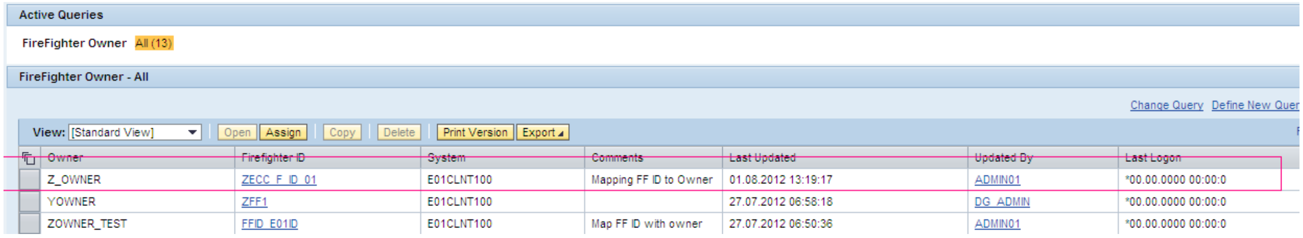
Available:

Firefighter ID	System
ZECC_F_ID_01	E01CLNT100

Selected:

Firefighter ID	System
ZECC_F_ID_01	E01CLNT100

Put your comments and save it.

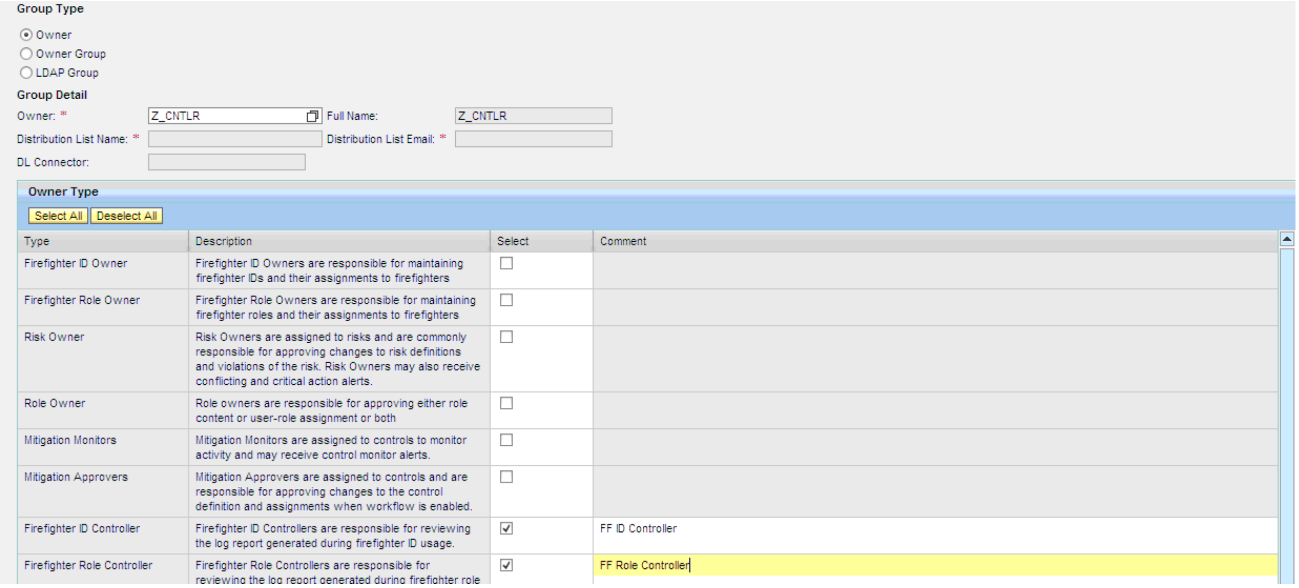


View: [Standard View]

Owner	Firefighter ID	System	Comments	Last Updated	Updated By	Last Logon
Z_OWNER	ZECC_F_ID_01	E01CLNT100	Mapping FF ID to Owner	01.08.2012 13:19:17	ADMIN01	*00.00.0000 00:00:0
YOWNER	ZFF1	E01CLNT100		27.07.2012 06:58:18	DG_ADMIN	*00.00.0000 00:00:0
ZOWNER_TEST	FFID_E01ID	E01CLNT100	Map FF ID with owner	27.07.2012 06:50:36	ADMIN01	*00.00.0000 00:00:0

For creating controllers, we need to follow the similar process as we did for OWNER.

Make sure to check the correct boxes for controllers as in below screenshot.



Group Type

● Owner
○ Owner Group
○ LDAP Group

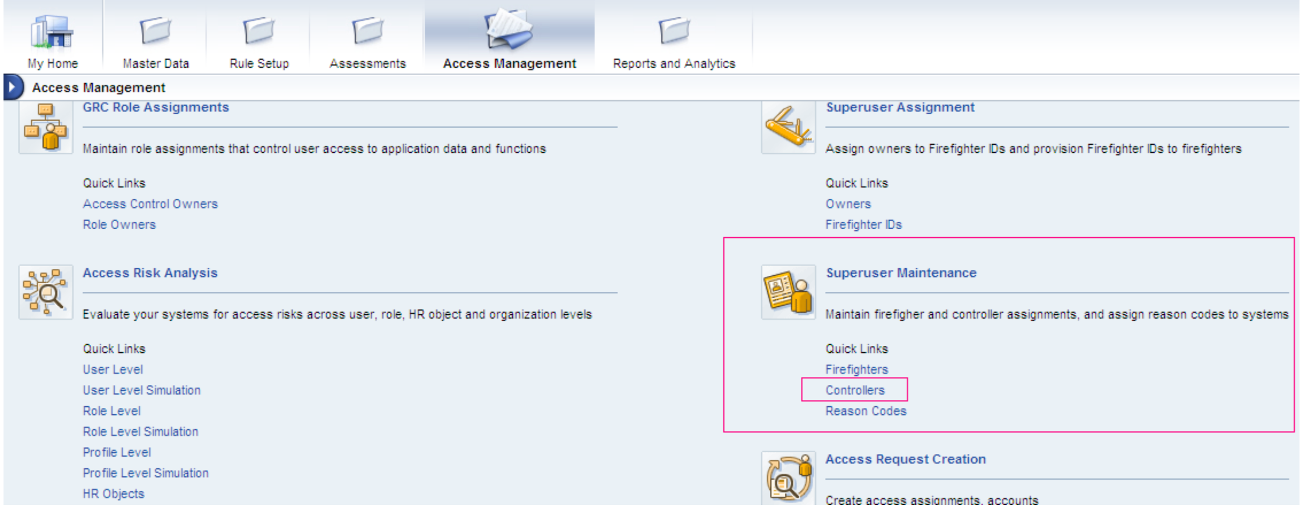
Group Detail

Owner: *	Z_CNTLR	Full Name:	Z_CNTLR
Distribution List Name: *		Distribution List Email: *	
DL Connector:			

Owner Type

Type	Description	Select	Comment
Firefighter ID Owner	Firefighter ID Owners are responsible for maintaining firefighter IDs and their assignments to firefighters	□	
Firefighter Role Owner	Firefighter Role Owners are responsible for maintaining firefighter roles and their assignments to firefighters	□	
Risk Owner	Risk Owners are assigned to risks and are commonly responsible for approving changes to risk definitions and violations of the risk. Risk Owners may also receive conflicting and critical action alerts.	□	
Role Owner	Role owners are responsible for approving either role content or user-role assignment or both	□	
Mitigation Monitors	Mitigation Monitors are assigned to controls to monitor activity and may receive control monitor alerts.	□	
Mitigation Approvers	Mitigation Approvers are assigned to controls and are responsible for approving changes to the control definition and assignments when workflow is enabled.	□	
Firefighter ID Controller	Firefighter ID Controllers are responsible for reviewing the log report generated during firefighter ID usage.	☑	FF ID Controller
Firefighter Role Controller	Firefighter Role Controllers are responsible for reviewing the log report generated during firefighter role	☑	FF Role Controller

Now for Controller Assignment, we need to click on Controllers as in below screenshot.



