



CONFIGURATION GUIDE | PUBLIC

Document Version: 1.0.1 – 2018-08-31

Configuration: Emergency Access Management for SAP Access Control 12.0

Content

1	Getting Started.	4
1.1	About This Document.	4
1.2	EAM Terminology.	4
2	Prerequisites.	5
3	Overview of Configuration.	6
4	Creating Roles.	7
5	Emergency Access Application Types.	9
6	Decentralized Firefighting.	10
7	Configuring EAM Log Notifications.	14
8	Configuring ID-based Firefighting.	15
8.1	Creating and Maintaining Firefighter IDs.	17
8.2	Assigning Owners.	19
8.3	Assigning Controllers.	20
8.4	Assigning Firefighters.	22
8.5	Maintaining E-mail Notifications for Emergency Access Logons.	24
8.6	Reason Codes.	25
	Creating and Maintaining Reason Codes.	25
	Assigning Systems to Reason Codes.	26
9	Configuring Role-based Firefighting.	27
10	Configuring Firefighter for HANA Target Systems.	28
10.1	Prerequisites.	28
10.2	Create Audit Policy for HANA Firefighting Sessions.	29
	Select Actions for Audit Policies.	30
10.3	Maintain Connectors on GRC System.	31
10.4	Maintain Sub-scenario Definition for ConnectorSystem.	32
10.5	Configuring Firefighter Assignment Reviews.	33
11	Configuration Parameters.	34
12	Time Zone Configuration.	36
13	Uploading and Downloading EAM User Assignments.	37

14	Schedule and Run Sync Jobs.	38
-----------	---	-----------

1 Getting Started

SAP Access Control is an enterprise software application that enables organizations to control access and prevent fraud across the enterprise, while minimizing the time and cost of compliance. The application streamlines compliance processes, including access risk analysis and remediation, business role management, access request management, emergency access maintenance, and periodic compliance certifications. It delivers immediate visibility of the current risk situation with real-time data.

The Emergency Access Management (EAM) capability enables you to implement your company's policies for managing emergency access. Users can create self-service requests for emergency access to systems and applications. Business process owners can review requests for emergency access and grant access. Compliance persons can perform periodic audits of usage and logs to monitor compliance with company guidelines.

1.1 About This Document

This document describes the prerequisites and procedures for configuring Emergency Access Management. It includes information for centralized and decentralized ID-based firefighting scenarios, and role-based firefighting.

1.2 EAM Terminology

The following concepts are important to understand emergency access management:

- **Firefighter:** the user who requires emergency access
- **Firefighter ID:** the user ID with elevated privileges.
- **Firefighting:** the act of using a Firefighter ID to perform tasks in an emergency
- **Owner:** the user responsible for a Firefighter ID and the assignment of controllers and Firefighters
- **Controller:** the user who reviews and approves (if required) the log files generated from firefighting activities
- **Centralized Firefighting:** using the GRC system as the centralized console through which Firefighters can logon to different system for firefighting
- **Decentralized Firefighting:** Firefighters can directly logon to the plug-in systems for firefighting; using the GRC system only for maintaining emergency access assignments and reporting

2 Prerequisites

You must have completed the following prerequisites before configuring EAM.

- You have completed the SAP Access Control 12.0 post-installation steps.
For more information, refer to the administrator guide at https://help.sap.com/viewer/p/SAP_ACCESS_CONTROL.
- You have set up GRC connectors for all target systems.
See [SAP NOTE 2413716](#) - Setup of Trusted RFC in GRC Access Control EAM.
- You have assigned the integration scenario SUPMG to all EAM relevant connectors.
- You have implemented **User Exit** per [SAP Note 1545511](#).
This restricts firefighter IDs from logging into target systems systems via SAP GUI.
- You have configured email settings (transaction SCOT).
- You have activated the following BC sets:
 - GRAC_SPM_CRITICALITY_LEVEL
 - GRAC_ACCESS_REQUEST_PRIORITY
 - GRC_MSMP_CONFIGURATION
 - GRAC_ACCESS_REQUEST_REQ_TYPE

3 Overview of Configuration

Use

The following is the overall procedure for configuring Emergency Access Management (EAM).

Process

1. Create the required roles for EAM.
See [Creating Roles \[page 7\]](#).
2. Select the emergency access application type.
See [Emergency Access Application Types \[page 9\]](#).
3. Configure ID-based or role-based firefighting.
See [Configuring ID-based Firefighting \[page 15\]](#) or [Configuring Role-based Firefighting \[page 27\]](#), per your application type.
4. Configure notifications for Firefighter ID logins.
See [Maintaining E-mail Notifications for Emergency Access Logons \[page 24\]](#).
5. Configure notifications for EAM logs.
See [Configuring EAM Log Notifications \[page 14\]](#).

4 Creating Roles

Emergency Access Management users include administrators, owners, controllers, and firefighters. The following table describes each role and the delivered roles that contain the recommended authorizations.

i Note

The delivered roles are sample roles. You must copy them into your own namespace if you want to use them.

Emergency Access Management Roles

Role Type	Description
Administrator	<p>Administrators have complete access to Emergency Access Management capability. They assign Firefighter IDs to owners and to Firefighters. Administrators run reports, maintain the data tables, and make sure that the Reason Code table is current. Administrators can enable e-mail notifications for Controllers through the Firefighter Assignment function and through Customizing.</p> <p>The delivered role for administrators is: <code>SAP_GRAC_SUPER_USER_MGMT_ADMIN</code>.</p> <div>i Note For decentralized firefighting scenarios, to enable the administrator to extend the validity period of firefighting assignments you must create this role on the relevant plug-in systems. Assign the authorization object <code>/GRCP1/001</code>, and enter the ACTVT field value as 70 or * (asterisk).</div>
Owner	<p>Owners can assign Firefighter IDs to Firefighters and define controllers. Owners can view the Firefighter IDs assigned to them by the administrator. They cannot assign Firefighter IDs to themselves.</p> <p>The delivered role for owners is: <code>SAP_GRAC_SUPER_USER_MGMT_OWNER</code>.</p> <div>i Note For decentralized firefighting scenarios, to enable the owner to extend the validity period of firefighting assignments you must create this role on the relevant plug-in systems. Assign the authorization object <code>/GRCP1/001</code>, and enter the ACTVT field value as blank (empty).</div>
Controller	<p>Controllers monitor Firefighter ID usage by reviewing the log report or log report workflow and receiving e-mail notification of Firefighter ID logon events.</p> <p>The delivered role for controller is: <code>SAP_GRAC_SUPER_USER_MGMT_CNTL</code>.</p>

Role Type	Description
Firefighter	<p>Firefighters can access Firefighter IDs assigned to them and can perform any tasks for which they have authorization. Firefighters use the Firefighter ID logons to run transactions during emergency situations.</p> <p>The delivered role for Firefighter is: <code>SAP_GRAC_SUPER_USER_MGMT_USER</code>.</p> <div> <p>i Note</p> <p>For decentralized firefighting scenarios, to enable the firefighter to use the EAM Launchpad, you must create this role on the relevant plug-in systems. Assign to the role the authorizations to use transactions <code>/GRCP1/GR1A_EAM</code> and <code>SU53</code>.</p> </div>
Firefighter ID	<p>The delivered role <code>SAP_GRAC_SPM_FFID</code>, when assigned to a user ID turns the ID into a Firefighter ID. Assign the role the authorization object <code>S_RFC</code> to enable remote logon.</p> <div> <p>i Note</p> <p>This role is used only for ID-Based firefighting.</p> </div>

For more information about roles and authorization objects, see the *SAP Access Control 10.0 Security Guide* at <http://help.sap.com/grc-ac>.

