Access Control 5.3
Implementation Considerations for Superuser Privilege Management

ID-Based Firefighting versus Role-Based Firefighting

Applies to:

Access Control 5.3

Summary

GRC Access Control identifies and prevents access and authorization risks in cross-enterprise IT systems to prevent fraud and reduce the cost of continuous compliance and control. This document discusses the key features of Superuser Privilege Management. It also provides scenarios to assist project teams in deciding whether to implement role-based or ID-based firefighting.

Author: Erin Hughes

Created on: 01 November 2008

Version 1.1

Typographic Conventions

Type Style	Description
Example Text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation
Example text	Emphasized words or phrases in body text, graphic titles, and table titles
`Example text`	File and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example text`	User entry texts. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, `F2` or `ENTER`.

Icons

Icon	Description
⚠	Caution
💡	Note or Important
✿	Example
⬆	Recommendation or Tip

Table of Contents

1. Management Overview

The Superuser Privilege Management capability of SAP GRC Access Control allows users to execute tasks outside normal job functions to resolve emergency situations. It enables managers to systematically control access exceptions or emergency situations by extending permissions and creating an auditing layer to monitor and record user activities.

Superuser Privilege Management is an ABAP-based application with web-based reporting capabilities. It automates activities related to firefighting, including defining firefighter IDs/roles and firefighters, assigning owners and controllers, and logging all transactions executed during firefighting.

Superuser Privilege Management is available for ABAP-based SAP applications only.

2. Key Features and Benefits

Superuser Privilege Management:

- Monitors use of Firefighter access
- Automates activities related to firefighting, including defining firefighter IDs/roles and firefighters, assigning owners and controllers, and logging all transactions executed during firefighting.
- Tracks actions performed while privileged access is being used
- Provides detailed, concise audit reports

3. Key Stakeholders

Superuser Privilege Management focuses on the following audiences:

- Firefighters –Require elevated privileges within the system to occasionally perform functions outside of their normal job responsibilities.
- Firefighter ID Owners – Define the users who are allowed access to the Firefighter ID or Role, and the time period for which they maintain the privileged access.
- Firefighter Controllers – Monitor the use of Firefighter access and review the actions during Firefighter sessions. Controllers may receive notification of logon and transaction usage with proper system configuration.
- Superuser Privilege Management Administrators – Define the configuration parameters and perform the initial and ongoing maintenance of the capability.
- Auditors – Review detailed reports and audit trails available for actions performed while using the Firefighter ID or Role.

4. Implementation Preparation

Preparing for implementation includes the following steps.

1. Define and assess the need for privileged access monitoring in your environment.
    a. Do you currently have a process for granting privileged access in emergency situations?
    b. To what types of users is privileged access typically granted?
2. Define what specific access will be controlled via SPM. Remember that:
    a. SPM is a tool to track emergency access only.
    b. SPM should not be used for normal, day-to-day tasks, even if they are considered sensitive transactions. Risk Analysis and Remediation is the tool that can be used to monitor access to critical actions and permissions
3. Define and assess whether ID-based firefighting or role-based firefighting is preferred in your environment.
    a. Superuser Privilege Management can be configured for **either** ID-based firefighting **or** role-based firefighting.
    b. In Compliant User Provisioning 5.3, a request can be submitted for Superuser access only if ID-based firefighting is in place.
4. Define how Controllers will be notified of Firefighter activities.
    a. Controllers can be notified via e-mail, SAP mail, or by viewing the logs generated within the Superuser Privilege Management capability on a periodic basis.
    b. If your company would like for controllers to be notified of firefighting activities via e-mail, the e-mail address must be maintained within each user’s master record (transaction SU01). See SAP Note 1065048 for additional details.

If your company would like for controllers to view the logs generated within the Superuser Privilege Management capability on a periodic basis, a policy should be established to dictate how often the logs will be reviewed.

