# Content

1 SAP Access Control ............................................................ 7

2 Overview of Access Control ................................................... 8

3 Cross-Component Topics ......................................................... 10
  3.1 Profiles and Logons .......................................................... 10
  End User Logon .............................................................. 10
  Administrator Logon ......................................................... 12
  Maintaining Your Profile ..................................................... 12
  3.2 Integration ................................................................. 13
  Integration of Shared Data (Data Model) .................................. 14
  Integration with Process Control and Risk Management ................. 14
  3.3 Custom Fields ............................................................. 15
  3.4 Navigation ................................................................. 15
  My Home Work Center ...................................................... 16
  Setup Work Center ........................................................... 27
  Access Management Work Center .......................................... 28
  Reports and Analytics ......................................................... 28
  3.5 Special Privileges .......................................................... 29
  3.6 Background Jobs .......................................................... 30
  Background Scheduler ........................................................ 30
  Scheduling Background Jobs ................................................ 31

4 Managing Access Requests .................................................... 32
  4.1 Access Request Creation .................................................. 33
  Simplified Access Requests .................................................. 33
  Creating Access Requests .................................................... 34
  Analyzing Risks When Submitting Access Requests ...................... 37
  Template Roles ............................................................... 40
  Creating Access Requests Based on Model Users ......................... 42
  Changing User Details ........................................................ 43
  Copying Requests ............................................................. 44
  Creating Organizational Assignment Requests ........................... 44

  4.2 Access Request Approval .................................................. 45
  Reviewing and Approving Access Requests ................................ 46
  Simplified Work Inbox ...................................................... 47
  Analyzing Risks When Approving Access Requests ...................... 48
  Mitigating Risks .............................................................. 50
Maintaining Tasks and Authorizations for Request Approvers ............................................. 51

4.3 Access Request Administration ....................................................................................... 54
Creating and Managing Templates ......................................................................................... 55
Searching Requests ........................................................................................................... 56
Viewing Provisioning Logs .................................................................................................. 57
Unlocking and Deleting Password Self-Service Accounts ............................................... 58
Approver Delegation ........................................................................................................... 59
Creating Access Requests Based on Templates ............................................................... 59

5  Managing Access Risks ........................................................................................................ 61
5.1 Mitigating Controls ........................................................................................................... 62
Searching Mitigating Controls ............................................................................................ 63
5.2 Rule Setup ....................................................................................................................... 63
Exception Access Rules ......................................................................................................... 64
Access Rule Maintenance ..................................................................................................... 74
Critical Access Rules .......................................................................................................... 89
5.3 Access Risk Analysis ........................................................................................................ 92
User Level Access Risk Analysis .......................................................................................... 93
User Level Simulation ........................................................................................................... 97
Role Level Access Risk Analysis ......................................................................................... 99
Role Level Simulation .......................................................................................................... 100
Profile Level Access Risk Analysis ...................................................................................... 102
Profile Level Simulation ....................................................................................................... 104
HR Objects Access Risk Analysis ......................................................................................... 105
HR Objects Simulation ......................................................................................................... 106
5.4 Mitigated Access ............................................................................................................... 108
Mitigated Users .................................................................................................................... 109
Mitigated User for Organization Rules ............................................................................... 110
Mitigated Roles .................................................................................................................... 111
Mitigated Profiles ................................................................................................................ 112
HR Objects Mitigation ......................................................................................................... 113
Mitigated Role for Organization Rules ................................................................................. 114
5.5 Analyzing Risks When Approving Access Requests ................................................... 115
5.6 Analyzing Risks When Submitting Access Requests ..................................................... 117
5.7 Analyzing Access Risks for Role Maintenance ............................................................. 118
5.8 Mitigating Risks ............................................................................................................... 120
5.9 Alerts ................................................................................................................................ 121
Searching Alerts .................................................................................................................. 122
Cleared Alerts ....................................................................................................................... 123
5.10 Background Jobs ............................................................................................................. 126
Background Scheduler .......................................................................................................... 127
9 Reports and Analytics .......................................................... 205

9.1 Access Dashboards. .......................................................... 205
   Access Provisioning Dashboard. ......................................... 206
   Access Requests Dashboard. ........................................... 207
   Access Rule Library Dashboard. ...................................... 208
   Alerts Dashboard. ....................................................... 209
   Mitigating Control Library Dashboard. ............................... 209
   Risk Violations Dashboard. ............................................ 210
   Role Analysis Dashboard. .............................................. 213
   Role Library Dashboard. ................................................. 214
   Service Level for Access Requests Dashboard. .................... 214
   User Analysis Dashboard. .............................................. 215
   Violations Comparisons Dashboard. ................................ 217
   Risk Violation in Access Request Dashboard. ..................... 217

9.2 Access Risk Analysis Reports. ........................................... 218
   Access Rule Summary Report. ......................................... 219
   Access Rule Detail Report. ............................................ 219
   Mitigated Object Report. ............................................... 220
   HR Object Risk Violation Report. ..................................... 221
   Mitigation Control Report. ............................................ 222
   Profile Risk Violation Report. ......................................... 223
   Role Risk Violation Report. ............................................ 225
   User Risk Violation Report. ............................................ 226

9.3 Access Request Reports. .................................................. 227
   Approver Delegation Report. ......................................... 228
   Requests by PD/Structural Profiles. ................................ 228
   Requests by Roles and Role Assignment Approvers Report. .... 229
   Requests with Conflicts and Mitigations Report. ................. 230
   Service Level for Requests Report. ................................ 231
   SoD Review History Report. .......................................... 232
   User Access Review History Report. ................................ 233
   User Review Status Report. .......................................... 234

9.4 Role Management Reports. .............................................. 235
   Compare Action in Menu and Authorization Report. ............. 235
   Compare User Roles Report. .......................................... 236
   List Actions in Roles Report. ......................................... 237
   Master to Derived Role Relationship Report. ...................... 237
   PFCG Change History Report. ........................................ 238
   Role by Date of Generation Report. ................................ 239
   Single to Composite Role Relationship Report. ................... 240
   User to Role Relationship Report. ................................ 241
9.5 Security Reports. ............................................................ 242
  Action Usage by User, Role, and Profile Report. .................. 242
  Count Authorization for Users Report. ............................. 243
  Count Authorization in Roles Report. ............................. 244
  List Expired and Expiring Roles for Users Report. .............. 244

9.6 Audit Reports. .................................................................. 245
  Change Log Report. .......................................................... 245
  Embedded Action Calls in Programs of SAP Systems Report. 246
  List Actions in Roles But Not in Rules Report. .................. 247
  List Permissions in Roles But Not in Rules Report. .............. 248

9.7 Emergency Access Management Reports. .......................... 248
  Consolidated Log Report. ................................................. 249
  Firefighter Log Summary Report. ....................................... 250
  Invalid Emergency Access Report. ................................. 251
  Reason Code and Activity Report. ..................................... 252
  SoD Conflict Report for Firefighter IDs. ............................. 252
  Transaction Log and Session Details Report. ...................... 253

9.8 Risk Terminator Log Report. ............................................ 254
1 SAP Access Control

Product Information

Table 1:

<table>
<thead>
<tr>
<th>Product</th>
<th>SAP Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>10.1</td>
</tr>
<tr>
<td>Based On</td>
<td>SAP NetWeaver 7.40 SP4</td>
</tr>
<tr>
<td>Documentation Published</td>
<td>November 2013</td>
</tr>
</tbody>
</table>

Use

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.
2 Overview of Access Control

SAP Access Control is an enterprise software application that allows organizations to manage their access governance policies and to monitor for compliance.

SAP Access Control is an add-on to SAP NetWeaver, and works with SAP applications and non-SAP applications, such as SAP Finance, SAP Sales and Distribution, Oracle, and JDE.

The application provides a framework for managing application authorization functions such as:

**Access Requests (ARQ)** – You can implement your company’s policies for creating and maintaining access requests in ARQ. Users can create requests to access systems and applications. Approvers can review the requests, perform analysis for user access and Segregation of Duties (SoD) risks, and then approve, reject, or modify the requests.

**Access Risk Analysis (ARA)** – You can implement your company’s policies for SoD and user access risk in ARA. Security analysts and business process owners run reports to determine if violations of SoD or user access policies have occurred. They can identify the root cause of the violations and remediate the risks.

Compliance persons can use this function to monitor compliance with company policies.

**Business Role Management (BRM)** – In an SAP landscape, users’ authorizations to applications are managed through the use of roles. Role designers, role owners, and security analysts can use BRM to maintain roles and analyze them for violations of company policies.

**Emergency Access Management (EAM)** – You can implement your company’s policies for managing emergency access in EAM. 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 policies.

**Periodic Reviews of User Access and Segregation of Duties (SoD)** – You can use the application to carry out your company’s policies on periodic reviews for compliance. Security and business process owners identify policies that require periodic reviews and define review processes. Reviewers perform the reviews and then security and business process owners determine if corrective actions are required.
Figure 1: Workflow according to Access Control users

Access Control

- Access risk analysis and management
- Access request management
- Compliance certification review
- Role management
- Role mining
- Super user access management
- Access control repository

Application Users
Security or IT Administrator

Configuration User

Web Dynpro ABAP via Web Browser

Customizing via SAP GUI

FIN

HR

CRM
3 Cross-Component Topics

SAP Access Control covers several different authorization functions such as Access Requests (ARQ), Access Risk Analysis (ARA), Business Role Management (BRM), Emergency Access Management (EAM), and Periodic Reviews of User Access and Segregation of Duties (SoD). This section of the application help includes topics that apply to more than one area including the following:

- Profiles and Logons [page 10]
- Integration [page 13]
- Custom Fields [page 15]
- Navigation [page 15]
- Special Privileges [page 29]

3.1 Profiles and Logons

Use

The topics in this section address how to manage both end user and administrator logons as well as how to manage your user profile.

More Information

End User Logon [page 10]
Administrator Logon [page 12]
Maintaining Your Profile [page 12]

3.1.1 End User Logon

Use

You can use the End User Logon screen to perform non-administrator provisioning tasks such as creating access requests, managing your password, and so on.

To access the end user logon screen, use the link provided by your administrator. For more information see, Managing the End User Logon [page 11].
Prerequisites

You have enabled the end user logon in the Customizing activity **Activate End User Logon**, under **Governance, Risk, and Compliance** ➤ **Access Control** ➤ **User Provisioning**.

More Information

[Administrator Logon](#) [page 12]

3.1.1.1 Managing the End User Logon

Use

The application allows you to enable and disable the following end user logon features:

- End user logon
- Links displayed on the **End User Logon** screen
- Requirement for users to enter their password

Procedure

**To enable and disable end user logon, and set the links displayed on the End User Logon screen:**

1. Log on to the access control backend, and then start transaction **SPRO**.
2. Open the Customizing activity **Activate End User Logon**, under **Governance, Risk, and Compliance** ➤ **Access Control** ➤ **User Provisioning**.
3. Maintain the settings as needed, and save the entry.

**To enable and disable the password requirement:**

1. Log on to the access control backend, and then start transaction **SPRO**.
2. Open the Customizing activity **Maintain Data Sources Configuration**, under **Governance, Risk, and Compliance** ➤ **Access Control**.
3. Double-click **End User Verification**.
4. In the **Authentication** field, choose **Yes** or **No** as needed, and then save your entry.

**More Information**

### 3.1.2 Administrator Logon

**Use**

You use the administrator logon to perform administrator tasks such as managing access requests, managing access risks, maintaining roles, and performing emergency access and firefighter tasks.

The application provides two options for administrator logon:

- **NetWeaver Business Client (NWBC)**
  
  To access the NWBC logon, use the SAP GUI to log onto the Access Control system, and start the NWBC transaction.

- **Portal**
  
  To access the Portal logon, use the link provided by the administrator.

**More Information**

End User Logon [page 10]

### 3.1.3 Maintaining Your Profile

**Context**

On the **My Profile** screen, you can do the following:

- View the status of your access
  
  You can filter the list by the following statuses: **Expiring**, **Expired**, **Active**, **Inactive**, **All**.

- View the validity dates for your access

- View the type of access in the **Item** column; for example, derived role, single role, profile, or system
• View the name of the system
• View the assignment
  If the access type is **Role**, the **Assignment** field displays the name of the role. If the access type is **System**, the **Assignment** field displays the name of the system.
• View your profile information, such as identity, communication, organization, and location

  **Note**
  In this section, the information is read-only. This information is maintained in the user data source system.

• Create or change access requests for yourself or another user

**Procedure**

1. From **My Home**, choose the **My Profile** quick link.

  **Note**
  If you are using the **End User Logon**, on the **End User Home** screen, choose the **My Profile** quick link.

2. To filter the list by status, select the **Status** dropdown list, and then choose the relevant status.
3. To create or change the access request for an existing assignment, in the **Select** (first) column, select the checkbox for the relevant items, and then choose **Request Access**.

  To create an access request for a new assignment or one that is not on your list, choose **Request Access** without selecting any items.

**3.2 Integration**

**Use**

**Important Integration Information**

The processes and user interfaces of the following products are linked since they have interconnected features:

• SAP Access Control
• SAP Process Control
• SAP Risk Management

You can access the features and documentation of these products after licensing and installing the relevant products.

• SAP Access Control 10.1 June 2013 SAP NetWeaver 7.40 Support Package 02
• SAP Process Control 10.1, June 2013 SAP NetWeaver 7.40 Support Package 02
• SAP Risk Management 10.1, June 2013 SAP NetWeaver 7.40 Support Package 02
More Information

Integration of Shared Data (Data Model) [page 14]
Integration with Process Control and Risk Management [page 14]

3.2.1 Integration of Shared Data (Data Model)

Use

SAP Access Control, SAP Process Control, and SAP Risk Management can share the following data:

- Organizations can optionally be shared between SAP Access Control, SAP Process Control, and SAP Risk Management. Some organization data may be shared and other data may be specific to a single application. The access to this data is controlled by the user’s authorizations.
- Controls may be shared between SAP Access Control and SAP Process Control. There is application-specific information for SAP Access Control and SAP Process Control applications. The access to this data is controlled by the user’s authorizations.
- You can configure UI properties of attributes (fields) to be application-specific.

More Information


3.2.2 Integration with Process Control and Risk Management

Use

The SAP Access Control, SAP Process Control, and SAP Risk Management applications share capabilities and menu areas related to .

Prerequisites

- You have configured the GRC application through the Customizing activities available through the SPRO transaction.
- You have started the GRC application.
Features

SAP Access Control and SAP Process Control have an integration point that enables you to initiate SAP Access Control risk analysis from SAP Process Control.

3.3 Custom Fields

Use

Custom fields are any fields that you choose to add to the application. They are also called user-defined fields. SAP delivers a standard set of fields with the application. Your company may require fields that are not part of the delivered set.

You can maintain your user-defined fields in the Customizing activity User-Defined Fields, under Governance, Risk, and Compliance General Settings.

Features

The application has the following features for maintaining user-defined fields:

- Adding HR user-defined fields
- Adding non-HR user-defined fields
- Verifying user-defined fields
- Maintaining user-defined fields in Web UI
- Including user-defined fields in online reporting

3.4 Navigation

The main features of the application are grouped in work centers. The work centers appear at the top of the main screens. They are organized to provide easy access to application activities and contain menu groups and links to further activities.

The main delivered work centers are:

- My Home
- Setup
- Access Management
- Reports and Analytics
3.4.1 My Home Work Center

Use

The My Home work center provides a central location to view and act on your assigned tasks, and accessible objects.

The My Home work center contains the following sections:

- Work Inbox
  Here, you can view all GRC workflow tasks assigned to you.

- My Delegation
  Here, you can delegate temporary approval of your workflow tasks to another person.

- Application Help
  Here, you can access Application Help for GRC Applications.

- My Profile
  Here, you can create and track your access requests, view your access assignments, and manage your security settings.

**Note**

The My Home work center is shared by the Access Control, Process Control, and Risk Management products in the GRC 10.0 application. The menu groups and quick links available on the screen are determined by the applications you have licensed. The content in this topic covers the functions specific to Access Control. If you have licensed additional products, such as Process Control or Risk Management, refer to the relevant topics below for the application-specific functions.

**More Information**

- Work Inbox [page 17]
- Delegating Your Approval Tasks [page 18]
- My Profile [page 18]
3.4.1.1  Work Inbox

Use

The Work Inbox lists the tasks you need to process using GRC applications.

Activities

To process a task, choose a hyperlink in the table. The appropriate workflow window appears. Process the task as required.

The STANDARDVIEW displays the columns.

To change the displayed columns, choose Settings, maintain the columns as required, and save the view.

The new view appears in the View dropdown list.

3.4.1.2  Simplified Work Inbox

Use

You use the Simplified Work Inbox to view the access requests that require approval.

Note

You can also use the regular work inbox to process access requests. For more information, see Work Inbox [page 17].

Procedure

Use the procedure below to find specific requests:

1. Using the slider bar or the date input boxes, select a specific date or a date range for the requests that you want to process.
2. Optionally, select a category such as New Account to narrow your search.
3. Optionally, select a number of results to show per page.
4. Optionally, select a sort criterion such as Request Number or Requested By.
   The system retrieves all requests that match your criteria.
5. Click a request number to drill into its details. Optionally, click the flag icon to mark a request for follow up.
### 3.4.1.3 Delegating Your Approval Tasks

#### Use

On the Approver Delegation screen, you can assign your task of approving a request to another user.

#### Procedure

2. Choose Delegate to select a user. The Delegate Approver Details screen appears.
3. In the relevant fields, select the ID for the approver, the validity dates, and the status of the approver.
4. Choose Save.

For information about an administrator’s ability to reassign approval tasks to another user, see .

### 3.4.1.4 My Profile

#### Use

You can use My Profile to create and track your access requests, view your access assignments, and manage your security settings.

#### Activities

- Maintaining your profile
- Viewing your request status
- Resetting user passwords
- Changing user names
- Registering security questions
3.4.1.4.1 Maintaining Your Profile

Context

On the My Profile screen, you can do the following:

- View the status of your access
  You can filter the list by the following statuses: Expiring, Expired, Active, Inactive, All.
- View the validity dates for your access
- View the type of access in the Item column; for example, derived role, single role, profile, or system
- View the name of the system
- View the assignment
  If the access type is Role, the Assignment field displays the name of the role. If the access type is System, the Assignment field displays the name of the system.
- View your profile information, such as identity, communication, organization, and location

Note
In this section, the information is read-only. This information is maintained in the user data source system.

- Create or change access requests for yourself or another user

Procedure

1. From My Home, choose the My Profile quick link.

   Note
   If you are using the End User Logon, on the End User Home screen, choose the My Profile quick link.

2. To filter the list by status, select the Status dropdown list, and then choose the relevant status.

3. To create or change the access request for an existing assignment, in the Select (first) column, select the checkbox for the relevant items, and then choose Request Access.

   To create an access request for a new assignment or one that is not on your list, choose Request Access without selecting any items.
3.4.1.4.2 Viewing Your Request Status

Context

You can use the Request Status quick link to view the status for access requests you created. The requests may be for you or on another person’s behalf.

Procedure

1. From the My Home screen, under the My Profile menu group, choose Request Status.

   ![Note]
   You can also access this function as follows: from the Access Management work group, under the Access Request menu group, choose Request Status.

   The Request Status screen appears.

2. To sort your requests by status, in the Request Status section, choose from the available statuses: Approved, Rejected, Decision Pending, Hold.

3. To view workflow information, select a request, and then choose Instance Status.

   The MSMP Instance Status screen appears, and displays information about the request, such as Created By, Creation Date, Path Status, Approvers of Selected Path, and Audit Log.

   ![Note]
   The information on this screen is read-only and cannot be modified.

4. To open an access request, select the request and open it. Depending on the status of the request, you can edit the request. For example, you have a request to Create a Mitigation Assignment. You can create a control for it. However, if the request is pending, then the buttons are disabled.

5. To view logs, select the request, and then choose View Provisioning Logs.
3.4.1.4.3  Resetting User Passwords

Prerequisites

- The administrator has maintained the password self–service option in the Customizing activity Maintain Password Self Service, under Governance, Risk, and Compliance > Access Control > User Provisioning.
- You have registered your security questions.

Context

On the Reset Password screen, you can maintain your user passwords for specific systems.

Procedure

1. From the My Home screen, choose the Reset Password quick link to open the Reset Password screen.
   
   **Note**

   If you are using the End User Logon, on the End User Home screen, choose the Password Self Service quick link.

2. Answer the security questions, and then choose Next.
   
   **Note**

   The administrator can set the requirement that a minimum number of questions must be answered. For example, require that answers to a minimum of three security questions must be provided to allow resetting of passwords. For more information, see the Customizing activity Maintain Password Self Service, under Governance, Risk, and Compliance > Access Control > User Provisioning.

3. Choose Add to select the systems for which you want to change your user password.

   The screen displays all the systems for which you have a valid account. Select the relevant systems and choose OK.

4. Choose Submit and then close the screen.

   The application sends the link to a new temporary password to you in an e-mail. The application provides a separate link for each system. You can use the temporary password to log on to the system and change the password.

   **Note**

   For security purposes, the link to the temporary password can be used only once. You can specify the period of time (in seconds) that the password is visible. You maintain the setting in the Customizing activity.
3.4.1.4.4 Changing User Names

Context

On the Name Change screen, you can change your user name for specific systems.

Procedure

1. On the My Home screen, choose the Name Change quick link.

   i Note
   If you are using the End User Logon, choose the Name Change quick link on the End User Home screen.

2. Answer the security questions, and choose Next.
3. In the respective fields, enter the old user ID and the new user ID, and then choose Next.
4. Choose Add, and select the systems for which you want to change your user name.
5. Under the Password column, enter the user password for each system.
6. Choose Submit.

3.4.1.4.5 Registering Security Questions

Prerequisites

The administrator has maintained the password self-service option in the Customizing activity Maintain Password Self Service, under Governance, Risk, and Compliance Access Control User Provisioning.
Context

On the Security Questions screen, you can maintain the security questions used to confirm your identity when resetting your user passwords.

Procedure

1. From the My Home screen, choose the Register Security Questions quick link to open the Security Questions screen.

   i Note
   If you are using the End User Logon, on the End User Home screen, choose the Register Self Service Questions quick link.

2. Choose Add to create your security questions.
   ○ To add your own questions, select User Defined Questions.
   ○ To add questions that are provided by the administrator, select Admin Defined Questions.

3. To disable a security question and keep it on your list, choose Status, and select Inactive.

4. Maintain the security questions as required, and then choose Save and Close.

3.4.1.4.6 Creating Access Requests

Use

On the Access Request screen, you can create access requests for yourself, for another user, or for multiple users.

Prerequisites

The administrator has completed the activities for the Customizing activity Maintain Provisioning Settings, under Governance, Risk, and Compliance > Access Control > User Provisioning.

Procedure

1. From the Access Management work center, under the Access Request menu group, choose Access Request Creation.
Note

- If you are using the End User logon, on the *End User Home* screen, choose *Access Request*.

2. Under the *Request Details* area, enter the required information in the fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Type</td>
<td>Examples: <em>New Account</em>, <em>Change Account</em>, <em>Superuser Access</em>, and so on. You can maintain the list of available request types in the Customizing activity <em>Define Request Types</em>, under <em>Governance, Risk, and Compliance</em> ➔ <em>Access Control</em> ➔ <em>User Provisioning</em>.</td>
</tr>
<tr>
<td>Request For</td>
<td>Choose to create a request for the following:</td>
</tr>
<tr>
<td></td>
<td>- <em>Self</em>, to create a request for yourself.</td>
</tr>
<tr>
<td></td>
<td>The <em>User</em> field is inactive and displays your user ID.</td>
</tr>
<tr>
<td></td>
<td>- <em>Other</em>, to create a request on behalf of another user.</td>
</tr>
<tr>
<td></td>
<td>The <em>User</em> field is active, and allows you to select the name of the user.</td>
</tr>
<tr>
<td></td>
<td>- <em>Multiple</em>, to create a request for multiple users.</td>
</tr>
<tr>
<td></td>
<td>The application displays the <em>Users</em> tab page, and allows you to select multiple users. Choose <em>Add</em> to add each user manually, or choose <em>Import</em> to use a template to import multiple users.</td>
</tr>
<tr>
<td>Priority</td>
<td>Examples: <em>High</em>, <em>Low</em>, and so on. You can maintain the list of available priorities in the Customizing activity <em>Maintain Priority Configurations</em>, under <em>Governance, Risk, and Compliance</em> ➔ <em>Access Control</em> ➔ <em>User Provisioning</em>.</td>
</tr>
<tr>
<td>Business Process</td>
<td>Examples: <em>HR and Payroll</em>, <em>Finance</em>, and so on. You can maintain the list of available business processes in the Customizing activity <em>Maintain Business Processes and Subprocesses</em>, under <em>Governance, Risk, and Compliance</em> ➔ <em>Access Control</em>.</td>
</tr>
<tr>
<td>Functional Area</td>
<td>Examples: <em>Sales</em>, <em>Human Resources</em>, and so on. You can maintain the list of available functional areas in the Customizing activity <em>Maintain Functional Areas</em>, under <em>Governance, Risk, and Compliance</em> ➔ <em>Access Control</em> ➔ <em>Role Management</em>.</td>
</tr>
</tbody>
</table>

3. On the *User Access* tab page, choose from the following options to select the roles that you want to be assigned, and the systems for which you are requesting access:

- Choose *Add* and select from the following:
  - Role
    - Click *Add* and then click *Role* to search for the roles that you want. After the system presents the results of your search, you can click a retrieved role name to access further details about the role such as the actions that are valid for a composite role.
If you select a **Business Role**, you can choose which environment you wish to provision. The environment options are: **All, Development, Production, and Testing**. This choice is only available to you if you set the Access Control configuration parameter **3026 (Enable Business Role Provisioning based on Environment)** to **Yes**. The default value for this parameter is **No**.

**Note**

For **Role Search**, the application allows you (requires administrator authorization) to configure the search criteria fields. You can add custom fields and configure their attributes. For example, you can set the default values and set whether the field is mandatory. You can configure the fields in Customizing for **Maintain Custom Field Attributes for Role Search Personalization** under **Governance, Risk, and Compliance ➤ Access Control ➤ User Provisioning**.

- System
- Firefighter ID
- Firefighter Role

**Note**

When requesting a Firefighter ID or a Firefighter Role, you can filter the search using **System** and **Action Code**. If you use **Action Code**, you must also specify the **System**. For both Firefighter ID and Firefighter Role requests, the owner displays in the **Assignment Approver** column.

- Choose **Existing Assignments** to select from the list of roles and systems currently assigned to the user. If the **Request For** field is set to **Multiple**, the application disables this button.

4. In the **Provisioning Actions** column, select the appropriate action, such as **Create User, Assign** (role), and so on. You can set the provisioning actions available in the drop-down list in the Customizing activity **Define Request Type**, under **Governance, Risk, and Compliance ➤ Access Control ➤ User Provisioning**.

5. In the **Comments** column, choose **Add Comment** and enter information about the request. You can set whether comments are mandatory in the Customizing activity **Maintain Configuration Settings**, under **Governance, Risk, and Compliance ➤ Access Control ➤ User Provisioning**. For the relevant columns, set the following values:
   - **Parameter Group**: **Access Request Role Selection**
   - **Parameter ID**: 2036
   - **Parameter Value**: **Yes** or **No**, as needed

6. On the **User Details** tab page, enter all required information.

7. Choose **Simulation**, if you want to run a risk analysis of the requested roles and system access before submitting the request.

8. Choose **Submit**.
The application sends an e-mail notification to the approver. You can configure e-mail in the Customizing activity **Maintain MSMP Workflows**, under **Governance, Risk, and Compliance** > **Access Control** > **Workflow for Access Control**. In the **Maintain Path** phase, under the **Maintain Stages** area, choose **Notification Settings**.

Approvers can also access and process the request from their **Work Inbox**.

End users can view the status of the request from the quick link.

**More Information**

Viewing Your Request Status [page 20]
Changing User Details [page 43]
Reviewing and Approving Access Requests [page 46]
Analyzing Risks When Submitting Access Requests [page 37]

### 3.4.1.4.7 Create Request-Simplified

**Context**

A simpler user interface allows you to request roles for addition, removal or extension.

**Procedure**

1. To request access for yourself or for others, enter the following information:

   **Note**
   An asterisk (*) on the screen designates a required field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Reason</td>
<td>Either select a reason from the dropdown list or select Others and write your reason in the box underneath.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Information</strong></td>
<td>The system fills in your information when the request for yourself. If the request is for others, you can search for user information by using the value help in the User ID field.</td>
</tr>
<tr>
<td><strong>Select Roles for Addition</strong></td>
<td>You can search for roles by role attributes such as name, system, Tcode, or key word. Wildcards such as * are valid. You can also use the Advanced Search for more granular search. You may use the filters on the left of the screen to further refine your search results. You can view the list of Tcodes defined in the role by clicking on the role name. You can further drill-down to get more information about the role by clicking on the Show More button in the pop-up screen.</td>
</tr>
<tr>
<td><strong>Select Roles for Removal</strong></td>
<td>Select this option to remove the role assignments from this user.</td>
</tr>
<tr>
<td><strong>Select Roles for Extension</strong></td>
<td>Select this option to extend the validity dates of the role.</td>
</tr>
</tbody>
</table>

2. When requesting access for other users, you can optionally run risk analysis by clicking on the Risk Analysis in the side panel.

   Optionally, you can view the system-added roles by clicking on the System Added Roles side panel.

3. Optionally, you can save the request as a draft to work on later.

4. When your request is complete, submit it for approval.

### 3.4.2 Setup Work Center

The Setup work center provides a central location to perform one time or infrequent setup activities such as creating access rule sets, creating mitigating rules, and so on.

The Setup work center contains the following sections:

- Access Rule Maintenance [page 74]
- Critical Access Rules [page 89]
- Using Emergency Access Management [page 164]
- Exception Access Rules [page 64]
- Generated Rules [page 71]
- Mitigating Controls [page 62]
3.4.3 Access Management Work Center

The Access Management work center provides a central location to perform tasks such as monitoring, testing, and enforcing access and authorization controls.

The Access Management work center contains the following sections:

- Access Risk Analysis [page 92]
- Mitigated Access [page 108]
- Access Request Administration [page 54]
- Access Request Creation [page 33]
- Role Management Considerations [page 129]
- Compliance Certification Reviews [page 193]
- Role Mining [page 152]
- Role Mass Maintenance [page 155]
- Alerts [page 121]
- Scheduling Background Jobs [page 31]

Note

The Access Management work center is shared by the Access Control, Process Control, and Risk Management products in the GRC Application. The menu groups and quick links available on the screen are determined by the applications you have licensed.

3.4.4 Reports and Analytics

The Reports and Analytics work center provides a central location to display reports and dashboards for Access Control information, such as alerts, user analysis, audit reports, and so on.

Note

The Reports and Analytics work center is shared by the Access Control, Process Control, and Risk Management products in the GRC application. The menu groups and quick links available on the screen are determined by the applications you have licensed. The content in this topic covers the functions specific to Access Control.

Table 4:

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Dashboards</td>
<td>Dashboards for access risk analysis, business role management, and user access management</td>
</tr>
<tr>
<td>Access Risk Analysis Reports</td>
<td>Reports related to access risk analysis, including user risk violations, role risk violations, profile risk violations, and HR Object risk violations</td>
</tr>
</tbody>
</table>
### Access Request Reports
Reports related to access requests, including service level for requests and requests with conflicts and mitigation

### Role Management Reports
Reports related to role management, including user-to-role relationships and master-to-derived role relationships

### Security Reports
Reports related to user, role, and profile security

### Audit Reports
Audit-related reports, including actions in roles (but not in rules) and permissions in roles (but not in rules)

### Emergency Access User Management Reports
Reports related to superuser activities, including invalid superusers and consolidated logs

## 3.5 Special Privileges

SAP Access Control users who have been assigned special privileges can be assigned as an owner. Users who can be assigned special privileges include the following:

### Table 5:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firefighter ID Owner</td>
<td>Firefighter ID owners are responsible for maintaining firefighter IDs and their assignments to firefighters. Firefighter ID owners use the default role <code>SAP_GRAC_SUPER_USER_MGMT_OWNER</code>.</td>
</tr>
<tr>
<td>Firefighter Role Owner</td>
<td>Firefighter role owners are responsible for maintaining firefighter roles and their assignments to firefighters. Firefighter role owners use the default role <code>SAP_GRAC_SUPER_USER_MGMT_OWNER</code>.</td>
</tr>
<tr>
<td>Risk Owner</td>
<td>Risk owners are assigned to risks and are commonly responsible for approving changes to risk definitions and violations of the risk.</td>
</tr>
<tr>
<td>Role Owner (ERM)</td>
<td>Role owners are responsible for approving either content or user-role assignment or both.</td>
</tr>
<tr>
<td>Mitigation Monitor</td>
<td>Mitigation monitors are assigned to controls to monitor activity and may receive control monitor alerts.</td>
</tr>
<tr>
<td>Mitigation Approver</td>
<td>Mitigation approvers are assigned to controls and are responsible for approving changes to the control definition and assignments.</td>
</tr>
<tr>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Firefighter ID Controller</td>
<td>Firefighter ID controllers are responsible for reviewing the log report generated during firefighter ID usage. Firefighter ID controllers use the default role SAP_GRAC_SUPER_USER_MGMT_CNTLR.</td>
</tr>
<tr>
<td>Firefighter Role Controller</td>
<td>Firefighter role controllers are responsible for reviewing the log report generated during firefighter role usage. Firefighter role controllers use the default role SAP_GRAC_SUPER_USER_MGMT_CNTLR.</td>
</tr>
<tr>
<td>Point of Contact</td>
<td>Point of contact is an approver for a specific functional area. Functional area is an attribute used to categorize users and roles.</td>
</tr>
<tr>
<td>Security Lead</td>
<td>Security lead is a group or individual that can provide secondary approval for access requests and reviews.</td>
</tr>
</tbody>
</table>

There are three group types for owners:
- Owner
- Owner group
- Lightweight Directory Access Protocol (LDAP) group

3.6 Background Jobs

Use

In the Access Management work center, under Scheduling, you can use the links to schedule and display background jobs.