5 Emergency Access Application Types

You can choose from the following application types to use for firefighting:

- **ID-Based Firefighter:** You provide Firefighter authorizations by assigning Firefighter IDs to users. The Firefighters use the Emergency Access Management (EAM) Launchpad to access their firefighting IDs and the relevant systems. Users can access the EAM Launchpad in the following ways:
 - Centralized (on the GRC system)
Log onto the GRC system, and use transaction `GRAC_EAM` to remotely access **all** authorized plug-in systems. In this scenario, the GRC system and the EAM Launchpad provide a centralized access point to the plug-in systems for firefighting.
 - Decentralized (on the plug-in systems)
Log onto the respective plug-in systems, and use transaction `/GRCPI/GRIA_EAM` to perform the firefighting activities. In this scenario, as firefighting is performed locally on each of the plug-in systems, you have uninterrupted firefighting access in case the GRC system is not available, however, you must make sure you have user accounts on each of the plug-in systems.
Functions such as assignments, and reporting is still maintained in the GRC system. For more information, see [Decentralized Firefighting \[page 10\]](#).

i Note

Both centralized and decentralized options are always available. You do not need to enable one or the other. For more information, see [Configuring ID-based Firefighting. \[page 15\]](#)

- **Role-Based Firefighter:** You create the Firefighter roles on the plug-in systems, and assign them to users on the GRC system. The Firefighter directly logs onto the plug-in system using their user ID and performs firefighting activities.

i Note

You can use only one application type at a time.

To set the application type as either **ID-Based** or **Role-Based**, configure parameter 4000 in the Customizing activity [Maintain Configuration Settings](#), under ► [Governance, Risks, and Compliance](#) ► [Access Control](#) ►

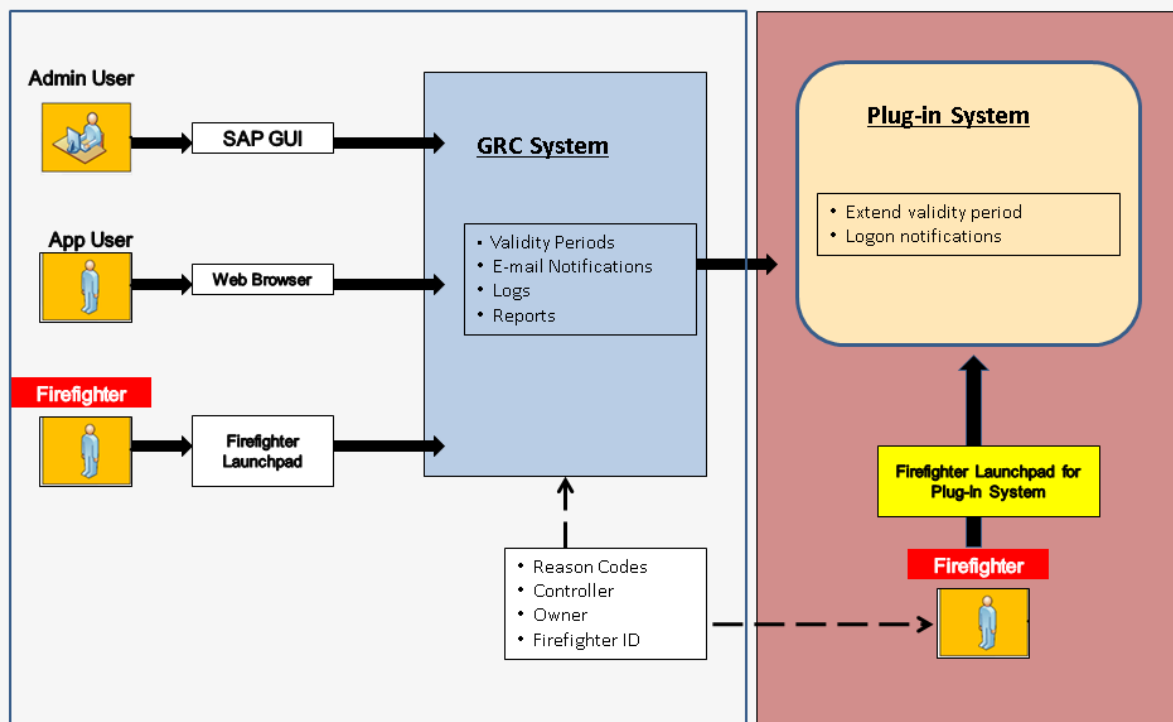
6 Decentralized Firefighting

Decentralized firefighting allows you to use the Emergency Access Management (EAM) Launchpad directly on the plug-in systems to perform firefighting activities in case the GRC system is not available.

To use the decentralized EAM Launchpad on the plug-in system, open SAP GUI and run transaction /GRCP1/GR1A_EAM. As this transaction is run locally, this also requires users to have accounts on the relevant plug-in systems in order to perform firefighting.

The following graphic illustrates that, for decentralized firefighting, the majority of the functions are still maintained in the GRC system. The following functions are available in the plug-in system:

- EAM launchpad for plug-ins
- Extending validity periods for firefighting assignments
- Enable Firefighter logon e-mail notifications
- Customize text for Firefighter logon e-mail notifications



Functions Maintained in GRC system versus Plug-in (for decentralized Firefighting)

Optional Configuration

You can also choose to maintain different role names for the Firefighter IDs for each plug-in system. For example, on Plug-in System01 you use `SAP_GRAC_EAM_FFID01`, and on Plug-in System02 you use `SAP_GRAC_EAM_FFID02`.

You can configure this in the Customizing activity, [Maintain Firefighter ID Role Name Per Connector](#), under [► Governance, Risks, and Compliance ► Access Control ► Emergency Access Management ►](#).

EAM Activities Maintained on the Plug-in Systems

The information in the following table describes which activities are maintained in the plug-system.

Activity	Comments
Creating users on systems to enable use of EAM Launchpad via SAP GUI.	As the EAM Launchpad is initiated locally, the user must have a user account on the plug-in systems in order to perform firefighting.
Creating Firefighter IDs	<p>You create Firefighter IDs on each plug-in system and synchronize them to the GRC repository.</p> <p>For more information, see Creating and Maintaining Firefighter IDs [page 17].</p>
Run firefighting launchpad	Run transaction <code>/GRCP1/GR1A_EAM</code> .
Extend validity period for firefighting assignments	<p>You can extend the validity period for firefighting assignments on either the GRC system or the plug-in system</p> <p>On the GRC system, open the Firefighter ID assignment and extend the assignment period.</p> <p>On the plug-in system, use the Customizing activities (transaction SPRO) to extend the validity period for Firefighter assignments on the plug-system.</p> <p>For more information, see Extending Validity Periods for Firefighting Assignments.</p>
Enable Firefighter Logon E-mail notification.	You can enable each plug-in system to notify the relevant firefighting controller when a Firefighter has logged into a firefighting session.
You can enable each plug-in system to notify the relevant firefighting controller when a Firefighter has logged into a firefighting session.	<p>The plug-in systems send notifications to the controllers and owners. This requires user accounts for the controllers and owners on the plug-in systems.</p> <p>On the plug-in systems, use the Customizing activities (transaction SPRO) to enable the notification.</p> <p>For more information, see Maintaining E-mail Notifications for Emergency Access Logons [page 24].</p>

Activity	Comments
Customize text for Firefighter Logon E-mail notification. You can customize the text for the notifications for each plug-in system.	<p>You can adapt the text for the notifications for each plug-in system.</p> <p>On the plug-in systems, use the Customizing activities (transaction SPRO) to enable the notification.</p> <p>For more information, see Maintaining E-mail Notifications for Emergency Access Logons [page 24].</p>

EAM Activities Maintained on the GRC System

The following table describes which activities are maintained in the GRC system.