5. Recommended Implementation Scenarios and Use Cases

Prior to configuring Superuser Privilege Management for the use cases below, please refer to and complete the initial configuration in the backend ABAP system as detailed in the Access Control 5.3 Configuration Guide. These steps include, but are not limited to:

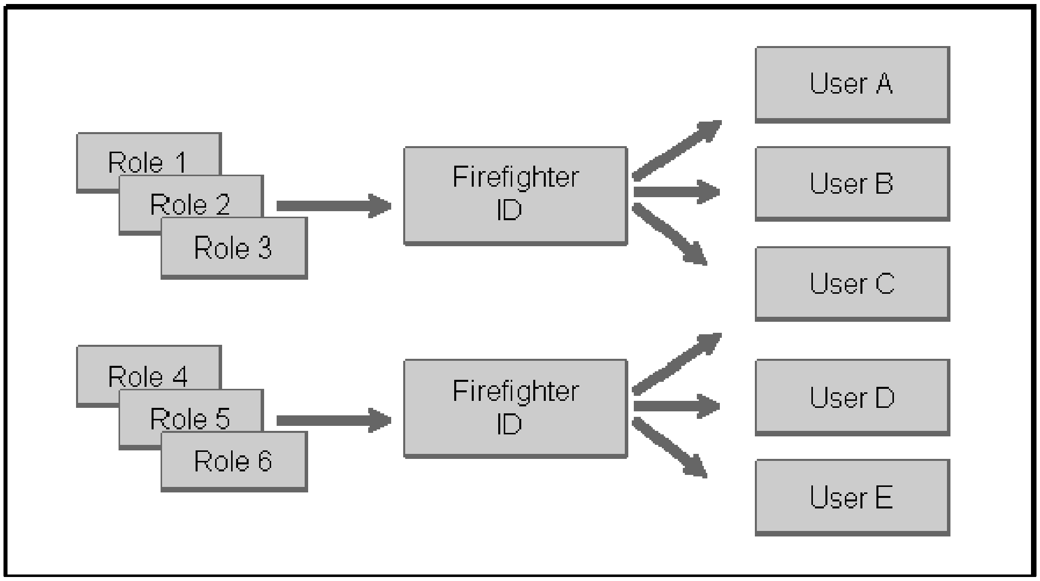
- □ Creating a Remote Function Call (RFC) destination for SPM.
- □ Defining the Background Job for Log Reports.
- □ Maintaining the basic Configuration Parameters, which include choosing whether to configure Firefighter IDs or Firefighter Roles.

The Access Control 5.3 Configuration Guide can be obtained from the Service Marketplace by selecting this link and then choosing SAP GRC Access Control 5.3. Please note that an SAP Service Marketplace ID and Password are required to access the Configuration Guide

5.1 ID-Based Firefighter Use Cases

5.1.1 Overall Concept

The concept behind the Firefighter ID use case is depicted below:



In this scenario:

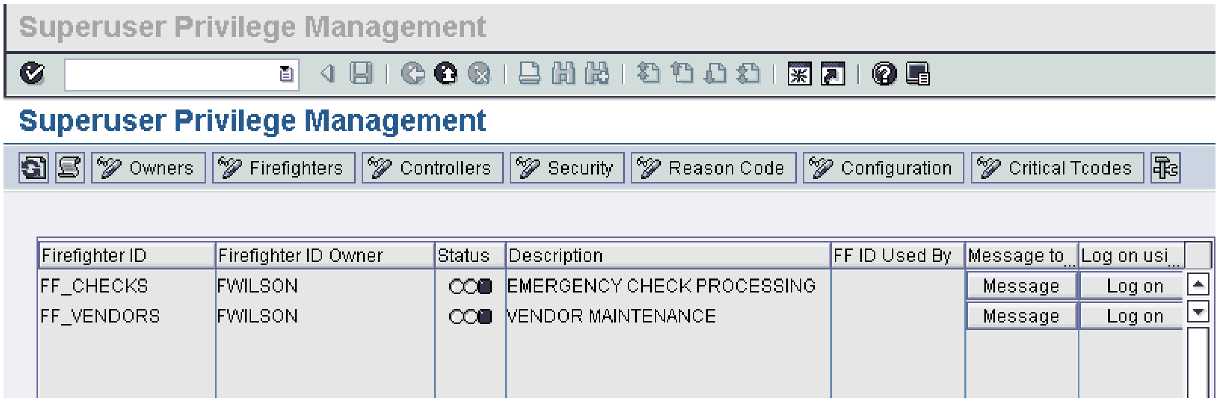
- ☐ Each Firefighter ID has its own User Master Record with roles assigned to it.
- ☐ An SAP End-user (Firefighter) executes a transaction code (*/n/virsa/vfat* in AC 5.3) and checks out an ID.
- ☐ Multiple users can check-out each Firefighter ID but only one user can have it checked out at any time.
- ☐ 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)
- ☐ Used widely by customers for granting emergency and elevated access.