Access Management

GRC Role Assignments

Maintain role assignments that control user access to application data and functions

Quick Links
Access Control Owners
Role Owners

Access Risk Analysis

Evaluate your systems for access risks across user, role, HR object and organization levels

Quick Links
User Level
User Level Simulation
Role Level
Role Level Simulation
Profile Level
Profile Level Simulation
HR Objects

Superuser Assignment

Assign owners to Firefighter IDs and provision Firefighter IDs to firefighters

Quick Links
Owners
Firefighter IDs

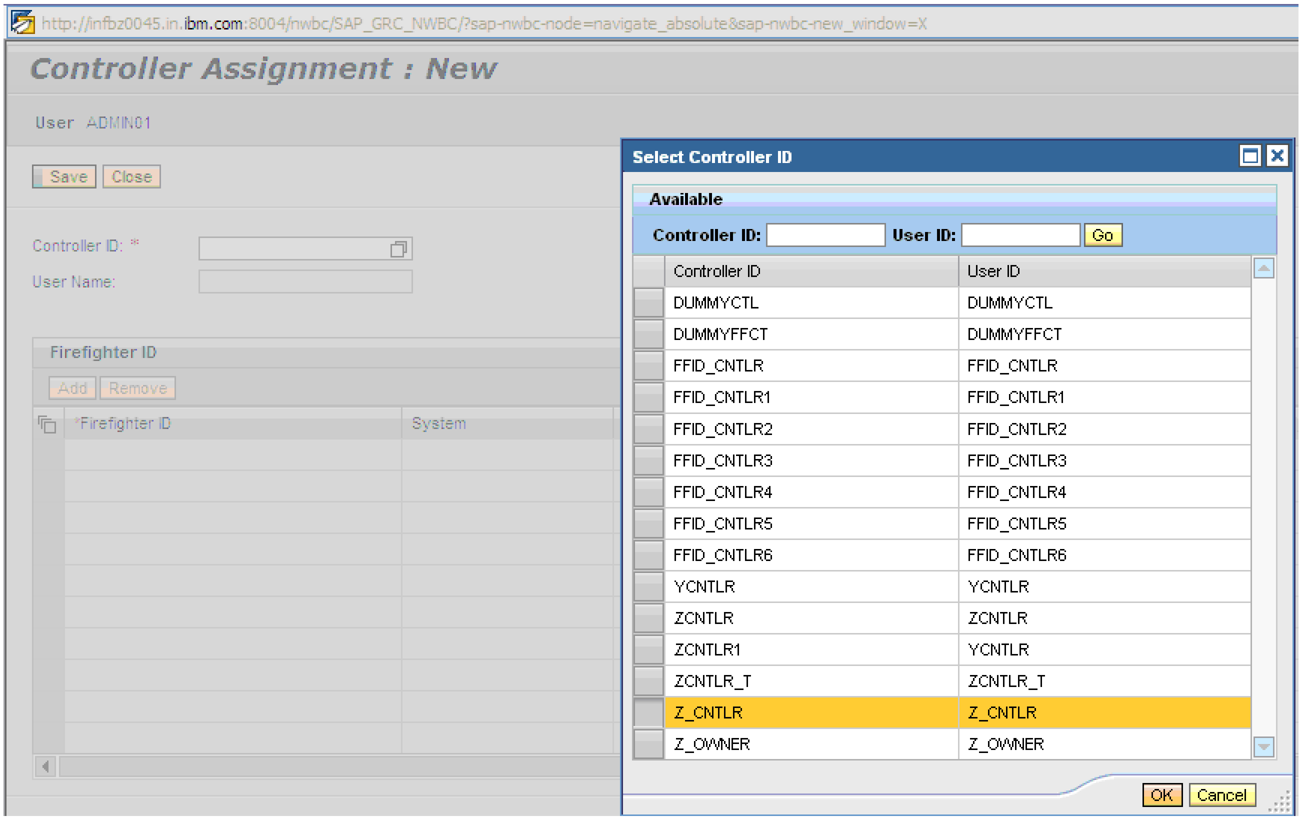
Superuser Maintenance

Maintain firefigher and controller assignments, and assign reason codes to systems

Quick Links
Firefighters
Controllers
Reason Codes

Access Request Creation

Create access assignments, accounts



http://infbz0045.in.ibm.com:8004/nwbc/SAP_GRC_NWBC/?sap-nwbc-node=navigate_absolute&sap-nwbc-new_window=X

Controller Assignment : New

User ADMIN01

Save | Close

Controller ID: *
User Name:

Firefighter ID

Add | Remove

*Firefighter ID	System

Select Controller ID

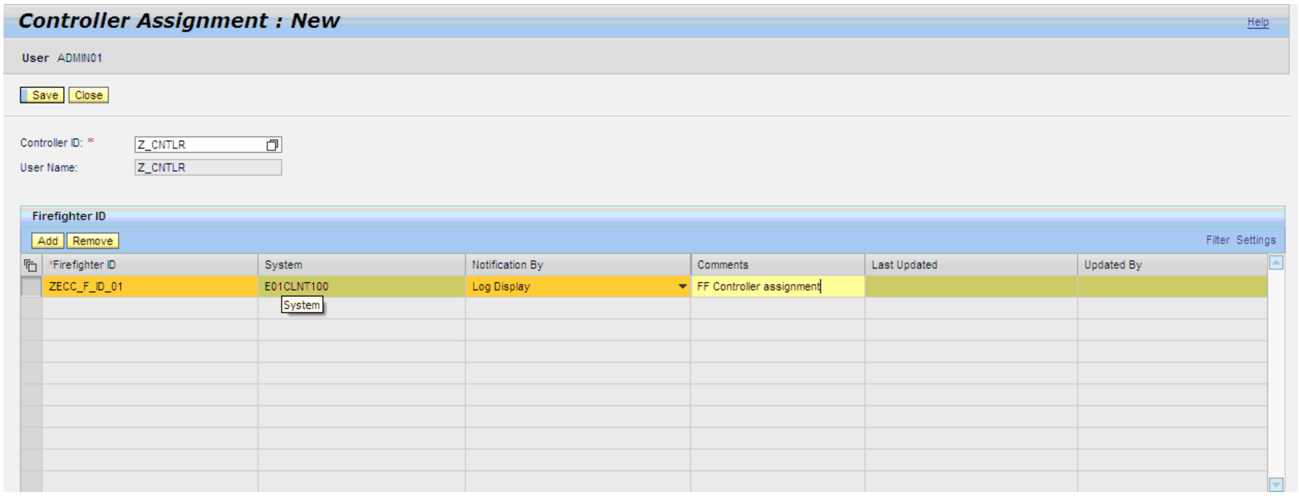
Available

Controller ID: ____ User ID: ____ Go

Controller ID	User ID
DUMMYCTL	DUMMYCTL
DUMMYFFCT	DUMMYFFCT
FFID_CNTLR	FFID_CNTLR
FFID_CNTLR1	FFID_CNTLR1
FFID_CNTLR2	FFID_CNTLR2
FFID_CNTLR3	FFID_CNTLR3
FFID_CNTLR4	FFID_CNTLR4
FFID_CNTLR5	FFID_CNTLR5
FFID_CNTLR6	FFID_CNTLR6
YCNTLR	YCNTLR
ZCNTLR	ZCNTLR
ZCNTLR1	YCNTLR
ZCNTLR_T	ZCNTLR_T
Z_CNTLR	Z_CNTLR
Z_OWNER	Z_OWNER

OK | Cancel

Add FireFighter to the controller



Controller Assignment : New Help

User ADMIN01

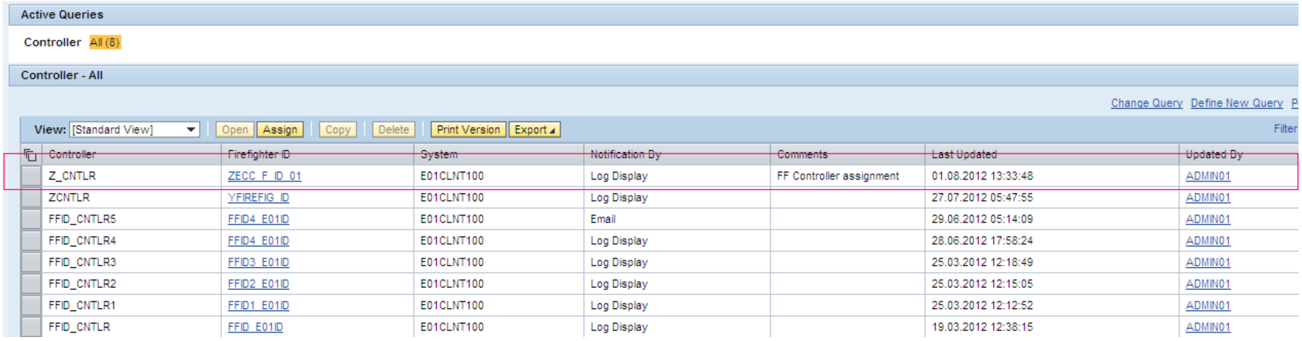
Save | Close

Controller ID: * Z_CNTLR
User Name: Z_CNTLR

Firefighter ID

Add | Remove | Filter Settings

*Firefighter ID	System	Notification By	Comments	Last Updated	Updated By
ZECC_F_ID_01	E01CLNT100	Log Display	FF Controller assignment		