Activity	Comments
Configure Emergency Access Maintenance and related master data	<p>The configuration and master data information is maintained in the GRC system and pushed to the plug-in systems.</p> <p>You must schedule periodic jobs for the application to sync the master data from the GRC system to the corresponding plug-in systems. We recommend you schedule the synchronization to run daily.</p> <p>You schedule the synchronization jobs in transaction SPRO: ► Governance, Risk, and Compliance ► Access Control ► Synchronization Jobs ► EAM Master Data Synchron.</p>
Creating Firefighter IDs	<p>You create Firefighter IDs on each plug-in system and synchronize them to the GRC repository.</p> <p>For more information, see Creating and Maintaining Firefighter IDs [page 17].</p>
Maintain Owners and Controllers for firefighting	Maintained on the GRC system
Assign owners to a Firefighter ID	Maintained on the GRC system
Assign a Firefighter ID to controllers	Maintained on the GRC system
Assign Firefighter IDs to Firefighters	Maintained on the GRC system
Synchronize user data	Maintained on the GRC system
Maintain Reason Codes	Maintained on the GRC system

Activity	Comments
Extend validity period for firefighting assignments	<p>You can extend the validity period for firefighting assignments on either the GRC system or the plug-in system.</p> <p>On the GRC system, open the Firefighter ID assignment and extend the assignment period.</p> <p>On the plug-in system, use the Customizing activities (transaction SPRO) to extend the validity period for Firefighter assignments on the plug-system.</p> <p>For more information, see Extending Validity Periods for Firefighting Assignments.</p>
Workflow-enabled assignments	Maintained on the GRC system
Maintenance and Synchronize logs	<p>All logs and user maintenance activities are maintained on the GRC system. We recommend scheduling the job for log collection to run every hour.</p> <p>The GRC system should not be down for extended periods of time because it impacts collection of the logs.</p>
Run reports	Maintained on the GRC system
Notification to controllers for logs, reports, and workflow activities.	Maintained on the GRC system

7 Configuring EAM Log Notifications

Use

You can choose to have the application send e-mail notifications when a log has been created. You can also customize the notification text. If you do not customize the text, the application uses the default message text.

Procedure

Centralized Firefighting

For the centralized firefighting scenarios, all e-mail notifications are handled on the GRC system.

To enable notifications for logs

1. Open the Customizing activities (transaction `SPRO`).
2. Navigate to ► [Governance, Risks, and Compliance](#) ► [Access Control](#) ► [Maintain Configuration Settings](#) ►
3. Set parameter 4009 to **Yes**.

To customize the notifications for logs

Configure the following Customizing activities under ► [Governance, Risks, and Compliance](#) ► [Access Control](#) ► [Workflow Access Control](#) ►.

- Maintain Custom Notification Messages
- Maintain Text for Custom Notification Messages

Decentralized Firefighting

For the decentralized firefighting scenarios, E-mail Notifications for logs are handled on each plug-in system. You maintain the following configuration settings for each plug-in system.

To enable notifications for logs

1. Open the Customizing activities (transaction `SPRO`).
2. Navigate to ► [Governance, Risks, and Compliance \(Plug-In\)](#) ► [Access Control](#) ► [Maintain Plug-In Configuration Settings](#) ►
3. Set parameter 4009 to **Yes**.

To customize the notifications for logs

Configure the following Customizing activities under ► [Governance, Risks, and Compliance \(Plug-In\)](#) ► [Access Control](#) ►.

- Maintain Custom Notification Messages for Emergency Access Logons (Plug-In)
- Maintain Text for Custom Notification Messages (Plug-In)

8 Configuring ID-based Firefighting

Use

This topic details the process for configuring ID-based firefighting.

Prerequisites

Ensure users can access the GRC system and open the SAP GUI.

Process

The information in this section is required for configuring all ID-based firefighting.

Note

For additional steps required for decentralized firefighting, see the **Additional Steps for Configuring Decentralized ID-based Firefighting** section below.

1. Create relevant application roles for Emergency Access Management.
For the list of required application roles, see [Creating Roles \[page 7\]](#).
2. Set the application type for ID-based Firefighting:
 1. In Customizing (transaction SPRO), open the activity [Maintain Configuration Settings](#), under [► Governance, Risks, and Compliance ► Access Control. ►](#)
 2. For parameter 4000, set the value as 1 for ID based firefighting.
3. Configure the [Firefighter ID Role Name](#).
You assign this role to user accounts to create Firefighter IDs.
 1. In Customizing, open the activity [Maintain Configuration Settings](#), under [► Governance, Risks, and Compliance ► Access Control. ►](#)
 2. For parameter 4010, enter the user-defined role name, for example, SAP_GRAC_EAM_FFID.
4. Synchronize the users and roles on the plug-in systems with the GRC system.
On the GRC system, open Customizing (transaction SPRO) and use the Customizing activity, [Repository Object Synch](#). It is located under [► Governance, Risks, and Compliance ► Access Control ► Synchronization Jobs ►](#).
5. On the plug-in systems, create the Firefighter IDs and then synchronize them to the GRC repository.
For more information, see [Creating and Maintaining Firefighter IDs \[page 17\]](#).
6. Maintain the following Access Control Owners:
 - Firefighter ID Owner
The Firefighter ID Owners are responsible for maintaining the roles and their assignments to Firefighters.

- Firefighter ID Controller
The Firefighter ID Controllers are responsible for reviewing the log reports generated during Firefighter usage.
For more information, see [Assigning Controllers \[page 20\]](#).
- 7. Assign an owner to a Firefighter ID.
For more information, see [Assigning Owners \[page 19\]](#).
- 8. Assign a controller to a Firefighter ID.
For more information, see [Assigning Controllers \[page 20\]](#).
- 9. Assign a Firefighter ID to a user to enable them to do firefighting.
For more information, see [Assigning Firefighters \[page 22\]](#).
- 10. Create reason codes.
For more information, see [Reason Codes \[page 25\]](#).
- 11. Maintain settings for Firefighter logon e-mail notifications.
The application sends notifications to the Controller when a Firefighter has logged on to a firefighting session.
 - To enable the application to send Firefighter Logon e-mail notifications, do the following:
 1. Open the Customizing activity, [Maintain Configuration Settings](#), under ► [Governance, Risks, and Compliance](#) ► [Access Control](#) ►.
 2. For parameter 4008, set the value to **1**.
 - Optionally, you can change the text of the logon e-mail notifications. (If you do not change the text, the application uses the default delivered text.)
To change the text, maintain the following Customizing activities:
 - Maintain Custom Notification Messages for Emergency Access Management
 - Maintain Text for Custom Notification Messages
 For more information, see [Maintaining E-mail Notifications for Emergency Access Logons \[page 24\]](#).