5.1.2 User Interface

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

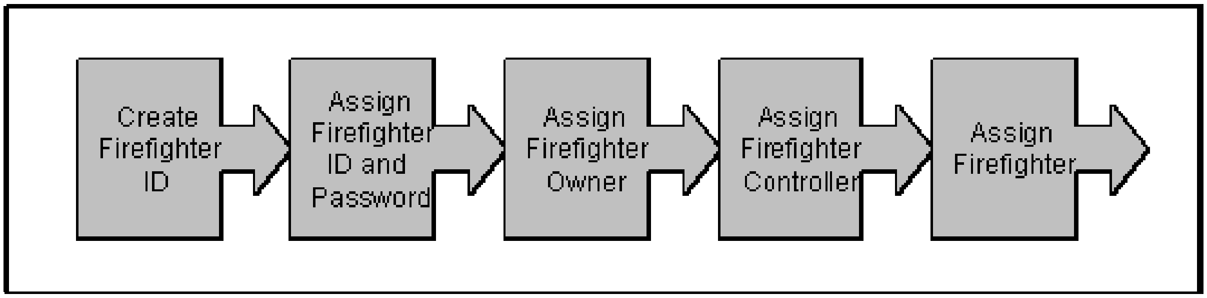


Firefighter ID	Firefighter ID Owner	Status	Description	FF ID Used By	Message to ...	Log on usi...
FF_CHECKS	FWILSON	○○●	EMERGENCY CHECK PROCESSING		Message	Log on
FF_VENDORS	FWILSON	○○●	VENDOR MAINTENANCE		Message	Log on

Superuser Privilege Management is delivered with ID-based firefighter as the default.

5.1.3 Process for Using ID-Based Firefighting

The process for then creating Firefighter IDs and assigning them to Firefighters (existing users) is as follows.


Create Firefighter ID
Assign Firefighter ID and Password
Assign Firefighter Owner
Assign Firefighter Controller
Assign Firefighter

Step 1: Create Firefighter ID:

- □ Create a user account in transaction *SU01* with user type "S" to be used as a Firefighter ID.
- □ A user exit should be implemented (see SAP Note 992200) to restrict users from logging in to the Firefighter ID through the SAP GUI. Users will only be able to access the Firefighter ID from Superuser Privilege Management after assigning the Firefighter ID and Password in the **Security** table in Step 2.

Step 2: Assign Firefighter ID and Password:

- □ Enter the Firefighter ID and defined password from transaction *SU01* in the **Security** table.
- □ Superuser Privilege Management will encrypt the password after these details are entered.
- □ A password will not be required by a user to access the Firefighter ID assigned to them.

Step 3: Assign Firefighter Owner:

- □ Assign an Owner to the Firefighter ID.

- Owners can assign Firefighting roles to Firefighters.
- Owners cannot assign Firefighter IDs to themselves.

Step 4: Assign Firefighter Controller:

□ Assign a Controller to the Firefighter ID. Controllers are responsible for reviewing the log report and can receive e-mail notification of firefighter ID use.

□ Firefighter ID Controllers can also be Firefighter ID Owners.

Step 5: Assign Firefighter:

□ Assign a Firefighter (existing SAP user ID) to the Firefighter ID. Firefighters can access the IDs assigned to them within the validity dates indicated in the **Firefighters** table, and as defined by Firefighter Owners.

For additional information on using Superuser Privilege Management, please refer to the *Access Control 5.3 Application Help* by selecting this link.

5.1.4 Reporting

Superuser Privilege Management contains detailed reports showing Firefighter ID activity. These reports can be viewed through:

□ Logs sent via e-mail or SAP mail to Firefighter ID Controllers.