Active Queries

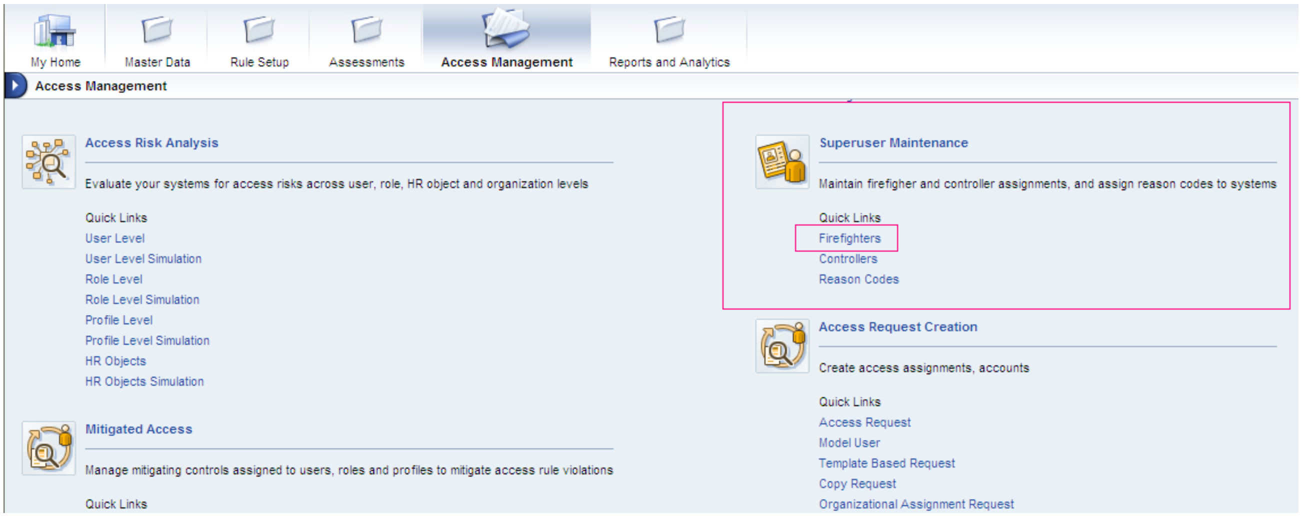
Controller All (8)

Controller - All

Controller	Firefighter ID	System	Notification By	Comments	Last Updated	Updated By
Z_CNTLR	ZECC_F_ID_01	E01CLNT100	Log Display	FF Controller assignment	01.08.2012 13:33:48	ADMIN01
ZCNTLR	YFIREFIG_ID	E01CLNT100	Log Display		27.07.2012 05:47:55	ADMIN01
FFID_CNTLR5	FFID4_E01ID	E01CLNT100	Email		29.06.2012 05:14:09	ADMIN01
FFID_CNTLR4	FFID4_E01ID	E01CLNT100	Log Display		28.06.2012 17:58:24	ADMIN01
FFID_CNTLR3	FFID3_E01ID	E01CLNT100	Log Display		25.03.2012 12:18:49	ADMIN01
FFID_CNTLR2	FFID2_E01ID	E01CLNT100	Log Display		25.03.2012 12:15:05	ADMIN01
FFID_CNTLR1	FFID1_E01ID	E01CLNT100	Log Display		25.03.2012 12:12:52	ADMIN01
FFID_CNTLR	FFID_E01ID	E01CLNT100	Log Display		19.03.2012 12:38:15	ADMIN01

As of now, we have assigned controllers to the FF Id.

Now for FireFighter mapping, we need to click on FireFighters under superuser maintenance.



Access Management

Access Risk Analysis

Evaluate your systems for access risks across user, role, HR object and organization levels

Quick Links
User Level
User Level Simulation
Role Level
Role Level Simulation
Profile Level
Profile Level Simulation
HR Objects
HR Objects Simulation

Mitigated Access

Manage mitigating controls assigned to users, roles and profiles to mitigate access rule violations

Quick Links

Superuser Maintenance

Maintain firefigher and controller assignments, and assign reason codes to systems

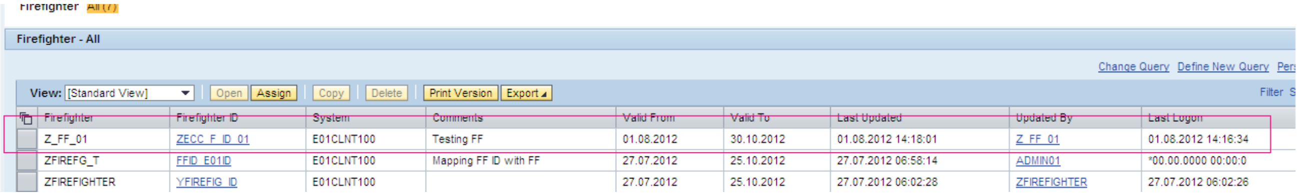
Quick Links
Firefighters
Controllers
Reason Codes

Access Request Creation

Create access assignments, accounts

Quick Links
Access Request
Model User
Template Based Request
Copy Request
Organizational Assignment Request

We then need to populate the FF Ids and map it with the Fire Fighter.



Firefighter All (7)

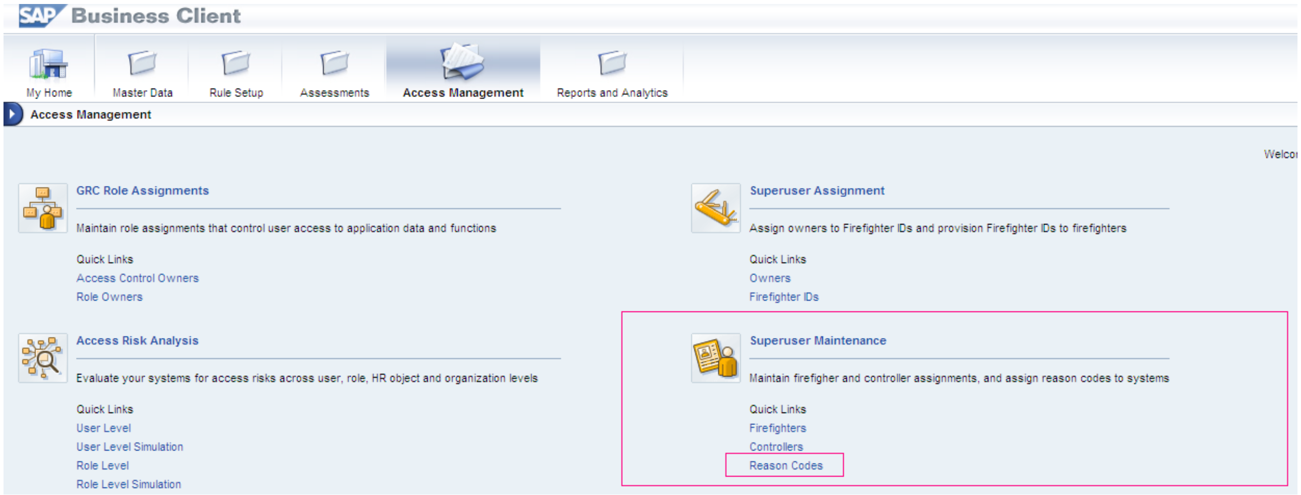
Firefighter - All

Firefighter	Firefighter ID	System	Comments	Valid From	Valid To	Last Updated	Updated By	Last Logon
Z_FF_01	ZECC_F_ID_01	E01CLNT100	Testing FF	01.08.2012	30.10.2012	01.08.2012 14:18:01	Z_FF_01	01.08.2012 14:16:34
ZFIREFG_T	FFID_E01ID	E01CLNT100	Mapping FF ID with FF	27.07.2012	25.10.2012	27.07.2012 06:58:14	ADMIN01	*00.00.0000 00:00:0
ZFIREFIGHTER	YFIREFIG_ID	E01CLNT100		27.07.2012	25.10.2012	27.07.2012 06:02:28	ZFIREFIGHTER	27.07.2012 06:02:26

FF Assignment has been completed now.