Additional Steps for Configuring Decentralized ID-based Firefighting

To configure decentralized firefighting, first complete the above tasks and then complete the following steps.

1. Ensure users have user accounts and roles on each of the plug-in systems to allow them to log on to each system. Firefighters must be able to directly access each plug-in system and use the EAM Launchpad locally.
2. Enable decentralized firefighting.
On the GRC system, in Customizing (transaction SPRO) use the activity, [Maintain Configuration Settings](#), under ► [Governance, Risks, and Compliance](#) ► [Access Control](#) ►.
Set parameter 4015 – Enable Decentralized Firefighting to **Yes**.
3. Synchronize the master data from the GRC system to the plug-in systems.
In Customizing (transaction SPRO) use the activity, [EAM Master Data Synch](#), under ► [Governance, Risks, and Compliance](#) ► [Access Control](#) ► [Synchronization Jobs](#) ►.
4. Optionally, you can maintain different Firefighter ID role names for each plug-in system. For example, on Plug-in System01 you use SAP_GRAC_EAM_FFID01 , and on Plug-in System 02 you use SAP_GRAC_EAM_FFID02.
 1. On the GRC system, open Customizing (transaction SPRO).
 2. Open the Customizing activity, [Maintain Firefighter ID Role Name Per Connector](#), under ► [Governance, Risks, and Compliance](#) ► [Access Control](#) ► [Emergency Access Management](#) ►.
 3. Maintain the Firefighter ID Role names as needed.

i Note

If you do not use this option, the application uses the default Firefighter ID Role name listed in parameter 4010 of the Customizing activity [Maintain Configuration Settings](#) for **all** systems.

5. Optionally, you can maintain separate Firefighter Logon e-mail notifications settings for each of the plug-in systems.
 - To enable each plug-in system to send its own logon e-mail notifications, do the following:
 1. On the plug-in system, open the Customizing activity, [Maintain Plug-in Configuration Settings](#), under ► [Governance, Risks, and Compliance \(Plug-In\)](#) ► [Access Control](#) ►.
 2. For parameter 4008, set the value to **1**.
 - To change the text of the logon e-mail notifications for each of the plug-in systems, maintain the following Customizing activities:
 - Maintain Custom Notification Messages for Emergency Access Management (plug-In)
 - Maintain Text for Custom Notification Messages (Plug-In)
- For more information, see [Maintaining E-mail Notifications for Emergency Access Logons \[page 24\]](#).

i Note

These configuration steps are **in addition** to the main configuration steps for ID-based firefighting. Make sure you complete the steps for creating and assigning owners, controllers, and Firefighters.

More Information

[Configuring Role-based Firefighting \[page 27\]](#)

8.1 Creating and Maintaining Firefighter IDs

Use

You create Firefighter IDs by assigning the **Firefighter ID role** to a user account.

For example, **User_Account01 + Firefighter_ID_role = Firefighter_ID01**.

You can use either transaction SU01 or the access request functionality in Access Control to create Firefighter IDs. This topic explains how to create and maintain Firefighter IDs using the access request functionality.

i Note

You must create Firefighter IDs for each plug-in system and then synchronize them to the GRC repository.

Prerequisites

- You have created the Firefighter ID role.
The delivered role is `SAP_GRAC_SPM_FFID`, but you can use your own role.
- You have configured the Firefighter ID role name in the Customizing activity (transaction SPRO) [Maintain Configuration Settings](#), parameter 4010.

Procedure

Creating Firefighter IDs

i Note

You can use either transaction `SU01` or the access request functionality in Access Control to create Firefighter IDs. These steps explain how to create Firefighter IDs using the access request functionality.

1. Open the [Access Request](#) screen.
2. In the [Request Type](#) dropdown list, choose [New Account](#).
3. In the [Request For](#) dropdown list, choose [Other](#).
4. In the [User](#) field, enter the name of the Firefighter ID, such as `FFID_01`.
5. On the [User Access](#) tab, choose [Add](#), and select [Role](#).
6. Add the Firefighter ID role you have configured, for example, `SAP_GRAC_SPM_FFID`.
7. Add any additional roles required for the necessary authorizations and system access for performing the firefighting tasks.
8. Submit the access request.
The new `FFID_01` user ID is now a Firefighter ID.

Maintaining Firefighter IDs

You can also use the access request functionality to maintain, change, or delete the Firefighter IDs.

1. Open the [Access Request](#) screen.
2. In the [Request Type](#) dropdown list, select from the available tasks such as [Change Account](#), [Delete Account](#), and so on.

i Note

You can type Firefighter, Owner, and Controller assignment entries directly into the Firefighter assignment screens in addition to selecting entries using the F4 help.

If you mistakenly type an invalid entry, an error message appears at the top of the screen. Then you can manually correct the entry or use F4 help to choose a valid entry

3. Optionally, if you want to reassign all of the assignments of a Firefighter ID, select [Reassign](#).
4. Save the entry.

More Information

[Creating Access Requests](#)

8.2 Assigning Owners

Use

This topic is applicable to both ID-based and role-based firefighting.

You must assign owners to Firefighter IDs and Firefighter Roles. The Owners then assign Firefighter IDs to Firefighters and define controllers.

Prerequisites

- For role-based firefighting, you have defined the Firefighter roles in the GRC system, and selected the [Enable for Firefighting](#) checkbox on the [Define Role](#) screen under [Access Management > Role Management > Role Maintenance](#).
- For ID-based firefighting, you have defined a Firefighter ID role on the ERP system, and assigned the role the remote logon authorization `S_RFC`.

Procedure

Creating a new assignment

1. Choose [Emergency Access Assignment > Owners](#).
The [Firefighter Owner](#) screen displays a table of existing assignments.
2. Choose [Assign](#).
The [Owner Assignment: New](#) screen appears.
3. In the [Owner ID](#) field select the owner.
4. In the [Firefighter ID](#) table, choose [Add](#), and then add one or multiple Firefighter IDs or roles.

i Note

If the Owner is not in the [Access Control Owners](#) table, a pop-up asks if you want it to be added and available for future use. If you choose [No](#), the Firefighter IID assignment is saved, but the Owner is not added to the [Access Control Owners](#) table.

5. Choose [Save > Close](#).

Viewing or Maintaining an Assignment

1. Choose ► [Emergency Access Assignment](#) ► [Owners](#) ►.
The [Firefighter Owner](#) screen displays existing assignments.
2. Select a row and choose [Open](#).
The [Owner Assignment](#) screen displays the assignment.

i Note

You can type Firefighter, Owner, and Controller assignment entries directly into the Firefighter assignment screens in addition to selecting entries using the F4 help.

If you mistakenly type an invalid entry, an error message appears at the top of the screen. Then you can manually correct the entry or use F4 help to choose a valid entry

3. To add an owner assignment:
 1. Choose [Add](#).
A new line appears in the table.
 2. Enter information in the required fields (marked with an asterisk (*)).
 3. Choose ► [Save](#) ► [Close](#) ►.
The assignment is completed for the owner.
4. To change all of the Owner's assignments, click the [Reassign](#) button.

i Note

For example, if an Owner is promoted to a new position, clicking [Reassign](#) will reassign all of his Firefighters to whoever you designate.