Features

- Background Scheduler [page 30]
- Scheduling Background Jobs [page 31]

3.6.1 Background Scheduler

Use

You can use Background Scheduler to create and maintain schedules for background jobs.
Activities

1. Enter the name for the schedule.
2. Select an activity for the background job.
3. Select whether to start the background job immediately.
4. Specify the start date and time.

3.6.2 Scheduling Background Jobs

Use

On the Scheduling screen, you can choose to schedule the job to run in the background at a specified time or choose to run the job in the foreground.

To execute the job in the foreground, select the Foreground checkbox, and choose Submit.

Procedure

To execute the job as a background job:

1. Under the Schedule section, select Background.
2. To set the job to recur multiple times, select the Recurring Plan option as Yes, then select the date and times. You can set the Frequency as: Hourly, Daily, Weekly, or Monthly. In the Recurrence field, you can set the background job to recur for every number of hours. For example, recur every 4 hours.
3. To set the job to execute only one time, select the Recurring Plan option to No. You can choose to start the job immediately or to start at a specific date and time.
4. Choose Submit.
4 Managing Access Requests

Use

SAP Access Control provides a standardized and centralized framework to request user access and to review and manage those requests.

This process explains how to monitor and prevent risks using approval workflow and risk analysis during user provisioning.

Prerequisites

- Outside the application, you have identified your business needs and evaluated your approach to system access.
- Within the application, you have maintained the review and approval workflows.

You maintain the workflows in the Customizing activity Manage MSMP Workflows, under Governance, Risk, and Compliance Access Control Workflow for Access Control.

Process

The basic user provisioning process, as suggested by most system administrators, is described below.

1. Create and submit user access request
   The user creates an access request by selecting appropriate applications and roles that provide system access to perform work tasks. Once all required fields are completed on the user access request, he or she submits it for approval.

2. Review request
   Each approver reviews the request for appropriate access.

3. Modify request
   If access is not appropriate, each approver may modify the request.

4. Perform risk analysis
   Risk analysis should be performed to ensure that the approval of the request does not introduce access risks into the environment.
   1. Modify request access to remove conflicts when possible.
   2. If access cannot be modified, the risk should be mitigated according to your company policies.

5. User Provisioning
   Once the request is approved, access is provisioned to users.
4.1 Access Request Creation

The SAP Access Control application allows you to create access requests to obtain access to systems and authorizations to perform tasks. You can create access requests for yourself, for another user, or for multiple users.

You can initiate the access request creation process on the following screens:

- For End User logon, go to the End User Home screen, and then choose Access Request.
- For NWBC logon or the Portal logon, go to the My Home work center or the Access Management work center, and then choose Access Request or Create Request - Simplified.

The Access Request menu groups functions that allow you to create requests for user access, system access, and organizational assignments. This menu group is available from the Access Management work center, where you can do the following:

- Use Access Request to create requests for yourself, for another user, or for multiple users.
- Use Model User to create access requests based on a model user.
- Use Template Based Request to create access requests based on a template.
- Use Copy a Request to leverage details of an existing request to create a new request.
- Use Organizational Assignment Request to create requests for organizational assignments.
- Use Create Request - Simplified to create requests using a streamlined user interface.

4.1.1 Simplified Access Requests

Simplified Access Request processing allows you to process access requests using redesigned screens with a streamlined user interface. You can use these screens in place of the traditional access request processing screens, or you can continue to use the traditional screens. The following redesigned screens are available

- Create Request-Simplified [page 26]
Procedure

1. To request access for yourself or for others, enter the following information:

   **Note**
   
   An asterisk (*) on the screen designates a required field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Reason</td>
<td>Either select a reason from the dropdown list or select Others and write your reason in the box underneath.</td>
</tr>
<tr>
<td>User Information</td>
<td>The system fills in your information when the request for yourself. If the request is for others, you can search for user information by using the value help in the User ID field.</td>
</tr>
<tr>
<td>Select Roles for Addition</td>
<td>You can search for roles by role attributes such as name, system, Tcode, or key word. Wildcards such as * are valid. You can also use the Advanced Search for more granular search. You may use the filters on the left of the screen to further refine your search results. You can view the list of Tcodes defined in the role by clicking on the role name. You can further drill-down to get more information about the role by clicking on the Show More button in the pop-up screen.</td>
</tr>
<tr>
<td>Select Roles for Removal</td>
<td>Select this option to remove the role assignments from this user.</td>
</tr>
<tr>
<td>Select Roles for Extension</td>
<td>Select this option to extend the validity dates of the role.</td>
</tr>
</tbody>
</table>

2. When requesting access for other users, you can optionally run risk analysis by clicking on the Risk Analysis in the side panel.

   Optionally, you can view the system-added roles by clicking on the System Added Roles side panel.

3. Optionally, you can save the request as a draft to work on later.

4. When your request is complete, submit it for approval.

### 4.1.2 Creating Access Requests

**Use**

On the Access Request screen, you can create access requests for yourself, for another user, or for multiple users.
Prerequisites

The administrator has completed the activities for the Customizing activity Maintain Provisioning Settings, under Governance, Risk, and Compliance > Access Control > User Provisioning.

Procedure

1. From the Access Management work center, under the Access Request menu group, choose Access Request Creation.

   **Note**
   - If you are using the End User logon, on the End User Home screen, choose Access Request.

2. Under the Request Details area, enter the required information in the fields:

   **Table 7:**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Type</td>
<td>Examples: New Account, Change Account, Superuser Access, and so on. You can maintain the list of available request types in the Customizing activity Define Request Types, under Governance, Risk, and Compliance &gt; Access Control &gt; User Provisioning.</td>
</tr>
</tbody>
</table>
   | Request For     | Choose to create a request for the following:  
   |                 | ☐ Self, to create a request for yourself. The User field is inactive and displays your user ID.  
   |                 | ☐ Other, to create a request on behalf of another user. The User field is active, and allows you to select the name of the user.  
   |                 | ☐ Multiple, to create a request for multiple users. The application displays the Users tab page, and allows you to select multiple users. Choose Add to add each user manually, or choose Import to use a template to import multiple users. |
   | Priority        | Examples: High, Low, and so on. You can maintain the list of available priorities in the Customizing activity Maintain Priority Configurations, under Governance, Risk, and Compliance > Access Control > User Provisioning. |
   | Business Process| Examples: HR and Payroll, Finance, and so on. You can maintain the list of available business processes in the Customizing activity Maintain Business Processes and Subprocesses, under Governance, Risk, and Compliance > Access Control. |
3. On the **User Access** tab page, choose from the following options to select the roles that you want to be assigned, and the systems for which you are requesting access:
   - Choose **Add** and select from the following:
     - **Role**
       - Click **Add** and then click **Role** to search for the roles that you want. After the system presents the results of your search, you can click a retrieved role name to access further details about the role such as the actions that are valid for a composite role.
       - If you select a **Business Role**, you can choose which environment you wish to provision. The environment options are: **All**, **Development**, **Production**, and **Testing**. This choice is only available to you if you set the Access Control configuration parameter **3026 (Enable Business Role Provisioning based on Environment)** to **Yes**. The default value for this parameter is **No**.

   - **System**
   - **Firefighter ID**
   - **Firefighter Role**

   **Note**

   For **Role Search**, the application allows you (requires administrator authorization) to configure the search criteria fields. You can add custom fields and configure their attributes. For example, you can set the default values and set whether the field is mandatory. You can configure the fields in Customizing for **Maintain Custom Field Attributes for Role Search Personalization** under **Governance, Risk, and Compliance > Access Control > User Provisioning**.

   - Choose **Existing Assignments** to select from the list of roles and systems currently assigned to the user.
   - If the **Request For** field is set to **Multiple**, the application disables this button.

   **Note**

   When requesting a Firefighter ID or a Firefighter Role, you can filter the search using **System** and **Action Code**. If you use **Action Code**, you must also specify the **System**. For both Firefighter ID and Firefighter Role requests, the owner displays in the **Assignment Approver** column.

4. In the **Provisioning Actions** column, select the appropriate action, such as **Create User**, **Assign (role)**, and so on.
You can set the provisioning actions available in the drop-down list in the Customizing activity Define Request Type, under Governance, Risk, and Compliance > Access Control > User Provisioning.  

5. In the Comments column, choose Add Comment and enter information about the request.
   You can set whether comments are mandatory in the Customizing activity Maintain Configuration Settings, under Governance, Risk, and Compliance > Access Control > Access Control. For the relevant columns, set the following values:
   ○ Parameter Group: Access Request Role Selection
   ○ Parameter ID: 2036
   ○ Parameter Value: Yes or No, as needed

6. On the User Details tab page, enter all required information.

7. Choose Simulation, if you want to run a risk analysis of the requested roles and system access before submitting the request.

8. Choose Submit.
   The application sends an e-mail notification to the approver. You can configure e-mail in the Customizing activity Maintain MSMP Workflows, under Governance, Risk, and Compliance > Access Control > Workflow for Access Control. In the Maintain Path phase, under the Maintain Stages area, choose Notification Settings.
   Approvers can also access and process the request from their Work Inbox.

End users can view the status of the request from the quick link.

More Information

Viewing Your Request Status [page 20]
Changing User Details [page 43]
Reviewing and Approving Access Requests [page 46]
Analyzing Risks When Submitting Access Requests [page 37]

4.1.3 Analyzing Risks When Submitting Access Requests

Use

On the Access Request screen, you can perform risk analyses and impact analyses on the following tab pages:

- Risk Violations
  If you want to save the results of the analysis, use the analysis function on this tab.
- User Access
  The Simulation feature allows you to perform the analysis first and then choose whether or not to save the results.
Note

- You can set the application to analyze risks automatically when someone submits an access request. For example, if the requester chooses to submit a request without analyzing the risks first, the application automatically performs an analysis and adds the results to the access request that appears in the approver’s Work Inbox.

You maintain this setting in the Customizing activity Maintain Configuration Settings, under Governance, Risk, and Compliance Access Control. For the parameter Enable risk analysis on form submission, enter the values as follows:

Table 8:

<table>
<thead>
<tr>
<th>Column</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter Group</td>
<td>Risk Analysis – Access Request</td>
</tr>
<tr>
<td>Parameter ID</td>
<td>1071</td>
</tr>
<tr>
<td>Parameter Value</td>
<td>Yes or No, as required</td>
</tr>
</tbody>
</table>

- You can set the application to include firefighter assignments in the risk analysis.

You maintain this setting in the Customizing activity Maintain Configuration Settings, under Governance, Risk, and Compliance Access Control. For the parameter Consider FF Assignments in Risk Analysis, enter the values as follows:

Table 9:

<table>
<thead>
<tr>
<th>Column</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter Group</td>
<td>Risk Analysis</td>
</tr>
<tr>
<td>Parameter ID</td>
<td>1038</td>
</tr>
<tr>
<td>Parameter Value</td>
<td>Yes or No, as required</td>
</tr>
</tbody>
</table>

Procedure

The following procedure is the same regardless of which tab page you choose to initiate it. The only difference is that the simulation feature allows you to choose whether or not to save the results.

1. On the screen, do one of the following:
   - Select the Risk Violations tab.
   - On the User Access tab, choose Simulation.

2. In the Analysis Type dropdown list, select the relevant analysis type:
   - You use Risk Analysis to determine violations pertaining to the authorizations assigned to the role. An example is when the authorizations result in segregation of duties violations.
   - You use Impact Analysis to determine authorization violations pertaining to other roles. That is, the authorizations for the selected role, in combination with authorizations for another role, results in violations.
3. Select the System and Rule Set from the respective fields.
4. In the Result Options area, select the format, type, and additional criteria for the analysis results.

Example

Table 10:

<table>
<thead>
<tr>
<th>Format</th>
<th>Executive Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type:</td>
<td>Action Level, Permission Level</td>
</tr>
<tr>
<td>Additional Criteria:</td>
<td>Include Mitigated Risks</td>
</tr>
</tbody>
</table>

5. Choose the Run Risk Analysis pushbutton.
6. In the Result area, you can choose different ways to view the analysis results.
7. If you are running the simulation feature, you can do the following:
   ○ Choose Cancel if you do not want to save the results of the analysis.
   ○ Choose Apply if you want to save the results. The information is saved to the Risk Violations tab and you can view it whenever you open the request. The results are also available to the approver of the request.

### 4.1.3.1 Mitigating Risks

#### Prerequisites

You have created mitigation controls.

#### Context

On the Assign Mitigation Controls screen, you can assign mitigation controls to risks found during risk analysis and impact analysis.

The screen also allows you to mitigate risks for roles that are not part of the current request. For example, you are currently mitigating risks for John_Current_Request. You can also mitigate risk violations for John_Other_Request1 and John_Other_Request2. Choose the Add pushbutton to add and complete the procedure below for step 4.

**Note**

The Mitigate Risk feature is available on multiple screens in the application. In the procedure below, we describe one access point; your access point may be different. The information is applicable regardless of the access point.
Procedure

1. On the Analyze Access Risk screen, under the Results section, select a risk violation or multiple violations, and then choose the Mitigate Risk pushbutton.

   The Assign Mitigation Controls screen appears. The application uses the information from the risk violation, such as the Access Risk ID, and displays the relevant mitigating control.

2. To use the mitigating control suggested by the application:
   1. Change the information in the relevant fields as needed, such as the validity dates, the Control ID, and so on.
   2. Choose Submit.

3. To create a new control:
   1. Choose Create Control and complete the tasks for creating a new control.
   2. Choose Add.
      The application adds an empty line to the mitigation controls list.
   3. Enter information in the relevant fields for the new control.
   4. Choose Submit.

4. To assign mitigating controls for other roles or requests:
   1. Choose Add.
      The application adds an empty line to the mitigation controls list.
   2. Enter information in the relevant fields for the new control.
   3. Choose Submit.

Next Steps

4.1.4 Template Roles

Use

You can use template roles to provide users with a set of attributes from which they can choose when creating access requests.

Example

For example, you specify that all Finance roles are valid for the template role. When a user requests a finance role, he or she can choose additional attributes such as Region, Business Unit, Plant, and so on.

Note

- You must enable the GRAC_TEMPLATE_ROLE BAdI to activate the template roles function.
In the BAdI, you can specify the role attributes from which the user can choose.

**Procedure**

1. On the [Access Request screen](User Access) tab page, select a role and then choose the Template Role button. A screen appears and displays the attributes from which the user can select for the role.

   - **Note**
   
   The button is only active if you select a role that is valid for the template role. You specify the valid roles for the template.

2. Select the attributes for the role and complete the access request.

**More Information**

Creating Access Requests [page 23]
Configuring Template Roles [page 41]

### 4.1.4.1 Configuring Template Roles

To enable template roles for access requests, you implement the `GRAC_TEMPALTE_ROLE` BAdI.

**Methods**

The following methods are available for the BAdI.

- **Note**

  The `IS_TEMPLATE_ROLE` method is the minimum required method for enabling template roles.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>IS_TEMPLATE_ROLE</code></td>
<td>You use this method to specify which business roles the application considers as template roles. For example, you can specify that any roles with the naming scheme of <code>Z_Template_role...</code> are considered template roles.</td>
</tr>
</tbody>
</table>
## Method Description

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET_URL</td>
<td>You use this method to get the URL of the custom application. This method is called when the template role is added to the request. The URL returned by this method is displayed as a new window and displays the details of the role.</td>
</tr>
<tr>
<td>VALIDATE_ROLE</td>
<td>You use this method to check the consistency of the template role. The application calls this method during submission of an access request. This method checks if the additional information provided in the custom application is consistent. This method implementation should return a list of error and success messages.</td>
</tr>
<tr>
<td>GET_PROVISIONING_TYPE</td>
<td>You use this method to determine whether standard or custom provisioning is required for the access request. The application calls this method during provisioning. Provisioning type of 1 means it is custom provisioning.</td>
</tr>
<tr>
<td>GET_PROVISIONING_OBJECTS</td>
<td>You use this method to return the list of objects to be provisioned. This method is called only when the GET_PROVISIONING_TYPE method returns a value of 1 (custom provisioning).</td>
</tr>
<tr>
<td>SET_PROVISIONING_STATUS</td>
<td>You use this method to provide the status of the provisioning.</td>
</tr>
</tbody>
</table>

### 4.1.5 Creating Access Requests Based on Model Users

#### Context

You can use the functions on the Model User Access screen to create access requests for new users by copying the authorizations of an existing user. This allows you to use the access settings of an existing user as a template and saves time in the access creation process.

For example, you add new employees to your team, and you want them to have the same access as other members of your team. Instead of entering the same information over and over, you select one of your current employees as the model user, and the application copies copy the access information from them to the access request for the new employees.
Procedure

2. On the Select User screen, select the Request For field, and choose either Self or Other.
3. On the User Details tab page, enter the relevant information in the required fields, and then choose Next.
4. Under the Select Model User area, select the User field, search for and choose the user.
5. Under the Select User Access area, from the Available list, select the access and authorizations from the model user that you want to copy to the new user.
6. Under the Request Type area, select the Request Type field, choose a request type, and then choose Next.
7. Enter the request details as needed, and then choose Submit.

This is the standard procedure for creating an access request in the application. For more information, see.

4.1.6 Changing User Details

Context

You can use the Access Request screen to change the details for your user, such as name, position, manager, organization, location, and so on.

Procedure

1. From the Access Management work center, under the Access Request Creations menu group, choose Access Request.

   i Note
   If you are using the End User logon, on the End User Home screen, choose Access Request.

2. Choose the Request Type field, and then choose Change Account.
3. On the User Access tab page, choose Add, and then select System.

   The Select System screen appears.
4. Select the relevant systems and then choose OK.

   On the User Access tab page, under the Provisioning Action column, the application automatically fills in the action as Change User.
5. Choose the User Details tab page, change the user information as needed, and then choose Submit.

   The application sends the request to the approver.
4.1.7 Copying Requests

Use

On the Copy Request screen, you can leverage information from previous access requests to create new requests.

Procedure

1. From the Access Management work center, under the Access Request menu group, choose Copy Request. The Copy Request screen appears.
2. In the Request Number field, select the request from which to copy the attributes.
3. In the Attributes table, select the attributes you want to copy, and then choose Next.
4. In the Request For field, select whether the request is for Self, Other, or Multiple.
5. Change the relevant information on the User Details and Users tab pages as needed, and then choose Next.

   i Note

   The Users tab page is available only if you choose Request For: Multiple.

6. Enter the relevant request details as needed, such as system or role access on the User Access tab page, and so on, and then choose Next.
7. Choose Submit.

   i Note

   For the above procedure, steps 1 through 3 are for copying the request. The remaining steps follow the standard procedure for creating a request. For more information, see .

4.1.8 Creating Organizational Assignment Requests

Context

On the Organizational Assignment Request screen you can assign roles to organizational management (OM) objects such as positions, jobs, or organizations, instead of users.
Procedure

1. From the Access Management work center, under the Access Request menu group, choose Organizational Assignment Request.

   The Organizational Assignment Request screen appears.

2. Under the Request Details area, select or enter information in the relevant fields.

3. In the OM Object Type field, select the object type you want to add: job, position, or organizational unit.

4. Search for and select the OM objects.
      The Select OM Object screen appears.
   2. Select the relevant system and choose Search.
   3. From the Available list, select the relevant OM objects, and choose OK.

5. Search for and assign roles to the OM objects.
   1. On the User Access tab page, select one or multiple OM objects, and choose Assign Role.
      The Search Roles screen appears.
   2. Search for and select the relevant roles, and then choose OK.

6. For each of the OM object and role assignments you can set the following:
   ○ Valid from
   ○ Valid to
   ○ Add comments
   ○ Provisioning action

7. Choose Submit.

4.2 Access Request Approval

Use

The SAP Access Control application provides a standardized and centralized framework to request user and system access and to review and manage those requests. The basic user provisioning process, as suggested by most system and security administrators, involves the steps described below.

Note

The process described is an example. Your company’s process may be different, and may have more or fewer steps. The application allows you to customize the steps as required. For more information, see the Customizing activity Maintain MSMP Workflows, under Governance, Risk, and Compliance > Access Control > Workflow for Access Control.
Prerequisites

- Outside the application, you have identified your business needs and evaluated your approach for managing user and system access.
- Within the application, you have maintained the review and approval workflows. You maintain the workflows in the Customizing activity Maintain MSMP Workflows, under Governance, Risk, and Compliance Access Control Workflow for Access Control.

Process

User Provisioning consists of the following procedures:

1. Reviewing access requests
2. Analyzing access risks
3. Managing risks
4. Approving requests

The application then provisions the user access requests.

You can configure provisioning settings such as e-mail notification, auto provisioning, and so on, using the Customizing activity Maintain Provisioning Settings, under Governance, Risk, and Compliance Access Control User Provisioning.

4.2.1 Reviewing and Approving Access Requests

Use

On the Access Request screen, approvers can review, reject, change, or approve access requests.

Process

1. To review an access request, do one of the following:
   - From the My Home work center, choose Work Inbox. From the Workitems list, choose an access request to open it.
   - From the Access Management work center, under the Access Request Administration menu group, choose Search Requests. Search for a request, and then choose the Administrator button to open and review it.

The application displays the Access Request screen, which is the same screen that requesters use when submitting the request. Approvers see all the information that the requester entered. In addition, approvers see more buttons and fields that allow them to review, reject, change, or approve the request.
You can configure the buttons and fields that approvers can see. For example, you can allow approvers to add roles to a request.

Review the request and perform actions as required, such as Approve, Reject, and so on.

2. In the upper right-hand corner, choose Stage to display information about the current stage of the approval workflow and its status.

3. On the Risk Violations tab page, you can view the results of the risk analysis that the requester performed or you can perform your own risk analysis.

You can configure the application to require that approvers perform a risk analysis before approving any requests.

4. When you are finished reviewing the request, choose Submit.

4.2.2 Simplified Work Inbox

Use

You use the Simplified Work Inbox to view the access requests that require approval.

You can also use the regular work inbox to process access requests. For more information, see Work Inbox [page 17].

Procedure

Use the procedure below to find specific requests:

1. Using the slider bar or the date input boxes, select a specific date or a date range for the requests that you want to process.
2. Optionally, select a category such as New Account to narrow your search.
3. Optionally, select a number of results to show per page.
4. Optionally, select a sort criterion such as Request Number or Requested By.
   The system retrieves all requests that match your criteria.
5. Click a request number to drill into its details. Optionally, click the flag icon to mark a request for follow up.
4.2.3 Analyzing Risks When Approving Access Requests

Use

On the Access Request screen, you can perform risk analysis and impact analysis before approving requests. You have the following options for performing the analysis:

- On the Risk Violations tab, you can perform the analysis and save the results.
- On the User Access tab, you can use the Simulation feature to first perform the analysis and then choose whether or not to save the results.

Procedure

The following procedure is the same regardless of the tab page you choose to initiate it. The only difference is that the Simulation allows you to choose whether or not to save the results.

1. From the My Home work center, select Work Inbox. On the Workitems screen, select Access Management. Choose an access request.
2. Do one of the following:
   - Select the Risk Violations tab.
   - On the User Access tab, choose Simulation.
3. In the Analysis Type dropdown list, select the relevant analysis type.
   - You use Risk Analysis to determine violations pertaining to the authorizations assigned to the role. For example, when the authorizations result in segregation of duties violations.
Note

You can customize SAP Access Control to include firefighter assignments automatically in the risk analysis.

You maintain this setting in the Customizing activity (transaction SPRO) **Maintain Configuration**

Settings, under **Governance, Risk, and Compliance** ➤ **Access Control** ➤ For the parameter **Consider FF Assignments in Risk Analysis**, enter the values as follows:

<table>
<thead>
<tr>
<th>Column</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter Group</td>
<td>Risk Analysis</td>
</tr>
<tr>
<td>Parameter ID</td>
<td>1038</td>
</tr>
<tr>
<td>Parameter Value</td>
<td>Yes or No, as required</td>
</tr>
</tbody>
</table>

You use **Impact Analysis** to determine authorization violations pertaining to other roles. That is, the authorizations for the selected role, in combination with authorizations for another role, result in violations.

4. Select the **System** and **Rule Set**.

5. Under the **Result Options** area, select the format, type, and additional criteria for the analysis results.

**Example**

<table>
<thead>
<tr>
<th>Format</th>
<th>Executive Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Action Level, Permission Level</td>
</tr>
<tr>
<td>Additional Criteria</td>
<td>Include Mitigated Risks</td>
</tr>
</tbody>
</table>

6. Choose the **Run Risk Analysis** pushbutton.

7. In the **Result** area, you can choose different ways to view the analysis results.

8. If you are running a simulation, you can do the following:
   - Choose **Cancel** if you do not want to save the results of the analysis.
   - Choose **Apply** if you want to save the results of the analysis. The information is saved to the **Risk Violations** tab and you can view it whenever you open the request. The results are also available to the approver of the request.

9. On the **Risk Violations** tab, you can choose to mitigate any risk by selecting the risk and choosing **Mitigate Risk**.
4.2.4 Mitigating Risks

Prerequisites

You have created mitigation controls.

Context

On the Assign Mitigation Controls screen, you can assign mitigation controls to risks found during risk analysis and impact analysis.

The screen also allows you to mitigate risks for roles that are not part of the current request. For example, you are currently mitigating risks for John_Current_Request. You can also mitigate risk violations for John_Other_Request1 and John_Other_Request2. Choose the Add pushbutton to add and complete the procedure below for step 4.

Note

The Mitigate Risk feature is available on multiple screens in the application. In the procedure below, we describe one access point; your access point may be different. The information is applicable regardless of the access point.

Procedure

1. On the Analyze Access Risk screen, under the Results section, select a risk violation or multiple violations, and then choose the Mitigate Risk pushbutton.

   The Assign Mitigation Controls screen appears. The application uses the information from the risk violation, such as the Access Risk ID, and displays the relevant mitigating control.

2. To use the mitigating control suggested by the application:
   1. Change the information in the relevant fields as needed, such as the validity dates, the Control ID, and so on.
   2. Choose Submit.

3. To create a new control:
   1. Choose Create Control and complete the tasks for creating a new control.
   2. Choose Add.
      The application adds an empty line to the mitigation controls list.
   3. Enter information in the relevant fields for the new control.
   4. Choose Submit.

4. To assign mitigating controls for other roles or requests:
1. Choose Add.
The application adds an empty line to the mitigation controls list.
2. Enter information in the relevant fields for the new control.
3. Choose Submit.

Next Steps

4.2.5 Maintaining Tasks and Authorizations for Request Approvers

Context

In the Stage Details screen of the MSMP Configuration, you can select the tasks that are available to approvers on the Access Request screen for approvers and specify what they are authorized to do. For example, you can allow approvers to reject a request or forward the request to another approver.

Procedure


   The MSMP Workflow Configuration screen appears.

2. In the Process Global Settings phase, select the process for Access Request Approval Workflow, and then choose the Maintain Paths phase.

3. Under the Maintain Stages area, choose Display Task Settings.

   The Stage Definition screen appears.

4. Under the Task Settings section, select the checkboxes for the features you want to be available to approvers on the access request screen.

Table 14:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Runtime Configuration Change OK</td>
<td>Use configuration changes available at runtime.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Path Reevaluation New Role | When applied to the access request workflow, this setting allows approvers to analyze the roles in the request against the initiators to determine if another parallel workflow must be created. You can choose from the following:  
  ○ All Roles in Evaluation Path   
    Reevaluate all roles.  
  ○ New Roles Only   
    Reevaluate only new roles.  
  ○ None   
    Do not reevaluate any roles. |
| Reroute                    | Allows approvers to reroute the request to a previous stage as an alternative to rejecting the request.                                                                                                                                                  |
| Confirm Approval           | Displays an additional screen that requires approvers to confirm that they approve the request.                                                                                                                                                             |
| Confirm Rejection          | Displays an additional screen that requires approvers confirm that they reject the request.                                                                                                                                                                   |
| Approve By E-mail          | Approvers receive e-mails informing them that a request requires their attention. Such e-mails include a link that opens the user provisioning screen.                                                                                                               |
| Reject by E-mail           | Approvers receive e-mails informing them that a request requires their attention. Such e-mails include a link that opens the user provisioning screen.                                                                                                               |
| Approve Despite Risk       | Allows approvers to approve requests despite risk violations.                                                                                                                                                                                                 |
| Reaffirm Approve           | Requires approvers to confirm their identities before approving requests.                                                                                                                                                                                     |
| Reaffirm Reject            | Requires approvers to confirm their identities before rejecting requests.                                                                                                                                                                                      |
| Change Request Details     | Allows approvers to change the content of requests.                                                                                                                                                                                                            |

**Note**

The approval workflow is comprised of stages and paths. For a standard approver, the application does not display the reroute option in the first stage, because there is no previous stage. For an administrator, the reroute option is available for all the stages because the administrator can send the request to different paths.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Approval Level| Allows approvers to approve requests for the following levels:  
  ○ Request  
    Approvers have the authority to approve all roles in a request. For example, security approvers can approve any role relevant to a request.  
  ○ Role  
    Approvers can approve only those roles that belong to them.  
  ○ System and Role  
    Approvers have the authority to approve systems and roles. |
| Rejection Level| Allows approvers to reject requests for the following levels:  
  ○ Request  
    Approvers have the authority to reject all roles in a request. For example, security approvers can reject any role relevant to a request.  
  ○ Role  
    Approvers can only reject those roles that belong to them.  
  ○ System and Role  
    Approvers have the authority to reject systems and roles. |
| Comments Mandatory | Requires approvers to enter comments when approving or rejecting a request. |
| EUP ID        | End User Personalization (EUP) allows you to define the behavior of the fields and pushbuttons on the Request Access screen, such as the following:  
  ○ Default values for the fields  
  ○ Whether the field is mandatory  
  ○ Whether the field is editable  
  ○ Whether the field is visible on the screen  
You set the parameters in the Customizing activity Maintain End User Personalization, under Governance, Risk, and Compliance Access Control User Provisioning.  
In the EUP ID field, you enter the ID of the end user personalization you want to use."
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Override Assign Type         | ○ Direct
Roles are assigned to users.  
○ Indirect  
Roles are assigned to positions or organizations.  
○ Combined provisioning |

**Note**
In the provisioning configuration, you must also set Manual Provisioning to True.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Assignment</td>
<td>Allows approvers to add assignments for roles or systems to the request.</td>
</tr>
<tr>
<td>Request Rejected</td>
<td>Allows approvers to reject requests.</td>
</tr>
<tr>
<td>Forward Allowed</td>
<td>Allows approvers to forward requests to another approver.</td>
</tr>
<tr>
<td>Display Review Screen</td>
<td>Allows approvers to see the Access Review screen.</td>
</tr>
<tr>
<td>Risk Analysis Mandatory</td>
<td>Requires approvers to perform risk analysis before approving or rejecting a request.</td>
</tr>
</tbody>
</table>
| E-mail Group                 | **Note**
The application does not use this field. We provide it only for backward compatibility. |
| Allow Manual Provisioning    | Allows approvers to provision directly from the stage approval screen.      |

5. Choose **Save**.

### 4.3 Access Request Administration

You can use the SAP Access Control application to manage and review access requests, assignments, accounts, and processes. The application displays these functions in the Access Request Administration menu group.

To locate the menu group, do the following:

1. From the NWBC logon or the Portal logon, choose the Access Management work center.
2. Under the Access Requests Administration menu group, choose the relevant activities:
   ○ Creating and Managing Templates [page 55]
   ○ Searching Requests [page 56]
   ○ Viewing Provisioning Logs [page 57]
4.3.1 Creating and Managing Templates

Prerequisites

You have created End User Personalization IDs (EUP ID) in the Customizing activity **Maintain End User Personalization** under **Governance, Risk, and Compliance** ➔ **Access Control** ➔ **User Provisioning**.

Context

You can use the **Access Request Template** screen to create, update, or delete templates. Templates allow you to facilitate the creation of access requests by defining details that you consistently use in access requests. For example, you know that members of the finance team always require access to the finance system and always require the **Finance_User** role. You can create a template with these details and you can use this template to create requests for new finance members. The application automatically inserts the information from the template into the new request.

Procedure

1. On the **Access Management** work center, under the **Access Request Administration** menu group, choose **Template Management**.
   
   The **Access Request Template** screen appears.
2. Choose **Create**.
3. In the **Template Details** tab page, enter information in the required fields.
   
   The EUP ID defines the fields and default values on the Access Request screen.
4. On the **Access Details** tab page, enter details for user, access, and so on, as needed.
5. Choose **Save**.
4.3.2 Searching Requests

Context

You can use the functions on the Search Request screen to create a report that lists requests, request type, priority, status, and due date, among other information. You can also use Search Request to open a specific request, to display request administration information, to display the audit log for a request, and to cancel a request instance or to make other changes, as allowed by your configuration.

Procedure


2. Specify the search criteria.

   Do the following:
   1. Choose the object type using the first dropdown list.
   2. Choose the operator using the second dropdown list, from among the following:
      ○ is
      ○ is not
      ○ starts with
      ○ contains
   3. Type or select the value in the third field.
   4. Optionally, add a line to the search criteria by choosing the plus (+) pushbutton and specifying the appropriate fields. Alternatively, remove a line from the search criteria by choosing the corresponding minus (-) pushbutton.

3. Optionally, save the search criteria as a variant by typing a name in the Save Variant as field and choosing Save.


5. To display the audit log, choose Audit Log. The Audit Log screen opens.

   You can choose to expand or collapse the audit log entries and to print the log.

6. To display the instance status, select a request in the table and choose Instance Status. The Access Request Search screen opens showing the instance details.

7. To open a specific request, select the request in the table. The Approve Access Request screen opens.

   You can view the following request details by choosing the corresponding tab:
   ○ User Access
4.3.3 Viewing Provisioning Logs

Context

You can use the Provisioning Logs screen to review provisioning activities and to confirm that provisioning was completed.

Note

The Provisioning Log only displays information for completed requests. To view the status of requests that are in process see .