CREATE REASON CODES

Whenever a firefighter starts a firefighter session the reason code needs to be specified and maintained. A Reason Code can be created and assigned multiple remote systems. This reduces the amount of duplicated administration across systems.



GRC Role Assignments

Maintain role assignments that control user access to application data and functions

Quick Links
Access Control Owners
Role Owners

Access Risk Analysis

Evaluate your systems for access risks across user, role, HR object and organization levels

Quick Links
User Level
User Level Simulation
Role Level
Role Level Simulation

Superuser Assignment

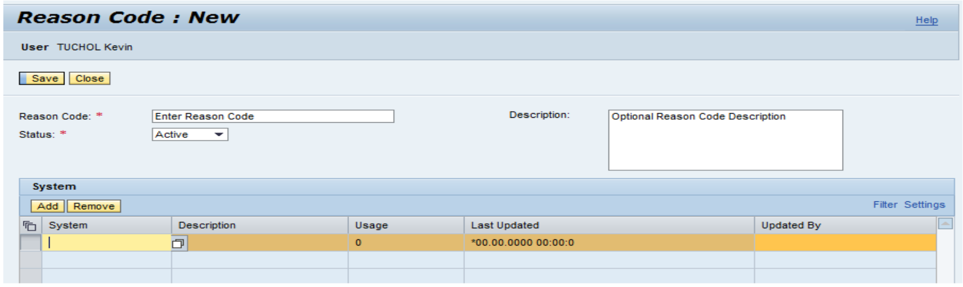
Assign owners to Firefighter IDs and provision Firefighter IDs to firefighters

Quick Links
Owners
Firefighter IDs

Superuser Maintenance

Maintain firefigher and controller assignments, and assign reason codes to systems

Quick Links
Firefighters
Controllers
Reason Codes



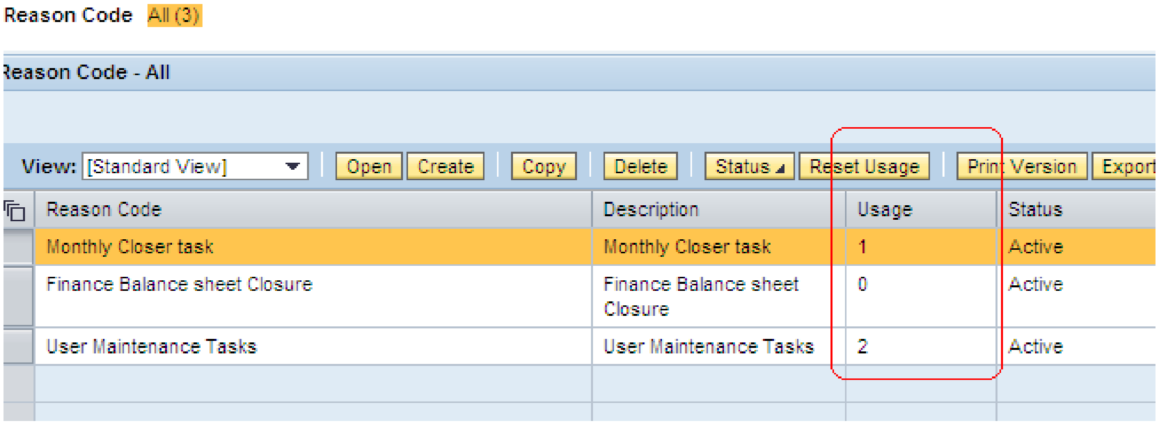
Reason Code : New

User TUCHOL Kevin

Reason Code: * Enter Reason Code
Status: * Active

Description: Optional Reason Code Description

System	Description	Usage	Last Updated	Updated By
		0	*00.00.0000 00:00:0	



Reason Code All (3)

Reason Code - All

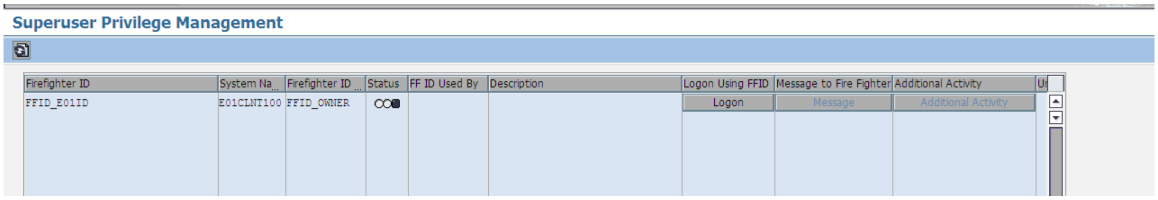
Reason Code	Description	Usage	Status
Monthly Closer task	Monthly Closer task	1	Active
Finance Balance sheet Closure	Finance Balance sheet Closure	0	Active
User Maintenance Tasks	User Maintenance Tasks	2	Active

Frequency of usage is tracked by reason code, by system. In the Reason Code list, you will see the total usage of the reason code across all systems to which it is assigned.

HOW TO ACCESS FIREFIGHTER ID

Logging into GRC box.

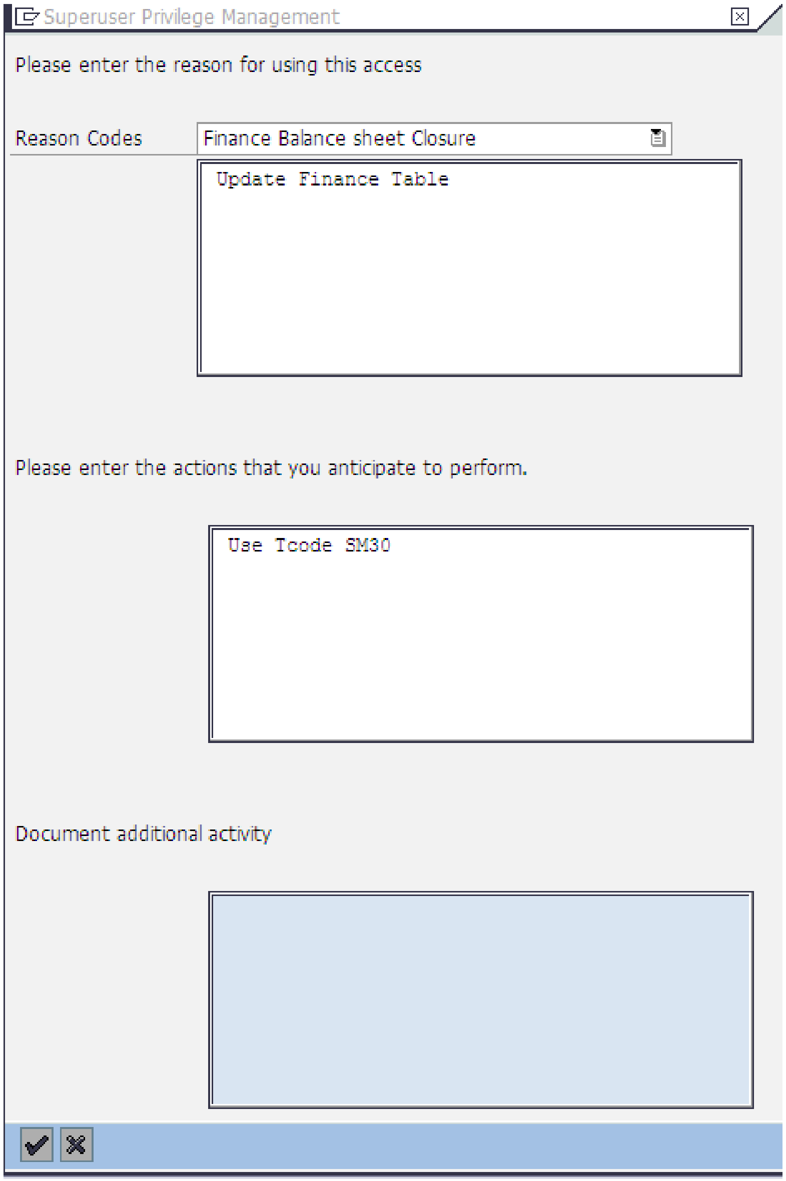
Use Tcode GRAC_SPM to login to SPM.