5. To remove the owner assignment, choose [Remove](#).
The selected assignment is deleted.
6. Choose ► [Save](#) ► [Close](#) ►.

8.3 Assigning Controllers

Use

This topic is applicable to both ID-based and role-based firefighting.

Owners assign controllers to Firefighting IDs and Firefighting roles. Controllers track and audit the activities of the Firefighter IDs and Firefighter roles. You can use the [Controller](#) screen to assign, add, or remove a controller for Firefighter IDs and roles.

i Note

Only one person can edit the controller assignments for a Firefighter ID or role at a time.

Procedure

1. Choose ► [Emergency Access Maintenance](#) ► [Controllers](#) ►. The [Controller](#) screen displays existing controllers, Firefighter IDs, and associated systems.
2. Choose [Assign](#).
The [Controller Assignment: New](#) screen appears.
3. In the [Controller ID](#) field, enter the user ID for the person you want to assign as controller.

Note

If the person is not in the [Access Control Owners](#) table, a pop-up asks if you want this person to be added as a Controller to the table and available for future use. If you choose [No](#), the Controller assignment is saved, but the Controller is not added to the [Access Control Owners](#) table.

4. Choose [OK](#).
5. Choose [Add](#), select the Firefighter ID from the list, and then choose [OK](#).
The [System](#) value is generated after you choose the Firefighter ID.
6. In the [Notification By](#) column, select from these options:
 - [E-mail](#)
To send a log report to an external e-mail inbox, such as Microsoft Outlook, or to an SAP inbox each time the [GRAC_SPM_LOG_SYNC_UPDATE](#) background job runs.
You can select options for notification by e-mail:
 - To send logon notifications, set the [Send Firefighter ID Login Notification](#) parameter to [YES](#). Logon notification is sent by e-mail only, independent of the [Notification By](#) option.
 - To send notification when a Firefighter ID logs on to the system, set the [Send Firefighter Login Notification Immediately](#) parameter to [YES](#).
 - To send log report notifications, set the [Log Report Execution Notification](#) parameter to [YES](#). Log report notification depends on the [Notification By](#) field.
 - To receive log report notifications as the logs are updated, set the [Send Log Report Execution Notification Immediately](#) parameter to [YES](#).
 - [Workflow](#)
To send log report notifications in the form of an SAP Workflow item.

Note

Users must have Portal authorization to access the workflow items.

- [Log Display](#)
To view Firefighter ID logon events from the [Emergency Access Management Administrator](#) screen. The controller manually generates the log report and views the report in the [Emergency Access Management Administrator](#) screen. The system does not send automated e-mail notifications.
7. Choose ► [Save](#) ► [Close](#) ►.

Viewing or Maintaining a Controller Assignment

1. On the [Controller](#) screen, select a row and choose [Open](#).
The [Controller Assignment](#) screen displays the assignment.

Note

You can type Firefighter, Owner, and Controller assignment entries directly into the Firefighter assignment screens in addition to selecting entries using the F4 help.

If you mistakenly type an invalid entry, an error message appears at the top of the screen. Then you can manually correct the entry or use F4 help to choose a valid entry

2. To add a Firefighter assignment, choose [Add](#).
A new row appears in the table.
3. Enter information in the required fields and select a notification method from the dropdown menu in the [Notification By](#) column.
4. To change all of the Controller's assignments, click the [Reassign](#) button.

i Note

For example, if a Controller is promoted to a new position, clicking [Reassign](#) will reassign all of his assignments to whomever you designate.

5. To remove a Firefighter assignment, choose [Remove](#).
The selected assignment is deleted.
6. Choose ► [Save](#) ► [Close](#) ✕.

8.4 Assigning Firefighters

Use

This topic is applicable to both ID-based and role-based firefighting.

You enable users to perform firefighting by assigning them Firefighter IDs (for ID-based firefighting) or Firefighter roles (for role-based firefighting). You use the functions on the [Firefighter ID](#) screen to maintain the Firefighter assignments.

i Note

Only one person can edit a Firefighter assignment at a time.

Prerequisites

- For role-based firefighting, you have defined the Firefighter roles in the GRC system, and selected the [Enable for Firefighting](#) checkbox on the [Define Role](#) screen under ► [Access Management](#) ► [Role Management](#) ► [Role Maintenance](#) ✕.
- For ID-based firefighting, you have defined a Firefighter ID role on the ERP system, and assigned the role the remote logon authorization S_RFC.

Procedure

1. Choose ► [Access Management](#) ► [Emergency Access Assignment](#) ► [Firefighter IDs](#) ►.
The *Firefighter ID* screen appears.
2. Choose [Assign](#).
The *Firefighter ID Assignment: New* screen appears.
3. In the *Firefighter ID* field, enter the Firefighter ID or Firefighter role.
The application automatically fills in the *System* field.
4. In the *Criticality* field, select a criticality level.
5. On the *Firefighter* tab, enter information in the required fields (marked with an asterisk (*)).
6. Choose the *Controller* tab page and add a controller assignment.
7. Choose ► [Save](#) ► [Close](#) ►.

Viewing or Maintaining a Firefighter ID or Role Assignment

1. On the *Firefighter ID* screen, select a row and choose [Open](#).
The *Firefighter ID Assignment* screen displays the assignment.

i Note

You can type Firefighter, Owner, and Controller assignment entries directly into the Firefighter assignment screens in addition to selecting entries using the F4 help.

If you mistakenly type an invalid entry, an error message appears at the top of the screen. Then you can manually correct the entry or use F4 help to choose a valid entry.

2. To add a Firefighter ID assignment, choose [Add](#).
A new row appears in the table.
3. Enter information in the required fields (marked with an asterisk (*)).
4. To remove a Firefighter ID assignment, choose [Remove](#).
The selected assignment is deleted.
5. To change all of the Firefighter ID assignments, click the [Reassign](#) button and choose who should complete these duties.

i Note

For example, if the person to whom the FFID is assigned is promoted to a new position, clicking [Reassign](#) will reassign all of his FFID's to someone else.

6. Choose ► [Save](#) ► [Close](#) ►.

8.5 Maintaining E-mail Notifications for Emergency Access Logons

Use

You can choose to have the application send e-mail notifications to controllers when a Firefighter logs on to perform ID-based firefighting.

You can also customize the notification text. If you do not customize the text, the application uses the default message text.

Process

Centralized

For the centralized firefighting scenarios, all firefighting logons and Firefighting Logon E-mail Notifications are handled on the GRC system.

To enable notifications for firefighting logons

1. Open Customizing activities (transaction `SPRO`).
2. Navigate to ► [Governance, Risks, and Compliance](#) ► [Access Control](#) ► [Maintain Configuration Settings](#) ►
3. Set parameter 4008 to **Yes**.

To customize the notifications for firefighting logons

Configure the following Customizing activities under ► [Governance, Risks, and Compliance](#) ► [Access Control](#) ► [Workflow Access Control](#) ►.