Procedure

1. On the Access Management work center, under the Access Request Administration menu group, choose Provisioning Logs.
   
   The Provisioning Logs screen appears.

2. In the search fields, select the relevant criteria, and then choose Search.
   
   In the Results table, the application displays the requests that meet your search criteria.

   The table displays information such as the status, provisioning action, time stamp, and so on.
4.3.4 Unlocking and Deleting Password Self-Service Accounts

Prerequisites

You have completed the configuration steps in the Customizing activity Maintain Password Self Service, under Governance, Risk, and Compliance ➔ Access Control ➔ User Provisioning.

Context

On the Manage Password Self Service screen, you can unlock or delete accounts that have been locked due to too many unsuccessful logon attempts.

Note

To configure password options such as enabling or disabling password self-service, the number of times a user may attempt to logon before their account is locked, and so on, use the Customizing activity Maintain Password Self Service, under Governance, Risk, and Compliance ➔ Access Control ➔ User Provisioning.

Procedure

1. From the Access Management work center, under the Access Request Administration menu group, choose Manage Password Self Service.

   The Manage Password Self Service screen appears.

2. In the User ID field, enter the user account.

3. To unlock the account, select it, and then choose Unlock User.

   This action resets the number of unsuccessful logon attempts to zero.

4. To delete the account, select it, and choose Delete.
4.3.5 Approver Delegation

Context

On the Admin Delegation screen, you can reassign the approval tasks from one user to another. For example, as the administrator, you have the authority to delegate the approval tasks of Approver_A to Approver_B.

Procedure

1. On the Access Management work center, under the Access Request Administration menu group, choose Admin Delegation.
   
   The Admin Delegation screen appears.
2. To change the validity dates or status of an existing delegation, select a delegation from the list, and then choose Open.
   
   Change the validity dates and status as needed, and choose Save.
3. To create a new delegation, choose Delegate.
   
   Under the Approver Details section, enter the information for the person who currently owns the approval tasks.
   
   Under the Delegated Approval Details section, enter the details for the person to whom you want to assign the approval tasks.

Next Steps

For information about delegating your own approval tasks to another user, see Delegating Your Approval Tasks [page 18].

4.3.6 Creating Access Requests Based on Templates

Prerequisites

The administrator has created the access request templates. For more information, see Creating and Managing Templates [page 55].
Context

You can use the Create Request with Template screen to create new access requests using templates. You store frequently used access request information in templates, and then use the templates to create new access requests that require the same information. The benefits of this method are consistency and time savings.

Procedure

1. On the Access Management work center, under the Access Request menu group, choose Template Based Request.
   The Create Request with Template screen appears.
2. Select a template and choose Next.
   The User Details tab page appears. The application automatically populates the fields with the user detail information from the template.
3. Enter information in the required fields and make any relevant changes, and then choose Next.
4. Enter request details as needed, and then choose Submit.
   These steps are part of the standard procedure for creating access requests.

Next Steps

For more information, see Creating Access Requests [page 23]
5 Managing Access Risks

Use

The manage risk process involves prioritization and taking appropriate actions to address the risk occurrences based on the risk analysis results. Depending on the risk characteristics, different methods can be employed.

Process

1. Perform access risk analysis
2. Prioritize risks violations
   Identify which risks should be addressed first based on risk criteria. Risks that have the highest potential impact across the organization should be given higher priority. The prioritization result should be agreed to or approved by key stakeholders.
3. Identify root causes
   Identify the specific authorizations which introduced the risks. For each individual, determine whether the access is appropriate to perform their job duties.
4. Modify access
   The preferred approach is to eliminate risks where possible. Elimination of a risk should begin at the lowest level possible by correcting the root cause.
5. Define controls to mitigate risk (as needed)
   Where a risk is unavoidable or is deemed acceptable, controls need to be defined and implemented to mitigate the risk. A control definition may include the associated risks, instructions for execution, responsible persons, and the action to be taken if the control detects a violation of policy.

   i Note
   If appropriate control already exists, then skip this step and go to step 6.
6. Assign controls to mitigate risk
   You identify a control appropriate to the risk, and assign a responsible person. Then you enable the control and assign it to the risk. In addition, you assign a person to monitor the mitigated risks.
7. Execute controls
   The responsible person (monitor) will be in charge of following the steps documented in the control and do it periodically as required.
Result

The detected risks are remediated by removal of the access and/or mitigation.

5.1 Mitigating Controls

Use

You can use Mitigating Controls to associate controls with risks, and assign them to users, roles, profiles, or HR objects. You can then define individuals as control monitors, or approvers, and assign them to specific controls. You can also create organizations and business processes to help categorize mitigating controls.

Using the Mitigating Controls section, you can complete the following tasks:

- Create mitigating controls (that you cannot remove)
- Assign mitigating controls to users, roles, and profiles that contain a risk
- Establish a period of time during which the control is valid
- Specify steps to monitor conflicting actions associated with the risk
- Create administrator, control monitors, approvers, and risk owners, and assign them to mitigating controls

More Information

Searching Mitigating Controls [page 63]

5.1.1 Searching Mitigating Controls

Context

You can search and view mitigating controls using the Mitigating Controls screen.

Procedure

1. Choose Setup Mitigating Controls Mitigating Controls
   The Mitigating Controls screen opens showing all defined Mitigating Controls.
2. Choose Filter, enter the criteria in the Control ID, Title, Description, and Organization fields, and press Enter.
   The matching controls appear in the table.
3. Choose a row in the table and select Open to display information about a particular control.

Next Steps

Mitigating Controls [page 62]

5.2 Rule Setup

The Rule Setup work center provides a central location to create and manage rules to mitigate access request risks.
The Rule Setup work center contains the following Access Control sections:

- Access Rule Maintenance [page 74]
- Critical Access Rules [page 89]
- Exception Access Rules [page 64]
- Generated Rules [page 71]

5.2.1 Exception Access Rules

Use

Exception rules eliminate false positives based on organizational-level restrictions. This enables exception-based reporting for organizational rules and supplemental rules.

More Information

Organization Rules [page 64]
Creating an Organization Rule using the Wizard [page 65]

5.2.1.1 Organization Rules

Use

The organization rules functionality provides an additional filter for your segregation of duties (SoD) reports. Organization rules are used to eliminate false positive risks in your access risk analysis reports. Use this functionality for exception-based reporting only.

Prior to implementation, companies should do analysis to ensure that their situation warrants the use of organization rules. You should not institute organization rules until the remediation phase of your project. It is only after identifying a possible organizational rule scenario that you should create organization rules.
Caution
If you create organizational rules incorrectly, you could potentially filter out too much. By filtering out too much, you cannot identify possible control concerns with your access. From a control perspective, it is much better to over-report (causing false positives) rather than under-report (causing false negatives).

Recommendation
Use organization rules exclusively for exception-based reporting to remove false positive conflicts that result from organization-level segregation.
Do not use organization rules for grouping users into reports by organizational level for the purpose of distributing SoD reports to various management levels.
Due to the sizable performance impact that organization rules can have, use them only those in situations where the company has made a conscious decision to segregate via organization levels.

Example
A customer has a shared service center that allows a team member to process vendor invoices and create accounts payable (AP) payments. In many cases, this action might be a high-risk conflict. However, the shared services center also segregated its team members so that the same individual cannot process the invoice and make the payments within the same organizational level.

More Information
Creating an Organization Rule [page 66]
Creating an Organization Rule using the Wizard [page 65]

5.2.1.11 Creating an Organization Rule using the Wizard

Use
The Organization Rule Wizard makes the process of creating an organization rule faster and eliminates possible invalid entries due to manual input.

Procedure
Follow the steps below:
1. From the Setup workcenter, locate the Exception Access Rules section. Select Organization Rule Creation Wizard.
2. **Overview** – Read the instructions on the first stage and choose *Next*.

3. **Select System and Rule set** – Select the ERP *System* that you need to work on.
   Select the *Rule Set(s)* required. You can select multiple rule sets by holding down the control button and selecting multiple rule sets. Choose *Next*.

4. **Review Organization Levels** – Select the *Organization Levels* from the existing risks. Choose *Next*.

5. **Select Org Values** – Select the *Organization Level Values* from the ERP system. You can also remove the values that you do not want to use. Choose *Next*.

6. **Review Organization Rules** – Review the rules. Use the *Organization Rule Format* field to add a common prefix to all the rules that will be generated for easier sorting. Choose *Next*.

7. **Generate Rules** – Select *Generate Rules* to complete the task.

### 5.2.1.1.2 Creating an Organization Rule

#### Use

Use this feature for exception-based reporting only.

#### Prerequisites

You can create organization rules only after you have identified a possible organizational rule scenario.

#### Procedure

To create an organization rule:

1. Choose **Setup** ➤ **Exception Access Rules** ➤ **Organization Rules** ➤ .
2. Choose **Create**. The *Organization Rules* screen appears.
3. Enter the relevant information in all required fields. Required fields are marked with an asterisk (*).

   **Note**
   
   - **Organization Rule ID**: The identification code for the organization rule. Enter a 10-character alphanumeric name, including underscores (_). No spaces are allowed.
   - **Parent OrgRule ID**: If you are creating a completely new organization rule, this field is not required. If you are creating an organization rule based on a previously created rule, choose the Parent OrgRule ID you want to use.
   - **Risk ID**: Select from the list of available risk IDs
   - **Description**: Enter a meaningful description for this rule.

4. Choose **System** if you want to activate the Organization rule for specific systems only.
5. Choose Add to assign more than one organization level and corresponding values for the organization rule’s duration, condition, and status. Choose Remove to remove a previously entered organization level.

6. Choose Save.
   A confirmation message appears stating that the data has been saved.

7. Choose Close to view the organization rule that you created.

Result

The organization rule ID is added to the list of organization rules.

More Information

Organization Rules [page 64]
Modifying an Organization Rule [page 67]
Deleting an Organization Rule [page 68]

5.2.11.3 Modifying an Organization Rule

Use

Use this feature to change an existing organization rule.

Procedure

   The Organization Rules screen appears.

2. Choose the Organization Rule ID for the organization rule that you want to change, and then choose Open.
   The screen for the organization ID that you chose appears where you can enter changes.

3. Modify the organization rules as needed.
   You can only change data in the following fields:
   ○ Parent Org Rule ID
   ○ Description
On the Org Level tab, you can only change data in the following fields:

- Value From
- Value To
- Condition
- Status

**Note**

You cannot modify information on the Systems tab for parent organization rule IDs.

4. Choose **Save**.
   A confirmation message appears stating that the data has been saved.
5. Choose **Close**.

**Modifying large volume of organization rules**

Administrators can use the following Customizing activities (from transaction SPRO), under Governance, Risk, and Compliance > Access Control > Access Risk Analysis > SOD Rules to create and modify large volume of organization rules:

- Additional Rules Upload
- Additional Rules Download

**More Information**

Creating an Organization Rule [page 66]
Deleting an Organization Rule [page 68]
Organization Rules [page 64]

### 5.2.1.1.4 Deleting an Organization Rule

**Context**

Use this to delete an existing organization rule.

**Caution**

Deleting an organization rule invalidates any rule generated from that organization rule.
Procedure

2. Choose the Organization Rule ID for the organization rule that you want to delete, and choose Delete.
   A confirmation screen appears.
3. Choose OK.
4. Choose Close.

Next Steps

Creating an Organization Rule [page 66]
Modifying an Organization Rule [page 67]
Organization Rules [page 64]

5.2.1.2 Creating a Supplementary Rule

Use

Create a supplementary rule to ensure correct analysis results for a violation that might be reported as a false positive.

Procedure

To create a supplementary rule:

1. Choose Setup ➤ Supplementary Rules ➤
2. Choose Create.
3. From the System dropdown list, select the target system where this supplementary rule resides.
   To create the same rule in multiple target systems, you must create a rule for each system.
4. Enter the Function ID that requires a supplemental check to determine whether the user can perform the function. If you do not know the function ID, choose Search.
5. Enter a Risk ID (optional). If you do not know the rule ID, choose Filter.
6. Enter a description for the supplementary rule.
7. Enter the Name of any database table.
   You can enter a custom table or an SAP-delivered table.
8. Enter the user ID or role name in the Check Field Name field (BNAME or UNAME).
9. The *Include Violations* dropdown list controls whether the SoD Conflict report includes or excludes the violations for the objects (user, role, profile, and so on) that meet the rule criteria based on the table entries. To indicate that the violations for the objects (user, role, profile, and so on) that meet the supplementary rule criteria are included in the reports, choose *Yes*. If you choose *No*, the report excludes the violations for the objects (user, role, profile, and so on) that meet the criteria of the supplementary check.

**Note**

When you match wildcard values, the wildcard value requires an exact match of the entry in the rule and the entry to be checked in the SAP table.

---

**Result**

If you set the parameter *Use Supplementary SoD Analysis to Yes*, the system considers the supplementary rule when it generates the report.

**More Information**

- [Modifying a Supplementary Rule](page 70)
- [Deleting a Supplementary Rule](page 71)

### 5.2.1.2.1 Modifying a Supplementary Rule

**Procedure**

1. Choose Setup > exception access rules > Supplementary Rules.
2. Choose Filter.
   
   An empty row appears at the top of the list of supplementary rules.
3. Enter search criteria to locate the supplementary rule you want to edit.
4. Once you find the supplementary rule, edit it, and then choose Save.
   
   A confirmation message appears.
Next Steps

Creating a Supplementary Rule [page 69]
Deleting a Supplementary Rule [page 71]

5.2.1.2.2 Deleting a Supplementary Rule

Procedure

2. Choose Filter.
   
   An empty row appears at the top of the list of supplementary rules.
3. Enter search criteria to locate the supplementary rule you want to delete.
4. Once you find the supplementary rule, select the check box next to it, and then choose Delete.
   
   A confirmation message appears.
5. Choose OK.

Next Steps

Creating a Supplementary Rule [page 69]
Modifying a Supplementary Rule [page 70]

5.2.1.3 Generated Rules

Use

Access risk analysis processes access risks that you define. It generates rules based on the actions or permissions that an access risk contains.

Use this feature to view the reports containing the results of rules generated by using the Access Risks feature.

When you generate segregation of duties (SoD) action risks, access risk analysis creates a separate rule for each combination of actions that pose a risk.
Example

If an access risk includes two functions, each of which has five actions, and the access risk applies to two systems, access risk analysis generates 20 distinct rules from the access risk.

Example

You might have an access risk (P086) that includes the following functions:

- MD12 with 21 actions
- BR08 with 46 actions
- TS22 with 34 actions

If this access risk applies to three different versions of SAP that all run in your environment, then P086 translates to 98,532 distinct rules (21x46x34x3).

Note

The maximum number of SoD rules allowed per risk is 1,679,615. When access risk analysis attempts to process an access risk that generates more than the maximum number of rules, the following error message appears:

ERROR: Risk: #### has exceeded the maximum number of rules (1,679,615) that can be generated for a risk

More Information

Access Rule Summary [page 72]
Access Rule Detail [page 73]
Access Risks [page 84]
Exception Access Rules [page 64]
Organization Rules [page 64]

5.2.1.3.1 Access Rule Summary

Context

Use the Access Rule Summary screen to view an access rule summary report.
Procedure

   The Access Rule Summary Report screen appears.
2. Enter the selection criteria to limit results for your report.
3. Choose Run in Foreground or Run in Background to view the report. Consider running the report in the background when generating a large set of results.
   If you choose Run in Background, the Background Scheduler dialog appears. Enter the scheduler details, and then choose OK. The job number appears on the User Level screen.
   To view the job, navigate to Access Management ➤ Scheduling ➤ Background Jobs.
   If you choose Run in Foreground, confirm that you want to run the analysis immediately by choosing OK. The analysis results appear in a new screen.

Results

The access rule summary report shows the relationships between functions and access risks.

Next Steps

Access Risks [page 84]
Access Rule Detail [page 73]
Generated Rules [page 71]

5.2.1.3.2 Access Rule Detail

Prerequisites

You must generate rules by using the Access Risks feature before you can view an access rule detail report.

Context

Use the Access Rule Detail screen to view an access rule detail report.
Procedure

   The Access Rule Detail Report screen appears.
2. Enter the selection criteria to limit results for your report.
3. Choose Run in Foreground or Run in Background.
   Consider running the report in the background when generating a large set of results.
   If you choose Run in Background, the Background Scheduler dialog appears. Enter the scheduler details and choose OK. The job number appears on the User Level screen.
   To view the job, navigate to Access Management ➤ Scheduling ➤ Background Jobs.
   If you choose Run in Foreground, confirm that you want to run the analysis immediately by choosing OK. The analysis results appear in a new window.

Results

The access rule details report shows the rules generated for both actions and permissions.

Next Steps

Access Risks [page 84]
Access Rule Summary [page 72]
Generated Rules [page 71]

5.2.2 Access Rule Maintenance

Use

You can use the Access Rule Maintenance section to manage the following access rule entities:

- Rule sets – These are categories or groupings of rules used primarily for determining the group of access risks to use when running an access risk analysis.
- Functions – These are a collection of one or more actions that an employee needs to complete to perform a specific goal.
- Access risks – These are objects that identify potential access problems that your enterprise might encounter.
Features

Using the Access Rule Maintenance section, you can do the following:

- Search and display existing rule sets, functions, and access risks
- Create new rule sets, functions, and access risks
- Modifying existing rule sets, functions, and access risks
- Delete rule sets, functions, and access risks, as necessary

More Information

Rule Sets [page 75]
Functions [page 80]
Access Risks [page 84]

5.2.2.1 Rule Sets

Use

Rule sets are arbitrary definitions that apply only to access risks and rules. They define categories or groupings of rules. A rule set is used mainly for determining the group of access risks that are to be used when running an access risk analysis.

When you choose the Rule Set link, the Rule Sets screen appears, showing the existing rule sets that you are authorized to access.

Using the Rule Set screen, you can do the following:

- Enter search criteria to find a particular rule set using the Filter button
- Define a new query
- Rearrange column settings to create a personalized view of the screen

Activities

The tasks associated with managing risks include creating, viewing, modifying, and deleting rule sets.

More Information

Creating a New Rule Set [page 76]
5.2.2.1.1 Creating a New Rule Set

**Context**

A rule set includes an identifier and a description. To create a rule set, you choose a name and enter a description.

**Procedure**

1. Choose **Setup** > **Access Rule Maintenance** > **Rule Sets**.
2. Choose **Create**.
   
   The **Rule Set:New** screen appears.

3. Enter appropriate values in the fields:
   
   - **Rule Set ID**: Enter a name for the rule set. This name should be clear to other users of your organization.
   - **Description**: Enter a description of the rule set. This description should be clear to other users in your organization.

4. Choose **Save**.

**Results**

Access risk analysis saves the new rule set.

**Next Steps**

- Viewing a Rule Set [page 77]
- Modifying a Rule Set [page 78]
- Deleting a Rule Set [page 78]
5.2.2.1.2 Viewing a Rule Set

Context

To modify a rule set or to delete it, you begin by searching for the rule set and viewing it.

Procedure

   The Rule Sets screen appears.
2. Choose Filter.
   An empty row appears at the top of the list of rule sets.
3. In the Rule Set ID and Description fields, enter text to filter the number of results, and then press Enter.
   The filter returns all the rule sets that meet the search criteria. If you do not filter the text in these fields, the search returns all existing rule sets. The search supports wildcards (*).

Results

The number of rule sets returned depends on how much you restricted your search criteria terms. If the search does not return the rule sets you expected, perform the search again with more restrictive search criteria.

Next Steps

Creating a New Rule Set [page 76]
Modifying a Rule Set [page 78]
Deleting a Rule Set [page 78]
5.2.2.1.3 Modifying a Rule Set

Context

You can change only the rule set description. After you have created a rule set, you cannot change its ID.

Procedure

1. Follow the procedure in to search for the rule set you want to edit.
2. Select the rule set and choose Open.
   The Description field for that rule set turns white to indicate that you can edit the text field.
3. Edit the text and choose Save.
   The Change History tab on the Rule Set screen shows all of the changes for a selected Rule Set.

Next Steps

Creating a New Rule Set [page 76]
Viewing a Rule Set [page 77]
Deleting a Rule Set [page 78]

5.2.2.1.4 Deleting a Rule Set

Prerequisites

Before you can delete a rule set, you must remove the rule set assignment from all access risks by assigning a different rule set to each access risk.
Context

You can delete a rule set. However, if the rule set is assigned to another rule set, an access risk, or a rule, you cannot delete it.

Procedure

1. Follow the procedure in to search for the rule set you want to delete.
2. Choose the rule set you want to delete, and then choose Delete.

A dialog box appears asking you to confirm that you want to delete the rule set.

Next Steps

Creating a New Rule Set [page 76]
Viewing a Rule Set [page 77]
Modifying a Rule Set [page 78]

5.2.2.2 Functions and Risks

Use

A function is a grouping of one or more actions. An access risk is an object that associates two or more conflicting functions or a critical action and critical permission. Critical actions and critical permissions are also referred to as attributes. The attributes impact how the access risk translates into an access rule.

When you define an access risk, you specify a combination of functions that represent an access risk to an employee.

Note

The definition of a risk includes other attributes that impact how the risk translates into rules. The condition that determines the presence of a risk is one or more functions that when combined, create a conflict.

Actions assigned to a function represent the tasks an employee must be able to perform for a specific purpose. However, combined functions can conflict.

Example

An employee who has access to inventory records should not have the authority to sign for deliveries. When these two functions are combined, they pose a SoD risk.
## Functions

### Use

*Functions* are the building blocks of access risks. They define a collection of one or more tasks that an employee needs to complete to perform a specific goal.

These tasks are called *Actions*.

### Features

*Functions* have the following attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function ID</td>
<td>The identification code for the function.</td>
</tr>
<tr>
<td>Description</td>
<td>A short, plain text description of the function that identifies the nature of the function to users.</td>
</tr>
<tr>
<td>Business Process</td>
<td>A value that defines to which business process this function belongs. It is used for categorization purposes.</td>
</tr>
<tr>
<td>Analysis Scope</td>
<td>A parameter that determines if the function applies only to a single system (for example, SAP), or to multiple systems.</td>
</tr>
</tbody>
</table>

### Activities

When you define a function, you associate one or more actions to the function. Each of these actions has an associated permission (security object) that defines the scope of access for the action.
5.2.2.1.1 Creating a Function

Context

You create a function by assigning it an ID, describing it, and by defining its attributes.

Procedure

1. Choose \textit{Setup} \textgreater \textit{Access Rule Maintenance} \textgreater \textit{Functions}.
2. Choose \textit{Create}.
   
   The \textit{Function: New} screen appears.
3. Enter the basic attributes of the function.
   1. In the \textit{Function ID} field, enter the eight-character code for the function.
      Most enterprises choose a naming convention for this code. Access Control assigns default functions a four-character code.
   2. In the \textit{Description} field, enter a plain-text description of the function.
      You use this description to identify the function in the interface.
   3. From the \textit{Business Process} dropdown list, select the business process to which this function belongs.
      The \textit{Business Process} field is a required field. It is highly recommended that you associate each function with its proper business process unless the function belongs to more than one process.
   4. From the \textit{Analysis Scope} dropdown list, select either \textit{Single System} or \textit{Cross System}.
      ○ Choose \textit{Single System} if the function applies to one enterprise platform (SAP or non-SAP system).
      ○ Choose \textit{Cross System} if the function applies to multiple enterprise platforms (SAP and non-SAP systems).
4. You can associate the function with an action or a permission. Use the \textit{Action} list to associate an action with a function, to add an action to the list, or to delete an action from the list.
5. (Optional) Choose the \textit{Permissions} tab.
   
   The \textit{Permissions} screen appears, displaying the permissions (authorization objects) for all of the actions that have been added to the function.
Caution

This screen allows you to further restrict the access defined in the permission object. You cannot expand the access or reconfigure the permission object.

To modify access restrictions:
○ If you do not need to modify an associated permission, use the Permission Definition dialog.
○ To view and evaluate the details of a permission before you modify it, use the Permissions tab to expand and view each permission.

6. Choose Save.

Next Steps

Searching and Viewing a Function [page 82]
Modifying a Function [page 83]
Deleting a Function [page 84]

5.2.2.2.1.2 Searching and Viewing a Function

Context

To modify a function or to delete it, you must first search for and view the function.

Procedure

2. Choose Filter.

An empty row appears at the top of the list of functions.

3. In the Function ID and Description fields, enter text to limit the number of results, and then press Enter.

The filter returns all of the functions that meet the search criteria.

Restrict your search with filters or search terms or the search returns all existing functions. The search supports wildcards (*).
5.2.2.2.1.3 Modifying a Function

Context

You can modify any aspect of a function, except its ID.

Procedure

1. Follow the procedure to find the function you want to edit.
2. After you find the function, select the row and choose the Open pushbutton.
3. Modify the function.
   - The modifications you can make to a function are the same as the attributes you define in .
4. Choose Save.

Next Steps

Creating a Function [page 81]
Modifying a Function [page 83]
Deleting a Function [page 84]
5.2.2.2.1.4 Deleting a Function

Context

Use caution when you delete a function. You must first remove the function from any existing risk before you delete it.

Procedure

2. Choose Filter.
   - An empty row appears at the top of the list of functions.
3. Enter search criteria to locate the function you want to delete.
   - You can refer to for instructions on searching for the function that you want to delete.
4. Once you find the function, select the row and choose the Delete pushbutton.
   - A confirmation message appears.
5. Choose OK.

Next Steps

Creating a Function [page 81]
Modifying a Function [page 83]
Searching and Viewing a Function [page 82]

5.2.2.2 Access Risks

Use

Access risks identify potential access problems that your enterprise may encounter.
Use this feature to create, view, modify, or delete an access risk.
More Information

Creating Access Risks [page 85]
Searching and Viewing Access Risks [page 87]
Modifying an Access Risk [page 88]
Deleting an Access Risk [page 88]

5.2.2.2.2.1 Creating Access Risks

Context

An access risk requires an identifier and defined attributes.

Procedure

2. Choose Create.
3. Enter the basic attributes for the access risk.
   1. In the Risk ID field, enter a 4-character alphanumeric code to identify the risk.
      This code must be unique to this access risk.
   2. In the Description field, enter a short description of the risk.
   3. From the Risk Type dropdown list, select the risk type.
      Risk types include:
      ○ Segregation of Duties (SoD) risk
      ○ Critical Action risk
      ○ Critical Permission risk
   4. From the Risk Level dropdown list, select the severity of the risk.
      Risk Levels include:
      ○ Low
      ○ Medium
      ○ High
      ○ Critical
   5. From the Business Process dropdown list, select the business process for this risk.
   6. From the Status dropdown menu, select either Enabled or Disabled to indicate whether to activate the risk when you save it.
4. Choose the Functions tab to display the Function screen.
You use this screen to identify functions for this risk:

1. Select the check box next to an empty row and click the down-arrow at the right side of the row to display a scrolling list of all defined functions.
2. Select the function you want to add to the risk.

Repeat these steps until you have included all the functions in the risk:

- For SoD risks, select at least two functions.
- For Critical Action and Critical Permission risks, select at least one function.

5. Choose the Detailed Description tab to display the Detailed Description text field. Enter a description of the risk.

6. Choose the Control Objective tab to display the Control Objective text field. Enter a description of the control objective targeted by the risk.

⚠️ Caution
Avoid Tab keyboard characters when you enter risk data in the Detailed Description and the Control Objective text fields. Tab keyboard characters can cause problems when you use the Export and Import utilities to move rules from one system to another.

7. Choose the Risk Owners tab to display the Owner ID screen.

⚠️ Caution
To assign a risk owner to an access risk, you must ensure that the user is assigned as an owner.

You use this screen to identify the employee or employees who own this risk:

1. Choose the plus icon to add a Risk Owner field.
2. Select the down arrow at the right side of the row to display a list of defined employees.
3. To assign to the risk, select an owner from the list.

Repeat these steps to assign all owners to the risk.

8. Choose the Rule Sets tab to display the Rule Set screen.

This screen identifies the rules sets to add to this risk:

1. Choose the plus icon to add a rule set field.
2. Select the down arrow at the right side of the row to display a scrolling list of all defined rule sets.
3. Select the rule set you want to add to the risk.

Repeat these steps until you have added all the rule sets to the risk.

9. Choose Save.

Next Steps

- Searching and Viewing Access Risks [page 87]
- Modifying an Access Risk [page 88]
- Deleting an Access Risk [page 88]
5.2.2.2.2 Searching and Viewing Access Risks

Context

This procedure describes how to search for and view an access risk.

Procedure

   The Access Risk screen appears.
2. Choose Filter.
   An empty row appears at the top of the list of access risks.
3. Enter search criteria to filter your results, and then press Enter.
   The search supports wildcards (*).
   When you press Enter, the application returns the access risks that meet the search criteria in the Search Results screen.

Results

If you did not filter the search, the application may return a long list of access risks. You can navigate through the list to find the access risk that you seek.

Next Steps

Creating Access Risks [page 85]
Modifying an Access Risk [page 88]
Deleting an Access Risk [page 88]
5.2.2.2.3 Modifying an Access Risk

Context

You can modify most access risk selection criteria. However, you cannot modify the ID and Risk Type.

Procedure

   
   The Access Risk screen appears.
2. Follow the procedure in to find the access risk you want to edit.
3. After you find the access risk, select the row, and then choose the Open pushbutton.
   
   The SOD Risk screen appears.
4. Modify the access risk as appropriate.
5. Choose Save.

Next Steps

Creating Access Risks [page 85]
Searching and Viewing Access Risks [page 87]
Deleting an Access Risk [page 88]

5.2.2.2.4 Deleting an Access Risk

Context

You can delete any access risk. However, deleting an access risk invalidates any rule generated from that access risk.
Procedure

   The Access Risk screen appears.
2. Follow the procedure in to find the access risk you want to edit.
3. When you find the access risk, select the row and choose the Delete pushbutton.
   A confirmation message appears.
4. Choose OK.

Next Steps

Creating Access Risks [page 85]
Searching and Viewing Access Risks [page 87]
Modifying an Access Risk [page 88]

5.2.3 Critical Access Rules

Use

Use this feature to identify individual roles and profiles that pose an access risk to your enterprise. For example, any person who has the role of master database administrator is a risk to your enterprise. Verify that an employee assigned to this role meets the authorization requirements for your enterprise. Make sure that you designate the role as a critical role. If your system uses profiles, you may have defined profiles that pose an access risk. Make sure that you designate each one as a critical profile.

More Information

Critical Profiles [page 91]
Access Risks [page 84]
5.2.3.1 Critical Role and Critical Profile Rules

Concept

Identify individual roles and profiles that pose an access risk to your company. For example, any person who has the role of master database administrator is a risk to your enterprise. Ensure that an employee assigned to this role has been properly authorized. Make sure that you designate the role as a critical role. If your system uses profiles, you may have defined profiles that pose a risk. Make sure that you designate each one as a critical profile.

More Information

Critical Access Rules [page 89]
Critical Profiles [page 91]

5.2.3.1.1 Critical Roles

Use

Use this feature to identify roles that pose a risk to your company.

Procedure

To create and maintain critical roles:

   The Critical Roles screen appears.
2. Choose Create.
3. Select the System, the Rule Set, the Risk Level, and the Status from the dropdown lists.
4. Browse for the Role name.
5. Choose the Role you want, and then choose OK.
6. Enter a risk description that describes why this role is a critical role.
7. Choose Save.

Searching for a Critical Role

Use the Filter option to search for and make changes to a critical role.
To search for a critical role:

   The Critical Roles screen appears.
2. Choose Filter.
   An empty row appears at the top of the list of critical roles.
3. Enter search criteria to find the role you want to change and then press Enter.
   The application returns the critical roles that meet the criteria in the Search Results screen.

More Information

Critical Access Rules [page 89]
Critical Profiles [page 91]

5.2.3.1.2 Critical Profiles

Use

Use this feature to identify profiles that pose a risk to your company.

Procedure

To create a critical profile:

   The Critical Profiles screen appears.
2. Choose Create.
3. Select the System, Rule Set, Risk Level, and Status from the dropdown lists.
4. Browse for the Profile name.
5. Choose the Profile you want, and then choose OK.
6. Enter a risk description that describes why this profile is a critical profile.
7. Choose Save.

Searching for a Critical Profile

Use the Filter option to search for and make changes to a critical profile.

To search for a critical profile:

   The Critical Profiles screen appears.
2. Choose Filter.
   An empty row appears at the top of the list of critical profiles.
3. Enter search criteria to find the profile you want to change, and then press Enter. The application returns the critical profiles that meet the search criteria in the Search Results screen.

More Information

Critical Access Rules [page 89]
Critical Roles [page 90]

5.3 Access Risk Analysis

Use

An access risk is one or more actions or permissions that, when available to a single user (or single role, profile, or HR Object), creates the potential for fraud or unintentional errors.

As part of business operations, you can define access risks that require additional control to ensure that your organization is operating appropriately. You can then monitor and control these risks to prevent users from exploiting vulnerabilities to commit fraud or post unintentional errors.

Access Control enables you to specify the following types of access risks:

- **Segregation of Duties** – This is defined as one individual having the ability to perform two or more conflicting functions to control a process from beginning to end without the involvement of others. For example, one person might be able to set up a vendor and process payments, or manipulate sales and customer invoices, to conceal kickbacks.

- **Critical Action** – Certain functions are so critical in nature that anyone who has access needs to be identified and assessed to ensure the access is appropriate. This is different from segregation of duties risks in that the person only needs to have access to a single function. For example, the ability to configure a production system is considered a critical action regardless of any other access the person might have.

- **Critical Permission** – Similar to a critical action, there are certain permissions (authorization objects) that are considered critical on their own. For example, having background job administration permissions might be considered critical by certain organizations.

After you have defined the risks, you can use the Access Risk Analysis section to generate reports presenting different types of information, including reports presenting access risks, conflicts, or the use of critical actions by user, role, profile, or HR object.