Superuser Privilege Management

Firefighter ID	System Na...	Firefighter ID ...	Status	FF ID Used By	Description	Logon Using FFID	Message to Fire Fighter	Additional Activity	Ur
FFID_E01ID	E01CLNT100	FFID_OWNER	○○■			Logon	Message	Additional Activity	

Maintain Reason Code



Superuser Privilege Management

Please enter the reason for using this access

Reason Codes: Finance Balance sheet Closure

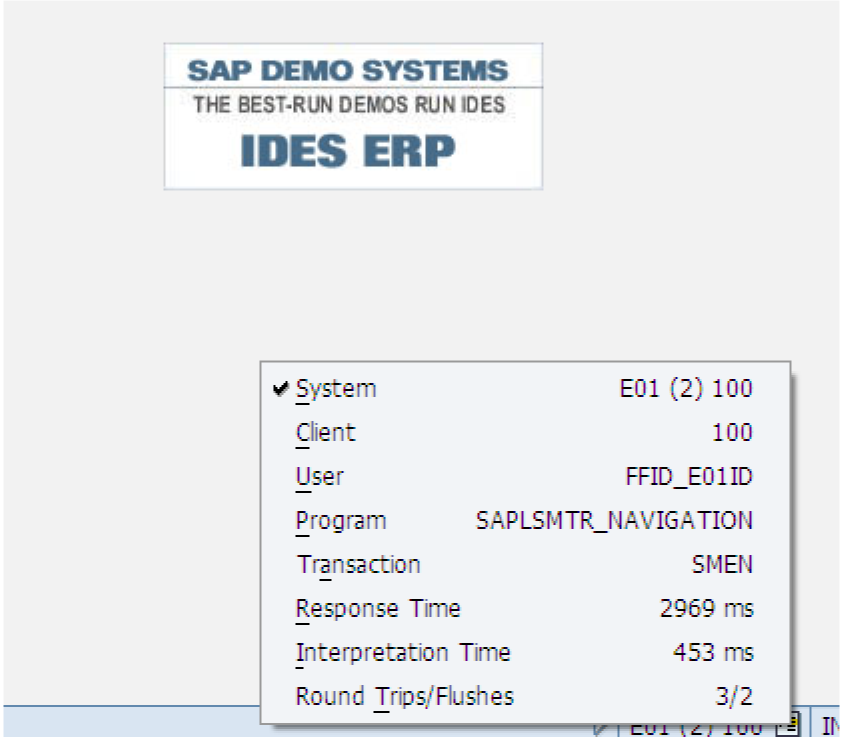
```
Update Finance Table
```

Please enter the actions that you anticipate to perform.

```
Use Tcode SM30
```

Document additional activity

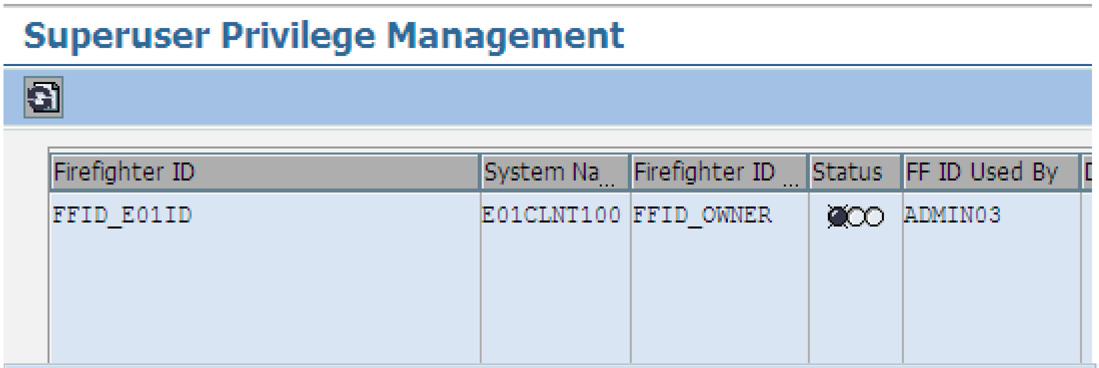
It will take you to R/3 system with FFID logon



SAP DEMO SYSTEMS
THE BEST-RUN DEMOS RUN IDES
IDES ERP

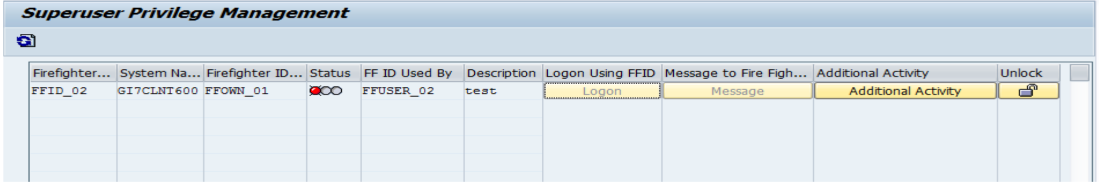
✓ System	E01 (2) 100
Client	100
User	FFID_E01ID
Program	SAPLSMTR_NAVIGATION
Transaction	SMEN
Response Time	2969 ms
Interpretation Time	453 ms
Round Trips/Flushes	3/2

Moreover the status will change to Red.



Superuser Privilege Management

Firefighter ID	System Na...	Firefighter ID ...	Status	FF ID Used By
FFID_E01ID	E01CLNT100	FFID_OWNER	●○○	ADMIN03



Superuser Privilege Management

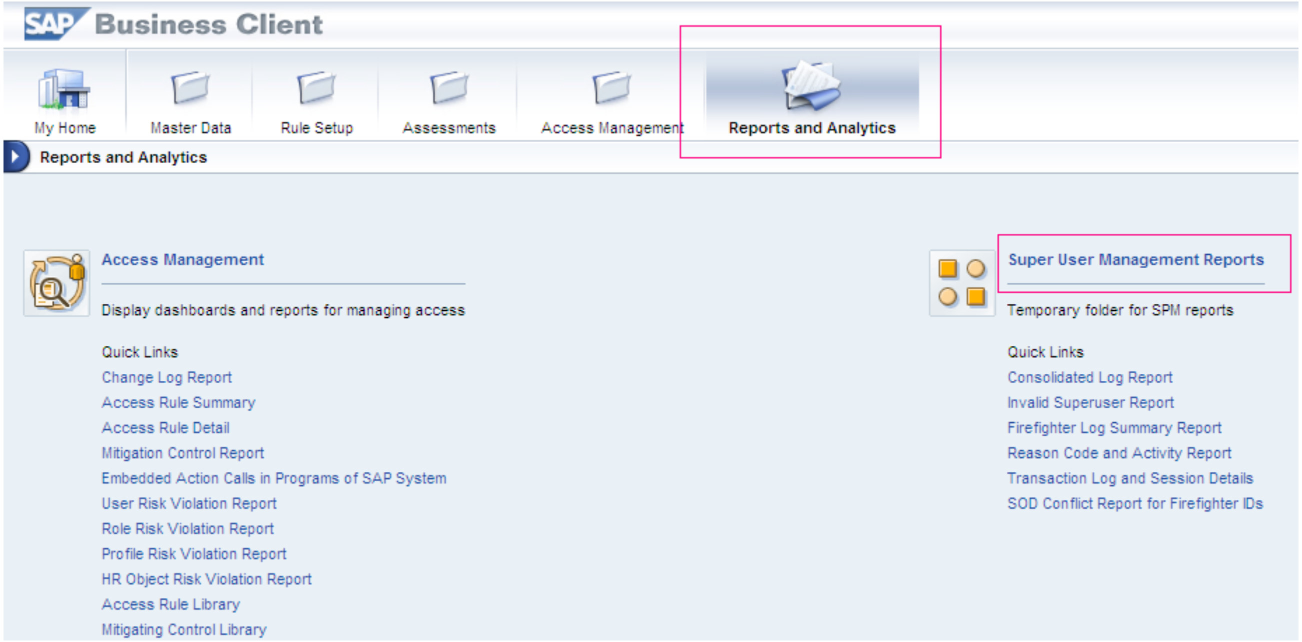
Firefighter...	System Na...	Firefighter ID...	Status	FF ID Used By	Description	Logon Using FFID	Message to Fire Figh...	Additional Activity	Unlock
FFID_02	GI7CLNT600	FFOWN_01	●○○	FFUSER_02	test	Logon	Message	Additional Activity	🔓

While a firefighter session is open the status of the firefighter ID will turn to red
A firefighter can click Additional Activity any time to enter more information.