- Maintain Custom Notification Messages
- Maintain Text for Custom Notification Messages

Decentralized

For the decentralized firefighting scenarios, all firefighting logons and firefighting logon e-mail notifications are handled on each plug-in system. You must maintain user accounts for the controllers and owners on the plug-in systems in order for them to receive notifications. You maintain the following settings for each plug-in system.

To enable notifications for firefighting logons

1. Open Customizing activities (transaction `SPRO`).
2. Navigate to ► [Governance, Risks, and Compliance \(Plug-In\)](#) ► [Access Control](#) ► [Maintain Plug-In Configuration Settings](#) ►.
3. Set parameter 4008 to **Yes**.

To customize the notifications for firefighting logons

Configure the following Customizing activities under ► [Governance, Risks, and Compliance \(Plug-In\)](#) ► [Access Control](#) ►.

- Maintain Custom Notification Messages for Emergency Access Logons (Plug-In)
- Maintain Text for Custom Notification Messages (Plug-In)

8.6 Reason Codes

Use

When a Firefighter uses the Emergency Access Management (EAM) Launchpad to logon to the system to carry out Firefighter activities, the Firefighter must provide a reason for logging on by choosing from available reason codes.

To open the *Reason Codes* screen, choose ► *Access Management* ► *Emergency Access Maintenance* ► *Reason Codes* ►.

More Information

[Creating and Maintaining Reason Codes \[page 25\]](#)

[Assigning Systems to Reason Codes \[page 26\]](#)

8.6.1 Creating and Maintaining Reason Codes

Procedure

Maintaining an Existing Reason Code

1. Select an existing reason code and choose *Open*.
The specific reason code screen appears.
2. Choose *Add* to assign a system to the reason code, or choose *Remove* to remove a system from the reason code.
3. Choose ► *Save* ► *Close* ►.
4. Verify that the status is set to *Active* when you want to begin using the assignment.

Creating a New Reason Code

1. To create a new reason code, choose *Create* on the *Reason Code - All* screen.
The *Reason Code New* screen appears.
2. In the *Reason Code* field, enter a name for the new reason code.
3. In the *Status* field dropdown menu, choose either *Active* or *Inactive*.
4. Enter a description.
5. In the *System* area, choose *Add* to add a system or systems to the new reason code.

6. Choose ► [Save](#) ► [Close](#) ►

The [Reason Code - All](#) screen appears with the new reason code displayed in the list.

More Information

[Assigning Systems to Reason Codes \[page 26\]](#)

8.6.2 Assigning Systems to Reason Codes

Context

You assign reason codes to one or many systems. The application tracks reason code usage across each system.

Procedure

1. Choose ► [Access Management](#) ► [Emergency Access Maintenance](#) ► [Reason Codes](#) ►.

The [Reason Codes](#) screen appears and displays a list of the existing reason codes and related fields and buttons.

2. Choose [Status](#) to set the existing reason codes as active or inactive.
3. To assign a system to a reason code, select an existing active reason code or create a new reason code.

Next Steps

[Creating and Maintaining Reason Codes \[page 25\]](#)

9 Configuring Role-based Firefighting

Use

The following workflow describes how to configure role-based firefighting.

Process

1. Create relevant application roles for Emergency Access Management.
For the list of required application roles, see [Creating Roles \[page 7\]](#).
2. Set the application type for role-based firefighting:
 1. In Customizing (transaction `SPRO`), open the activity [Maintain Configuration Settings](#), under [► Governance, Risks, and Compliance ► Access Control. ►](#)
 2. For parameter `4000`, set the value as `2` for role-based firefighting.
3. Synchronize the users and roles on the plug-in systems with the GRC system.
You do this using the Customizing activity, [Repository Object Synch](#), under [► Governance, Risks, and Compliance ► Access Control ► Synchronization Jobs ►](#).
4. Create firefighting roles in the respective plug-in systems via PFCG or Access Control's business role management functionality.
For more information, see [Defining Roles..](#)
5. Maintain the following Access Control Owners in the GRC application:
 - Firefighter Role Owner
The Firefighter Role Owners are responsible for maintaining the roles and their assignments to Firefighters.
 - Firefighter Role Controller
The Firefighter Role Controllers are responsible for reviewing the log reports generated during Firefighter usage.
6. Assign an Owner to a Firefighter role.
For more information, see [Assigning Owners \[page 19\]](#).
7. Assign a Controller to a Firefighter role.
For more information, see [Assigning Controllers \[page 20\]](#).
8. Assign a Firefighter role to a user to enable them to do firefighting.
For more information, see [Assigning Firefighters \[page 22\]](#).

More Information

[Configuring ID-based Firefighting \[page 15\]](#)

10 Configuring Firefighter for HANA Target Systems

The procedure to configure firefighting for HANA target systems follow the same core steps as the procedure for configuring ID-based firefighting. The information in this section describes the additional steps required to set up firefighting for HANA target systems.

Overview

The table below shows an overview of the configuration steps.

Carry Out This Step	On This System
Create audit policy for HANA firefighting sessions	HANA target system
Maintain the firefighter role on the target system	HANA target system
Maintain connectors to the HANA system	GRC system
Maintain firefighter roles for the HANA system	GRC system
Maintain scenario-connections for HANA connectors	GRC system
Run synch jobs	GRC system

For more information, see [Configuring ID-based Firefighting \[page 15\]](#).

10.1 Prerequisites

You must have completed the following prerequisites before proceeding with the configuration procedures.

- You have installed the SAP Access Control 12.0 plug-in for S/4HANA/ERP HR functions: `GRCPIERP V1200_S4`, version `SAP GRC PLUGIN S4HANA 1610+`.
- In access control, you have created and configured connectors for the S/4HANA target system.

10.2 Create Audit Policy for HANA Firefighting Sessions

This procedure creates an audit policy for tracking and logging actions on the HANA system when someone performs firefighting activities it.

Create Audit Policy

1. In HANA Studio, right-click the target system, and choose ► **Security** ► **Open Security Console** ►.
2. Ensure **Auditing Status** is set to **Enabled**, and **Audit Trail Target** is set to **Database Table**.
3. Enter a name for the audit policy that is meaningful to you. For example, in the bottom graphic, we have used SAPGRCFirefighterAudit.

i Note

You will need to enter the audit policy name in the later step for configuring the connector.

Security HD2 (SYSTEM) HD2

Auditing | Password Policy | SAML Identity Providers | Data Volume Encryption

System Settings for Auditing

Global Settings

Auditing Status: **Enabled** | Audit Trail Target: **Database Table** | Directory Name:

Audit Level Trail Targets

Audit Level	Audit Trail Tar...
EMERGENCY	
ALERT	
CRITICAL	

Audit Policies

Policy	Policy Status	Audited Actions
--------	---------------	-----------------

For efficiency, and ease of readability, we recommend creating four separate audit policies and selecting specific actions to track in each.

- User and Role Management
- Structured Privilege Management
- Session Management and System Configuration
- Granting and Revoking of Authorization

For specific recommendations as to which actions to select, see [Select Actions for Audit Policies \[page 30\]](#).

10.2.1 Select Actions for Audit Policies

The following are suggested actions to include for the respective audit policies. We recommend consulting with your administrator or compliance officer as your company may have specific guidelines and requirements for logging information.