**Note**

The administrator can configure the application to include firefighter (FF) assignments in the risk analysis. If the feature is enabled, the Risk Analysis screen displays the Include FFIDs checkbox. You can then choose whether or not to include firefighter assignments for your specific risk analysis.
The administrator configures this in the Customizing activity *Maintain Configuration Settings*, under

- Governance, Risk, and Compliance
- Access Control

For the parameter *Consider FF Assignments in Risk Analysis*, enter the values as follows:

<table>
<thead>
<tr>
<th>Column</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter Group</td>
<td>Risk Analysis</td>
</tr>
<tr>
<td>Parameter ID</td>
<td>1038</td>
</tr>
<tr>
<td>Parameter Value</td>
<td>Yes or No, as required</td>
</tr>
</tbody>
</table>

When you identify an access risk in a report, you can resolve or remediate the risk by either removing it or by applying a mitigating control. You can also use reports in the *Access Risk Analysis* section to view mitigated risks and risks that have not yet been remediated.

**More Information**

- User Level Access Risk Analysis [page 93]
- User Level Access Risk Analysis [page 93]
- Profile Level Access Risk Analysis [page 102]
- HR Objects Access Risk Analysis [page 105]

### 5.3.1 User Level Access Risk Analysis

**Context**

You can create a report displaying the user-level access risk analysis for your organization.

**Procedure**

1. Choose *Access Management ➔ Access Risk Analysis ➔ User Level*.
   
   The *Risk Analysis: User Level* screen appears.
2. Specify the analysis criteria.
1. Choose the object type using the first dropdown list, which contains the following options:
   - System
   - Custom Group

   **Note**
   You can use custom user groups to perform risk analysis for the group instead of separately for each user. For example, you create Group_A, and then add User_01 through User_10. You can then run risk analysis on Group_A. For more information, see Creating a Custom User Group. [page 96]

   - Include Users
   - Include Role Assignment
   - Org Level
   - Org Rule
   - User ID
   - Org Unit
   - Org Value
   - Risk by Process
   - Access Risk ID
   - Risk Level
   - Rule Set
   - User

   **Note**
   On an ad hoc basis, you can run a risk analysis for a filtered list of users based on their SU01 attributes. To do this, select **Multiple Selections** in the middle column. Then select **Add Selection**. Then select **Search SU01** to identify the attributes you want to analyze.

   - User Group
   - User Type
   - Validity Date

2. Choose the operator using the second dropdown list, from among the following:
   - is
   - is not
   - starts with
   - contains
   - is between
   - multiple selections

3. In the **Value** field, enter or select the value in the third field.

4. Optionally, add a line to the analysis criteria by choosing the plus (+) pushbutton and specifying the fields. Or you can remove a line by selecting the minus (-) pushbutton.

3. Specify the report options.
   1. In the **Format** section, select the format type and view.
      You can choose from among the following format types:
      - Summary
      - Detail
You can choose from among the following views:

- Management View
- Executive View
- Remediation View

**Note**

This view allows you to start remediation actions directly from the report. For more information, see [Remediation View](#) [page 211].

- Technical View
- Business View

4. In the **Type** section, select the report type:
   - Access Risk Analysis – Select Action Level, Permission Level, Critical Action, Critical Permission, and Critical Role/Profile.
   - Access Risk Assessment
   - Mitigating Analysis – Choose either Mitigating Controls or Invalid Mitigating Controls.

5. In the **Additional Criteria** section, select any additional reporting criteria.

6. Optionally, save the analysis criteria as a variant by typing a name in the **Save Variant as** field and choosing **Save**.

7. Choose **Run in Foreground** or **Run in Background**.

   If you choose **Run in Background**, the **Background Scheduler** dialog appears. Enter the scheduler details and choose **OK**. The job number appears on the **User Level** screen.

   To view the job, navigate to [Access Management] [Scheduling] [Background Jobs]

   If you choose **Run in Foreground**, confirm that you want to run the analysis immediately by choosing **OK**. The analysis results appear in a new window.

**Next Steps**

- [Access Risk Analysis](#) [page 92]
- [User Level Simulation](#) [page 97]
- [Creating a Custom User Group](#) [page 96]
- [Remediation View](#) [page 211]
### 5.3.1.1 Creating a Custom User Group

#### Use

You can use custom user groups to perform activities, such as risk analysis, for the group instead of separately for each user. For example, you create Group_A, and then add User_01 through User_10. You can then perform the activity on Group_A.

#### Prerequisites

This functionality is applicable to two scenarios, User Level Analysis and User Level Simulation.

#### Procedure

**Note**

There are two ways to create a Custom User Group.

- You can use the Customizing activity (transaction SPRO). Locate the activity and documentation at Governance, Risk and Compliance > Access Control > Maintain Custom User Group.
- You can create it directly from the application, if you have authorization. The steps below give instructions how to create the group through the application. This method also allows you to add users to the group based on their SU01 attributes.

2. Locate the Custom Group in the list of Analysis Criteria.
3. Accept the default of is in the second column.
4. In the next column, select F4 to see the Custom Group Search screen.
5. Enter the new Custom User Name.

**Note**

To see the existing groups, select Reset to clear the field. Then click Search. The left column lists the existing Custom Group Names. The right column shows the User IDs of the members of the selected Custom User Group. If you need to limit the number of Custom User Groups shown, you can use wildcards (such as the asterisk).

6. Click Create. The Custom Group screen appears.
7. Enter a Description of the new group.
8. Choose the SU01 Attributes that your users have in common. System is required and it must be a SAP system.
10. Select the User IDs you want from the list.
11. Click Selected Users to see the list of the users that you have chosen for your Custom User Group. Verify that these are the users you wanted in your Custom User Group.
12. Select Save to save your group with its members.

More Information

Access Risk Analysis [page 92]
User Level Access Risk Analysis [page 93]
User Level Simulation [page 97]

Creating a Custom User Group (through SPRO): Governance, Risk and Compliance > Access Control > Maintain Custom User Group

5.3.2 User Level Simulation

Context

You can use the functions on the User Level Simulation screen to perform user-level simulation as part of the access risk analysis for your organization.

Procedure

   The Simulation: User Level screen appears and displays the Define Analysis Criteria phase.
2. Define the analysis criteria:
   ○ Use an existing set of analysis criteria by entering its name in the Saved Variants field.
   ○ Use the fields available on the screen to specify new analysis criteria:
     1. In the Analysis Criteria area, use the fields to specify the analysis criteria, such as System, User, and so on.
     i Note
        You can use the plus (+) and minus (-) pushbuttons to add or remove criteria fields.
2. Under the Report Options area, choose from the following:
   ○ Format, such as Summary, Detail, Management Summary, and Executive Summary
View, such as Technical View and Business View

Type, only Access Risk Analysis is available and is automatically selected. You can select from the following access risk analysis options: Action Level, Permission Level, Critical Action, Critical Permission, Critical Role/Permission

Additional Criteria, such as Include Mitigated Risks, Show All Objects and Consider Org Rule.

3. Optionally, you can save the analysis criteria for future use by entering a name in the Save Variant as field and choosing Save.

4. Choose Next.

3. On the Define Simulation Criteria screen, specify the criteria:

○ Use an existing set of simulation criteria by entering the name in the Saved Variants field.

○ Use the fields available to specify new simulation criteria:

1. Choose the Actions tab to add or remove actions, or add or remove permissions associated with actions.
2. Choose the Roles tab to add or remove roles, or add or remove permissions associated with roles.
3. Choose the Profiles tab to add or remove profiles, or add or remove permissions associated with profiles.
4. In the Additional Criteria section, select any additional reporting criteria such as Exclude Values and Risk from Simulation Only.
5. Optionally, save the simulation criteria as a variant by entering a name in the Save Variant as field and choosing Save.
6. Choose Run in Foreground to start the simulation immediately or choose Run in Background to schedule a time and date to start the simulation.

Note

To view the status of background jobs, navigate to Access Management > Scheduling > Background Jobs

7. If you choose Run in Foreground, confirm you want to run the analysis immediately by choosing OK. The simulation results appear in the Confirmation screen.

4. On the Confirmation screen, review the results.

Optionally, choose Export Result Sets to export the results to your local machine.

Next Steps

Access Risk Analysis [page 92]
User Level Access Risk Analysis [page 93]
5.3.3 Role Level Access Risk Analysis

Context

You can create a report displaying the role-level access risk analysis for your organization.

Procedure

1. Choose [Access Management] [Access Risk Analysis] [Role Level].
   The Risk Analysis: Role Level screen appears.
2. Specify the analysis criteria.
   Do the following:
   1. Choose the object type using the first dropdown list, from among the following:
      - System
      - Org Level
      - Org Rule
      - Org Unit
      - Org Value
      - Risk by Process
      - Access Risk ID
      - Risk Level
      - Role
      - Role Type
      - Rule Set
      - Validity Date
   2. Choose the operator using the second dropdown list, from among the following:
      - is
      - is not
      - starts with
      - contains
      - is between
      - multiple selections
   3. In the Value field, enter or select the value in the third field.
   4. Optionally, add a line to the analysis criteria by choosing the plus (+) button and specifying the appropriate fields. Alternatively, remove a line from the analysis criteria by choosing the corresponding minus (-) button.
3. Specify the report options.
Do the following:

1. In the **Format** section, select the format type and view.
   - You can choose from among the following format types:
     - Summary
     - Detail
     - Management View
     - Executive View
   - You can choose from among the following views:
     - Technical View
     - Business View

4. In the **Type** section, select the report type from among the following:
   - Access Risk Analysis – You can select Action Level, Permission Level, Critical Action, Critical Permission, Critical Role/Profile, and Analytical Report.
   - Access Risk Assessment
   - Mitigating Analysis – You can choose either Mitigating Controls or Invalid Mitigating Controls.

5. In the **Additional Criteria** section, select any additional reporting criteria.

6. Optionally, save the analysis criteria as a variant by typing a name in the **Save Variant as** field, and then choosing **Save**.

7. Choose **Run in Foreground** or **Run in Background**.

   If you choose **Run in Background**, the **Background Scheduler** dialog appears. Enter the scheduler details and choose **OK**. The job number appears on the **User Level** screen.

   To view the job, navigate to **Access Management ➤ Scheduling ➤ Background Jobs**.

   If you choose **Run in Foreground**, confirm that you want to run the analysis immediately by choosing **OK**. The analysis results appear in a new window.

**Next Steps**

- Access Risk Analysis [page 92]
- Role Level Simulation [page 100]

**5.3.4 Role Level Simulation**

**Context**

You can use the functions on the **Role Level Simulation** screen to perform role-level simulation as part of the access risk analysis for your organization.
Procedure

   The Simulation: Role Level screen appears and displays the Define Analysis Criteria phase.

2. Define the analysis criteria by the following methods:
   - Use an existing set of analysis criteria by entering its name in the Saved Variants field.
   - Use the fields available on the screen to specify new analysis criteria by doing the following:
     1. Under the Analysis Criteria area, use the available fields to specify the analysis criteria, such as System, Analysis Type, and so on.

   Note
   You can use the plus (+) and minus (-) pushbuttons to add or remove criteria fields.

   2. Under the Report Options area, select and choose from the following:
      - Format, such as Summary, Detail, Management Summary, and Executive Summary
      - View, such as Technical View and Business View
      - Type, only Access Risk Analysis is available and is automatically selected. You can select from the following access risk analysis options: Action Level, Permission Level, Critical Action, Critical Permission, Critical Role/Permission
      - Additional Criteria, such as Include Mitigated Risks and Show All Objects

   3. Optionally, you can, save the analysis criteria as a variant by entering a name in the Save Variant as field and choosing Save.

4. Choose Next.

3. On the Define Simulation Criteria screen, specify the criteria for the simulation by the following methods:
   - Use an existing set of simulation criteria by entering its name in the Saved Variants field.
   - Use the fields available on the screen to specify new simulation criteria by doing the following:
     1. Choose the Actions tab page to add actions, remove actions, or add and remove permissions associated with actions.
     2. Choose the Roles tab page to add roles, remove a role, or add and remove permissions associated with roles.
     3. Choose the Profiles tab page to add profiles, remove profiles, or add and remove permissions associated with profiles.
     4. In the Additional Criteria section, select any additional reporting criteria such as Exclude Values and Risk from Simulation Only.
     5. Optionally, save the simulation criteria as a variant by entering a name in the Save Variant as field and choosing Save.
     6. Choose Run in Foreground to start the simulation immediately or choose Run in Background to schedule a time and date to start the simulation.

   Note
   To view the status of background jobs, navigate to Access Management ➤ Scheduling ➤ Background Jobs ➤.

7. If you choose Run in Foreground, confirm you want to run the analysis immediately by choosing OK. The simulation results appear in the Confirmation screen.
4. On the **Confirmation** screen, review the results.
   Optionally, choose **Export Result Sets** to export the results to your local machine.

**Next Steps**

- Access Risk Analysis [page 92]
- Role Level Access Risk Analysis [page 99]

### 5.3.5 Profile Level Access Risk Analysis

**Context**

You can create a report displaying the profile-level access risk analysis for your organization.

**Procedure**

1. Choose **Access Management** ➤ **Access Risk Analysis** ➤ **Profile Level**.
   The **Risk Analysis: Profile Level** screen appears.

2. Specify the analysis criteria.
   Do the following:
   
   1. Choose the object type using the first dropdown list, from among the following:
      - System
      - Profile
      - Risk by Process
      - Access Risk ID
      - Risk Level
      - Rule Set
      - Validity Date
   
   2. Choose the operator using the second dropdown list, from among the following:
      - is
      - is not
      - starts with
      - contains
      - is between
3. Specify the report options.

Do the following:

1. In the **Format** section, select the format type and view. You can choose from among the following format types:
   - Summary
   - Detail
   - Management View
   - Executive View
   You can choose from among the following views:
   - Technical View
   - Business View
2. In the **Type** section, select the report type from among the following:
   - Access Risk Analysis – Select *Action Level, Permission Level, Critical Action, Critical Permission*, and *Critical Role/Profile*.
   - Access Risk Assessment
   - Mitigating Analysis – Choose either *Mitigating Controls* or *Invalid Mitigating Controls*.
3. In the **Additional Criteria** section, select any additional reporting criteria.
4. Optionally, save the analysis criteria as a variant by typing a name in the **Save Variant as** field and choosing **Save**.
5. Choose **Run in Foreground** or **Run in Background**.

If you choose **Run in Background**, the **Background Scheduler** dialog appears. Enter the scheduler details and choose **OK**. The job number appears on the **User Level** screen.

To view the job, navigate to **Access Management ➔ Scheduling ➔ Background Jobs**.

If you choose **Run in Foreground**, confirm that you want to run the analysis immediately by choosing **OK**. The analysis results appear in a new window.

**Next Steps**

- Access Risk Analysis [page 92]
- Profile Level Simulation [page 104]
5.3.6 Profile Level Simulation

Context

You can use the functions on the Profile Level Simulation screen to perform profile-level simulation as part of the access risk analysis for your organization.

Procedure


   The Simulation: Profile Level screen appears and displays the Define Analysis Criteria phase.

2. Define the analysis criteria by the following methods:
   ○ Use an existing set of analysis criteria by entering its name in the Saved Variants field.
   ○ Use the fields available on the screen to specify new analysis criteria by doing the following:
     1. Under the Analysis Criteria area, use the available fields to specify the analysis criteria, such as System, Analysis Type, and so on.

      i  Note
      You can use the plus (+) and minus (-) pushbuttons to add or remove criteria fields.

     2. Under the Report Options area, select and choose from the following:
        ○ Format, such as Summary, Detail, Management Summary, and Executive Summary
        ○ View, such as Technical View and Business View
        ○ Type, only Access Risk Analysis is available and is automatically selected. You can select from the following access risk analysis options: Action Level, Permission Level, Critical Action, Critical Permission, Critical Role/Permission
        ○ Additional Criteria, such as Include Mitigated Risks and Show All Objects

3. Optionally, you can save the analysis criteria as a variant by entering a name in the Save Variant as field and choosing Save.

4. Choose Next.

3. On the Define Simulation Criteria screen, specify the criteria for the simulation by the following methods:
   ○ Use an existing set of simulation criteria by entering its name in the Saved Variants field.
   ○ Use the fields available on the screen to specify new simulation criteria by doing the following:
     1. Choose the Actions tab page to add actions, remove actions, or add and remove permissions associated with actions.
     2. Choose the Roles tab page to add roles, remove a role, or add and remove permissions associated with roles.
     3. Choose the Profiles tab page to add profiles, remove profiles, or add and remove permissions associated with profiles.
4. In the Additional Criteria section, select any additional reporting criteria such as Exclude Values and Risk from Simulation Only.

5. Optionally, save the simulation criteria as a variant by entering a name in the Save Variant as field and choosing Save.

6. Choose Run in Foreground to start the simulation immediately or choose Run in Background to schedule a time and date to start the simulation.

   **Note**

   To view the status of background jobs, navigate to Access Management > Scheduling > Background Jobs.

7. If you choose Run in Foreground, confirm you want to run the analysis immediately by choosing OK. The simulation results appear in the Confirmation screen.

4. On the Confirmation screen, review the results.

   Optionally, choose Export Result Sets to export the results to your local machine.

### Next Steps

Access Risk Analysis [page 92]
Profile Level Access Risk Analysis [page 102]

### 5.3.7 HR Objects Access Risk Analysis

#### Context

You can create a report that displays the access risk analysis for HR Objects for your organization.

#### Procedure


2. Choose from one of the following methods to create a risk analysis report for HR objects:
   - Use an existing set of analysis criteria by entering its name in the Saved Variants field.
   - Use the fields available on the screen to specify new analysis criteria by doing the following:
     1. Under the Analysis Criteria area, use the available fields to specify the analysis criteria, such as System, Analysis Type, and so on.
2. Under the **Report Options** area, select and choose from the following:
   - **Format**, such as **Summary**, **Detail**, **Management Summary**, and **Executive Summary**
   - **View**, such as **Technical View** and **Business View**
   - **Additional Criteria**, such as **Include Mitigated Risks** and **Show All Objects**

3. In the **Type** area, select from the following types and options:
   - **Access Risk Analysis**
     You can select from the following access risk analysis options: **Action Level**, **Permission Level**, **Critical Action**, **Critical Permission**, **Critical Role/Permission**
   - **Access Risk Assessment**
   - **Mitigation Analysis**
     You can select from the following mitigation analysis options: **Mitigating Controls**, or **Invalid Mitigating Controls**.

4. Optionally, you can save the analysis criteria as a variant by entering a name in the **Save Variant as** field and choosing **Save**.

3. Choose **Run in Foreground** to start the analysis immediately or choose **Run in Background** to schedule a time and date to start the analysis.

   **Note**

   To view the status of background jobs, navigate to **Access Management** ➔ **Scheduling** ➔ **Background Jobs**.

4. If you choose **Run in Foreground**, confirm you want to run the analysis immediately by choosing **OK**.

**Next Steps**

Access Risk Analysis [page 92]

HR Objects Simulation [page 106]

**5.3.8 HR Objects Simulation**

**Context**

You can perform HR object-level simulation as part of the access risk analysis for your organization.
Procedure


2. Define the analysis criteria by the following methods:
   ○ Use an existing set of analysis criteria by entering its name in the Saved Variants field.
   ○ Use the fields available on the screen to specify new analysis criteria by doing the following:
     1. Under the Analysis Criteria area, use the available fields to specify the analysis criteria, such as System, Analysis Type, and so on.

   **Note**
   You can use the plus (+) and minus (-) pushbuttons to add or remove criteria fields.

   2. Under the Report Options area, select and choose from the following:
      ○ Format, such as Summary, Detail, Management Summary, and Executive Summary
      ○ View, such as Technical View and Business View
      ○ Type, only Access Risk Analysis is available and is automatically selected. You can select from the following access risk analysis options: Action Level, Permission Level, Critical Action, Critical Permission, Critical Role/Permission
      ○ Additional Criteria, such as Include Mitigated Risks and Show All Objects

3. Optionally, you can, save the analysis criteria as a variant by entering a name in the Save Variant as field and choosing Save.

4. Choose Next.

3. On the Define Simulation Criteria screen, specify the criteria for the simulation by the following methods:
   ○ Use an existing set of simulation criteria by entering its name in the Saved Variants field.
   ○ Use the fields available on the screen to specify new simulation criteria by doing the following:
     1. Choose the Actions tab page to add actions, remove actions, or add and remove permissions associated with actions.
     2. Choose the Roles tab page to add roles, remove a role, or add and remove permissions associated with roles.
     3. Choose the Profiles tab page to add profiles, remove profiles, or add and remove permissions associated with profiles.
     4. In the Additional Criteria section, select any additional reporting criteria such as Exclude Values and Risk from Simulation Only
     5. Optionally, save the simulation criteria as a variant by entering a name in the Save Variant as field and choosing Save.
     6. Choose Run in Foreground to start the simulation immediately or choose Run in Background to schedule a time and date to start the simulation.

   **Note**
   To view the status of background jobs, navigate to Access Management ➔ Scheduling ➔ Background Jobs.

7. If you choose Run in Foreground, confirm you want to run the analysis immediately by choosing OK. The simulation results appear in the Confirmation screen.
4. On the Confirmation screen, review the results.
   Optionally, choose Export Result Sets to export the results to your local machine.

Next Steps

Access Risk Analysis [page 92]
HR Objects Access Risk Analysis [page 105]

5.4 Mitigated Access

Use

Mitigated Access allows you to manage the risks associated with access control by identifying risks, assessing the level of those risks, and assigning mitigating controls to users, roles, and profiles to mitigate access rule violations.

A risk is identified through risk analysis and cannot be mitigated unless the control has been previously defined.

The first step in defining or creating a mitigating control is to create a mitigating control ID. This ID appears in risk analysis reports. All risk IDs associated with the control must also be mitigated with this control.

Features

- Create mitigating controls that you cannot remove
- Assign mitigating controls to users, roles, and profiles that contain a risk
- Establish a period of time during which the control is valid
- Specify steps to monitor conflicting actions associated with the risk
- Create administrator, control monitors, approvers, and risk owners and assign mitigating controls to them.

You can print all search results in mitigation or export them to an Excel file. Due to screen size limitations, the printed and exported versions of the search results may contain more data fields than the screen can display.

More Information

Mitigated Users [page 109]
Mitigated User for Organization Rules [page 110]
5.4.1 Mitigated Users

Use

Use the Mitigated Users area to make new mitigated users by associating them with predefined mitigating controls individually or with blanket mitigation. Blanket mitigation allows you to mitigate access risks for several users at one time.

You can also use this feature to search for users already mitigated by association of a user and a mitigating control.

Prerequisites

You must first define a mitigating control before you can assign it to users to mitigate an access risk.

Assigning a Mitigating Control to a User

   The Mitigated Users screen appears showing a list of existing users to whom mitigating controls have been assigned.
2. Choose the Assign pushbutton.
   The User Mitigation window appears.
3. Enter information in the required fields marked with an asterisk (*).
   ○ Access Risk ID – Select the field to enter the access risk ID.
   ○ Control ID – Select the field to enter the control ID.
   ○ Monitor – Automatically populated with system data after you choose the control ID.
   ○ Valid From – Start of the mitigating control period.
   ○ Valid To – End of the mitigating control period.
   ○ Status – Choose Active or Inactive from the dropdown list.
4. Choose the Add pushbutton to associate a system to the mitigating control.
5. Choose the Add pushbutton to associate a user to the mitigating control.
6. Choose Submit > Close.
   The mitigating control you assigned is included in the list on the Mitigated Users screen.

Deleting a Mitigating Control from a User

   The Mitigated Users screen appears showing a list of existing users to whom mitigating controls have been assigned.
2. Select the user you want to delete and choose the Delete pushbutton.
   Confirm your decision to delete this mitigating control.
3. Choose the Yes pushbutton.  
The mitigating control is removed from the Mitigated Users screen.

More Information

5.4.2 Mitigated User for Organization Rules

Use

Prerequisites
You must first define a mitigating control before you can assign it to an organization to mitigate an access risk.

Assigning a Mitigating Control to an Organization Rule

The Mitigated User Organization Rule screen appears showing a list of existing organizations to which mitigating controls have been assigned.

2. Choose Assign.  
The User Org Mitigation screen appears.

3. Enter information in the required fields. The required fields are marked with an asterisk (*).
   ○ Org. Rule ID – Select the field to enter the organization rule ID.
   ○ Access Risk ID – Select the field to enter the access risk ID.
   ○ Control ID – Enter the control ID.
   ○ Monitor – Automatically populated with system data after you choose the control ID.
   ○ Valid From – Start of the mitigating control period.
   ○ Valid To – End of the mitigating control period.
   ○ Status – Choose Active or Inactive from the dropdown list.

4. Choose Add to associate a system to the mitigating control.

5. Choose Add to associate a user to the mitigating control.

6. Choose Submit ➤ Close.  
The mitigating control you assigned is included in the list on the Mitigated Users screen.

Deleting a Mitigated User Organization Rule

The Mitigated User Organization Rule screen appears showing a list of existing organizations to which mitigating controls have been assigned.

2. Select the user you want to delete and choose Delete.  
Confirm your decision to delete this mitigating control.

3. Choose Yes.  
The mitigating control you deleted is removed from the Mitigated User Organization Rule screen.
5.4.3 Mitigated Roles

Use

Use the Mitigated Roles screen to assign mitigating controls to a role.

Prerequisites

You must first define a mitigating control before you can assign it to a role to mitigate an access risk.

Assigning Mitigating Controls to Roles

1. Choose Access Management Mitigated Access Mitigated Roles. The Mitigated Roles screen displays a list of existing roles to which mitigating controls have been assigned.
2. Choose Assign. The Roles Mitigation dialog box opens.
3. Enter information in the required fields marked with an asterisk (*).
   - Access Risk ID – Select the field to enter the access risk ID.
   - Control ID – Enter the control ID.
   - Monitor – Automatically populated with system data after you choose the control ID.
   - Valid From – Start of the mitigating control period.
   - Valid To – End of the mitigating control period.
   - Status – Choose Active or Inactive from the dropdown list.
4. Choose Add to associate a system to the mitigating control.
5. Choose Add to associate a role to the mitigating control.
6. Choose Submit Close. The mitigating control you assigned is included in the list on the Mitigated Roles screen.

Deleting Mitigating Controls from Roles

1. Choose Access Management Mitigated Access Mitigated Roles. The Mitigated Roles screen displays a list of existing roles to which mitigating controls have been assigned.
2. Select the role you want to delete and choose Delete. Confirm your decision to delete this mitigating control.
3. Choose Yes. The mitigating control is removed from the Mitigated Roles screen.
5.4.4 Mitigated Profiles

Use

Use the Mitigated Profiles screen to assign mitigating controls to a profile.

Prerequisites

You must first define a mitigating control before you can assign it to a profile to mitigate an access risk.

Assigning a Mitigating Control to a Profile

1. Choose Access Management ➤ Mitigated Access ➤ Mitigated Profiles. The Mitigated Profiles screen shows a list of existing profiles to which mitigating controls have been assigned.
2. Choose Assign. The Profile Mitigation screen appears.
3. Enter information in the required fields, which are marked with an asterisk (*).
   - Access Risk ID – Select the field to enter the access risk ID.
   - Control ID – Select the field to enter the control ID you want to add.
   - Monitor – This field is automatically populated with system data after you choose the control ID.
   - Valid From – This is the start of the period for the mitigating control.
   - Valid To – This is the end of the period for the mitigating control.
   - Status – Choose Active or Inactive from the dropdown list.
4. Choose Add to associate a system to the mitigating control.
5. Choose Add to associate a role to the mitigating control.
6. Choose Submit Close. The mitigating control you assigned is included in the list on the Mitigated Profiles screen.

Deleting a Mitigating Control from a Profile

1. Choose Access Management ➤ Mitigated Access ➤ Mitigated Profiles. The Mitigated Profiles screen shows a list of existing profiles to which mitigating controls have been assigned.
2. Select the profile you want to delete and choose Delete. Confirm your decision to delete this mitigating control.
3. Choose Yes. The mitigating control you deleted is removed from the Mitigated Profiles screen.

More Information
5.4.5 HR Objects Mitigation

Use

You can use the functions on the HR Mitigation screen to mitigate access risks by assigning mitigating controls to human resource (HR) objects.

Prerequisites

You have defined mitigating controls.

For more information, see .

Procedure

Assigning Mitigating Controls to HR Objects

   The HR Mitigation screen displays the list of existing HR objects to which mitigating controls have been assigned.
2. Choose Assign.
   The HR Object Mitigation screen appears.
3. Enter information in the required fields.
   ○ Object Type – Select the field to enter the object type.
   ○ Access Risk ID – Enter the access risk ID.
   ○ Control ID – Enter the control ID.
   ○ Monitor – Automatically populated with system data after you choose the control ID.
   ○ Valid From – Start of the mitigating control period.
   ○ Valid To – End of the mitigating control period.
   ○ Status – Choose Active or Inactive from the dropdown list.
4. In the Systems table, choose Add to associate a system to the mitigating control.
5. In the HR Object table, choose Add to associate an HR object to the mitigating control.
6. Choose Submit if workflows are enabled.
   If workflows are not enabled, choose Save.
7. Choose Close.

Deleting Mitigating Controls from HR Objects

   The HR Mitigation screen displays the list of existing HR objects to which mitigating controls have been assigned.
2. Select an HR object and then choose Delete.
3. On the Confirm dialog screen, choose Yes.
5.4.6 Mitigated Role for Organization Rules

Use the Role Organization Mitigation screen to assign mitigating controls to an organization rule for a role.

Prerequisites

You must first define a mitigating control before you can assign it to an organization role to mitigate an access risk.

Assigning Role Organization Mitigation

1. Choose ➔ Access Management ➔ Mitigated Access ➔ Role Organization Mitigation ➔. The Role Organization Mitigation screen shows a list of existing organization roles to which mitigating controls have been assigned.
2. Choose Assign. The Role Org Mitigation window opens.
3. Enter information in the required fields, which are marked with an asterisk (*).
   - Org. Rule ID – Select the field to enter the organization rule ID.
   - Access Risk ID – Select the field to enter the access risk ID.
   - Control ID – Select the field to enter the control ID you want to add.
   - Monitor – This field is automatically populated with system data after you choose the control ID.
   - Valid From – This is the start of the period for the mitigating control.
   - Valid To – This is the end of the period for the mitigating control.
   - Status – Choose Active or Inactive from the dropdown menu.
4. Choose Add to associate a system with the mitigating control.
5. Choose Add to associate an organization role with the mitigating control.
6. Choose ➔ Submit ➔ Close ➔. The mitigating control you assigned is included in the list on the Role Organization Mitigation screen.

Deleting Mitigating Controls from Roles

1. Choose ➔ Access Management ➔ Mitigated Access ➔ Role Organization Mitigation ➔. The Role Organization Mitigation screen shows a list of existing organization roles to which mitigating controls have been assigned.
2. Select the organization role you want to delete and choose Delete. Confirm your decision to delete this mitigating control.
3. Choose Yes. The mitigating control you deleted is removed from the Role Organization Mitigation screen.
5.5  Analyzing Risks When Approving Access Requests

Use

On the Access Request screen, you can perform risk analysis and impact analysis before approving requests. You have the following options for performing the analysis:

- On the Risk Violations tab, you can perform the analysis and save the results.
- On the User Access tab, you can use the Simulation feature to first perform the analysis and then choose whether or not to save the results.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>● You can set the requirement that approvers must analyze risks before approving access requests. You maintain this setting in the Customizing activity (transaction SPRO) Maintain MSMP Workflows, under Governance, Risk, and Compliance &gt; Access Control &gt; Workflow for Access Control. In the Maintain Paths phase, under the Maintain Stages section, select Display Task Settings. Select the Risk Analysis Mandatory field and choose Yes or No as needed.</td>
</tr>
<tr>
<td>● You can allow approvers to approve access requests despite risks. You maintain this setting in the Customizing activity Maintain MSMP Workflows, under Governance, Risk, and Compliance &gt; Access Control &gt; Workflow for Access Control. In the Maintain Paths phase, under the Maintain Stages section, select Display Task Settings. Select the checkbox for the Approve Despite Risk field.</td>
</tr>
</tbody>
</table>

Procedure

The following procedure is the same regardless of the tab page you choose to initiate it. The only difference is that the Simulation allows you to choose whether or not to save the results.

1. From the My Home work center, select Work Inbox. On the Workitems screen, select Access Management. Choose an access request.
2. Do one of the following:
   - Select the Risk Violations tab.
   - On the User Access tab, choose Simulation.
3. In the Analysis Type dropdown list, select the relevant analysis type.
   - You use Risk Analysis to determine violations pertaining to the authorizations assigned to the role. For example, when the authorizations result in segregation of duties violations.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can customize SAP Access Control to include firefighter assignments automatically in the risk analysis.</td>
</tr>
</tbody>
</table>
You maintain this setting in the Customizing activity (transaction SPRO) Maintain Configuration Settings, under Governance, Risk, and Compliance Access Control. For the parameter Consider FF Assignments in Risk Analysis, enter the values as follows:

<table>
<thead>
<tr>
<th>Parameter Group</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Analysis</td>
<td></td>
</tr>
<tr>
<td>Parameter ID</td>
<td>1038</td>
</tr>
<tr>
<td>Parameter Value</td>
<td>Yes or No, as required</td>
</tr>
</tbody>
</table>

- You use Impact Analysis to determine authorization violations pertaining to other roles. That is, the authorizations for the selected role, in combination with authorizations for another role, result in violations.

4. Select the System and Rule Set.
5. Under the Result Options area, select the format, type, and additional criteria for the analysis results.

Example

<table>
<thead>
<tr>
<th>Format</th>
<th>Executive Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Action Level, Permission Level</td>
</tr>
<tr>
<td>Additional Criteria</td>
<td>Include Mitigated Risks</td>
</tr>
</tbody>
</table>

6. Choose the Run Risk Analysis pushbutton.
7. In the Result area, you can choose different ways to view the analysis results.
8. If you are running a simulation, you can do the following:
   - Choose Cancel if you do not want to save the results of the analysis.
   - Choose Apply if you want to save the results of the analysis. The information is saved to the Risk Violations tab and you can view it whenever you open the request. The results are also available to the approver of the request.
9. On the Risk Violations tab, you can choose to mitigate any risk by selecting the risk and choosing Mitigate Risk.
5.6 Analyzing Risks When Submitting Access Requests

Use

On the Access Request screen, you can perform risk analyses and impact analyses on the following tab pages:

- **Risk Violations**
  If you want to save the results of the analysis, use the analysis function on this tab.