If a firefighter ID is in use by another firefighter, then notification can be sent to the other firefighter by clicking Message.
Unlock can be used to unlock the firefighter ID in the event it is locked.

REPORTING

The reports can be accessed using the NWBC or the Portal and are located under
Reports and Analytics →Superuser Management Reports


SAP Business Client
My Home
Master Data
Rule Setup
Assessments
Access Management
Reports and Analytics
Reports and Analytics
Access Management
Quick Links
Change Log Report
Access Rule Summary
Access Rule Detail
Mitigation Control Report
Embedded Action Calls in Programs of SAP System
User Risk Violation Report
Role Risk Violation Report
Profile Risk Violation Report
HR Object Risk Violation Report
Access Rule Library
Mitigating Control Library
Super User Management Reports
Quick Links
Consolidated Log Report
Invalid Superuser Report
Firefighter Log Summary Report
Reason Code and Activity Report
Transaction Log and Session Details
SOD Conflict Report for Firefighter IDs

Display dashboards and reports for managing access

Temporary folder for SPM reports

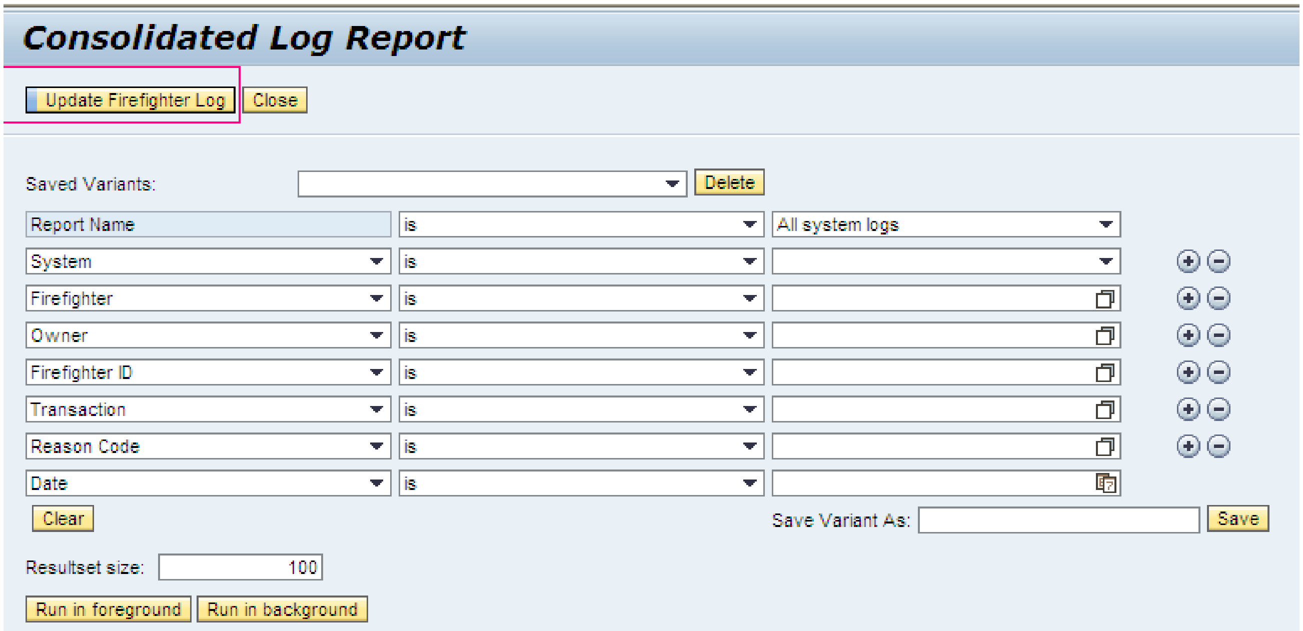
Consolidated Log Report: This report provides information based on the following logs from the remote system.

Transaction Log: Captures transaction execution from transaction STAD
Change Log: Captures change log from change document objects (tables CDPOS and CDHDR)
System Log: Captures Debug & Replace information from transaction SM21.
Security Audit Log: Captures Security Audit Log from transaction SM20
OS Command Log: Captures changes to OS commands from transaction SM49.
Invalid Superuser Report: This Report gives the details of all the users (firefighter, controller, owner, firefighter ID) who are Expired, Locked or Deleted. In the case of Role Based Firefighter, it gives the details of whether the role has been generated or not.
Firefighter Log Summary: Provides details of the session the firefighter logged into the remote system using the FFID for the ID based FF Application.
Reason Code and Activity Report: This Report provides the details of information of Reason and Activity used by the firefighter.

SOD Conflict Report for Firefighter ID: When the firefighter logs in to the remote system using the FFID in to the remote system and performs certain transactions which violates access risk rules.

Log Collection Overview: The details of the transaction executed by the firefighter lies in the remote system in the CDHDR, CDPOS, STAD, SM19, SM49, and debug & replace information. The data from the remote system can be fetched using the Log Collector which can be executed as a foreground or background job.

Foreground Job: The foreground Job for Log Collection can be executed from the Update firefighter log button which can be found in the Consolidated Log Report



Consolidated Log Report

Update Firefighter Log | Close

Saved Variants: | Delete

Report Name	is	All system logs
System	is	
Firefighter	is	
Owner	is	
Firefighter ID	is	
Transaction	is	
Reason Code	is	
Date	is	

Clear | Save Variant As: | Save

Resultset size: 100

Run in foreground | Run in background

Background Job: The Background Job for log collection can be scheduled from SM36which can be scheduled on a periodic basis. The status of the background job can be checked from the SM37 transaction.

The program name for the background job is: **GRAC_SPM_LOG_SYNC_UPDATE**

Consolidated Log Report Transaction Log: The consolidated log report allows filtering criteria like System, Firefighter, FFID, Reason Code, Transaction, Date or Owner.

System Log: The System Log can also be found in the consolidated Log Report by choosing the Report type as System Log.

Audit Log: The Audit Log is also contained in the consolidated Log Report as Report type as Audit Log. This audit function will show the details of the user(s) subject to auditing.
The user(s) to be audited are configured/selected in transaction SM19.

OS Command Log: An OS Command Log can be retrieved from the consolidated Log Report by selecting the Report type as OS Command.
This logs tracks the changes which the user makes in SM49 for OS Command.

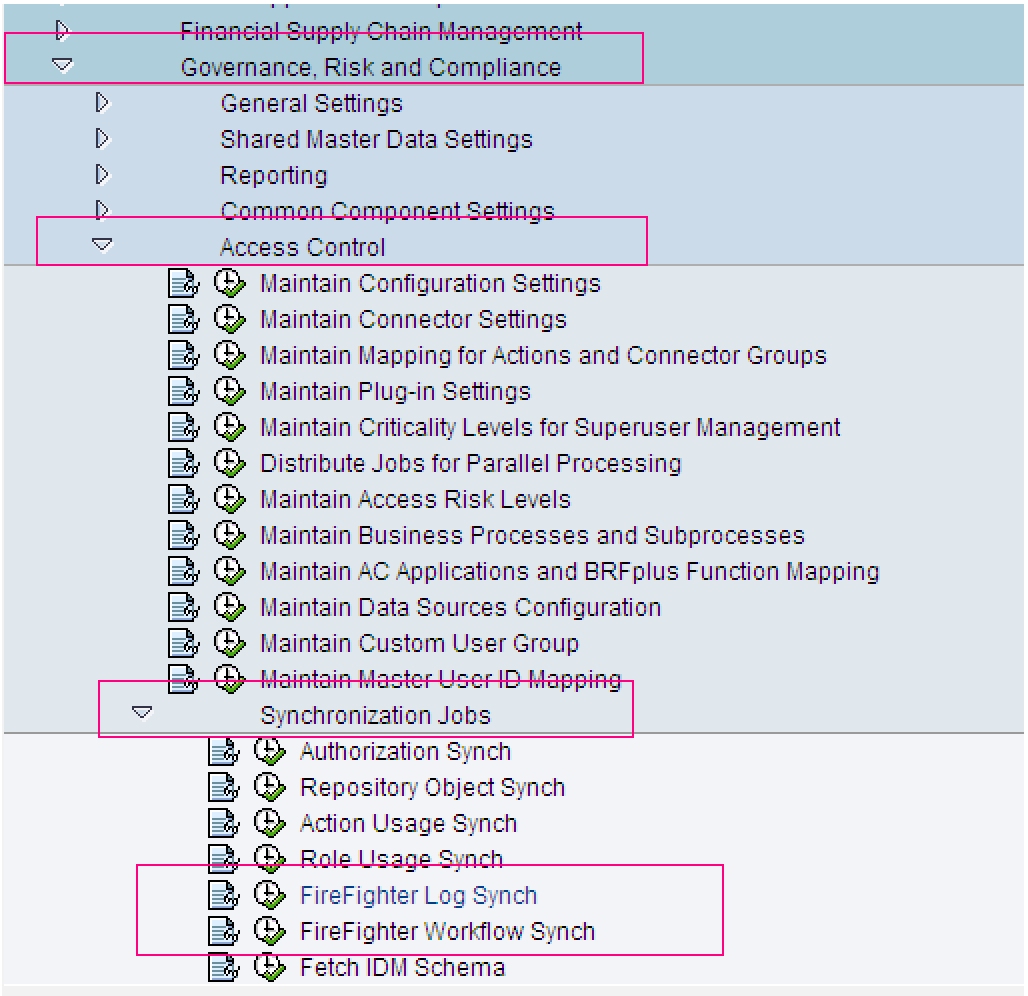
Invalid SuperuserReport: The Invalid Superuser Log is launched by the according link from the Super User Management Reports area.
This Log is used to analyze the users who are expired, locked or deleted.