User and Role Management

SAPGRCFireFighterAudit_UserRoleManagement		
▼	<input checked="" type="checkbox"/> User and Role Management	
	<input checked="" type="checkbox"/> ALTER USER	Changes to users
	<input checked="" type="checkbox"/> CREATE ROLE	Creation of roles
	<input checked="" type="checkbox"/> CREATE USER	Creation of users
	<input checked="" type="checkbox"/> DROP ROLE	Deletion of roles
	<input checked="" type="checkbox"/> DROP USER	Deletion of users

Structured Privilege Management

SAPGRCFireFighterAudit_StrPrvManagement		
▼	<input checked="" type="checkbox"/> Structured Privilege Management	
	<input checked="" type="checkbox"/> ALTER STRUCTURED PRIVILEGE	Changes to analytic privileges
	<input checked="" type="checkbox"/> CREATE STRUCTURED PRIVILEGE	Creation of analytic privileges
	<input checked="" type="checkbox"/> DROP STRUCTURED PRIVILEGE	Deletion of analytic privileges

Session Management and System Configuration

SAPGRCFireFighterAudit_SystemManagement		
▼	<input checked="" type="checkbox"/> Session Management and System Configuration	
	<input checked="" type="checkbox"/> CANCEL SESSION	Cancellation of statement execution in sessions
	<input checked="" type="checkbox"/> CONNECT	User connections to the database
	<input checked="" type="checkbox"/> DISCONNECT SESSION	User disconnections from the database
	<input checked="" type="checkbox"/> STOP SERVICE	Stopping of service
	<input checked="" type="checkbox"/> SYSTEM CONFIGURATION CHANGE	Changes to system configuration files (for example, *.ini files)

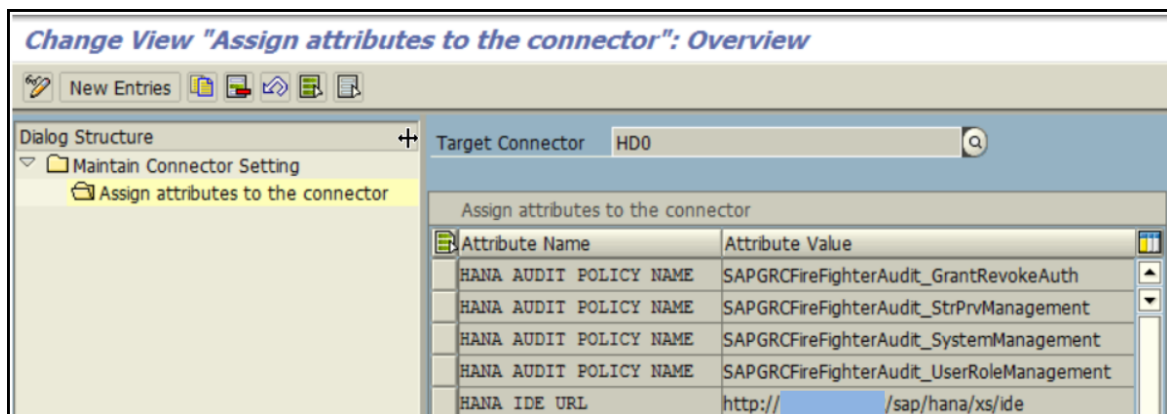
Granting and Revoking of Authorization

SAPGRCFireFighterAudit_GrantRevokeAuth		
▼ <input checked="" type="checkbox"/>	Granting and Revoking of Authorization	
<input checked="" type="checkbox"/>	GRANT ANY	Granting of all privileges and roles to users and roles
<input checked="" type="checkbox"/>	GRANT APPLICATION PRIVILEGE	Granting of application privileges to users and roles
<input checked="" type="checkbox"/>	GRANT PRIVILEGE	Granting of system privileges, object privileges, and package privileges to users and roles
<input checked="" type="checkbox"/>	GRANT ROLE	Granting of roles to users and roles
<input checked="" type="checkbox"/>	GRANT STRUCTURED PRIVILEGE	Granting of analytic privileges to users and roles
<input checked="" type="checkbox"/>	REVOKE ANY	Revocation of all privileges and roles from users and roles
<input checked="" type="checkbox"/>	REVOKE APPLICATION PRIVILEGE	Revocation of application privileges from users and roles
<input checked="" type="checkbox"/>	REVOKE PRIVILEGE	Revocation of system privileges, object privileges, and package privileges from users and roles
<input checked="" type="checkbox"/>	REVOKE ROLE	Revocation of roles from users and roles
<input checked="" type="checkbox"/>	REVOKE STRUCTURED PRIVILEGE	Revocation of analytic privileges from users and roles

10.3 Maintain Connectors on GRC System

1. Use SAP Logon to log onto the GRC system and run transaction SPRO.
2. Open ► *Governance, Risk and Compliance* ► *Access Control* ► *Maintain Connector Settings* ►.
3. Add a connector for the HANA target system. Ensure the *Appl Type* is **17**. Save the connector settings.
4. Select the connector and double-click *Assign attributes to the connector*.
5. Create the following attributes and enter the attribute values as follows:

Attribute Name	Instructions for Attribute Value
HANA AUDIT POLICY NAME	Enter the name of the audit policy you created on the HANA target system.
	<div> i Note The value must match the name on the HANA system. </div>
HANA IDE URL	The syntax for the HANA IDE URL is as follows: http://<system name>:<port><instance>/sap/hana/xs/ide . See the image below for an example.



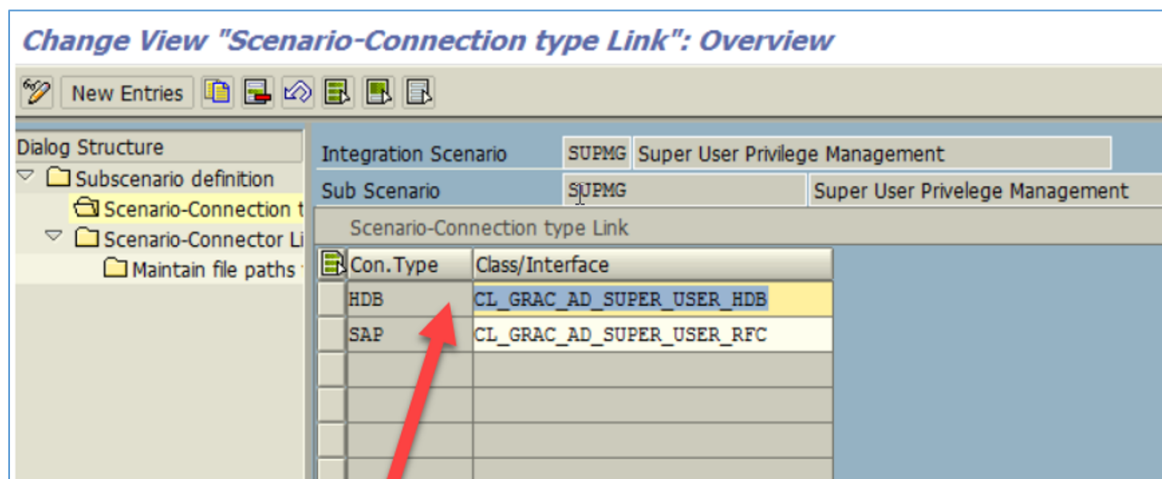
6. Save the connector settings.