- **User Access**
  The Simulation feature allows you to perform the analysis first and then choose whether or not to save the results.

**Note**

- You can set the application to analyze risks automatically when someone submits an access request. For example, if the requester chooses to submit a request without analyzing the risks first, the application automatically performs an analysis and adds the results to the access request that appears in the approver’s Work Inbox.
  You maintain this setting in the Customizing activity Maintain Configuration Settings, under Governance, Risk, and Compliance > Access Control. For the parameter Enable risk analysis on form submission, enter the values as follows:

<table>
<thead>
<tr>
<th>Column</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter Group</td>
<td>Risk Analysis – Access Request</td>
</tr>
<tr>
<td>Parameter ID</td>
<td>1071</td>
</tr>
<tr>
<td>Parameter Value</td>
<td>Yes or No, as required</td>
</tr>
</tbody>
</table>

- You can set the application to include firefighter assignments in the risk analysis.
  You maintain this setting in the Customizing activity Maintain Configuration Settings, under Governance, Risk, and Compliance > Access Control. For the parameter Consider FF Assignments in Risk Analysis, enter the values as follows:

<table>
<thead>
<tr>
<th>Column</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter Group</td>
<td>Risk Analysis</td>
</tr>
<tr>
<td>Parameter ID</td>
<td>1038</td>
</tr>
<tr>
<td>Parameter Value</td>
<td>Yes or No, as required</td>
</tr>
</tbody>
</table>
Procedure

The following procedure is the same regardless of which tab page you choose to initiate it. The only difference is that the simulation feature allows you to choose whether or not to save the results.

1. On the screen, do one of the following:
   ○ Select the Risk Violations tab.
   ○ On the User Access tab, choose Simulation.

2. In the Analysis Type dropdown list, select the relevant analysis type:
   ○ You use Risk Analysis to determine violations pertaining to the authorizations assigned to the role. An example is when the authorizations result in segregation of duties violations.
   ○ You use Impact Analysis to determine authorization violations pertaining to other roles. That is, the authorizations for the selected role, in combination with authorizations for another role, results in violations.

3. Select the System and Rule Set from the respective fields.

4. In the Result Options area, select the format, type, and additional criteria for the analysis results.

   Example

   Table 21:

<table>
<thead>
<tr>
<th>Format</th>
<th>Executive Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Action Level, Permission Level</td>
</tr>
<tr>
<td>Additional Criteria</td>
<td>Include Mitigated Risks</td>
</tr>
</tbody>
</table>

5. Choose the Run Risk Analysis pushbutton.

6. In the Result area, you can choose different ways to view the analysis results.

7. If you are running the simulation feature, you can do the following:
   ○ Choose Cancel if you do not want to save the results of the analysis.
   ○ Choose Apply if you want to save the results. The information is saved to the Risk Violations tab and you can view it whenever you open the request. The results are also available to the approver of the request.

5.7 Analyzing Access Risks for Role Maintenance

Use

You can use the Analyze Access Risk phase to perform the following analysis types:

- You use Risk Analysis to determine violations from the authorizations assigned to the role, for example, the authorizations result in segregation of duties violations.
- You use Impact Analysis to determine authorization violations with other roles. That is, the authorizations for this role, in combination with authorizations for another role result in violations.
Procedure

To perform risk analysis:
1. In the Analysis Type dropdown list, select Risk Analysis.
2. Select the System and Rule Set from the respective fields.
3. Under the Result Options area, select the format for the analysis results and the object for analysis, such as action level, permission level, and so on.

   i Note
   The Select Options for Impact Analysis area is only enabled when Impact Analysis is selected.

4. In the middle area of the screen, choose to run the analysis job in the foreground or background.
5. In the View Results For area, select Risk Analysis from the dropdown list, and then choose Go.
6. In the Result area, you can choose different ways to view the analysis results.
7. Choose Mitigate Risk, to mitigate any violations.

To perform impact analysis:
1. In the Analysis Type dropdown list, select Impact Analysis.
2. Select the System and Rule Set from the respective fields.
3. Under the Result Options area, select the format for the analysis results and the object for analysis, such as action level, permission level, and so on.
4. In the Select Options for Impact Analysis area, choose to perform impact analysis for any of the following: Users, Composite Roles, or Business Roles.
5. In the middle area of the screen, choose to run the analysis job in the foreground or background.
6. In the View Results For area, select Impact Analysis from the dropdown list, select the impact analysis option, and then choose Go.
7. In the Result area, you can choose different ways to view the analysis results.
8. Choose Mitigate Risk, to mitigate any violations.

More Information

Rule Sets [page 75]
Mitigating Risks [page 39]
5.8 Mitigating Risks

Prerequisites

You have created mitigation controls.

Context

On the Assign Mitigation Controls screen, you can assign mitigation controls to risks found during risk analysis and impact analysis.

The screen also allows you to mitigate risks for roles that are not part of the current request. For example, you are currently mitigating risks for John_Current_Request. You can also mitigate risk violations for John_Other_Request1 and John_Other_Request2. Choose the Add pushbutton to add and complete the procedure below for step 4.

Note

The Mitigate Risk feature is available on multiple screens in the application. In the procedure below, we describe one access point; your access point may be different. The information is applicable regardless of the access point.

Procedure

1. On the Analyze Access Risk screen, under the Results section, select a risk violation or multiple violations, and then choose the Mitigate Risk pushbutton.

   The Assign Mitigation Controls screen appears. The application uses the information from the risk violation, such as the Access Risk ID, and displays the relevant mitigating control.

2. To use the mitigating control suggested by the application:
   1. Change the information in the relevant fields as needed, such as the validity dates, the Control ID, and so on.
   2. Choose Submit.

3. To create a new control:
   1. Choose Create Control and complete the tasks for creating a new control.
   2. Choose Add.
      The application adds an empty line to the mitigation controls list.
   3. Enter information in the relevant fields for the new control.
   4. Choose Submit.
4. To assign mitigating controls for other roles or requests:
   1. Choose Add.
      The application adds an empty line to the mitigation controls list.
   2. Enter information in the relevant fields for the new control.
   3. Choose Submit.

Next Steps

5.9 Alerts

Use

When a user performs critical or conflicting actions, the system can send an escalation alert to the appropriate personnel. You can use the Alerts feature to monitor Conflicting and Critical Access and Mitigating Control alerts, as appropriate.

Specifically, you can do the following:

- Search and filter alerts to display
- Clear alerts
- Search and filter cleared alerts

More Information

Searching Alerts [page 122]
Cleared Alerts [page 123]
Clearing Alerts [page 124]
Searching Cleared Alerts [page 125]
5.9.1 Searching Alerts

Context

You can search the following types of alerts:

- Conflicting and Critical Access Alerts
- Mitigating Controls

Procedure


2. Specify the search criteria.
   1. Choose the object type using the first dropdown list.
      For Conflicting and Critical Access Alerts, you can choose from among the following object types:
      - Business Process
      - System
      - Date Time Executed
      - Access Risk ID
      - Risk Level
      - Risk Owner
      - Risk Type
      - User ID
      - Alert Date Time
      For Mitigating Control Alerts, you can choose from among the following object types:
      - Action
      - System
      - Control ID
      - Date Time Executed
      - User ID
      - Alert Date Time
   2. Choose the operator using the second dropdown list, from among the following:
      - is
      - is not
      - starts with
      - contains
      - is between
○ Multiple Selections
3. Type or select the search value in the third field.
4. Optionally, add a line to the search criteria by choosing the plus (+) pushbutton and specifying the fields. Alternatively, remove a line from the search criteria by choosing the corresponding minus (-) pushbutton.

3. Choose Search.
   The search results appear in the table.
4. Optionally, save the search criteria as a variant by typing a name in the Save Variant as field and choosing Save.

Next Steps

Alerts [page 121]
Cleared Alerts [page 123]
Clearing Alerts [page 124]
Searching Cleared Alerts [page 125]

5.9.2 Cleared Alerts

Use

After an alert message has been delivered and cleared, or deleted, it remains as an archived record. You can continue to track and monitor these alerts using the Cleared Alerts tab of the Conflicting and Critical Risk Alerts and Mitigating Controls screens.

More Information

Alerts [page 121]
Searching Alerts [page 122]
Clearing Alerts [page 124]
Searching Cleared Alerts [page 125]
5.9.2.1 Clearing Alerts

Context
You can clear the following types of alerts, as needed:

- Conflicting and Critical Access Alerts
- Mitigating Controls

Procedure

   
   The Conflicting and Critical Access Alerts or Mitigating Control Alerts screen opens.
2. Specify the search criteria.
3. Choose Search.
   
   The search results appear in the table.
4. Select the alert to clear by selecting the box to the left and choosing Clear Alert.
   
   The Clear Alert dialog appears.
5. Enter a reason for clearing the alert, and choose OK.
   
   The alert is cleared. You can view cleared alerts using the Cleared Alerts tab. For more information, see .

Next Steps

Alerts [page 121]
Searching Alerts [page 122]
Cleared Alerts [page 123]
Searching Cleared Alerts [page 125]
5.9.2.2 Searching Cleared Alerts

Context

You can search the following types of cleared alerts:

- Conflicting and Critical Access Alerts
- Mitigating Controls

Procedure

   
   The Conflicting and Critical Access Alerts or Mitigating Control Alerts screen opens.

2. Select the Cleared Alerts tab.

3. Specify the search criteria.
   
   1. Choose the object type using the first dropdown list.
      - For Conflicting and Critical Access Alerts, you can choose from among the following object types:
        - Business Process
        - System
        - Date Time Executed
        - Access Risk ID
        - Risk Level
        - Risk Owner
        - Risk Type
        - User ID
        - Alert Date Time
      - For Mitigating Control Alerts, you can choose from among the following object types:
        - Action
        - System
        - Control ID
        - Date Time Executed
        - User ID
        - Alert Date Time

   2. Choose the operator using the second dropdown list, from among the following:
      - is
      - is not
      - starts with
      - contains
is between
• Multiple Selections
3. Type or select the search value in the third field.
4. Optionally, add a line to the search criteria by choosing the plus (+) pushbutton and specifying the fields. Alternatively, remove a line from the search criteria by choosing the corresponding minus (-) pushbutton.


The search results appear in the table.

5. Optionally, save the search criteria as a variant by typing a name in the Save Variant as field and choosing Save.

6. To display the reason an alert was cleared, choose the Comments link in the Reason field for the corresponding alert.

   The Clear Alert dialog appears displaying the reason. Choose Cancel to dismiss the dialog.

Next Steps

Alerts [page 121]
Searching Alerts [page 122]
Cleared Alerts [page 123]
Clearing Alerts [page 124]

5.10  Background Jobs

Use

In the Access Management work center, under Scheduling, you can use the links to schedule and display background jobs.

Features

• Background Scheduler [page 30]
• Scheduling Background Jobs [page 31]
5.10.1 Background Scheduler

Use

You can use *Background Scheduler* to create and maintain schedules for background jobs.

Activities

1. Enter the name for the schedule.
2. Select an activity for the background job.
3. Select whether to start the background job immediately.
4. Specify the start date and time.
6 Managing Roles

Use

This overview process explains how to monitor and prevent risks during role creation and update.

Process

1. Maintain and/or refine role definition
   If the applicable role does not already exist, the first step is to define and document the business requirements and major attributes for the new role.
   1. For what business reasons is the role needed?
   2. Which part of the organization does it belong to; for example, business process, subprocess, functional area, and so on.
   3. Who is the person responsible for the role content? Who will approve user access to the role?

2. Maintain role technical details
   Once the role definition is created or updated, the next step is to identify the technical details to perform the work process tasks that are defined in the role definition.

3. Perform risk analysis
   1. Refine role technical details to remove conflicts when possible.
   2. If the technical details cannot be refined, the risk should be mitigated with the appropriate controls.

4. Maintain authorization data
   Once the technical details are defined, the next step is to identify the authorization data to restrict the work process tasks based on job responsibility and organization assignment.

5. Perform risk analysis
   After authorization data is defined or updated, risk analysis is performed to check if the role contains access risk violations.
   1. Refine role authorization data to remove conflict when possible.
   2. If the authorization data cannot be refined, the risk should be mitigated with the appropriate controls.

6. Role Owner Approval
   Role is ready to be submitted for role owner approval if it does not contain access risk violations or if they are mitigated. If the role is rejected by role owner, it could be redefined, updated, or deleted.

7. Create and update roles
   After the role is approved by role owner, the role is created or updated in the system.

8. Perform testing and documenting results
   Testing is performed to ensure that the role has the proper access. The test results are documented.

9. User provisioning
   Approved and tested roles are ready to be provisioned to users to provide them with system access.
Result

Roles are introduced into environments without risks or with mitigated risks to provide compliant user access.

6.1 Role Management Considerations

Use

Role Management allows you to manage roles from multiple systems with a single unified role repository. The roles can be documented, designed, analyzed for control violations, approved, and then automatically generated. It enables standardized practices to ensure that role definitions, development, testing, and maintenance are consistent across the entire enterprise.

Implementation Considerations

- Designing a logical role naming convention
- Creating a well-thought-out integration of role management into ongoing role development, testing, and change management processes
- Identifying users when defining roles, such as role owners, security administrators, and user administrators
- Defining goals, such as role optimization or consolidation, user access optimization, and risk and change request reduction.
- Identifying custom reports

Features

The application allows role owners and security administrators to:

- Track progress during role implementation
- Monitor the overall quality of the implementation
- Perform risk analysis at role design time
- Set up a workflow for role approval
- Provide an audit trail for all role modifications
- Maintain roles after they are generated to keep role information current

Roles and Role Assignment

A role is a predefined set of access permissions. In this model, access is not granted to individual users, but rather to roles.
To provision access to a financial application for a user, you must assign to that user a role that has access to the application. If the user is assigned to the requisite role, the user automatically has access to the application.

Different users need to access the same module or application yet require different levels of access. Typically, for any given application, multiple roles exist that include some form of access. Therefore, role assignment defines both the application to which the user has access, and the level of access the user is granted within the application.

**Risk Analysis and Mitigation**

One key element of provisioning is the identification and mitigation of risk.

**Example**

In most organizations, the roles Receiving, Inventory, and Accounts Payable are mutually exclusive. To prevent the risk of fraud, a person responsible for cataloging deliveries cannot have the ability to catalog inventory, and to authorize payment for a delivery.

**Recommendation**

To facilitate role planning and role maintenance, see the set of reports in the **Reports and Analytics** work center that include reports for:

- Facilitating overall role quality management
- Providing valuable information for creating precise role definitions
- Minimizing ongoing role maintenance

### 6.1.1 Role Creation Methodology

**Use**

Role Creation Methodology allows you to customize the role management process to match your requirements. You can also set up multiple methodologies; for example, create one methodology for finance roles and another for security roles.

A role creation methodology consists of predefined actions and the steps associated with those actions. The steps are then used to create a methodology process that guides you step-by-step through the process of defining, generating, and testing a role during role creation.

The methodology process is flexible and can be configured. For example, you can repeat a step multiple times, such as requiring an approval step several times in your process, or you can remove steps you do not need.
You can use the role creation methodology delivered with the application, change it, or create your own.

To customize the role maintenance process, you define condition groups. A condition group uses the role attribute values, such as the role type or role name, to define a rule that is used to select a specific methodology. For example, users with the **Finance** role use the finance methodology, and users with **Security** roles use the security methodology.

**Note**

You can have multiple condition groups associated to one methodology process; however, you cannot have multiple processes associated with one condition group.
Process

To create your own role creation methodology:

1. Generate BRFplus applications, approvers, and methodology functions by using the Customizing activity Generate BRFplus Applications, Approvers, and Methodology Functions under Governance, Risk, and Compliance Access Control Role Management.

2. In BRFplus, create condition groups and define the relevant set of attributes, such as role type, and so on.

3. Assign the condition groups to the BRFplus function using the Customizing activity Assign Condition Groups to BRFplus Functions, under Governance, Risk, and Compliance Access Control Role Management.


5. Assign the methodology processes to the condition group using the Customizing activity Associate Methodology Process to Condition Group, under Governance, Risk, and Compliance Access Control Role Management.

6.1.1.1 Reapply Methodology

Use

You use Reapply Methodology to update an existing role’s methodology because of a change to the role methodology, role content, or conditions.

The following changes are relevant to the Reapply Methodology function:

- The methodology has changed.
  For example, you add an approval phase or remove a phase.
- A condition that affects the methodology has changed.
  For example, the condition for using a particular process, such as Process_01, is changed to Process_02.
- The role content, such as a role attribute, has changed and it affects the methodology.
  For example, the subprocess attribute for a role was changed from Accounts_Payable_01 to Accounts_Receivables_01. The role must use a different methodology if you had set up different methodologies based on this attribute.

The application applies the changes and resets the current phase to the definition phase (first phase).

You can access the function in the application as follows:

- Role Maintenance
  On all the role maintenance screens, choose the Reapply Methodology button.

- Updating Multiple Roles
  1. On the Role Mass Update screen, under the Select Criteria section, select All Attributes, and choose Next.
  2. Select the Reapply role methodology checkbox, and then choose Next.

Conditions
The Reapply Methodology function has the following conditions:

- Roles in the approval stage are not updated. The approval must be complete before the roles are updated.
- Roles in the edit mode are not updated; that is, the internal status of the role is locked.
- If the role contains derived roles, and the new methodology does not contain the Derivation step, you must first remove all the derived roles and update the roles separately.

More Information

6.1.1.2 Role Derivation

Role derivation allows administrators to derive one or more roles from a single master role. The master role serves as the template for the authorizations and attributes. The derived roles are differentiated from the master role and each other by organizational levels.

You can choose any role of the role type **Single Role** to be a master role. The application automatically creates the relationship between the master role and the derived roles.

The attributes, such as business process, are propagated to the derived roles only when the derived roles are created. After creation, they are independent roles, and any changes to the attributes in the master role are not propagated.

The authorization data, such as transactions, objects, fields, and so on, continues to be propagated but not automatically. You can choose to manually propagate authorization data changes to the master role by going to the **Maintain Authorization** screen and doing the following:

- For the master role, choose the **Propagate Authorizations** pushbutton to propagate authorizations to the derived roles.
- For the derived roles, choose the **Copy Authorization** pushbutton to copy authorizations from the master role.

**Note**

All authorization data is propagated, except for organizational levels.

6.1.2 Role Maintenance

Use

The application provides a standardized and centralized framework to design, test, and maintain roles. The basic role maintenance process, as suggested by most system and security administrators, involves the steps described below.
Maintaining and Changing Role Settings

The process described below is an end-to-end process for creating roles. Once you have created a role, you can use the Go to Phase button to go directly to a stage and change the information. For example, to change the authorizations, open the role and then go to the Maintain Authorization phase.

Note

To edit a role, on the Business Role Management screen, you must select the role, and then choose the Open button. For some phases, such as Define Role and Maintain Authorizations, you must also choose the Edit button at the top of the phase screen.

If you select the role by choosing its name, the application displays the role in read-only mode. All the buttons are disabled and you can only view the information.

When you change a business role, for example, by adding or deleting a technical role, any users who are assigned to that business role are automatically notified of those changes via e-mail after you click Update Assignment.

We deliver a template that you can use for the notifications. You can also create your own custom template for user notifications in Customizing under SAP Reference IMG  Governance, Risk, and Compliance  Access Control  Workflow for Access Control  Maintain Customer Notification Messages.

Prerequisites

- Outside the application, you have identified your business needs, and evaluated your approach for managing roles.
- In the application, you have maintained the role methodology process and steps by:
  - Completing the activities in the Customizing activity Define Methodology Processes and Steps, under Governance, Risk, and Compliance  Access Control  Role Management
  - Activating the business configuration (BC) set for Role Management Methodology Process and Steps

Process

Role Maintenance consists of the following procedures:

1. Defining roles
2. Maintaining authorizations
3. Deriving roles
4. Analyzing access risks
6.1.2.1 Defining Roles

Context

You use Define Roles to create and maintain attributes for various role types. The role types are categorized as either technical roles or business roles.

Technical roles are roles that physically exist on the back-end system. You assign a technical role to a user to grant them authorization and access to the back-end system that contains the role. For example, you want to grant HR authorizations to a user for system Sys_1. You would create a technical role HR_USER_SYS_1 with the necessary authorizations and assign the technical role to the user in the back end.

Business roles are logical roles that exist only in the access control application; they do not exist in the back-end systems. They allow you to grant authorizations to a user for multiple roles. The roles may be from multiple systems, rather than manually assigning separate roles for each system.

Procedure

1. Choose Create, and then select a role type to create.
   
   The New Role screen appears. The application displays different tab pages, based on the role you are creating.

2. On the Details tab page, enter information for:
   ○ Application type
   ○ Landscape
   ○ Business process
   ○ Subprocess
   ○ Project release
   ○ Role name

3. On the Properties tab page, do the following:
   1. In the Certification Period in Days field, enter the number of days you want to allow for reviewing and approving the role.
   2. Under the Properties area, enter information for Critical Level, Sensitivity, and Identifier as needed.
   3. Under the Role Reaffirm area, in the Reaffirm Period in Days field, enter the number of days you after which the role must be reaffirmed. For example, you can specify that after 180 days, the role owner, or approver, must review the role and reaffirm that it is still valid.
4. Under the User Provisioning area, select the following checkboxes:
   ○ **Comments Mandatory**, to require the approver or owner enter a comment when approving or rejecting the role
   ○ **Enable for Firefighting**, to make the role available as a firefighting role.

4. On the **Functional Area** tab page, select the required functional areas.
   You maintain the list of functional areas in the Customizing activity **Maintain Functional Areas** under Governance, Risk, and Compliance ➤ Access Control ➤ Role Management ➤ .

5. On the **Company** tab page, select the required companies.
   You maintain the list of companies in the Customizing activity **Define Companies** under Governance, Risk, and Compliance ➤ Access Control ➤ Role Management ➤ .

6. On the **Custom Fields** tab page, maintain any custom fields that you have defined.
   You maintain the list of custom fields in the Customizing activity **Define Custom Fields** under Governance, Risk, and Compliance ➤ General Settings ➤ User-Defined Fields ➤ .

7. On the **Owners/Approvers** tab page, do the following:
   1. Choose **Edit** to enable the pushbuttons.
   2. Choose **Add**, and then select a role to be the owner or approver.
   3. Select the respective checkboxes to specify the role as **Assignment Approver**, **Role Owner**, or both.
   4. In the **Alternate** column, select a user to serve as a backup if the owner or approver is not able to perform their duties.
   5. Choose **Default Approvers** to use the default approvers, rather than specifying specific owners or approvers.

   **Note**
   Before you can change the Owners/Approvers tab page, you must save the role. The functions for this tab page are disabled in Create mode.

8. On the **Roles** tab page, select the roles to associate with this role. This is available only for composite roles and business roles.

9. On the **Prerequisite** tab page, add any prerequisites that are required in order for the user to be assigned this role.
   1. Select the **Verify on Request** checkbox, to require the application verify that the user has completed all the prerequisites before allowing the role assignment.
   2. Select the **Active** checkbox, to enable the prerequisite.
   
   You maintain the prerequisites in the Customizing activities **Define Prerequisite Types** and **Define Role Prerequisites** under Governance, Risk, and Compliance ➤ Access Control ➤ Role Management ➤ .

10. On the **Role Mapping** tab page, you can assign roles as child roles. This allows anyone who is assigned this role to be assigned the authorizations and access for the child roles also.

    Select the **Consider Parent Role Approver** checkbox to use only the approvers associated with the parent roles and ignore any approvers associated with the child roles.

    **Note**
    If you are using a business role, you do not need this function.
Next Steps

Using Emergency Access Management [page 164]

6.1.2.2 Additional Details

Use

You can use the Additional Details tab page to maintain supplementary information for the role. The tab page is available on all the role maintenance screens, so you can maintain the information for all the phases of the role maintenance process.

Features

- Detail Description
  A free text entry field you can use to enter any relevant information.
- Provisioning
  Maintain provisioning settings for the role. For more information, see Maintaining Role Provisioning Settings [page 137].
- Where-Used Roles
  A list of the system landscapes where the roles are used. The list includes the business process and subprocess.
- Assigned Users
  A list of all the users that are assigned the role, the relevant system, and the validity period.
- Attachments
  Attach any files or documents required for the role.
- Change History
  A history of the changes to the role in SAP Access Control.
- PFCG Change History
  A history of the changes to the role done in the PFCG transaction.

6.1.2.3 Maintaining Role Provisioning Settings

Use

You maintain these settings to control how the application provisions the role.
Procedure

1. Select the **Role Status** field, and choose a status. If you want the role to be for provisioning, you must choose **Production**.
   You maintain the list of role statuses in the Customizing activity **Maintain Role Status**, under **Governance, Risk, and Compliance > Access Control > Role Management**.

2. To set the validity period for a system, select a system, and then choose the **Set Default Period**.

3. To allow users to search for the role and request to be assigned to the role, select **Provisioning Allowed**, and then choose **Yes**.

4. To allow the application to automatically provision roles to users once their user access request has been approved, select **Allow Auto-Provisioning**, and then choose **Yes**.

5. Choose **Save**.

   **Note**
   The application performs provisioning only for roles that are set as productive and where provisioning is allowed. That is, if the role is set as productive, but both **Provisioning Allowed** and **Allow Auto-provisioning** are set to **No**, the application does not provision the role.

6.1.2.4 Maintaining Authorizations

Use

You can use the **Maintain Authorizations** phase to maintain the role authorization data for the **Single** role type. This phase is not relevant for other role types and is not displayed for them.

   **Note**
   - If you are updating an existing role, choose the **Edit** button to enable the buttons on the screen.
   - When in Edit mode, you cannot navigate to other phases. You must choose **Save** to make the **Go To Phase** button active.

Prerequisites

- You have access and authorizations to the required back-end system.
- You have added the back-end system to the SAP GUI.
- In your Windows system, you have configured SAP GUI as the default program for opening files with the **SAP** file extension.
- You have assigned the default back-end system in the Customizing activity **Maintain Mapping for Actions and Connector Groups**, under **Governance, Risk, and Compliance > Access Control**.
Procedure

The application provides different features for maintaining PFCG role authorizations and non-PFCG role authorizations.

Maintaining non-PFCG Authorizations

1. On the Actions tab page, choose from the following features:
   - Choose the Add button to select from a list of available actions.
   - Choose the Download Template and Upload buttons to use the delivered file to add actions.
2. On the Functions tab page, choose to add or remove functions.
3. Save the entries.

Maintaining PFCG Authorizations

1. On the Maintain Authorizations tab page, choose from the following features:
   - Add/Delete Function to maintain the functions for the role
   - Maintain Authorization Data to start the PFCG transaction on the back-end system
   - Synch. with PFCG to pull the role authorization data from PFCG and overwrite the role authorization data in access control

   Note

   In this mode, the application disables the Add/Delete Function and Maintain Authorization Data buttons. To cancel the synchronization and enable the buttons, choose the Cancel PFCG Synch. button.

   - Propagate to Derived Roles to push any changes of role authorization data to all derived roles associated with this role
   - Push Authorization Data to Back-end System to push the role authorization data from access control to the back-end system and overwrite the authorization data in PFCG

2. Save the entries.

Note

The following tab pages are read-only and display authorization data from the back-end system for the role:

- Actions
- Permissions
- Organizational Levels
- Functions
6.1.2.5 Deriving Roles

Prerequisites

- You have created and saved the master role in the PFCG back-end system.
- You have assigned the default back-end system in the Customizing activity Maintain Mapping for Actions and Connector Groups, under Governance, Risk, and Compliance > Access Control.
- If you want to allow role derivation using org value maps without a leading org, you have maintained Parameter ID 3025 in the Customizing activity: Maintain Configuration Settings, under Governance, Risk, and Compliance > Access Control.

Context

Role derivation allows administrators to derive one or more roles from a single master role. The master role serves as the template for the authorizations and attributes. The derived roles are differentiated from the master role and each other by organizational values. A Leading Org that the system uses to filter the Org Value Maps during role derivation may or may not be required depending on how your system is configured.

Note

As delivered, the system requires that Org Value Maps that are used for role derivation contain a leading org. If you want to allow role derivation from maps that do not contain a leading org, your administrator can maintain Parameter ID 3025 in the Customizing activity: Maintain Configuration Settings, under Governance, Risk, and Compliance > Access Control.

You can only use the role type Single Role for master roles; therefore, you can only derive roles from single roles.

Procedure

1. Search for role that has been created and is in the derivation phase.
   The system displays the role in the search result grid.
2. Select the desired row and click Open.
   The role opens in a new window with the methodology process active on the Derivation tab.
3. Click Derive.
   The system displays the Manage Derived Role screen.
4. To derive a role without a leading organizational value:
   1. Select the No Leading Org, Level checkbox.
The system disables the Leading Org, Level, Org. Value From, and Org Value To fields. You use this option if you want to copy only the authorization data from the master role and then use transaction PFCG to change the organizational values.

**Note**
You can only derive one role at a time when using this option.

2. Selecting **No Leading Org** gives you the following two choices:

<table>
<thead>
<tr>
<th>To derive the role without using org value maps, do the following:</th>
<th>To derive the role using org value maps that do not contain leading orgs, do the following:</th>
</tr>
</thead>
</table>
| 1. Click **Next**. 2. Go to step 6. | **Note**
To use this option, Parameter ID 3025 must be set to **Yes** in Customizing. |
|   | 1. Click **Add** to select an Org Value Map. 2. Select one or more maps. 3. Click **OK** then click **Next**. 4. Go to step 6. |

5. To derive a role using organizational value maps that contain a leading org:
   1. Select the Leading Org, Level.
   2. Enter the organizational values.
      To specify just one organizational value, only enter a value in Organizational Value From field.
   3. Under the Org, Value Mapping area, choose **Add** to select one or more organizational value maps.
   4. Choose **Next**.

6. In the **Derived Role Name** field, give the derived role a name and then choose **Next**.

**Note**
You can configure naming conventions for role names in the Customizing activity Specify Naming Conventions, under Governance, Risk, and Compliance > Access Control > Role Management.

7. Review the information for the derived role, and then choose **Save**.

The application saves the derived role. To generate the derived role, go to the Generate Roles phase.
6.1.2.6 Analyzing Access Risks for Role Maintenance

Use

You can use the **Analyze Access Risk** phase to perform the following analysis types:

- You use **Risk Analysis** to determine violations from the authorizations assigned to the role, for example, the authorizations result in segregation of duties violations.
- You use **Impact Analysis** to determine authorization violations with other roles. That is, the authorizations for this role, in combination with authorizations for another role result in violations.

Procedure

To perform risk analysis:
1. In the **Analysis Type** dropdown list, select **Risk Analysis**.
2. Select the **System** and **Rule Set** from the respective fields.
3. Under the **Result Options** area, select the format for the analysis results and the object for analysis, such as action level, permission level, and so on.
   
   **Note**
   The **Select Options for Impact Analysis** area is only enabled when Impact Analysis is selected.

4. In the middle area of the screen, choose to run the analysis job in the foreground or background.
5. In the **View Results For** area, select **Risk Analysis** from the dropdown list, and then choose **Go**.
6. In the **Result** area, you can choose different ways to view the analysis results.
7. Choose **Mitigate Risk**, to mitigate any violations.

To perform impact analysis:
1. In the **Analysis Type** dropdown list, select **Impact Analysis**.
2. Select the **System** and **Rule Set** from the respective fields.
3. Under the **Result Options** area, select the format for the analysis results and the object for analysis, such as action level, permission level, and so on.
4. In the **Select Options for Impact Analysis** area, choose to perform impact analysis for any of the following: Users, Composite Roles, or Business Roles.
5. In the middle area of the screen, choose to run the analysis job in the foreground or background.
6. In the **View Results For** area, select **Impact Analysis** from the dropdown list, select the impact analysis option, and then choose **Go**.
7. In the **Result** area, you can choose different ways to view the analysis results.
8. Choose **Mitigate Risk**, to mitigate any violations.

More Information

**Rule Sets [page 75]**
6.1.2.6.1 Mitigating Risks

Prerequisites

You have created mitigation controls.

Context

On the Assign Mitigation Controls screen, you can assign mitigation controls to risks found during risk analysis and impact analysis.

The screen also allows you to mitigate risks for roles that are not part of the current request. For example, you are currently mitigating risks for John_Current_Request. You can also mitigate risk violations for John_Other_Request1 and John_Other_Request2. Choose the Add pushbutton to add and complete the procedure below for step 4.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
</table>

The Mitigate Risk feature is available on multiple screens in the application. In the procedure below, we describe one access point; your access point may be different. The information is applicable regardless of the access point.

Procedure

1. On the Analyze Access Risk screen, under the Results section, select a risk violation or multiple violations, and then choose the Mitigate Risk pushbutton.

   The Assign Mitigation Controls screen appears. The application uses the information from the risk violation, such as the Access Risk ID, and displays the relevant mitigating control.

2. To use the mitigating control suggested by the application:
   1. Change the information in the relevant fields as needed, such as the validity dates, the Control ID, and so on.
   2. Choose Submit.

3. To create a new control:
   1. Choose Create Control and complete the tasks for creating a new control.
   2. Choose Add.

   The application adds an empty line to the mitigation controls list.
3. Enter information in the relevant fields for the new control.
4. Choose *Submit*.

4. To assign mitigating controls for other roles or requests:
   1. Choose *Add*.
      The application adds an empty line to the mitigation controls list.
   2. Enter information in the relevant fields for the new control.
   3. Choose *Submit*.

Next Steps

6.1.2.7 Generating Roles

Context

In the *Generate Roles* phase, you can submit roles for generation.