FireFighter Log Synch:
In this Customizing activity, you can get the logs of firefighter activities from the back-end system and store them in the GRAC repository. The synchronization gets data for firefighter activities from the time the activity was last executed to the current time.
The activity performs the log synchronization in the background and does not display any screens. The cursor spins to indicate the application is performing the task. Once the cursor stops spinning, the task is done.
The following tables are updated:

GRACAUDITLOG
GRACCHANGELOG
GRACOSCMDLOG
GRACSYSTEMLOG
GRACFFLOG

This log is only updated during FireFighter Log synch if you have maintained the Send Log Report Execution Notification Immediately parameter as Yes, or else it is updated during Firefighter Workflow Synch. You maintain this in the Customizing activity Maintain Configuration Settings, parameter ID 4007.

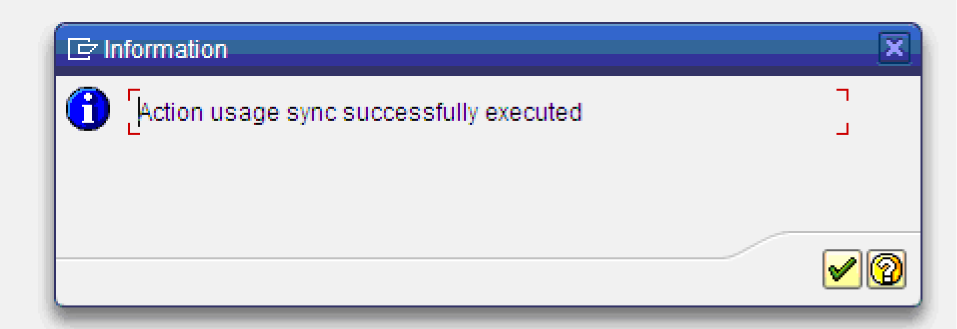
GRACROLEFFLOG
This log is updated for role based applications. You can set whether an application is Role or User based in the Customizing activity. This log is updated for role based applications. You can set whether an application is Role or User based by using the Customizing activity Maintain Configuration Settings, parameter ID 4000 - Application Type.



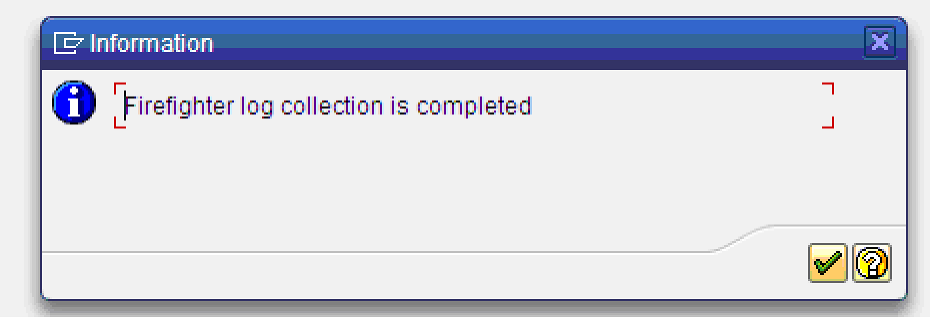
- Financial Supply Chain Management
- Governance, Risk and Compliance
  - General Settings
  - Shared Master Data Settings
  - Reporting
  - Common Component Settings
  - Access Control
    - Maintain Configuration Settings
    - Maintain Connector Settings
    - Maintain Mapping for Actions and Connector Groups
    - Maintain Plug-in Settings
    - Maintain Criticality Levels for Superuser Management
    - Distribute Jobs for Parallel Processing
    - Maintain Access Risk Levels
    - Maintain Business Processes and Subprocesses
    - Maintain AC Applications and BRFplus Function Mapping
    - Maintain Data Sources Configuration
    - Maintain Custom User Group
    - Maintain Master User ID Mapping
    - Synchronization Jobs
      - Authorization Synch
      - Repository Object Synch
      - Action Usage Synch
      - Role Usage Synch
      - FireFighter Log Synch
      - FireFighter Workflow Synch
      - Fetch IDM Schema

FireFighter Workflow Synch:

In this Customizing activity, you can generate requests for the FFID log and send the workflow to controller. The activity updates the GRACFFLOG and GRACROLEFFLOG tables , triggers the firefighter workflow, and creates firefighter work items.



Action usage sync successfully executed

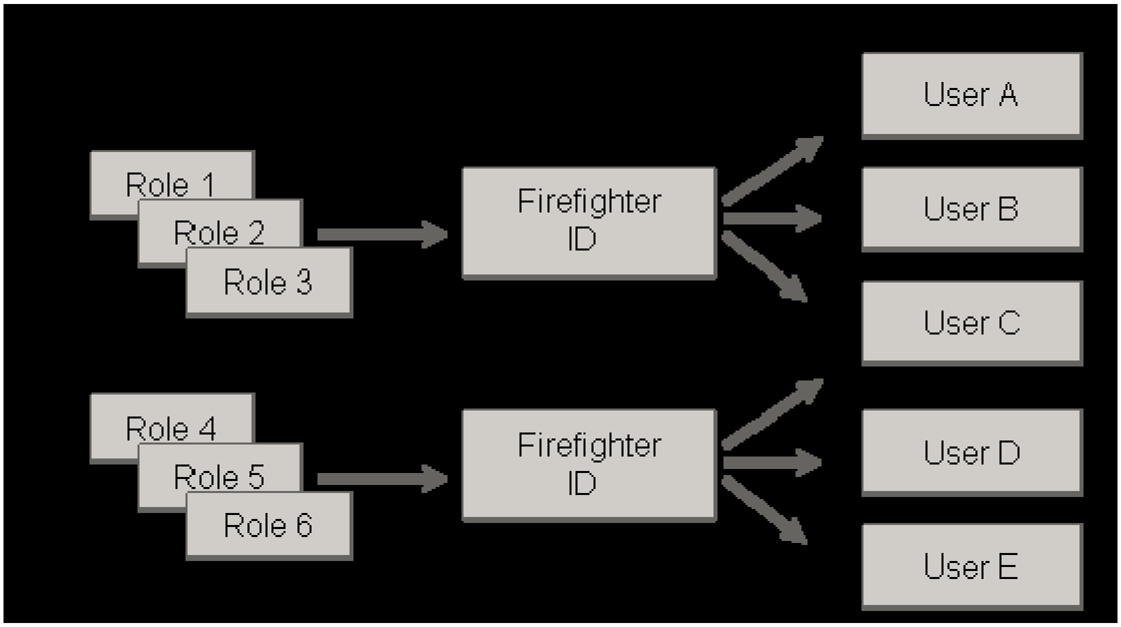


Firefighter log collection is completed

FIREFIGHTER APPLICATION TYPES

ID Based Firefighter:

The firefighterID created in the remote system will be assigned to the user in the GRC system, either manually or via an access request. The firefighter accesses their assigned firefighterID in the GRC server using the SAP GUI and transaction GRAC_SPM. The firefighterID for all remote systems assigned to the firefighter will be accessed from this transaction.