10.4 Maintain Sub-scenario Definition for ConnectorSystem

1. In SPRO, open **Governance, Risk and Compliance** > **Common Component Settings** > **Integration Framework** > **Maintain Connector Settings**.
2. In the **Integration Scenario Work Area**, select **SUPMG**.
3. Create a **sub-scenario** for **SUPMG** with the following values.

Con. Type	Class/Interface
HDB	CL_GRAC_AD_SUPER_USER_HDB
SAP	CL_GRAC_AD_SUPER_USER_RFC

For an example, see the image below



10.5 Configuring Firefighter Assignment Reviews

You do the following to enable the Firefighter ID review workflow. The review process of Firefighter IDs is similarly to the User Access Review (UAR): the workflow sends current Firefighter ID assignments to reviewers' inboxes, and reviewers either accept or remove the assignments.

Prerequisites

- Activate BC sets for new MSMP workflow configuration. Go to transaction SCPR20 and search for BC set: GRC_MSMP_CONFIGURATION. Please note that activating the BC set will overwrite standard MSMP configuration and hence must be performed very carefully. Best-practice always recommends to use customer namespace for any customization. In this case, even though you have customized your stages and paths in the customer namespace, please make sure to note down the Process Initiators as the global setting will get overwritten. Once activated, you have to manually set the custom initiators for all your process IDs.
- Make sure user WF-BATCH has authorization for object GRAC_FFOWN to read the Firefighter owners.

Configuration

1. MSMP configuration
Once you have activated the BC sets, the process ID SAP_GRAC_FFID_REVIEW is available in the MSMP configuration. The customization of the workflow follows the standard behavior of other MSMP workflows.
2. From the frontend, go to ► [Access Management](#) ► [Scheduling](#) ► [Background Scheduler](#) ► Create a new schedule. In the *Schedule Activity* field, select **Generates data for access request Firefighter ID review**.

→ Tip

To quickly generate workflow items without using the Background Scheduler, you can run report GRAC_FFID_REVIEW_GEN from SE38

3. To check the generated workflow items, use the Search Request application as an administrator, and select the process ID **Firefighter ID Review Workflow**. The Firefighter Owner receives the access request in their work inbox.
Processing the workflow is very similar to the User Access Review (UAR). A Firefighter Owner has two choices: approving the assignment or removing it. Each line item must be processed and the necessary action set. The *Action* column changes accordingly. Once reviewed, the workflow can be submitted and will follow the workflow path. After all, approvals are given, the system automatically provisions the required changes, e.g., remove Firefighter assignments.

For additional information, see <https://blogs.sap.com/2017/09/29/sap-access-control-grc-firefighter-id-review/>.

11 Configuration Parameters

The following lists the parameters relevant for configuring EAM. You maintain the parameters in SPRO

► [Governance, Risk and Compliance](#) ► [Access Control](#) ► [Maintain Configuration Settings](#) ► .

Parameter ID	Description
4000	Application Type
4001	Default Firefighter Validity Period (in days)
4003	Retrieve Change Log
4004	Retrieve System Log
4005	Retrieve Audit Log
4006	Retrieve O/S Command Log
4007	Send Log Report Execution Notification Immediately
4008	Send Firefight ID Logon Notification
4009	Log Report Execution Notification
4010	Firefighter ID Role Name
4012	Default users for forwarding the Audit Log workflow
4013	Firefighter ID owner can submit request for Firefighter ID owned
4014	Firefighter ID controller can submit request for Firefighter ID
4015	Enable decentralized Firefighting
4017	Enable CUP request number to show in Firefighter ID/Role Assignment Screen
4018	Enable detailed application logging (SLG1) for Firefighter log synchronization programs
4020	Generate EAM log Firefighter sessions with no activity
4021	Use ALV Grid for Firefighter filter transaction
5033	Allow creation of Firefighters with no Controller

For more information, see the Configuration Parameters Guide at https://help.sap.com/viewer/p/SAP_ACCESS_CONTROL.

12 Time Zone Configuration

For logs to be properly captured, the time zones in the connected target systems need to be configured to match the operating system and also the SAP GRC server time zone. Even a slight difference (e.g. 2 minutes) can cause logs to be missed.

To maintain time zones, go to ► [SPRO](#) ► [SAP Netweaver](#) ► [General Setetings](#) ► [Time Zones](#) ► [Maintain System Settings](#) ► . ►

13 Uploading and Downloading EAM User Assignments

Enable mass changes and additions to Emergency Access Management (EAM) user assignments.

Before beginning the mass maintenance process, ensure that the following prerequisites are followed:

- Owners and Controllers must already exist as Access Control Owners (located on the [Setup](#) tab, in the [Access Owners](#) section).
- The FFIDs, Controller IDs and Owner IDs must already be in the Access Control repository.
- If only FFIDs are being uploaded, they must have their respective Owners maintained. You can verify this in the [Emergency Access Assignment](#) section, [Owners](#) link.
- A user cannot upload himself as Owner or Firefighter user.
- The Owner and Firefighter user for a record cannot be the same.
- The Controller and FFID for a record cannot be the same.
- Validity dates for existing assignments will be updated with the uploaded information.

After verifying the prerequisites, complete the following steps:

1. On the [Setup](#) tab, in the [Emergency Access Management](#) section, select [Mass Maintenance](#). This displays the [Upload Emergency Access Assignments](#) page.
2. Select the [Download](#) button.
 - To download the template, select the [Template](#) button. Ensure that *all* the checkboxes are selected. Select [Download](#).

i Note

The downloaded XML file contains 6 tabs (Owners_Data, Owners_Comments, Firefighters_Data, Firefighters_Comments, Controllers_Data and Controllers_Comments). It is mandatory to preserve the downloaded format of the XML file.

- To download data, select the [Data](#) button. Select the desired system(s). Select the content to download (Owners, Firefighters, Controllers). Select [Download](#).
3. Input your changes to the existing data or add new information into the blank template.
4. Select the [Upload](#) button from the [Upload Emergency Access Assignments](#) page.
5. Select [Choose File](#) to upload the completed XML file from your computer.
6. Select [Upload](#) and [Validate](#).
7. Verify the information was uploaded:
 - If the status is green, the records are validated. Select [Save](#) to save the data. The message will change to [Record Saved Successfully](#).
 - If the status is yellow, this is a warning message indicating some tabs do not have data. If this is what you intended, you can select [Save](#) and proceed.
 - If the status is red, this is an error. The XML file cannot be uploaded and needs to be corrected. Verify the format is still in the original format.
8. View the modified and uploaded data in the [Emergency Access Assignment](#) section, [Owners](#) link and the [Emergency Access Maintenance](#) section, [Firefighters](#) and [Controllers](#) link.

14 Schedule and Run Sync Jobs

Run the following sync jobs in SPRO.

Open SPRO, and go to ► *Governance, Risk and Compliance* ► *Access Control* ► *Synchronizations Jobs* ►.



- *Repository Object Synch* to synchronize the user, role, and profile data.
- *Firefighter Log Synch* to synchronize firefighter logs from target systems to the GRC repository.
- *EAM Master Data Synch* to synchronize master data from the target system to the GRC repository.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.

About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
 - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
 - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

© 2018 SAP SE or an SAP affiliate company. 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 SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company 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.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.