Procedure

1. On the *Generate Roles* screen, choose the *Generate* button.

   The screen displays a summary of the following for the roles to be generated:
   - Default system
     The application pulls the default system information from the system landscape. You maintain the default system information in the Customizing activity *Maintain Mapping for Actions and Connector Groups*, under [Governance, Risk, and Compliance ➔ Access Control](#).
   - Other systems
     The application pulls the system information from the system landscape. You maintain the default system information in the Customizing activity *Maintain Mapping for Actions and Connector Groups*, under [Governance, Risk, and Compliance ➔ Access Control](#).
   - Derived roles
     The application displays a list of the roles derived from this master role.

2. Choose *Next*.

3. The job for generating the roles, and choose *Next*.

4. Analyze risks.
The application performs risk analysis. If it does not detect any risk, it immediately goes to the Confirmation phase.

**Note**

You can configure whether or not the application performs risk analysis before it generates roles. To do so, set parameter ID 3011 in the Customizing Activity Maintain Configuration Settings, under Governance, Risk, and Compliance under Access Control.

5. Choose Submit to submit the job for generating roles.

**Note**

You can configure whether or not the application generates roles even with risks. To do so, set parameter IDs 3014 to 3018 in the Customizing Activity Maintain Configuration Settings, under Governance, Risk, and Compliance under Access Control.

### 6.1.2.8 Maintaining Test Cases

**Use**

You can use the Maintain Test Cases phase to document test results for any testing done for the role. You can enter single test cases, upload multiple test cases, or attach documents.

**Procedure**

To enter single test cases:

1. Choose Create to enter single test cases.
2. On the Test Results screen, enter the test case name and all required fields.
3. In the Attachments area, choose Add, and add either a file or a link.
4. Choose Save.

To enter multiple test cases:

1. Choose Import From File.
   - The application provides a template you can use to create multiple test cases.
2. Choose Browse to navigate to the file, and then choose OK.
6.1.3 Approving Role Requests

Use

The process of approving role requests consists of procedures for the person making the request and for the person approving the request.

Prerequisites

You have selected the role owners and role approvers in the Define Role phase.

Process

1. In the Request Approval phase, the requestor chooses the Initiate Approval Request button to initiate the workflow for approving the role. The requestor can also monitor the request status and read any comments for the request.

2. In the Work Inbox, the approver receives the task for approving the request, and then chooses from the following actions:
   - Reject
   - Forward
   - Hold
   - Request Information

   You can configure the list of available actions and the approval workflow in the Customizing activity Maintain MSMP Workflows, under Governance, Risk, and Compliance Access Control Workflow for Access Control.

3. (Optional) In Customizing (transaction SPRO), configure e-mail notifications.
   - To configure custom e-mail notifications to inform the requestor that their request has been approved or rejected, you maintain the Customizing activity Maintain Custom Notification Messages, under Governance, Risk, and Compliance Access Control Workflow for Access Control.

   You can configure it so that all recipients of the same notification event receive the same message, or you can configure it so that different recipients of the same notification event receive different messages. For example, you can configure it so that recipients from the Finance department receive a message with wording specific to Finance.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>To use the standard delivered notifications, no configuration is required. The application automatically uses the delivered notifications.</td>
</tr>
</tbody>
</table>

   - To configure e-mail notifications for the person approving the role request, you maintain the Customizing activity Maintain MSMP Workflows, under Governance, Risk, and Compliance Access Control Workflow for Access Control.
6.1.4 Reprovisioning Business Roles

Use

You can use this feature to reprovision business roles to users when the technical roles assigned to the business roles have changed.

The application allows you to assign multiple technical roles to a logical role called a business role. This allows you to provision the authorizations from multiple technical roles to a user in one step by provisioning the single business role. This feature allows you to reprovision the business roles to users if the technical role assignments changed after you initially provisioned the roles.

Example

The following figure illustrates that the business role, Business_Role_01, changed its technical role assignments from Technical_Role_03 to Technical_Role_05 and Technical_Role_06.
Figure 4: Changing Technical Role Assignments

![Diagram showing Old Role Assignments and New Role Assignments]

### Note
This feature is available **only** for business roles.

### Prerequisites
You have enabled the **Provisioning** phase for the role methodology.
You maintain the phase in the Customizing activity. **Define Methodology and Steps**, under **Governance, Risk and Compliance → Access Control → Role Management**.

### Process
2. Select a business role and choose Open. The business role maintenance screen appears.

**Note**

The workflow graphic at the top of the screen displays the Provisioning phase only if both these requirements are met:

- You are maintaining a business role.
- You have enabled the Provisioning phase in Customizing.

3. In the **Definition** phase, change the assignment of the technical roles to the business role as needed and then choose **Save and Continue**.

4. Complete the phases of the workflow as required, such as **Analyzing Risks**, to get to the **Provisioning** phase. The **Provisioning** tab page is displayed only if you have completed the conditions above.

   It has the following sub-tabs and functions:

   **Table 23:**

<table>
<thead>
<tr>
<th>Tab</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Provisioning</strong></td>
<td>Choose the <em>Update Assignment</em> button and the application performs a background job to reprovision the business role to the associated users. The application performs the background job immediately, but depending on your system setup, it may take some time.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The <em>Update Assignment</em> button is enabled only if the business role has been assigned via the access request process.</td>
</tr>
<tr>
<td>The table displays the relevant background jobs and its status. Choose the <em>Refresh</em> button to refresh the status. When the <em>Result</em> column displays <em>Complete</em>, the background has finished reprovisioning the business role.</td>
<td></td>
</tr>
<tr>
<td><strong>Summary by User</strong></td>
<td>This tab displays the results of the reprovisioning background job by user. This allows you know which users were affected by this reprovisioning. The <em>Result</em> column displays whether the reprovisioning was <em>Successful</em> or <em>Failed</em>.</td>
</tr>
</tbody>
</table>
### Tab | Functions
--- | ---
**Details**  | This tab displays the details of the reprovisioning job. It lists the following information:
- Job ID
- User
- Associated Role
- System
- Valid From
- Valid To
- Action
  Whether the job *added* or *deleted* the role.
- Result
- Reason
  For example, the reason why reprovisioning failed.
- Provisioned On
  Time and date the application provisioned the roles.
- Initiated On
  Time and date the background was started.
- Initiated By
  The person who initiated the provisioning job.

5. Choose *Save and Continue*, and then complete any remaining phases in the workflow as needed.

### More Information

- Defining Roles [page 135]
- Role Maintenance [page 133]

### 6.1.5 Role Search

#### Use

You can search for roles based on role attributes such as role type, role name, and so on. Choose the plus (+) button to add additional criteria.

#### Note

The application allows you to search for roles from several screens. On the Access Request screen, the application allows you (requires administrator authorization) to configure the search criteria fields. You can add custom fields and configure their attributes. For example, you can set the default values and set whether the field is mandatory. You can configure the fields in Customizing for *Maintain Custom Field Attributes for Role Search Personalization* under **Governance, Risk, and Compliance > Access Control > User Provisioning**.
Recommendation
We recommend that you restrict the search criteria to produce more targeted results.

Activities

On the search results screen, you can change, copy, delete, or export the roles.

- To change the role, choose Open. This opens the role in the role maintenance workflow screen.
- To define a new role name based on an existing role, select a role, and then choose Copy. On the Role Copy screen, select the attributes you want to copy, and then choose Submit.
- To delete a role, select the role or roles you wish to delete, and then choose Delete.
- To export roles and role details to a Microsoft Excel spreadsheet, select the roles and choose the Export and Role Details Export as required.

More Information

Role Maintenance [page 133]

6.1.6 Default Roles

Use

You use Default Roles to specify roles the application assigns to a user automatically during provisioning.

Process

To create default roles:
1. Choose Create.
2. Select an Attribute and Attribute Value, and then choose Add.
3. Select a system and a role name from the respective columns.
4. Save the entries.
Example

You have two roles for inventory employees in your system: Inventory_Clerk and Inventory_Manager. You used Default Roles to specify that the application use the role Inventory_Clerk, if a user access request for system Inventory01 contains the attribute Subprocess, attribute value Check_Inventory, and no specific role name.

Table 24:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Subprocess</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Value</td>
<td>Check_Inventory</td>
</tr>
<tr>
<td>System</td>
<td>Inventory01</td>
</tr>
<tr>
<td>Role Name</td>
<td>Inventory_Clerk</td>
</tr>
</tbody>
</table>

Two employees submitted access requests with the following results:

- Employee_01 specified only that they required authorization for the Check_Inventory subprocess. The application automatically provisions their access with the default role Inventory_Clerk.
- Employee_02 specified that they required authorization for the Check_Inventory subprocess and for the role Inventory_Manager. The application provisions their access with two roles: Inventory_Clerk and Inventory_Manager.

6.2 Role Mining

Use

Role Mining groups together features that allow you to target roles of interest, analyze the roles, and then take action. For example, find all roles that are due to expire and affirm if they are still relevant.

Features

- Action Usage [page 153]
- Role Comparison [page 153]
- Role Reaffirm [page 154]
6.2.1 Action Usage

Use

You use Action Usage to generate a report listing action usage by roles, users, and profiles. You can view the last execution date of the action and number of times the action is executed in a specific time period for SAP systems. The Action Usage report screen shows the usage for the specified action for the specified date range and for the selected system.

The report shows action usage information only for the system where the role was associated with the action.

Activities

To view an Action Usage report, enter information in the fields as needed, and then choose either Run in Foreground or Run in Background.

You can save the analysis criteria and use it again to generate reports by entering a name in the Save Variant As field, and choosing Save.

6.2.2 Role Comparison

Use

You use Role Comparison to compare two or more roles in the access control application or between the application and another system. You can compare roles by Comparison Type and Comparison Level. If there is a difference between the roles, you can synchronize the roles by choosing to overwrite the values of one role with another. For more information, see below.

Process

Role Comparison consists of the following procedures:

1. Selecting roles
   - On the Select Roles screen, choose Add, search for, and then select roles. You must select at least two roles.
2. Selecting comparison criteria
   - On the Comparison Criteria screen, select the comparison level and type. If you choose to Compare roles between Access Control and System, you must select a system in the System field.
3. Reviewing the comparison results
   - On the Comparison Results screen, the results are displayed on the Actions and Permissions tab pages.
4. Synchronizing the roles
SAP Access Control
Managing Roles

On the Synchronization screen, select from the following options:
- **Access Control to System**
  You are choosing to overwrite the role information on the selected system with the role information from Access Control.
- **System to Access Control**
  You are choosing to overwrite the role information in Access Control with the role information from the selected system.

**Note**

Synchronization is only valid if you select the **Type** as **Compare roles between Access Control and System** on the **Comparison Criteria** screen.

For more information, see the example below.

5. **Scheduling the job for synchronizing the roles**

On the **Schedule** screen, enter information in the required fields to schedule the synchronization job. You can choose to run the job in the **Foreground** or **Background**.

The **Confirmation** screen displays your activities.

**Example**

In the following example, the access control application is the role management interface for the following back-end systems: Financial (FIN) and Human Resources (HR). It illustrates that the **FIN_ROLE_01** role on the FIN system does not have the same authorizations as the role in the access control application. This may occur if someone has bypassed the access control application and made changes directly to the roles on the system.

Role Comparison allows you to synchronize the roles by overwriting the role information between the access control application and the selected system.

**6.2.3 Role Reaffirm**

You use **Role Reaffirm** to reaffirm permissions and authorizations for selected roles that are due to expire. For example, over a period of time, employees may change employment positions within a company or leave the company. It is standard practice for companies to have their managers review whether or not the authorizations and roles assigned to their employees are still relevant.

On the **Role Reaffirm** screen, you can search for roles, and then choose from the following actions: Approve, Remove, or Hold.
6.3  Role Mass Maintenance

Use

You can use Role Mass Maintenance to import and change authorizations and attributes for multiple roles.

Process

The Role Mass Maintenance process is composed of the following procedures:

1. Importing Multiple Roles [page 155]
2. Updating Multiple Roles [page 158]
3. Updating Org. Values for Multiple Derived Roles [page 160]
4. Deriving Multiple Roles [page 161]
5. Analyzing Risk for Multiple Roles [page 162]
6. Generating Multiple Roles [page 163]

Note

If you have completed importing the roles or if the roles are already in the access control application, you can perform the procedures in any order required.

6.3.1 Importing Multiple Roles

Use

You can use Role Import to bring multiple roles from other systems into the access control application.

Process

The role import process includes the following procedures:

1. Specify the type of role to import, the source system, application type, and landscape.
2. Enter the information for the Role Attribute Source and the Role Authorization Source, such as location of the attribute and authorization files.
3. Reviewing
On the Review screen, choose from the following review options:
- No Preview
- Preview all roles
- Preview subset of roles
  You can enter the quantity of roles you want to preview.

4. Schedule the background job for importing the roles or choose to run the job in the foreground.

### 6.3.1.1 Defining Criteria

#### Use

On the Define Criteria screen, you can specify the role type, import source, and other parameters for importing multiple roles.

#### Procedure

To define the criteria, do the following:

1. In the Role Selection area, select the role type.

   **Note**

   When you select a role type, the application makes inactive fields that are not applicable for that type. For example, if you select Business Role, the application makes inactive the User Input and Role Authorization Source fields.

2. In the Import Source area, select the Role Attribute Source and the Role Authorization Source.

   **Note**

   You must have the authorization S_CTS_SADM to use the option File on Server.

**Role attributes** are details for the role, and may include information such as role name, process, subprocess, and so on. Depending on the role type, the role attribute source may be from the following: User Input, File on Server, or File on Desktop.

The **role authorization source** is the object that provides the authorization information for the roles. Depending on the role type, the role authorization source may be from the following: Backend System, File on Server, or File on Desktop. The settings are applicable to both PFCG and non-PFCG role authorizations.

**Note**

For technical roles, you can choose Skip to specify that the role authorization source is not applicable.
3. In the Templates area, you can download templates for the following:
   ○ Role attributes file
   ○ Non-PFCG role authorizations file

4. In the Definition Criteria section, you can choose the application type, landscape, and whether or not to overwrite the existing role.

   **Note**
   The application types available in the Application Type dropdown list changes depending on the role type you select.

5. In the Role Selection Criteria area, you can further refine the roles you want to import by specifying the source system, range of roles, and so on.
   You can choose to import all roles except SAP Predefined Roles. That is, only import roles you have created or customized; do not import the standard roles provided by SAP.
   In the Methodology Status field, you can choose to import only roles of a specific status, such as Complete or Initial.

### 6.3.1.2 Selecting Role Data

**Use**

On the Select Role Data screen, you enter the information for the Role Attribute Source and the Role Authorization Source, such as location of the attribute and authorization files.

Based on the options you chose for Role Attribute Source and Role Authorization Source, the application displays the applicable fields. For example, if you chose File on Server for the Role Attribute Source, the application displays the File Source field for you to enter the location of the file on the server. It also includes a link for you to download a template for the role attributes.

If you chose User Input for the Role Attribute Source, the application displays additional tabs and fields.

**Procedure**

To enter User Input role data:

1. In the Attribution Selection section, choose from the following options:
   ○ Default Values
     Select this option to use the attributes provided in the Role Attributes section.
     The default values are maintained in the Customizing activity Maintain Configuration Settings, under Governance, Risk, and Compliance ➤ Access Control ➤ Maintain parameter IDs 3000 to 3004, inclusive.
   ○ User Defined Attributes
     Select this option to enter your own information in the Role Attributes section, such Critical Level, Project Release, Role Status, and so on.
2. On the Functional Area tab page, choose Add to select and add a functional area from the list.

3. On the Owners/Approvers tab page, you can do the following:
   ○ Choose Add to select and add users.
   ○ Select the appropriate checkbox to specify that the user is an Assignment Approver, or Role Owner, or both.
   ○ In the Alternate column, select a user to be the backup for the primary user.

4. On the Custom Fields tab page, you enter information for any new fields you have created in addition to the standard fields provided by SAP.

### 6.3.1.3 Scheduling Background Jobs

**Use**

On the Scheduling screen, you can choose to schedule the job to run in the background at a specified time or choose to run the job in the foreground.

To execute the job in the foreground, select the Foreground checkbox, and choose Submit.

**Procedure**

To execute the job as a background job:

1. Under the Schedule section, select Background.
2. To set the job to recur multiple times, select the Recurring Plan option as Yes, then select the date and times. You can set the Frequency as: Hourly, Daily, Weekly, or Monthly.
   In the Recurrence field, you can set the background job to recur for every number of hours. For example, recur every 4 hours.
3. To set the job to execute only one time, select the Recurring Plan option to No. You can choose to start the job immediately or to start at a specific date and time.
4. Choose Submit.

### 6.3.2 Updating Multiple Roles

**Use**

You can use Role Update to change the attributes for multiple roles. The available actions are update, delete, or add.
The role update process includes the following procedures:

1. Selecting Roles
   1. On the Select Roles screen, choose Add.
   2. Search for and select roles based on criteria, such as role name, critical level, business process, and so on.
   3. Choose OK and then Next.

2. Selecting Criteria
   1. On the Select Criteria screen, choose the Attributes dropdown list and select an attribute to update.
   2. Choose the Actions dropdown list, and select an available action. You can choose to update, delete, or add.

   **Note**
   The actions displayed in the dropdown list are dependent on the attribute. Multiple valued attributes display Update, Delete, and Add. Single valued attributes display only Update. For example, for the attribute business processes, only the action Update is available.

   3. Select your option for Reset Role Methodology. Choose Yes to set the roles back to the first phase of the role methodology. For example, a role is in the fourth phase of a role methodology; this function sets the role back to the first phase.

3. Selecting Values
   On the Select Values screen, enter the old value you want to change, and the new value you want to change it to.
   If you selected All Attributes on the Select Criteria screen, the Select Values screen displays all attributes. Select the attributes you want to change.

4. Schedule the background job for updating the roles or choose to run the job in the foreground.

**Reapply Role Methodology**

You can use the following procedure to reapply the role methodology to multiple roles:

1. Select the roles.
2. On the Select Criteria screen, choose the Attributes dropdown list, select All Attributes, and then choose Next.
3. On the Select Values screen, select the Reapply role methodology checkbox, and then choose Next.
4. Schedule the background job for updating the roles or choose to run the job in the foreground.

**Note**
The following is a clarification about the Reset Role Methodology function and the Reapply Role Methodology function:

- Reset Role Methodology sets the roles back to the first phase of the role methodology. For example, a role is in the fourth phase of a role methodology; this function sets the role back to the first phase. It does not consider whether the role methodology has changed. This means that even if the methodology has changed, the role continues to use the old methodology.
- Reapply Role Methodology applies any updates to the methodology, and resets the current phase back to the first phase.
6.3.3 Updating Org. Values for Multiple Derived Roles

Context

You can use Derived Role Organizational Values Update to push updates of the organizational field values to multiple derived roles.

To change the authorization data for derived roles, you must propagate the authorization data from the master role. To change the organizational values for the derived roles, you must open and change it for each role. This feature allows you to use organizational value maps to update values for multiple roles at one time.

Procedure

1. Select the organizational value map.
   1. Search for, and then choose the value map.
   2. Select one of the following update types:
      ○ Merge organizational field values: If the organizational values are different for the organizational value map and the derived roles, the application appends any differences from the organizational value map to the derived role.
      ○ Overwrite field values: If the organizational values are different for the organizational value map and the derived roles, the application replaces the values in the derived roles with the values from the organizational value map.

2. Review the affected roles.

   The Impacted Roles screen displays the all derived roles in the landscape that are affected by the changes.

3. Schedule the job.

Next Steps

Role Derivation [page 133]
Maintaining Authorizations [page 138]
6.3.4 Deriving Multiple Roles

Context

You can use Role Derivation to derive multiple roles for selected organizational levels. A Leading Org that the system uses to filter the Org Value Maps during derivation may or may not be required depending on how your system is configured.

Example

You want to create three roles for your organizations on the west coast: HR_Recruiter, Accountant, and Manager. Instead of manually creating each role separately, you want to derive these roles from existing master roles that have the required authorization data. To facilitate this task, you group the respective organizational levels and values into an organizational value map West_Coast, select the respective master roles, and then derive the new roles.

Note

As delivered, the system requires that Org Value Maps that are used for role derivation contain a leading org. If you want to allow role derivation from maps that do not contain a leading org, your administrator can maintain Parameter ID 3025 in the Customizing activity: Maintain Configuration Settings, under Governance, Risk, and Compliance.

Procedure

1. On the Mass Role Derivation screen, select the organizational value map.
   1. Enter either the map name or the leading organizational level. The leading organizational level is the parent organizational level in an organizational value map.
   2. If you want to only search for a subset of the available values in the organizational map, select the Consider Range for Values checkbox, and then enter the values in the Value From and Value To fields.
   3. Choose OK, and then choose Next.
2. If Parameter 3025 is set to Yes in Customizing, follow the steps below; if not, go to step 3.
   1. On the Select Master Role screen, you can enter values for the following search filters:
      ○ Role Name
      ○ Role Description
      ○ Business Process
      ○ Sub Process
      ○ Landscape
      ○ Exclude master roles have been derived for selected leading org
      ○ Exclude master roles that do not have the selected leading org
2. Choose Search to display all available single roles.
3. Select the master roles from the results list, and choose Next.

3. Derive the roles.

The application derives one new role for each master role.

1. In the Derive Roles table, select the Name field, and enter a name for each of the new roles.
2. In the Schedule area, choose a scheduling option.
3. Choose Submit.

Next Steps

Scheduling Background Jobs [page 31]
Role Derivation [page 133]

6.3.5 Analyzing Risk for Multiple Roles

Context

You can use Role Risk Analysis to perform risk analysis on multiple roles.

Procedure

1. Choose Add.
   The search screen appears.
2. Search for and select the roles, and then choose OK.
3. Choose Submit.
   The application automatically creates a background job for the role risk analysis.

Next Steps
6.3.6 Generating Multiple Roles

Context

You can use Role Generation to generate multiple roles.

Procedure

1. Select from the following options for updating the role methodology:
   - Do not change methodology
     The application does not change the methodology for any of the roles.
   - Keep in generation phase
     The application changes the phases for all the roles to the generation phase.
   - Complete generation phase
     The application completes the generation phase for all the roles.
2. In the Select Roles table, choose Add to search for and select the roles.
3. Choose Submit.

   The application creates a background job to generate the role. For more information about viewing the status of the background job, see.
7 Using Emergency Access Management

Use

You can implement your company’s policies for managing emergency access in Emergency Access Management (EAM). 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 policies. For more information, see Creating Roles [page 167] and EAM Terminology [page 165].

Recommendation

- Verify with your Administrator if your system is ID-based or Role-based. For more information, see .
- Track and approve requests for emergency access through a formal, documented process.
- Review the intended and actual usage of emergency access in a formal, documented process. Investigate any differences between intended and actual usage.
- Implement a periodic audit of Firefighter ID usage and logs. Verify that Firefighter activities are documented and reviewed, and that exceptions are investigated according to policy.

Process

1. The firefighter requests emergency access.
   The firefighter creates a self-service request for emergency access.
   The request should include the activities to be performed for audit purposes.
   See Requesting Emergency Access [page 185].
2. The business process owner reviews and approves emergency access requests.
   The business process owner reviews the request for emergency access and can approve or reject it.
   See Reviewing and Approving Access Requests [page 46].
   
   i Note
   The Business Process Owner is the person assigned to these duties according to business need. For example, a Firefighter ID owner or a Firefighter Role Owner may be assigned to approve the Firefighter request. A Controller may be assigned to review the Firefighter activities.

3. The firefighter accesses the systems and perform firefighting activities.
   Once access is granted, the firefighter can perform the activities documented during the request process.
   See Accessing Systems to Perform Firefighting Activities [page 188].
4. The business process owner reviews the emergency access activities.
   The business process owner can review firefighting activities via the EAM reports and logs.
   See Reviewing Emergency Access Activities [page 191].
5. Compliance persons (such as administrators) perform periodic audits of usage and sign-off via the EAM reports and logs.
Result

The result of this process is that a process for requesting, granting and monitoring emergency access is in place.

7.1 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
7.2 Configuring Emergency Access

Use

The following is the workflow for setting up the Emergency Access Management (EAM) portion of the Access Control application.

Process

1. Create the required roles for EAM.
   See Creating Roles [page 167].
2. Select the emergency access application type.
   See Selecting the Emergency Access Application Type [page 166].
3. Configure ID-based or role-based firefighting.
   See Configuring ID-based Firefighting [page 173] or Configuring Role-based Firefighting [page 183], per your application type.
4. Configure notifications for Firefighter ID logins.
   See Maintaining E-mail Notifications for Emergency Access Logons [page 180].
5. Configure notifications for EAM logs.
   See Configuring EAM Log Notifications [page 184].

7.2.1 Selecting the Emergency Access Application

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 /GRCP1/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 169].
Both centralized and decentralized options are always available. You do not need to enable one or the other. For more information, see

- **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.

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**

### 7.2.1.1 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.

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

<table>
<thead>
<tr>
<th>Role Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>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. The delivered role for administrators is: <strong>SAP_GRAC_SUPER_USER_MGMT_ADMIN</strong>.</td>
</tr>
</tbody>
</table>

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 **/GRCPI/001**, and enter the **ACTVT** field value as 70 or * (asterisk).
<table>
<thead>
<tr>
<th>Role Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>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. The delivered role for owners is: <strong>SAP_GRAC_SUPER_USER_MGMT_OWNER</strong>.</td>
</tr>
<tr>
<td>Note</td>
<td>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 /GRCPI/001, and enter the <strong>ACTVT</strong> field value as blank (empty).</td>
</tr>
<tr>
<td>Controller</td>
<td>Controllers monitor Firefighter ID usage by reviewing the log report or log report workflow and receiving e-mail notification of Firefighter ID logon events. The delivered role for controller is: <strong>SAP_GRAC_SUPER_USER_MGMT_CNTL</strong>.</td>
</tr>
<tr>
<td>Firefighter</td>
<td>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. The delivered role for Firefighter is: <strong>SAP_GRAC_SUPER_USER_MGMT_USER</strong>.</td>
</tr>
<tr>
<td>Note</td>
<td>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 /GRCPI/GRIA_EAM and S53.</td>
</tr>
<tr>
<td>Firefighter ID</td>
<td>The delivered role <strong>SAP_GRAC_SPM_FFID</strong>, when assigned to a user ID turns the ID into a <strong>Firefighter ID</strong>. Assign the role the authorization object <strong>S_RFC</strong> to enable remote logon.</td>
</tr>
<tr>
<td>Note</td>
<td>This role is used only for ID-Based firefighting.</td>
</tr>
</tbody>
</table>


### 7.2.1.2 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_SPM 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.

- **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.

**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.

### 7.2.1.3 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 /GRCPI/GRIA_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
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.
Table 26:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating users on systems to enable use of EAM Launchpad via SAP GUI.</td>
<td>As the EAM Launchpad is initiated locally, the user must have a user account on the plug-in systems in order to perform firefighting.</td>
</tr>
<tr>
<td>Creating Firefighter IDs</td>
<td>You create Firefighter IDs on each plug-in system and synchronize them to the GRC repository.</td>
</tr>
<tr>
<td>Run firefighting launchpad</td>
<td>Run transaction /GRCPI/GRIA_EAM.</td>
</tr>
<tr>
<td>Extend validity period for firefighting assignments</td>
<td>You can extend the validity period for firefighting assignments on either the GRC system or the plug-in system</td>
</tr>
<tr>
<td></td>
<td>On the GRC system, open the Firefighter ID assignment and extend the assignment period.</td>
</tr>
<tr>
<td></td>
<td>On the plug-in system, use the Customizing activities (transaction SPRO) to extend the validity period for Firefighter assignments on the plug-system.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Extending Validity Periods for Firefighting Assignments [page 187].</td>
</tr>
<tr>
<td>Enable Firefighter Logon E-mail notification.</td>
<td>You can enable each plug-in system to notify the relevant firefighting controller when a Firefighter has logged into a firefighting session.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>On the plug-in systems, use the Customizing activities (transaction SPRO) to enable the notification.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Maintaining E-mail Notifications for Emergency Access Logons [page 180].</td>
</tr>
<tr>
<td>Customize text for Firefighter Logon E-mail notification.</td>
<td>You can customize the text for the notifications for each plug-in system.</td>
</tr>
<tr>
<td></td>
<td>On the plug-in systems, use the Customizing activities (transaction SPRO) to enable the notification.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Maintaining E-mail Notifications for Emergency Access Logons [page 180].</td>
</tr>
</tbody>
</table>

EAM Activities Maintained on the GRC System

The following table describes which activities are maintained in the GRC system.
<table>
<thead>
<tr>
<th>Activity</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Emergency Access Maintenance and related master data</td>
<td>The configuration and master data information is maintained in the GRC system and pushed to the plug-in systems. 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. You schedule the synchronization jobs in transaction SPRO.</td>
</tr>
<tr>
<td>Creating Firefighter IDs</td>
<td>You create Firefighter IDs on each plug-in system and synchronize them to the GRC repository. For more information, see Creating and Maintaining Firefighter IDs [page 175].</td>
</tr>
<tr>
<td>Maintain Owners and Controllers for firefighting</td>
<td>Maintained on the GRC system</td>
</tr>
<tr>
<td>Assign owners to a Firefighter ID</td>
<td>Maintained on the GRC system</td>
</tr>
<tr>
<td>Assign a Firefighter ID to controllers</td>
<td>Maintained on the GRC system</td>
</tr>
<tr>
<td>Assign Firefighter IDs to Firefighters</td>
<td>Maintained on the GRC system</td>
</tr>
<tr>
<td>Synchronize user data</td>
<td>Maintained on the GRC system</td>
</tr>
<tr>
<td>Maintain Reason Codes</td>
<td>Maintained on the GRC system</td>
</tr>
<tr>
<td>Extend validity period for firefighting assignments</td>
<td>You can extend the validity period for firefighting assignments on either the GRC system or the plug-in system. On the GRC system, open the Firefighter ID assignment and extend the assignment period. On the plug-in system, use the Customizing activities (transaction SPRO) to extend the validity period for Firefighter assignments on the plug-system. For more information, see Extending Validity Periods for Firefighting Assignments [page 187].</td>
</tr>
<tr>
<td>Workflow-enabled assignments</td>
<td>Maintained on the GRC system</td>
</tr>
<tr>
<td>Maintenance and Synchronize logs</td>
<td>All logs and user maintenance activities are maintained on the GRC system. We recommend scheduling the job for log collection to run every hour. The GRC system should not be down for extended periods of time because it impacts collection of the logs.</td>
</tr>
<tr>
<td>Run reports</td>
<td>Maintained on the GRC system</td>
</tr>
</tbody>
</table>
7.2.2 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 167].
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 175].

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 178].

7. Assign an owner to a Firefighter ID.
   For more information, see Assigning Owners [page 177].

8. Assign a controller to a Firefighter ID.
   For more information, see Assigning Controllers [page 178].

9. Assign a Firefighter ID to a user to enable them to do firefighting.
   For more information, see Assigning Firefighters [page 179].

10. Create reason codes.
    For more information, see Reason Codes [page 181].

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 180].

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.

**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 180].

**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 183]

### 7.2.2.1 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 by using the access request functionality.

**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

Note
You can use either transaction SU01 or the access request functionality in Access Control to create Firefighter IDs. The steps below explain how to create and maintain Firefighter IDs by 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 to provide 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.
3. Save the entry.

More Information

Creating Access Requests [page 23]
7.2.2.2 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

You have completed the following:

- 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

   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.
5. Choose Save > Close.

Viewing or Maintaining an Assignment

   The Firefighter Owner screen displays a table of existing assignments.
2. Select a row and choose Open.
   The Owner Assignment screen displays the particular assignment.
3. To add an owner assignment, do the following:
   1. Choose Add.
      A new line appears in the table.
   2. Enter relevant information in the required fields.
      On the screen, required fields are marked with an asterisk (*).
   3. Choose Save > Close.
      The assignment is completed for the selected owner.
4. To remove the owner assignment, choose Remove. The selected assignment is deleted.

5. Choose Save Close.

### 7.2.2.3 Assigning Controllers

**Use**

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

You 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 functions on the Controller screen to assign, add, or remove a controller for Firefighter IDs and roles.

**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 appears and displays existing controllers, Firefighter IDs, and associated systems.
3. In the Controller ID field, enter the user ID for the person you want to assign as controller.
4. Choose OK.
5. Choose Add, select the Firefighter ID from the list, and then choose OK. The System field value is automatically generated after you choose the Firefighter ID.
6. In the Notification By column, select from the following 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 from the following 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 immediately once 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.
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 appears and displays the particular assignment.
2. To add a Firefighter assignment, choose **Add**. A new row appears in the table.
3. Enter the relevant information in the required fields and select a notification method from the dropdown menu in the **Notification By** column.
4. To remove a Firefighter assignment, choose **Remove**. The selected assignment is deleted.
5. Choose **Save > Close**

### 7.2.2.4 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.

- **Note**
  Only one person can edit a Firefighter assignment at a time.

**Prerequisites**

You have completed the following:

- 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

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 the relevant information in the required fields. On the screen, required fields are 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 particular assignment.
2. To add a Firefighter ID assignment, choose Add. A new row appears in the table.
3. Enter the relevant information in the required fields. On the screen, the required fields are marked with an asterisk (*).
4. To remove a Firefighter ID assignment, choose Remove. The selected assignment is deleted.
5. Choose Save > Close.

7.2.2.5 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).
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).
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)

7.2.2.6 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 182]
Assigning Systems to Reason Codes [page 182]

7.2.2.6.1 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
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 182]

7.2.2.6.2 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

   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 182]

7.2.3 Configuring Role-based Firefighting

Use

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

Process

   For the list of required application roles, see Creating Roles [page 167].
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 [page 135].
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 177].
7. Assign a Controller to a Firefighter role.  
   For more information, see Assigning Controllers [page 178].
8. Assign a Firefighter role to a user to enable them to do firefighting.  
   For more information, see Assigning Firefighters [page 179].

More Information

Configuring ID-based Firefighting [page 173]

7.2.4 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).
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).


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)

7.3 Requesting Emergency Access

Prerequisites

Before you request emergency access, your administrator must have previously set-up the Emergency Access Management functionality. The administrator can also inform you if you will be using ID-based Firefighting or Role-based Firefighting. For more information, see Accessing Systems to Perform Firefighting Activities [page 188].