□ The Superuser Privilege Management Toolbox.

□ The Web-based Superuser Privilege Management reporting interface.

There are seven different reports that display Firefighter ID usage in different contexts.

□ Log Summary Report: displays Firefighter usage by Firefighter ID, Firefighter ID Owner, or Firefighter.

□ Log Report: displays usage details from the Firefighter ID session.

□ Transaction Usage Report: displays transactions executed during the Firefighter ID session.

□ Reason / Activity Report: displays the reasons (based upon reason code) and expected activity as entered by the firefighter when initiating a session.

□ Invalid Firefighter IDs, Controllers or Owners Report: displays Firefighter IDs that have been defined in Superuser Privilege Management but are no longer valid because they have expired, have been deleted, or are locked.

□ SoD Violations Report: displays whether a Firefighter ID has executed transaction codes that would cause a SOD violation during a Firefighting session.

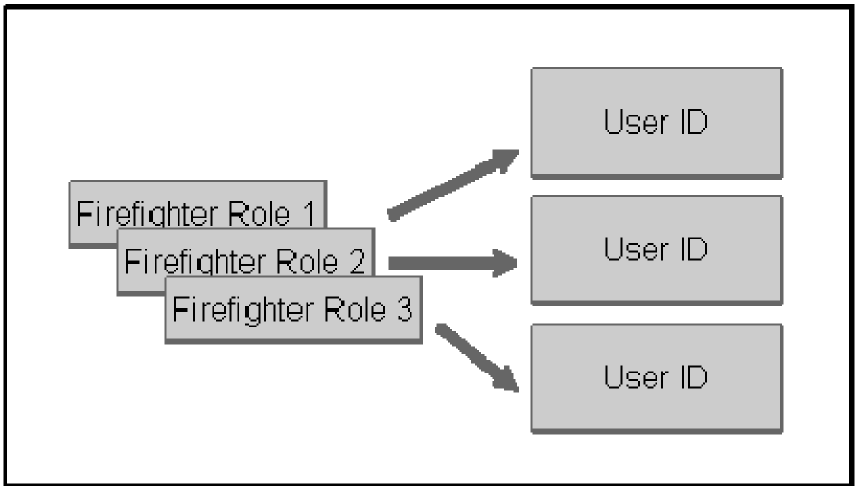
□ Configuration Change Log Report: displays the changes made to the Firefighter configuration table.

For additional information on ID-based firefighter reporting, please refer to the *Access Control 5.3 Application Help* by selecting this link.

5.2 Role-Based Firefighter Use Case

5.2.1 Overall Concept

The concept behind the Firefighter Role use case is depicted below:



In this scenario:

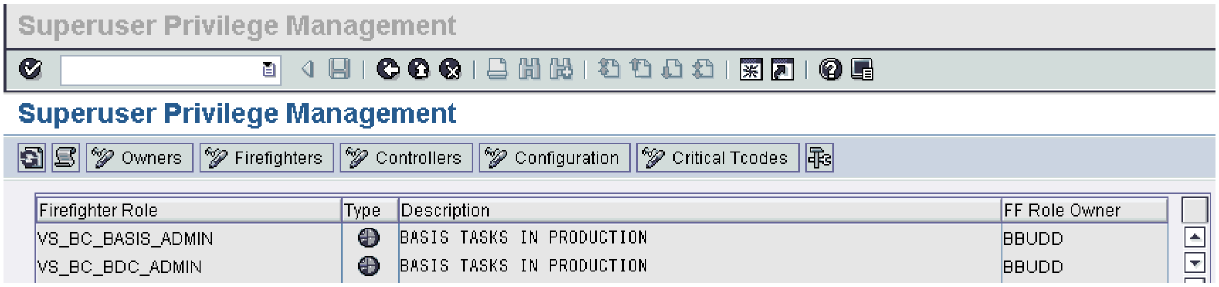
- □ Each Firefighter Role is assigned through Superuser Privilege Management to an SAP end-user.
- □ End-users do not check out a separate ID.
- □ Transaction and change history is logged with the user's own ID.
- □ The end-user is not aware when they are utilizing emergency / firefighter access.

Firefighter role-based usage:

- □ 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.