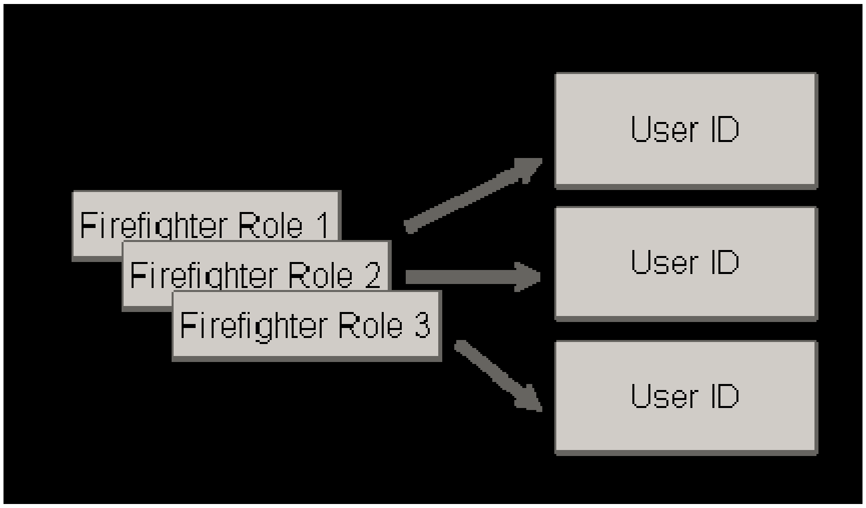
In this scenario:
Each Firefighter ID has its own User Master Record with roles assigned to it.
An SAP End-user (Firefighter) executes a transaction code (/n/virsa/vfat in AC 5.3) and checks out an ID. Multiple users can check-out each Firefighter ID but only one user can have it checked out at any time.
A reason and the expected activity must be documented prior to gaining firefighter access.

Relevant changes in SAP are captured in the change history under the Firefighter ID, not the user's normal ID.

ID-Based Firefighter usage is available in all versions of Superuser Privilege Management (formerly Firefighter). It is used widely by customers for granting emergency and elevated access.

Role Based Firefighter:

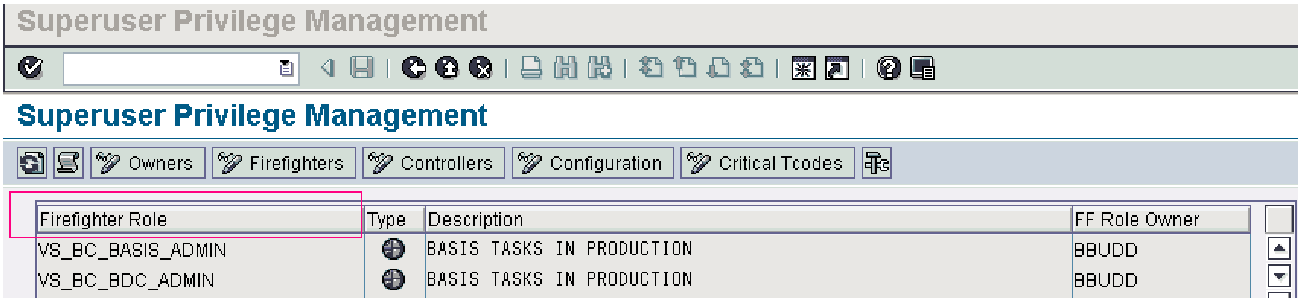
The firefighter roles created in the remote system will be assigned to the user in the GRC server. The firefighter directly logs into the remote system using their user ID and performs activities which are provided in the user's role and firefighter role assigned to the user.



In this scenario:
Each Firefighter Role is assigned through Superuser Privilege Management to an SAP end-user.
End-users do not check out a separate ID.
Transaction and change history is logged with the user's own ID.
The end-user is not aware when they are utilizing emergency / firefighter access.

Firefighter role-based usage:
It is available in versions 5.2 and above of Superuser Privilege Management (formerly Firefighter)
Was created for customers that did not want users to have access with two IDs.

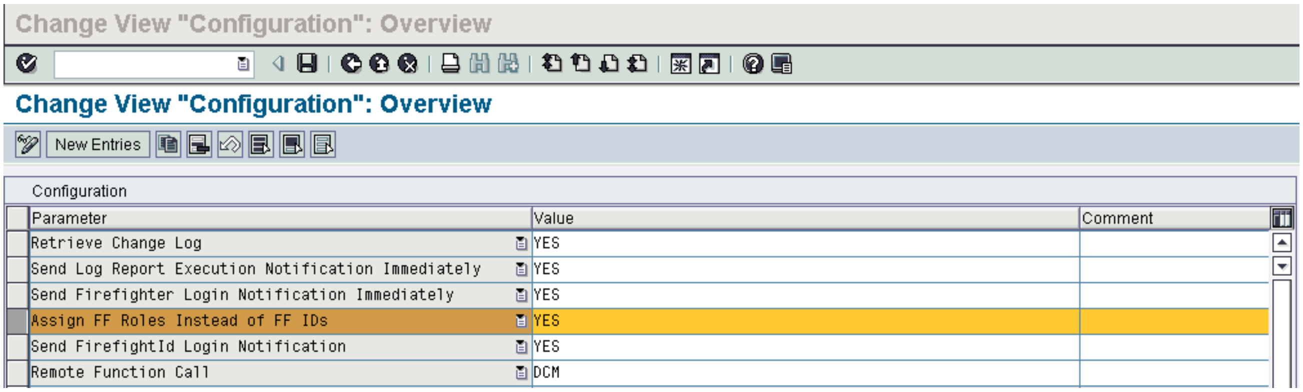
When role-based firefighter is chosen, the Superuser Privilege Management screen will display the following configuration:



Superuser Privilege Management

Firefighter Role	Type	Description	FF Role Owner
VS_BC_BASIS_ADMIN	●	BASIS TASKS IN PRODUCTION	BBUDD
VS_BC_BDC_ADMIN	●	BASIS TASKS IN PRODUCTION	BBUDD

In order for this configuration to be displayed, *the configuration parameter Assign FF Roles Instead of FF IDs must be set to YES* as shown below.



Change View "Configuration": Overview

Configuration

Parameter	Value	Comment
Retrieve Change Log	YES	
Send Log Report Execution Notification Immediately	YES	
Send Firefighter Login Notification Immediately	YES	
Assign FF Roles Instead of FF IDs	YES	
Send FirefightId Login Notification	YES	
Remote Function Call	DCM	

Steps:

Step 1: Create Firefighter Role:

Role should be created using transaction PFCG with specific security for performing the task assigned to the Firefighter role. Preferred practice is to assign specific security and not to assign access similar to 'SAP_ALL'.
The role(s) should not be assigned to any user via transaction SU01 or PFCG and should only be assigned as Firefighter level access.

Step 2: Assign Firefighter Owner:

Assign an Owner to the Firefighter Role.
Owners can assign Firefighting roles to Firefighters.
Owners cannot assign Firefighter Roles to themselves. Same as above, think they need to have config option turned on to prevent this.

Step 3: Assign Firefighter Controller:
Assign a Controller to the Firefighter Role. Controllers are responsible for reviewing the log report, and can receive e-mail notification of firefighter role use.
Firefighter Role Controllers can also be Firefighter Role Owners.

Step 4: Assign Firefighter:
Assign a Firefighter (existing SAP user ID) to the Firefighter Role. Firefighters can access the roles assigned to them within the validity dates indicated in the Firefighters table, and as defined by Firefighter Owners.

Additional Points:

1. One ffid can be assigned to multiple fire fighters but they cannot use at a time.
2. In out EAm, Additional activity is one extra tab added to maintain extra activities.
3. We can send a message to existing ff if we would like to use the same ffid.
4. We can also unlock the ffid which is being used by another ff.
5. FF owner can assign ffids which are owneed by him/her to fire fighters and controllers.
6. Decentralized fire figthing concept is also available in GRC 10 from Support pack 10 onwards.