Context

You can request emergency access to systems in your SAP landscape to perform firefighting. To create a request for emergency access, you use the main access request creation process, and specify that you want to be assigned a Firefighter ID or Firefighter Role.

For more information, see Creating Access Requests [page 23].

Procedure

1. On the User Access tab page, choose Add and select from the following:
   - Firefighter ID
   - Firefighter Role

   **Note**

   When requesting a Firefighter ID or a Firefighter Role, you can filter the search using System and Action Code. If you use Action Code, you must also specify the System. For both Firefighter ID and Firefighter Role requests, the owner(s) displays in the Assignment Approver column.
2. Choose Submit.

7.4 Reviewing and Approving Access Requests

Use

On the Access Request screen, approvers can review, reject, change, or approve access requests.

Process

1. To review an access request, do one of the following:
   - From the My Home work center, choose Work Inbox. From the Workitems list, choose an access request to open it.
   - From the Access Management work center, under the Access Request Administration menu group, choose Search Requests. Search for a request, and then choose the Administrator button to open and review it.

The application displays the Access Request screen, which is the same screen that requesters use when submitting the request. Approvers see all the information that the requester entered. In addition, approvers see more buttons and fields that allow them to review, reject, change, or approve the request.

Note

You can configure the buttons and fields that approvers can see. For example, you can allow approvers to add roles to a request.

Review the request and perform actions as required, such as Approve, Reject, and so on.

2. In the upper right-hand corner, choose Stage to display information about the current stage of the approval workflow and its status.

3. On the Risk Violations tab page, you can view the results of the risk analysis that the requester performed or you can perform your own risk analysis.

Note

You can configure the application to require that approvers perform a risk analysis before approving any requests.

4. When you are finished reviewing the request, choose Submit.
7.5 Extending Validity Periods for Firefighting Assignments

Use

Authorized persons, such as owners of Firefighter IDs and administrators, can extend the validity periods of firefighting assignments.

You can also set the default validity period (in days) in parameter 4001. You maintain the parameter in the Customizing activity, *Maintain Configuration Settings*, under *Governance, Risks, and Compliance > Access Control*.

You can override the default validity period for each assignment by manually updating them.

Process

Centralized Firefighting

You can extend the validity periods by using the *Firefighter ID Assignment* screens:

1. Choose *Emergency Access Assignment > Firefighter IDs*.
   The *Firefighter ID* screen appears.
2. Select a row and choose *Open*.
   The *Firefighter ID Assignment* screen displays the particular assignment.
3. Select a row and update the information in the *Valid From* and *Valid To* fields as needed.
4. Save the entry and close the screen.

Decentralized Firefighting

On the plug-in system, you use the Customizing activity (transaction SPRO) *Maintain Validity Dates for Firefighter Assignments*.

   The *Validity Period* table appears and displays the expired assignments that you are authorized to see.
2. Select a Firefighter ID or Firefighter Role, and then adjust the validity dates as needed.
3. Save your entry.

i Note

To enable administrators and owners to extend the validity period of firefighting assignments, you must create the roles on the relevant plug-in systems, and assign to them the authorization object /GRCPI/001. For the administrator role, enter the *ACTVT* field value as 70 or * (asterisk). For the owner role, enter the *ACTVT* field value as blank (empty).
More Information

Emergency Access Application Types [page 168]
Decentralized Firefighting [page 169]

7.6 Accessing Systems to Perform Firefighting Activities

Use

This topic details how to access the correct system, depending on how your system is configured, to perform firefighting activities.

Prerequisites

You have been granted emergency access by the administrator.

Activities

The application allows you to use one of the following methods to access systems to perform firefighting activities:

Note

Your administrator will inform you of which method to use.

- If your company uses ID-based firefighting, you use the EAM Launchpad to log on to the systems.
  - If decentralized firefighting is enabled, you can log on to the plug-in systems to perform firefighting activities.
  - If your company is using centralized firefighting, you must log on to the GRC system to perform firefighting activities.
  
  For more information, see Using the EAM Launchpad [page 189].

- If your company uses role-based firefighting, you can directly log on to the systems.

More Information

Emergency Access Application Types [page 166]
EAM Terminology [page 165]
7.6.1 Using the Emergency Access Management Launchpad

Context

For ID-based firefighting, you can use the Emergency Access Management (EAM) Launchpad to access your assigned Firefighter IDs. The EAM Launchpad is available for both centralized and decentralized firefighting. The functionality described below is the same for both centralized and decentralized firefighting, except for the following:

- For centralized firefighting, you use this transaction to open the EAM Launchpad on the GRC system: GRAC_EAM.

  **Note**
  The transaction GRAC_SPM is also available for backward compatibility.

- For decentralized firefighting, you use this transaction to open the EAM Launchpad on the plug-in systems: /GRCPI/GRIA_EAM.

  **Note**
  For decentralized firefighting scenarios, to enable the firefighter to use the EAM Launchpad, you must create the Firefighter role on the relevant plug-in systems. Assign to the role the authorizations to use transactions /GRCPI/GRIA_EAM and SU53.

  **Note**
  The launchpad for centralized firefighting displays all the plug-in systems to which you have access. The launchpad for decentralized firefighting does not display any systems because it allows you to access only the current plug-in system.

The EAM Launchpad screen has the following elements:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firefighter ID</td>
<td>This is the name of the Firefighter ID you are authorized to use. You may have one or several.</td>
</tr>
<tr>
<td>Element</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>System Name</td>
<td>This is the name of the system the Firefighter ID is authorized to access.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This field is only displayed for centralized firefighting.</td>
</tr>
<tr>
<td>Firefighter ID Owner</td>
<td>This is the name of the owner of the Firefighter ID.</td>
</tr>
<tr>
<td>Status</td>
<td>Green indicates the Firefighter ID is available for you to use. Red indicates the Firefighter ID is in use by another Firefighter. You can choose to notify the Firefighter by using the Message to Firefighter button.</td>
</tr>
<tr>
<td>FFID Used By</td>
<td>This is the Firefighter who is currently using the Firefighter ID.</td>
</tr>
<tr>
<td>Description</td>
<td>This is the description of the Firefighter ID.</td>
</tr>
<tr>
<td>Logon</td>
<td>Use this button to logon onto the system.</td>
</tr>
<tr>
<td>Message to Firefighter</td>
<td>Use this button to send a pre-formatted message to the Firefighter that you want to use the Firefighter ID after they are done.</td>
</tr>
<tr>
<td>Additional Activity</td>
<td>After you choose Logon, you must enter a description of the activities you plan to perform. You had to carry out additional activities, choose the Additional Activity button to open the Reason Code screen, and enter the additional information in the Additional Activity field.</td>
</tr>
<tr>
<td>Unlock</td>
<td>Use this button to log out of the firefighting session, and allow others to use the Firefighter ID.</td>
</tr>
</tbody>
</table>

**Procedure**

1. In the SAP GUI, enter the transaction (GRAC_EAM OR /GRCPI/GRIA_EAM) to open the EAM Launchpad.
2. On the EAM Launchpad screen, find the relevant Firefighter ID and choose the Logon button. The Reason Codes screen appears.
3. In the Reason Codes field, select the relevant reason code, and enter any additional information as needed.
4. In the available field, enter the actions you plan to perform.
5. Choose the Execute button to logon.
7.7 Reviewing Emergency Access Activities and Reports

Context

The administrator, business process owner and controller need to have a formalized process of reviewing the emergency access activities that have been conducted by firefighters. They can use the following reports to analyze the activities.

Procedure

1. Read through the Consolidated Log Report to identify problems or propose solutions.
   - **Consolidated Log Report** – This is the most commonly used report. The Controller of the Firefighter IDs can receive this by e-mail or through the workflow. On this report, they can see what Firefighter ID is accessing what system, what transactions have been made and the details. How often it is delivered (daily, weekly, and so forth) can be configured according to the business need.

2. If needed and authorized, the business process owner, controller or compliance person can create these additional reports to investigate details of the emergency access activities.
   - **Invalid Emergency Access Report** – This report specifies the user types for emergency access that are expired, deleted, or locked, such as Firefighter IDs, Controllers, or Owners.
   - **Firefighter Log Summary Report** – This report captures transaction data from the selected system connector for Firefighter IDs.
   - **Reason Code and Activity Report** – This report displays data from the selected system connector for each Firefighter ID. The report lists the reason and activity for each login event.
   - **Transaction Log and Session Details Report** – This report captures transaction data from the selected system connector for Firefighter IDs and Firefighters. It displays the number and type of transactions accessed for each Firefighter ID and for each Firefighter.
   - **SoD Conflict Report for Firefighter IDs** – This report provides the history of actions performed on SoD review tasks including mitigation reaffirm.
8 Managing Periodic Access Reviews

Use

This process explains how periodic access reviews are defined and deployed.

Process

1. Identify policies that impact Periodic Access Reviews
   In this step, organizational policies that impact periodic access reviews are identified and analyzed to ensure that policy requirements are considered when defining the review process. This step is performed for the initial review and for policy or environment changes only.

2. Define review process
   The review process parameters are defined. Examples of parameters include frequency of review, reviewers, and users or access to be reviewed. This step is performed for the initial review and for policy or environment changes only.

3. Identify data to support review process
   Additional data may be required to support the review process. For example, if the reviewer in the user access review is a Manager, a data source from which to extract or gather Manager information must be identified. Perform this step for the initial review and for policy or environment changes only.

4. Prepare review information
   Once all required data and review attributes have been defined, the user access reviews must be prepared to be sent out for review.

5. Perform review
   Each reviewer performs the review as dictated by policy.

6. Take action as indicated
   Based upon policy requirements, approve continued access or request removal of access for each user.

7. Retain review results
   Retain the results of the access reviews for audit purposes.

Result

A process for periodically reviewing access is defined and deployed based upon policy.
8.1 Compliance Certification Reviews

Use

Administrators can schedule periodic reviews of user access and segregation of duties (SoD) risks. During these reviews, Access Control automatically forwards review requests to designated managers and reviewers within a predefined workflow that is customized for the enterprise. Compliance Certification Reviews enable you to complete these periodic reviews to ensure that user access and SoD risks are properly maintained within your organization.

Within Access Control, coordinators are responsible for verifying that all reviewers (managers or role owners) perform user access and SoD risk reviews. As part of your compliance certification reviews, you can review requests that do not have a reviewer or coordinator assigned, and assign corresponding reviewers and coordinators as required.

You can also manage coordinator-to-reviewer mappings as part of your compliance certification reviews, including creating, importing, modifying, and deleting these mappings, as required. Finally, you can manage rejections, including searching for rejected users, generating review requests, and canceling review request generations (for requests that have not been completed).

Features

You can complete the following tasks when performing Compliance Certification Reviews:

- Assign coordinators to reviewers
- Review requests
- Manage rejections

More Information

Managing Coordinators [page 193]
Managing Rejections [page 198]

8.1.1 Managing Coordinators

Use

As part of your compliance certification review, you can assign coordinators to reviewers, and manage these relationships to help monitor user access reviews. Access Control uses the coordinator information for SoD and user access reviews and to generate reports that you can use while managing the review process.
Using the Manage Coordinators screen, you can complete the following tasks:

- Create or import coordinator-to-reviewer mappings
- Search and display existing coordinator-to-reviewer mappings
- Modify current coordinator-to-reviewer mappings
- Delete existing coordinator-to-reviewer mappings
- Export coordinator-to-reviewer mappings to a Microsoft Excel spreadsheet

More Information

Creating Coordinator Mappings [page 194]
Modifying Coordinators [page 195]
Searching Coordinators [page 196]

8.1.1.1 Creating Coordinator Mappings

Use

You can manually map coordinators to reviewers or import multiple coordinator-to-reviewer mappings using the functions on the Manage Coordinators screen.

Procedure

To map coordinators to reviewers:

1. Choose Access Management \ Compliance Certification Reviews \ Manage Coordinators. The Manage Coordinators screen appears.
2. Choose the Create pushbutton. The Create Mapping screen appears.
3. Enter or select the Coordinator ID.
4. Enter or select the Reviewer ID.
5. Choose Save.
6. Choose Close. The mapping appears in the table on the Manage Coordinators screen.

To import coordinator-to-reviewer mappings:

1. Choose Access Management \ Compliance Certification Reviews \ Manage Coordinators. The Manage Coordinators screen appears.
2. Choose the Import pushbutton. The Import Coordinators screen appears.
3. Enter or select the file using the Select File field.
4. Choose Save.
8.1.1.2 Modifying Coordinators

Context

You can modify coordinator-to-reviewer mappings or delete a mapping, using the Manage Coordinators screen.

Procedure

To modify a coordinator-to-reviewer mapping:

2. Select the mapping you want to modify, and choose the Open pushbutton. The Change Mapping screen appears.
3. Enter or select a new Coordinator ID, as required.
4. Enter or select a new Reviewer ID, as required.
5. Choose Save.
6. Choose Close. The updated mapping appears in the table on the Manage Coordinators screen.

To delete a coordinator-to-reviewer mapping:

8. Select the mapping you want to delete and choose the Delete pushbutton. A confirmation dialog box appears.
9. Choose Yes.

Next Steps
8.1.3 Searching Coordinators

Context

You can search for coordinator-to-reviewer mappings and export the results to a Microsoft Excel spreadsheet using the Manage Coordinators screen.

Procedure

2. Choose the Filter link. An empty row appears at the top of the table.
3. Type appropriate values in the corresponding columns and press Enter. The table displays the filtered results based on the values you entered.
4. To export the results to a Microsoft Excel spreadsheet, choose Export > Export to Microsoft Excel.
   Choose Save, navigate to the appropriate folder, and choose Save again.

8.1.2 Reviewing Requests

Prerequisites

You need to schedule and run the following activities using the Background Scheduler before reviewing requests:

- Generate data for access request UAR review
- Generate data for access request SoD review

Verify that you have also scheduled the following activities using the Background Scheduler:

- Update workflow for UAR request
- Update workflow for SoD request
Context

You can review requests, including user access and segregation of duties (SoD) risks, using the functions on the Request Review screen. Using this screen, you can verify that requests have a reviewer or coordinator assigned and change reviewers or cancel requests.

Note

In the Customizing activity Maintain Configuration Settings under Governance, Risk, and Compliance Access Control, verify that the UAR Review parameter (2007) is set to YES. This specifies that an administrator needs to review requests before the requests reach reviewers. If the parameter is set to NO, requests are routed directly to reviewers (managers or role owners).

Procedure

1. Choose Access Management Compliance Certification Reviews Request Review.

   The Request Review screen opens.

2. Specify the search criteria.

   Do the following:
   1. Choose the Process Type, using the dropdown list, from among the following:
      ○ User Access Review Workflow
      ○ SOD Risk Review Workflow
   2. Choose the Request Type using the dropdown list.
   3. Enter or choose the User ID.
   4. Enter or choose the Reviewer ID.
   5. Enter or choose the Coordinator ID.
      To specify no coordinator, select the No Coordinator checkbox.
   6. Enter or choose the Date From/To in the corresponding fields.
   7. Enter the Job ID.
   8. Specify the maximum number of results in the Maximum Search No. field.


4. To change reviewers, select an assignment and choose the Change Reviewers pushbutton. The Assign Reviewers dialog box appears.

   Select one more reviewers and coordinators from the Available list and choose the right-arrow pushbutton to move the entry to the Selected list. After assigning the reviewers, choose OK.

5. To cancel a request, select an assignment and choose the Cancel Request pushbutton.

   A confirmation dialog box appears. Choose Yes to mark the users as rejected for request regeneration.
Next Steps

Compliance Certification Reviews [page 193]
Managing Coordinators [page 193]
Managing Rejections [page 198]
Background Scheduler [page 30]

8.1.3 Managing Rejections

Context

You can manage rejections, including searching for rejected users, generating review requests, and canceling review request generations (for those requests that have not been completed), using the functions on the Manage Rejections screen.

Note

You schedule and run the Generates new request for UAR rejected request activity using the Background Scheduler after managing rejections.

Procedure

   The Manage Rejections screen opens.
2. Specify the search criteria.
   Do the following:
   1. Enter or select the Start Date and End Date, as appropriate.
   2. Choose the Status using the corresponding dropdown list, from among the following:
      ○ New—Requests submitted by the reviewer.
      ○ Error—The generation background job has encountered an error.
      ○ To Generate—The user is marked for regeneration, but the generation background job has not started. You can click Cancel Generation to cancel the request generation.
      ○ In Process—The background generation job has started but has not completed. You cannot cancel requests with this status because the background job has started.
      ○ Completed—The generation background job has completed. The new request number is updated.
3. Choose the Reason from the corresponding dropdown list.
4. Choose the **Process Type** from the corresponding dropdown list.

3. Choose **Search**. The search results appear in the table.

4. To generate a request, select a rejection in the table and choose the **Generate Requests** pushbutton.

Before generating requests for rejected users, make sure that the users have the correct reviewer information. This precaution prevents incorrect information from entering the request cycle again. For example, if the reviewer information is stored in an LDAP data source and is incorrect, you must update the information in the LDAP data source so that new requests are generated with the correct reviewer name.

**Note**

If you select multiple requests for generation in which some of the requests are grouped by user and others are grouped by role/risk owner, the system does not combine the requests when generating.

**Example**

Consider the case when a request is grouped by risk/role owner and by manager:

- **Request grouped by risk/role owner:**
  - Risk1 User1
  - Risk2 User1
- **Request grouped by manager:**
  - User1 Role1
  - User2 Role2

In this case, if you select the four requests for generation (with grouping by manager) you can expect the following results:

- **Request grouped by risk/role owner:**
  - Risk1 User1 – 5 is the new request number
  - Risk2 User1 – 5 is the request number
- **Request grouped by manager:**
  - User1 Role1 – 6 is the request number
  - User2 Role2 – 7 is the request number

5. To cancel a generation, select a rejection in the table and choose the **Cancel Generation** pushbutton.

You can cancel generations only for rejections with a status of **To Generate**. After the request status is **In Process**, the background job has started and the request cannot be canceled.

6. To export the results to a Microsoft Excel spreadsheet, choose **Export**. Choose **Export to Microsoft Excel**.

Choose **Save**, navigate to the appropriate folder, and choose **Save** again.

**Next Steps**

- Compliance Certification Reviews [page 193]
- Managing Coordinators [page 193]
- Reviewing Requests [page 196]
8.2 Alerts

Use

When a user performs critical or conflicting actions, the system can send an escalation alert to the appropriate personnel. You can use the Alerts feature to monitor Conflicting and Critical Access and Mitigating Control alerts, as appropriate.

Specifically, you can do the following:

- Search and filter alerts to display
- Clear alerts
- Search and filter cleared alerts

More Information

Searching Alerts [page 122]
Cleared Alerts [page 123]
Clearing Alerts [page 124]
Searching Cleared Alerts [page 125]

8.2.1 Searching Alerts

Context

You can search the following types of alerts:

- Conflicting and Critical Access Alerts
- Mitigating Controls

Procedure


   The Conflicting and Critical Access Alerts or Mitigating Control Alerts screen opens.
2. Specify the search criteria.
   1. Choose the object type using the first dropdown list.
      For **Conflicting and Critical Access Alerts**, you can choose from among the following object types:
         - Business Process
         - System
         - Date Time Executed
         - Access Risk ID
         - Risk Level
         - Risk Owner
         - Risk Type
         - User ID
         - Alert Date Time
      For **Mitigating Control Alerts**, you can choose from among the following object types:
         - Action
         - System
         - Control ID
         - Date Time Executed
         - User ID
         - Alert Date Time
   2. Choose the operator using the second dropdown list, from among the following:
      - is
      - is not
      - starts with
      - contains
      - is between
      - Multiple Selections
   3. Type or select the search value in the third field.
   4. Optionally, add a line to the search criteria by choosing the plus (+) pushbutton and specifying the fields.
      Alternatively, remove a line from the search criteria by choosing the corresponding minus (-) pushbutton.

3. Choose **Search**.
   The search results appear in the table.

4. Optionally, save the search criteria as a variant by typing a name in the **Save Variant as** field and choosing **Save**.

**Next Steps**

- Alerts [page 121]
- Cleared Alerts [page 123]
- Clearing Alerts [page 124]
- Searching Cleared Alerts [page 125]
8.2.2 Cleared Alerts

Use

After an alert message has been delivered and cleared, or deleted, it remains as an archived record. You can continue to track and monitor these alerts using the Cleared Alerts tab of the Conflicting and Critical Risk Alerts and Mitigating Controls screens.

More Information

Alerts [page 121]
Searching Alerts [page 122]
Clearing Alerts [page 124]
Searching Cleared Alerts [page 125]

8.2.2.1 Clearing Alerts

Context

You can clear the following types of alerts, as needed:

- Conflicting and Critical Access Alerts
- Mitigating Controls

Procedure

   
   The Conflicting and Critical Access Alerts or Mitigating Control Alerts screen opens.

2. Specify the search criteria.

3. Choose Search.

   The search results appear in the table.

4. Select the alert to clear by selecting the box to the left and choosing Clear Alert.

   The Clear Alert dialog appears.
5. Enter a reason for clearing the alert, and choose OK.

The alert is cleared. You can view cleared alerts using the Cleared Alerts tab. For more information, see.

Next Steps

Alerts [page 121]
Searching Alerts [page 122]
Cleared Alerts [page 123]
Searching Cleared Alerts [page 125]

8.2.2.2 Searching Cleared Alerts

Context

You can search the following types of cleared alerts:

- Conflicting and Critical Access Alerts
- Mitigating Controls

Procedure

   
   The Conflicting and Critical Access Alerts or Mitigating Control Alerts screen opens.

2. Select the Cleared Alerts tab.

3. Specify the search criteria.

   1. Choose the object type using the first dropdown list.
      
      For Conflicting and Critical Access Alerts, you can choose from among the following object types:
      
      - Business Process
      - System
      - Date Time Executed
      - Access Risk ID
      - Risk Level
      - Risk Owner
      - Risk Type
For **Mitigating Control Alerts**, you can choose from among the following object types:

- Action
- System
- Control ID
- Date Time Executed
- User ID
- Alert Date Time

2. Choose the operator using the second dropdown list, from among the following:

- is
- is not
- starts with
- contains
- is between
- Multiple Selections

3. Type or select the search value in the third field.

4. Optionally, add a line to the search criteria by choosing the plus (+) pushbutton and specifying the fields. Alternatively, remove a line from the search criteria by choosing the corresponding minus (-) pushbutton.

5. Choose **Search**. The search results appear in the table.

6. Optionally, save the search criteria as a variant by typing a name in the **Save Variant as** field and choosing **Save**.

7. To display the reason an alert was cleared, choose the Comments link in the **Reason** field for the corresponding alert. The **Clear Alert** dialog appears displaying the reason. Choose **Cancel** to dismiss the dialog.

**Next Steps**

- Alerts [page 121]
- Searching Alerts [page 122]
- Cleared Alerts [page 123]
- Clearing Alerts [page 124]
9 Reports and Analytics

The Reports and Analytics work center provides a central location to display reports and dashboards for Access Control information, such as alerts, user analysis, audit reports, and so on.

**Note**

The Reports and Analytics work center is shared by the Access Control, Process Control, and Risk Management products in the GRC application. The menu groups and quick links available on the screen are determined by the applications you have licensed. The content in this topic covers the functions specific to Access Control.

<table>
<thead>
<tr>
<th>Table 29: Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Dashboards</td>
<td>Dashboards for access risk analysis, business role management, and user access management</td>
</tr>
<tr>
<td>Access Risk Analysis Reports</td>
<td>Reports related to access risk analysis, including user risk violations, role risk violations, profile risk violations, and HR Object risk violations</td>
</tr>
<tr>
<td>Access Request Reports</td>
<td>Reports related to access requests, including service level for requests and requests with conflicts and mitigation</td>
</tr>
<tr>
<td>Role Management Reports</td>
<td>Reports related to role management, including user-to-role relationships and master-to-derived role relationships</td>
</tr>
<tr>
<td>Security Reports</td>
<td>Reports related to user, role, and profile security</td>
</tr>
<tr>
<td>Audit Reports</td>
<td>Audit-related reports, including actions in roles (but not in rules) and permissions in roles (but not in rules)</td>
</tr>
<tr>
<td>Emergency Access User Management Reports</td>
<td>Reports related to superuser activities, including invalid superusers and consolidated logs</td>
</tr>
</tbody>
</table>

9.1 Access Dashboards

Access Control provides the following dashboards:

- **Access Provisioning Dashboard** [page 206]
  
  This dashboard displays the number of roles assigned to or removed from individual requests grouped by role action in one view. In another view, it displays the total number of processed users grouped by user action.

- **Access Requests Dashboard** [page 207]
This dashboard displays access requests by status and type using the numerous filtering criteria such as date, system, and priority.

- This dashboard displays views of rules by risk level and business process. You can group the results by various criteria such as action and permission.
- **Alerts Dashboard [page 209]**
  This dashboard displays alerts by month and SOD alerts by process.
- **Mitigating Control Library Dashboard [page 209]**
  This dashboard displays controls by risk level and controls by process.
- **Risk Violations Dashboard [page 210]**
  This dashboard displays the number of Access Risk Violations by role, user, or profile for all systems or for a selected system. It shows the total number of users analyzed and the total number of violations.
- **Role Analysis Dashboard [page 213]**
  This dashboard displays the number of mitigated roles with no risk violations and roles with risk violations by the severity level of those violations. It also displays a breakdown of the SOD violations in bar graph format at the role and user level for the selected system.
- **Role Library Dashboard [page 214]**
  This dashboard displays all the roles in your application. It displays the total number of roles and the number of roles with violations.
- **Service Level for Access Requests Dashboard [page 214]**
  This dashboard displays request count by month/year and number of service level violations.
- **User Analysis Dashboard [page 215]**
  This dashboard displays the number of users who are mitigated or who have risk violations by severity level. It also displays a breakdown of the number of users with critical actions and critical role profiles.
- **Violations Comparisons Dashboard [page 217]**
  This dashboard displays quarterly or monthly risk violations as well as the SoD remediation progress completed for each analysis type as a graphical percentage as of a certain date.
- **Risk Violation in Access Request Dashboard [page 217]**
  This dashboard displays access risk violations grouped by violations and mitigation. It also displays access risk violation details.

### 9.1.1 Access Provisioning Dashboard

**Use**

The **Access Provisioning Dashboard** displays two views:

- **Assignment Assigned or Removed**
  This dashboard displays the number of roles assigned to or removed from individual requests grouped by role action.
- **Users Processed**
  This dashboard displays the total number of processed users grouped by user action.

You can filter the results by the following criteria:

- **Start Date**
- **To Date**
● **System**
  The dashboard only displays systems that you have authorization to view.

- **Approver**
- **Employee Type**
- **Location**
- **Process Type**

You click the bar graph to drill down into the detailed information. You can use *Print* to create a PDF file or *Export* to download the detailed results of the requests for which roles were assigned or removed.

**Drill down Function**

On the drill down screen, the application displays *only* objects that you are authorized to see. For example, on the main dashboard screen you may see the totals for the entire company; whereas on the drill down screen, you may only see the totals for North America, if you are only authorized to see North America.

**Note**

To view access request data in this report, you must be assigned to a role with authorization to view access request objects.

**More Information**

**9.1.2 Access Requests Dashboard**

**Use**

The *The Access Requests Dashboard* displays access requests by status and type using the following filtering criteria:

- **Start/To Dates**
- **System**
  The dashboard only displays systems that you have authorization to view.
- **Process Type**
- **Priority**
- **Functional Area**
- **Request Type**
- **Status**

The pie chart divides requests into the following categories:

- Approved
Drill down Function

You drill down into the detailed information by clicking a specific area of the pie chart. On the drill down screen, the application displays only objects that you are authorized to see. For example, on the main dashboard screen you see the totals for the entire company; whereas on the drill down screen, you may only see the totals for North America, if you are only authorized to see North America.

Note

To view access request data in this report, you must be assigned to a role with authorization to view access request objects.

More Information

9.1.3 Access Rule Library Dashboard

Use

The Access Rule Library Dashboard displays views of Rules by Risk Level and Business Process. You can group the results by the following criteria:

- Action
- Permission
- Critical Action
- Critical Permission
- Access Risk

This dashboard also shows the number of active risks, the number of disabled risks, and the number of functions.

You click the pie chart or the bar graph to drill down into the detailed information. You can use Export to download the details.

Drill Down Function

You drill down into the detailed information by clicking a specific area of the pie chart or bar graph. On the drill down screen, the application displays only objects that you are authorized to see. For example, on the main dashboard screen you see the totals for the entire company; whereas on the drill down screen, you may only see the totals for North America, if you are only authorized to see North America.
9.1.4 Alerts Dashboard

Use

The *Alerts Dashboard* displays two views:

- **Alerts by Month**
  This dashboard displays a line graph that represents the number of alerts generated across the time period that you specify. You can ask to see the following alert types: *All, Mitigation, or SOD*. You can drill down on the circles to see the alert details at particular points on the line.

- **SOD Alerts by Process**
  This dashboard displays the total number of uncleared SOD alerts by business process in both table and bar chart formats. The results are filtered by time period and alert type. You can click either the table or the bar chart to view the report details.

You can use *Print* to produce a PDF file of the detailed results or you can use *Export* to download the detailed results to a Microsoft *Excel* spreadsheet.

Drill down Function

You drill down into the detailed information by clicking a specific area of the line graph, bar chart, or table. On the drill down screen, the application displays *only* objects that you are authorized to see. For example, on the main dashboard screen you may see the totals for the entire company; whereas on the drill down screen, you may only see the totals for North America, if you are only authorized to see North America.

9.1.5 Mitigating Control Library Dashboard

Use

The *Mitigating Control Library Dashboard* displays two views:

- **Controls by Risk Level**
  This dashboard displays the total number of controls by the risk levels *Critical, High, Medium, and Low*. It also shows the number of active and inactive controls. You can choose to see all organizations or a particular organization. You click on a slice of the pie chart to view the details.
• **Controls by Process**
  This dashboard displays the total number of controls by business process. You click on an area of the bar chart to display the details of each business process.

You can use *Print* to produce a PDF file of the detailed results or you can use *Export* to download the detailed results to a Microsoft Excel spreadsheet.

**Drill down Function**

You drill down into the detailed information by clicking on the pie chart, the bar graph, or the table. On the drill down screen, the application displays *only* objects that you are authorized to see. For example, on the main dashboard screen you may see the totals for the entire company; whereas on the drill down screen, you may only see the totals for North America, if you are only authorized to see North America.

**More Information**

**9.1.6 Risk Violations Dashboard**

**Use**

The *Risk Violations Dashboard* displays the number of *Access Risk Violations* by role, user, or profile for all systems or for a selected system. It shows the total number of users analyzed and the total number of violations.

The *Risk Violations Dashboard* displays access risk violations using the following filtering criteria:

- **Year/Month**
- **System**
  You only see the systems that you are authorized to view.
- **Analysis Type**
- **User Group**
- **Violation Count by**

The bottom half of the *Risk Violations Dashboard* displays risk violations by business process.

**Features**

**Run Risk Analysis from Report**

You access the detailed information by clicking the pie chart, legend or bar graph.

1. Select the chart, legend or the graph.
2. Analyze the detailed information.
On the drilldown screen, the application displays only objects that you are authorized to see. For example, on the main dashboard screen you see the totals for the entire company; whereas on the drilldown screen, you may only see the totals for North America.

Clicking on a pie chart element displays more risk detail for a user, role or profile in a separate table for the current or last executed month only. Because of the mass quantity of records stored, this feature is only available for the current or last executed month. To view risk details from prior months store your data in Business Warehouse.

3. Optional, if needed, select the Run Risk Analysis button. This produces the Risk Violations Drilldown report.
4. Choose how to run the report (Run in the Foreground or Run in Background). If you choose Run in Background, the Background Scheduler screen will open so you can input your schedule choices.

To view the status of background jobs, navigate to Access Management > Scheduling > Background Jobs.

5. Choose whether to perform the tasks in Realtime or Offline.
6. On the resulting detailed remediation view, you can assign a mitigating control in the Risk ID or Rule ID column or remove a role in the Rule ID column.

More Information

Remediation View [page 211]

9.1.6.1 Remediation View

Prerequisites

You must have already selected your parameters and Run Risk Analysis from the initial report to see the detailed remediation view. This functionality can be accessed from the following:

- Access the Remediation View from Reports and Analytics workcenter > Access Dashboards > Risk Violations Dashboard [page 210] and User Analysis Dashboard [page 215].
- Access the Remediation View from Access Management > Access Risk Analysis > User Level Access Risk Analysis [page 93]
**Context**

The remediation view graphically identifies the access risk violations and allows users to make informed decisions. You can take remediation action directly from the results of user-level access risk analysis. You can initiate a workflow to update user or role authorization assignments, validity dates and mitigate access.

The type of report you see (Remediation, Business or Technical view) from the dashboard depends on the default selected by your System Administrator. From the Customizing activities (transaction SPRO), you can change the view.

**Procedure**

1. Analyze the report. For more information, select entries in the User, Risk, Rule ID and Access columns. A side-panel appears with detailed information for each of these.

2. Decide how to mitigate the risk. From the remediation view, you can:
   - Assign a mitigating control in the Risk column (to apply to all rules) or the Rule ID column (for one rule). Select the mitigation icon to access the Assign Mitigating Controls screen.

   **⇒ Recommendation**
   For more information, see Mitigating Risks [page 39].

   - Remove a role in the Access column. Select the mitigation icon to perform this functionality.

   **⇒ Recommendation**
   For more information, see Role Maintenance [page 133].

3. After completing your actions, there are icons that reflect the status.
   - Green indicates the action is completed.
   - Yellow indicates it is in progress.
   - Red indicates there is a problem.
9.1.7 Role Analysis Dashboard

Use

The Role Analysis Dashboard displays two views:

- **Segregation of Duties**
  This dashboard displays the number of mitigated roles with no risk violations and roles with risk violations by the severity level of those violations. For the specified filters, it also displays:
  - The number of users analyzed
  - Users with no violations
  - Users with violations
  You can filter the results by the following selections:
  - **Year/Month**
  - **System**
    The system only displays systems for which you have authorization.
  - **Analysis Type**
  - **Violation count by Access Risk or Permission**
  The dashboard generates a pie chart showing Critical, High, Medium, and No Violations as well as Mitigated Roles.
  You can drill down on areas of the pie chart to view the details of the roles analyzed.