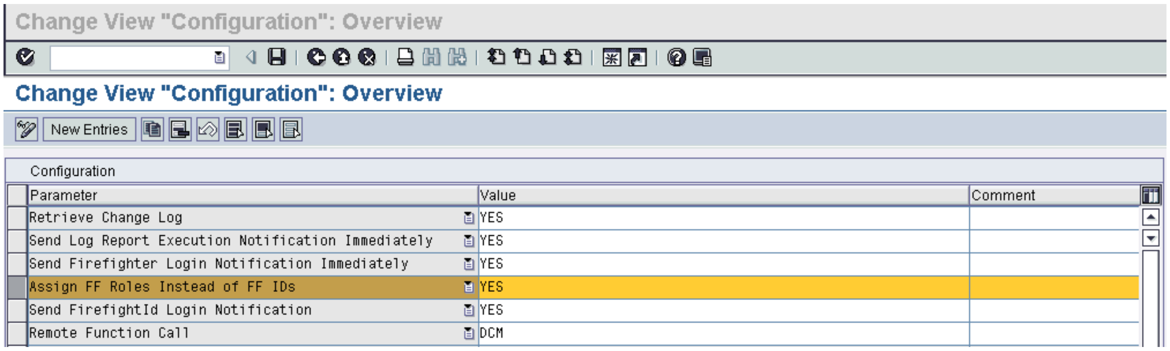
5.2.2 User Interface

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


Superuser Privilege Management
Superuser Privilege Management
Owners
Firefighters
Controllers
Configuration
Critical Tcodes

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

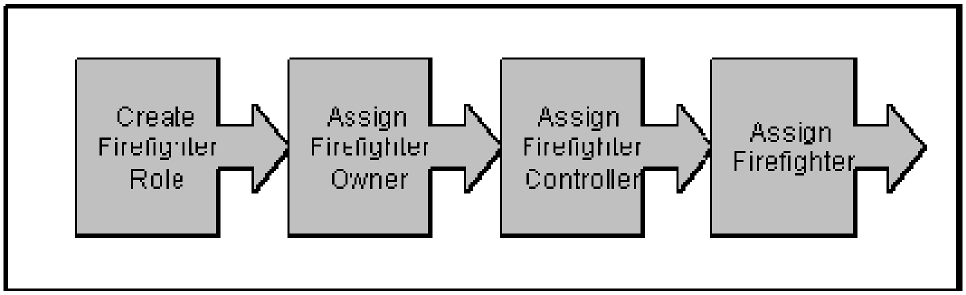
In order for this configuration to be displayed, the configuration parameter *Assign FF Roles Instead of FF IDs* must be set to *YES* as shown below.



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	

5.2.3 Process for Using Role-Based Firefighting

The process for then creating Firefighter Roles and assigning them to Firefighters (existing users) is as follows:



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.
  - o Owners can assign Firefighting roles to Firefighters.
  - o 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.

For additional information on using Superuser Privilege Management, please refer to the *Access Control 5.3 Application Help* by selecting this link.

5.2.4 Reporting

Superuser Privilege Management contains detailed reports showing Firefighter ID activity. These reports can be viewed through:

- □ Logs sent via e-mail or SAP mail to Firefighter Role Controllers.
- □ The Superuser Privilege Management Toolbox.
- □ The Web-based Superuser Privilege Management reporting interface.

There are two different reports that display Firefighter Role usage.

- □ Log Report: displays usage details from the Firefighter Role session
- □ Configuration Change Log Report: displays the changes made to the Firefighter configuration

For additional information on Role-based firefighter reporting, please refer to the *Access Control 5.3 Application Help* by clicking on this link.

6. Related Content

Getting Started with GRC Access Control

Preferred Practices for GRC Access Control

GRC Forum

7. Copyright

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

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

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

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

SAP NetWeaver “How-to” Guides are intended to simplify the product implementation. While specific product features and procedures typically are explained in a practical business context, it is not implied that those features and procedures are the only approach in solving a specific business problem using SAP NetWeaver. Should you wish to receive additional information, clarification or support, please refer to SAP Consulting.

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

Disclaimer

Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressively prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP’s Support Services and may not be modified or altered in any way.