- **Access Risk Violations by Role and User**
  This dashboard displays a breakdown of the SOD violations in bar graph format at the role and user level for the selected system. You can drill down on the graph for more details.

You can use Print to produce a PDF file of the detailed results or you can use Export to download the detailed results to a Microsoft Excel spreadsheet.

**Drill down Function**

You drill down into the detailed information by clicking a specific area of the pie chart or bar graph. On the drill down screen, the application displays only objects that you are authorized to see. For example, on the main dashboard screen you may see the totals for the entire company; whereas on the drill down screen, you may only see the totals for North America, if you are only authorized to see North America.

**Note**

Clicking on a pie chart element displays more risk detail for a role or profile in a separate table for the current or last executed month only. Because of the mass quantity of records stored, this feature is only available for the current or last executed month. To view risk details from prior months, store your data in Business Warehouse.
9.1.8 Role Library Dashboard

Use

The Role Library Dashboard displays all the roles in your application. It displays the total number of roles and the number of roles with violations. There are two views:

- Enterprise roles grouped by role type
- Roles grouped by business process

You can filter the results by the following criteria:

- System Type
- System Landscape
- Role Owner

You click the pie chart, the bar graph, or the table to drill down into the detailed information.

Drill Down Function

You drill down into the detailed information by clicking a specific area of the pie chart or bar graph. On the drill down screen, the application displays only objects that you are authorized to see. For example, on the main dashboard screen you see the totals for the entire company; whereas on the drill down screen, you may only see the totals for North America, if you are only authorized to see North America.

More Information

9.1.9 Service Level for Access Requests Dashboard

Use

The Service Level for Access Requests Dashboard displays two views:

- Request Count by Month/Year
- Service Level Violation

You can use the following items to filter your results:

- Date
- System
  The dashboard only displays systems that you have authorization to view.
- Request Type
- Process type
- Priority
Both dashboards show the results in line graph format. You can click on the beginning or end of the line to see the detailed results by request number.

**Note**
You can use *Print* to produce a PDF file of the detailed results or you can use *Export* to download the detailed results to a Microsoft Excel spreadsheet.

**Drill down Function**
You drill down into the detailed information by clicking either end of the line graph. On the drill down screen, the application displays *only* objects that you are authorized to see. For example, on the main dashboard screen you may see the totals for the entire company; whereas on the drill down screen, you may only see the totals for North America, if you are only authorized to see North America.

**Note**
To view access request data in this report, you must be assigned to a role with authorization to view access request objects.

**More Information**

**9.1.10 User Analysis Dashboard**

**Use**

The *User Analysis Dashboard* displays two views:

- **Segregation of Duties**
  This dashboard displays the number of users who are mitigated or who have risk violations by severity level. It also displays *Number of Users Analyzed, User with No Violations,* and *Users with Violations.*

- **Critical Actions and Roles**
  This dashboard displays a breakdown of the number of users with critical action and critical role profiles.

You can filter the results by the following criteria:

- **Month/Year**
- **System**
  The dashboard only displays systems that you have authorization to view.
- **User Group**
Violation Count by

You click the pie chart, legend or the bar graph to drill down into the remediation view. You can use Print to create a PDF file or Export to download the detailed results.

Features

Run Risk Analysis from Report

You access the detailed information by clicking the pie chart, legend or bar graph.

1. Select the chart, legend or the graph.
2. Analyze the detailed information.

**Note**

On the drilldown screen, the application displays only objects that you are authorized to see. For example, on the main dashboard screen you see the totals for the entire company; whereas on the drilldown screen, you may only see the totals for North America.

**Note**

Clicking on a pie chart element displays more risk detail for a user in a separate table for the current or last executed month only. Because of the mass quantity of records stored, this feature is only available for the current or last executed month. To view risk details from prior months, store your data in Business Warehouse.

3. Optional, if needed, select the Run Risk Analysis button. This produces the Risk Violations Drilldown report.
4. Choose how to run the report (Run in the Foreground or Run in Background). If you choose Run in Background, the Background Scheduler screen will open so you can input your schedule choices.

**Note**

To view the status of background jobs, navigate to Access Management > Scheduling > Background Jobs.

5. Choose whether to perform the tasks in Realtime or Offline.
6. On the resulting detailed remediation view, you can assign a mitigating control in the Risk ID or Rule ID column or remove a role in the Rule ID column.

More Information

Remediation View [page 211]
9.1.11 Violations Comparisons Dashboard

Use

The Violations Comparisons Dashboard displays two views:

- **Quarterly/Monthly Comparison**
  This dashboard displays quarterly or monthly risk violations filtered by the following selections:
  - Calendar Type
  - From/To Dates
  - System
    - You only see systems for which you have authorization.
  - Analysis Type
  - Violation count by Access Risk or Permission

**Drill down Function**
You can drill down on selected points of the line graph to view the details of the risk violations at a point in time.
You drill down by clicking a specific area of the line graph. On the drill down screen, the application displays only objects that you are authorized to see. For example, on the main dashboard screen you may see the totals for the entire company; whereas on the drill down screen, you may only see the totals for North America, if you are only authorized to see North America.
You can use Print to produce a PDF file of the detailed results or you can use Export to download the detailed results spreadsheet.

- **Remediation Progress**
  This dashboard displays the SoD remediation progress completed for each analysis type as a graphical percentage as of a certain date.

More Information

9.1.12 Risk Violation in Access Request Dashboard

Use

The Risk Violation in Access Request Dashboard displays two views:

- Access risk violations grouped by violations and mitigation
- Access risk violation details

You can filter the results by using the following criteria:

- **Start Date**
- **End Date**
- **System**  
  You only see the systems that you are authorized to view.

- **Request Type**
- **Priority**
- **Functional Area**
- **Workflow Type**

The bottom half of the dashboard displays risk violations by criticality: **Critical, High, Medium, and Low**. Click the pie chart, the table, or the bar graph to drill down into the details.

You can use **Print Version** to produce a PDF file of the detailed results or you can use **Export** to download the detailed results to a Microsoft **Excel** spreadsheet.

**Drill down Function**

On the drill down screen, the application displays **only** objects that you are authorized to see. For example, on the main dashboard screen you may see the totals for the entire company; whereas on the drill down screen, you may only see the totals for North America, if you are only authorized to see North America.

**Note**

To view access request data in this report, you must be assigned to a role with authorization to view access request objects.

**More Information**

**9.2 Access Risk Analysis Reports**

Access Control provides the following risk analysis reports:

- **Access Rule Summary** [page 72]
- **Access Rule Detail** [page 73]
- **Mitigation Control Report** [page 222]
- **User Risk Violation Report** [page 226]
- **Role Risk Violation Report** [page 225]
- **Profile Risk Violation Report** [page 223]
- **HR Object Risk Violation Report** [page 221]
- **Mitigated Object Report** [page 220]
9.2.1 Access Rule Summary Report

Use

This report lists risks and conflicting functions for all risk types.

To run the report, designate values for the following filtering criteria:
- **Access Risk ID**
- **Access Risk Description**
- **Business Process ID**
- **Rule Set**

** Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from Saved Variants and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose Export Results Sets to download the data or Print Version to create a PDF file.

**Report Details**

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

More Information

9.2.2 Access Rule Detail Report

Use

This report lists risks, functions, transaction codes, and associated permission details for all risk types.

To run the report, designate values for the following filtering criteria:
- **System**
  The report only displays systems that you have authorization to view.
- **User ID**
- **User Group**
- **Valid To**
** Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from **Saved Variants** and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose **Export Results Sets** to download the data or **Print Version** to create a PDF file.

**Report Details**

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

**More Information**

**9.2.3 Mitigated Object Report**

**Use**

This report shows all mitigated **Users, Roles, Profiles, User Organizations, Role Organizations**, and HR Objects with associated mitigation controls.

To run the report, designate values for the following filtering criteria:

- **Mitigating Control ID**
- **Access Rule ID**
- **System**
  - The report only displays systems that you have authorization to view.
- **Approver**
- **User Group**
- **User ID**
- **Monitor ID**
- **Organization ID**
- **Access Risk ID**
- **Risk Level**
- **Status**
- **Mitigating Control Valid From**
- **Mitigating Control Valid To**

Additionally, you can choose to report by one of the following:

- **User**
- Role
- Profile
- User Org
- Role Org
- HR Object

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from Saved Variants and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose Export Results Sets to download the data.

**Report Details** – The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

**More Information**

### 9.2.4 HR Object Risk Violation Report

**Use**

This report lists all the risk violations for selected HR objects. To run the report, designate values for the following filtering criteria:

- **System**
  The report only displays systems that you have authorization to view.
- **Analysis Type**
- **Object Type**
- **Object ID**
- **Risk Level**
- **Rule Set**
The report contains the following options:

Table 30:

<table>
<thead>
<tr>
<th>Option</th>
<th>Choices</th>
</tr>
</thead>
</table>
| Format          | • Summary  
|                 | • Detail  
|                 | • Management Summary  
|                 | • Executive Summary  |
| View            | • Technical  
|                 | • Business  |
| Type            | Access Risk Analysis  
|                 | • Action Level  
|                 | • Critical Action  
|                 | • Critical Role/Profile  
|                 | • Permission Level  
|                 | • Critical Permission  |
| Additional Criteria | • Include Mitigated Risks  
|                  | • Show All Objects  |

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from Saved Variants and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose Export Results Sets to download the data, Print Version to create a PDF file, or Mitigate Risk to assign mitigation controls to selected objects.

**Report Details** – The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

**More Information**

**9.2.5 Mitigation Control Report**

**Use**

This report lists all mitigating controls with control details and descriptions.
To run the report, designate values for the following filtering criteria:

- **Mitigating Control ID**
- **Short Description**
- **Access Risk ID**
- **Organization ID**

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from **Saved Variants** and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose **Export Results Sets** to download the data or **Print Version** to create a PDF file.

**Report Details** – The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

**More Information**

### 9.2.6 Profile Risk Violation Report

**Use**

This report lists all the risk violations for selected profiles. To run the report, designate values for the following filtering criteria:

- **System**
  
  The report only displays systems that you have authorization to view.
- **Profile**
- **Risk by Process**
- **Access Risk ID**
- **Risk Level**
- **Rule Set**
The report contains the following options:

Table 31:

<table>
<thead>
<tr>
<th>Option</th>
<th>Choices</th>
</tr>
</thead>
</table>
| **Format**   | ● Summary  
               ● Detail  
               ● Management Summary  
               ● Executive Summary |
| **View**     | ● Technical  
               ● Business |
| **Type**     | Access Risk Analysis  
               ● Action Level  
               ● Critical Action  
               ● Critical Role/Profile  
               ● Permission Level  
               ● Critical Permission |
| **Additional Criteria** | ● Include Mitigated Risks  
                   ● Show All Objects |

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from *Saved Variants* and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose *Export Results Sets* to download the data, *Print Version* to create a PDF file, or *Mitigate Risk* to assign mitigation controls to selected objects.

**Report Details** – The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

**More Information**
9.2.7 Role Risk Violation Report

Use

This report lists all the risk violations for selected roles. To run the report, designate values for the following filtering criteria:

- **System**
  The report only displays systems that you have authorization to view.
- **Profile**
- **Risk by Process**
- **Access Risk ID**
- **Risk Level**
- **Rule Set**

The report contains the following options:

Table 32:

<table>
<thead>
<tr>
<th>Option</th>
<th>Choices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>● Summary&lt;br&gt;● Detail&lt;br&gt;● Management Summary&lt;br&gt;● Executive Summary</td>
</tr>
<tr>
<td>View</td>
<td>● Technical&lt;br&gt;● Business</td>
</tr>
<tr>
<td>Type</td>
<td>Access Risk Analysis&lt;br&gt;● Action Level&lt;br&gt;● Critical Action&lt;br&gt;● Critical Role/Profile&lt;br&gt;● Permission Level&lt;br&gt;● Critical Permission</td>
</tr>
<tr>
<td>Additional Criteria</td>
<td>● Include Mitigated Risks&lt;br&gt;● Show All Objects</td>
</tr>
</tbody>
</table>

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from **Saved Variants** and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose **Export Results Sets** to download the data, **Print Version** to create a PDF file, or **Mitigate Risk** to assign mitigation controls to selected objects.

Report Details
The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

More Information

9.2.8 User Risk Violation Report

Use

This report lists all the risk violations for selected users. To run the report, designate values for the following filtering criteria:

- **System**
  The report only displays systems that you have authorization to view.
- **User**
- **User Group**
- **Access Risk ID**
- **Custom Group**
- **Risk Level**
- **Rule Set**

The report contains the following options:

Table 33:

<table>
<thead>
<tr>
<th>Option</th>
<th>Choices</th>
</tr>
</thead>
</table>
| Format | ● Summary  
         | ● Detail  
         | ● Management Summary  
         | ● Executive Summary  |
| View   | ● Remediation  |

**Note**

This option allows you to assign a mitigating control or remove or delimit a role directly from the report.

- Technical
- Business
<table>
<thead>
<tr>
<th>Option</th>
<th>Choices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Access Risk Analysis</td>
</tr>
<tr>
<td></td>
<td>● Action Level</td>
</tr>
<tr>
<td></td>
<td>● Critical Action</td>
</tr>
<tr>
<td></td>
<td>● Critical Role/Profile</td>
</tr>
<tr>
<td></td>
<td>● Permission Level</td>
</tr>
<tr>
<td></td>
<td>● Critical Permission</td>
</tr>
<tr>
<td>Additional Criteria</td>
<td>● Include Mitigated Risks</td>
</tr>
<tr>
<td></td>
<td>● Show All Objects</td>
</tr>
</tbody>
</table>

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from Saved Variants and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose Export Results Sets to download the data, Print Version to create a PDF file, or Mitigate Risk to assign mitigation controls to selected objects.

**Report Details**

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America if that is what you are authorized to see.

**More Information**

### 9.3 Access Request Reports

Access Control provides the following access request reports:

- **Approver Delegation Report [page 228]**
  This report enables you to search for specific delegations filtered by Delegated for Userid and Delegated to Userid among other criteria.
- **Requests by PD/Structural Profiles [page 228]**
  This report allows you to search for requests by specifying PD profiles.
- **Requests by Roles and Role Assignment Approvers Report [page 229]**
  This report lists requests by roles and role approvers.
- **Requests with Conflicts and Mitigations Report [page 230]**
  This report lists requests with mitigated and unmitigated conflicts.
• **Service Level for Requests Report [page 231]**
  This report lists requests by service level.

• **SoD Review History Report [page 232]**
  This report provides the history of actions performed on SoD review tasks including mitigation reaffirm.

• **User Access Review History Report [page 233]**
  This reports provides the history UAR requests and the action that were taken for those requests.

• **User Review Status Report [page 234]**
  This report lists request status for SoD review and user access review requests.

### 9.3.1 Approver Delegation Report

This report enables you to search for configured delegations.

To run the report, you can designate values for the following filtering criteria:

- **Delegated for Userid**
- **Delegated to Userid**
- **Start Date**
- **End Date**
- **Status**

#### Recommendation

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from *Saved Variants* and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose *Export* to download the data.

### 9.3.2 Requests by PD/Structural Profiles

#### Use

This report allows you to search for requests by specifying PD profiles.

To run the report, you can designate values for each of the following filtering criteria:

- **Process Type**
- **Creation Date**
- **Status**
- **System**
  The report only displays systems that you have authorization to view.
- **PD Profile Name**
- **Description**
**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from *Saved Variants* and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose *Export* to download the data.

**Report Details**

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

**Note**

To view access request data in this report, you must be assigned to a role with authorization to view access request objects.

**More Information**

**9.3.3 Requests by Roles and Role Assignment Approvers Report**

**Use**

This report lists requests by roles and role approvers.

To run the report, you can designate values for the following filtering criteria:

- *Process Type*
- *Creation Date*
- *Role Name*
- *Status*
- *Approver*

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from *Saved Variants* and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose *Export* to download the data.
Report Details

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

**Note**

To view access request data in this report, you must be assigned to a role with authorization to view access request objects.

More Information

9.3.4 Requests with Conflicts and Mitigations Report

Use

This report lists requests with mitigated and unmitigated conflicts.

To run the report, designate values for the following filtering criteria:

- Report Name
- System
  - You only see the systems for which you are authorized.
- Process Type
- Request Number
- Creation Date
- Requestor
- Status
- Risk ID
- Approver
- Mitigate Controls

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from Saved Variants and the system automatically inserts your values.

You may run the report in the foreground or the background.

You can choose Export to download the data.

Report Details
The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

**Note**

To view access request data in this report, you must be assigned to a role with authorization to view access request objects.

---

**More Information**

---

**9.3.5 Service Level for Requests Report**

**Use**

This report lists requests by service level.

To run the report, designate values for the following filtering criteria:

- **Process Type**
- Display only requests that exceed service level
- **Service Level Agreement**
- **Request Number**
- **Creation Date**
- **Requestor**
- **Status**
- **Approver**

---

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from Saved Variants and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose Export Result Set to download the data.

**Report Details**

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.
**Note**

To view access request data in this report, you must be assigned to a role with authorization to view access request objects.

---

**More Information**

**9.3.6 SoD Review History Report**

**Use**

This report provides the history of actions performed on SoD review tasks including mitigation reaffirm.

To run the report, designate values for the following filtering criteria:

- Request Number
- Creation Date
- Escalated
- User ID
- Status
- Risk ID
- System
  
  You only see the systems for which you are authorized.

- Reviewer ID
- Coordinator ID
- Action

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from Saved Variants and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose Export to download the data.

**Report Details**

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.
Note
To view access request data in this report, you must be assigned to a role with authorization to view access request objects.

More Information

9.3.7 User Access Review History Report

Use

This report provides the history of UAR requests and the action that were taken for those requests.

To run the report, you can designate values for the following filtering criteria:

- Request Number
- Creation Date
- Escalated
- User ID
- Status
- System
  - The report only displays systems that you have authorization to view.
- Reviewer ID
- Coordinator ID
- Background Job ID
- Action

 Recommendation

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from Saved Variants and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose Export to download the data.

Report Details

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.
Note
To view access request data in this report, you must be assigned to a role with authorization to view access request objects.

More Information

9.3.8 User Review Status Report

Use

This report lists the request status for SoD review and user access review.

To run the report, designate values for the following filtering criteria:

- Process Type
- Request Number
- Creation Date
- Escalated
- User ID
- Status
- Reviewer ID
- Coordinator ID

Recommendation

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from Saved Variants and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose Export Results Sets to download the data.

Report Details

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

Note
To view access request data in this report, you must be assigned to a role with authorization to view access request objects.
9.4 Role Management Reports

Access Control provides the following role management reports:

- **Compare Action in Menu and Authorization Report** [page 235]
  This report compares the actions in the role menu to the authorizations to identify any discrepancies.

- **Compare User Roles Report** [page 236]
  This report compares roles assigned to two user IDs or personnel numbers for SAP systems.

- **List Actions in Roles Report** [page 237]
  This report lists all the actions that are in certain roles.

- **Master to Derived Role Relationship Report** [page 237]
  This report lists the relationship between master and derived roles including the organization level at which the derivation is made.

- **PFCG Change History Report** [page 238]
  This report displays change documents for role administration for a specified system.

- **Role by Date of Generation Report** [page 239]
  This report lists roles by generation date.

- **Single to Composite Role Relationship Report** [page 240]
  This report lists the relationship between single and composite roles.

- **User to Role Relationship Report** [page 241]
  This report lists users and their assigned roles.

- **Role Relationship with User/User Group Report** [page 241]
  This report lists the roles assigned to users and user groups.

9.4.1 Compare Action in Menu and Authorization Report

**Use**

This report compares the actions in the role menu to the authorizations to identify any discrepancies.

To run the report, you can designate values for the following filtering criteria:

- **Application Type**
- **Landscape**
- **Role Name**
- **Role Type**
**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from **Saved Variants** and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose **Export Results Sets** to download the data.

**Report Details**

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

**More Information**

**9.4.2 Compare User Roles Report**

**Use**

This report compares roles assigned to two user IDs or personnel numbers for SAP systems.

To run the report, you must designate values for each of the following filtering criteria:

- **System**
  - The report only displays systems that you have authorization to view.
- **Source Type**
- **Source Value**
- **Target Type**
- **Target Value**

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from **Saved Variants** and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose **Export Results Sets** to download the data.

**Report Details**

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.
9.4.3 List Actions in Roles Report

Use

This report lists all the *Actions* that are in roles.

To run the report, designate values for the following filtering criteria:

- **Application Type**
- **Landscape**
- **Role Name**
- **Role Type**

Recommendation

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from *Saved Variants* and the system automatically inserts your values.

You may run the report in the foreground or the background.

Report Details

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

9.4.4 Master to Derived Role Relationship Report

Use

This report lists the relationship between master and derived roles including the organization level at which the derivation is made. The report is useful when you audit master and derived roles.
Note

The report displays based on the *Master Role* authorization and not on the *Derived Role* authorization.

To run the report, designate values for each of the following filtering criteria:

- **System**
  The report only displays systems that you have authorization to view.
- **Role Name**

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from *Saved Variants* and the system automatically inserts your values.

You may run the report in the foreground or the background.

**Report Details**

You can choose *Export Results Sets* to download the data or *Print Version* to create a PDF file.

**More Information**

9.4.5 PFCG Change History Report

**Use**

This report displays change documents for role administration for a specified system.

To run the report, designate a system or systems for which you have authorization.

Note

The report only displays systems that you have authorization to view. If you are not authorized to any system, PFCG Change history button is disabled.

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from *Saved Variants* and the system automatically inserts your values.
Activities

1. Choose Display PFCG History to start the report.
2. Click Open to launch the SAP GUI.
3. Enter the User Name and Password for the relevant SAP system.
4. Click Log On to launch the PFCG Change History report execution screen in the plug-in system.
5. You may specify the following parameters to run the report:
   ○ Role Name
   ○ Changed By
   ○ From/To Date
   ○ From/To Time
   ○ Document Change Number
6. You may choose among the following options to view different types of change documents:
   ○ Overview
   ○ Create/Delete roles
   ○ Role description
   ○ Single roles in composite roles
   ○ Transactions in role menu
   ○ Other objects in role menu
   ○ Authorization data
   ○ Organizational level
   ○ Authorization profile
   ○ Attributes
   ○ MiniApps
   ○ Composite role home page
   ○ User assignment
   ○ All change documents (technical view)
7. Click Execute to run the report.

Note

This report is based on data from backend systems. System authorization is the only security parameter available.

9.4.6 Role by Date of Generation Report

Use

This report lists roles by generation date.

To run the report, designate values for the following filtering criteria:

- Generated By
- Generation Date
Recommendation

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from `Saved Variants` and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose `Export Results Sets` to download the data.

Report Details

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

More Information

9.4.7 Single to Composite Role Relationship Report

Use

This report lists the relationship between single and composite roles.

Note

The report displays based on the `Composite Role` authorization and not on the `Single Role` authorization.

To run the report, designate values for the following filtering criteria:

- System
  - The report only displays systems that you have authorization to view.
- Role Name

Recommendation

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from `Saved Variants` and the system automatically inserts your values.

You may run the report in the foreground or the background.

Report Details
You can choose *Export Results Sets* to download the data or *Print Version* to create a PDF file.

**More Information**

### 9.4.8 User to Role Relationship Report

**Use**

This report lists users and their assigned roles.

To run the report, designate values for the following filtering criteria:

- **System**
  - The report only displays systems that you have authorization to view.
- **Include Expired Roles**
- **Profile Name**
- **Role Name**

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from *Saved Variants* and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose *Export Results Sets* to download the data.

**More Information**

### 9.4.9 Role Relationship with User/User Group Report

This report lists the roles assigned to users and user groups.

To run the report, designate values for the following filtering criteria:

- **System**
  - The report only displays systems that you have authorization to view.
**User Type**

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from **Saved Variants** and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose **Export Results Sets** to download the data or **Print Version** to create a PDF file.

**Note**

This report is based on data from backend systems. System authorization is the only security parameter available.

### 9.5 Security Reports

Access Control provides the following security reports:

- **Action Usage by User, Role, and Profile Report** [page 242]
  
  This report lists actions by user, role, and profile.

- **Count Authorization for Users Report** [page 243]
  
  This report counts user authorizations and highlights the ones outside the system limits.

- **Count Authorization in Roles Report** [page 244]
  
  This report provides the authorization count for roles by role name.

- **List Expired and Expiring Roles for Users Report** [page 244]
  
  This report lists roles that have expired or are about to expire based on the dates you specify.

### 9.5.1 Action Usage by User, Role, and Profile Report

**Use**

This report lists actions by user, role, and profile.

To run the report, you can designate values for the following filtering criteria:

- **System**
- **Action Usage Date**
- **Action**
- **Action Description**
- **Report By (User, Role, or Profile)**
- **User ID**
- **User Group**
Only displays actions that are not used
Report Type (Actions Defined in Risks or All)
Access Risk ID
Access Risk ID Description

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from Saved Variants and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose Export to download the data.

**Report Details**

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

**More Information**

9.5.2 Count Authorization for Users Report

**Use**

This report counts user authorizations and highlights those outside the system limits.

To run the report, you must designate values for each of the following filtering criteria:

- **System**
- **User**
- **User Group**

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from Saved Variants and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose Export Results Sets to download the data or Print Version to produce a PDF file.

**Report Details**

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.
9.5.3 Count Authorization in Roles Report

Use

This report provides the authorization count for roles by role name.

To run the report, you must designate values for each of the following filtering criteria:

- Application Type
- System
- Role Name
- Role Type

Recommendation

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from Saved Variants and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose Export Results Sets to download the data or Print Version to produce a PDF file.

Report Details

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

9.5.4 List Expired and Expiring Roles for Users Report

This report lists roles that have expired or are about to expire based on the dates you specify.

To run the report, designate values for the following filtering criteria:

- System
  You only see the systems for which you are authorized.
- User ID
Recommendation

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from Saved Variants and the system automatically inserts your values.

You may run the report in the foreground or the background.

You can choose Export Set Results to download the data or Print Version to create a PDF file.

9.6 Audit Reports

Access Control provides the following audit reports:

- **Change Log Report** [page 245]
  This report provides change information on Access Control objects such as role, risk, and profile. The information includes who changed the object, the timestamp, new and old values, the entity name and type, attributes, and the type of change.

- **Embedded Action Calls in Programs of SAP Systems Report** [page 246]
  This report identifies embedded transaction calls in custom programs.

- **List Actions in Roles But Not in Rules Report** [page 247]
  This report lists all the actions that are in roles but are not part of the rule library.

- **List Permissions in Roles But Not in Rules Report** [page 248]
  This report lists all the permissions that are in roles but are not part of the rule library.

9.6.1 Change Log Report

Use

This report provides change information on Access Control objects such as role, risk, and profile. The information includes who changed the object, the timestamp, new and old values, the entity name and type, attributes, and the type of change.

To run the report, designate values for the following filtering criteria:

- **Changed On**
- **Critical Profile**
- **Critical Role**
- **Owner**
- **Controller**
Firefighter Role
FF Owner
Reason Code
Firefighter
Function
Organization Rule
Risk
Role
Rule Set
Supplementary Rule
User ID

Click Search to run the report in the foreground. Click Clear to clear the search value field.

You can choose Export to download the data or Print Version to create a PDF file.

Note
To save the results of your search for later retrieval, enter a name beside Save Search As, then click Save. Use the Load button to retrieve the saved search and the Delete button to delete the saved search.

Caution
This report only supports report-level security. That is, if you have authorization to view this report, you can view all the possible fields with no restrictions.

More Information

9.6.2 Embedded Action Calls in Programs of SAP Systems Report

Use

This report identifies embedded transaction calls in custom programs.

To run the report, designate values for each of the following filtering criteria:

- Action
- System
- Program
**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from *Saved Variants* and the system automatically inserts your values.

You may run the report in the foreground or the background.

**Report Details**

You can choose *Export Results Sets* to download the data or *Print Version* to create a PDF file.

**Report Details**

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

**More Information**

**9.6.3 List Actions in Roles But Not in Rules Report**

**Use**

This report lists all the actions that are in roles but are not part of the rule library.

To run the report, designate values for the following filtering criteria:

- *System*
- *Profile*
- *Role*

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from *Saved Variants* and the system automatically inserts your values.

You may run the report in the foreground or the background.

You can choose *Export Results Sets* to download the entire data set, *Export* to download the results on the screen, or *Print Version* to create a PDF file. You can also mark individual items as having been analyzed.

**Report Details**

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.
More Information

9.6.4 List Permissions in Roles But Not in Rules Report

Use

This report lists all the permissions that are in roles but are not part of the rule library. To run the report, designate values for the following filtering criteria:

- **System**
- **Profile**
- **Role**

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from **Saved Variants** and the system automatically inserts your values.

You may run the report in the foreground or the background.

You can choose **Export Results Sets** to download the entire data set, **Export** to download the results on the screen, or **Print Version** to create a PDF file. You can also mark individual items as having been analyzed.

**Report Details**

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

More Information

9.7 Emergency Access Management Reports

Access Control provides the following reports for emergency access management:

- **Consolidated Log Report [page 249]** – This report captures data from the selected system connector for Firefighters. The report provides information based on the following logs from the remote systems: Transaction Log, Change Log, System Log, Security Audit Log, OS Command Log. This is the most
commonly-used report. You can configure your system to receive this report either through e-mail or the workflow.

You must be authorized to view the following reports by an Administrator. If, after looking at the Consolidated Log Report, you have a need to do further investigation, access these reports:

- **Invalid Emergency Access Report [page 251]** – This report allows you to specify the user types for emergency access that are expired, deleted, or locked, such as Firefighters IDs, Controllers, or Owners.
- **Firefighter Log Summary Report [page 250]** – This report captures transaction data from the selected system connector for Firefighter IDs.
- **Reason Code and Activity Report [page 252]** – This report displays data from the selected system connector for each Firefighter ID. The report lists the reason and activity for each login event.
- **Transaction Log and Session Details Report [page 253]** – This report captures transaction data from the selected system connector for Firefighter IDs and Firefighters. It displays the number and type of transactions accessed for each Firefighter ID and each Firefighter.
- **SoD Conflict Report for Firefighter IDs [page 252]** – This report provides the history of actions performed on Segregation of Duties (SoD) review tasks including mitigation reaffirm.

### 9.7.1 Consolidated Log Report

**Use**

This report captures data from the selected system connector for Firefighter IDs. The report provides information based on the following logs from the remote systems:

<table>
<thead>
<tr>
<th>Log</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction Log</td>
<td>Captures transaction executions from transaction STAD.</td>
</tr>
<tr>
<td>Document Objects Change Log</td>
<td>Captures change log of change document objects from tables CDPOS and CDHDR.</td>
</tr>
<tr>
<td>Table Data Change Log</td>
<td>Captures change logs when table changes are performed using transactions SE16/SE16N/SE17/SM30/SM31 and so forth.</td>
</tr>
<tr>
<td>System Log</td>
<td>Captures Debug &amp; Replace information from transaction SM21.</td>
</tr>
<tr>
<td>Security Audit Log</td>
<td>Captures Security Audit Log from transaction SM20.</td>
</tr>
<tr>
<td>OS Command Log</td>
<td>Captures changes to OS commands from transaction SM49.</td>
</tr>
</tbody>
</table>

To run the report, designate values for the following filtering criteria:

- **Report Name**
- **System**
  You only see the systems for which you are authorized.
Recommendation

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from Saved Variants and the system automatically inserts your values.

You may run the report in the foreground or the background.

You can choose Export to download the data or Print Version to create a PDF file.

Report Details

The application displays objects that you are authorized to see. For example, if you are only authorized to see North America, on the report results you will only see data related to North America.

More Information

9.7.2 Firefighter Log Summary Report

Use

This report captures transaction data from the selected system connector for Firefighter IDs.

To run the report, designate values for the following filtering criteria:

- System
  - You only see the systems for which you are authorized.
- Firefighter
- Owner
- Firefighter ID
- Date
- Result set Size

Recommendation

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from Saved Variants and the system automatically inserts your values.
You may run the report in the foreground or the background.
You can choose Export to download the data or Print Version to create a PDF file.

**Report Details**

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

**More Information**

**9.7.3 Invalid Emergency Access Report**

**Use**

This report allows you to specify the user types (Firefighter IDs, Controllers, or Owners) that are expired, deleted, or locked.

To run the report, designate values for the following filtering criteria:

- **System**
  You only see the systems for which you are authorized.
- **Firefighter**
- **Owner**
- **Firefighter ID**
- **Controller**
- **Result Set Size**

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from Saved Variants and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose Export to download the data or Print Version to create a PDF file.

**Report Details** – The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

**More Information**
9.7.4 Reason Code and Activity Report

Use

This report displays data from the selected system connector for each Firefighter ID. The report lists the reason and activity for each login event.

To run the report, designate values for the following filtering criteria:

- **System**
  - You only see the systems for which you are authorized.
- **Firefighter**
- **Owner**
- **Firefighter ID**
- **Date**
- **Result Set Size**

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from **Saved Variants** and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose **Export** to download the data or **Print Version** to create a PDF file.

**Report Details** – The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

More Information

9.7.5 SoD Conflict Report for Firefighter IDs

Use

This report provides the history of actions performed on SoD review tasks including mitigation reaffirm.

To run the report, designate values for the following filtering criteria:

- **System**
- **Firefighter ID**
- **Owner**
Report Options – The following options are available for this report:

- **Format**
  - Summary
  - Detail
  - Management Summary
  - Executive Summary
  - Technical View/Business View

- **Access Risk Analysis Type**
  - Action / Permission Level
  - Critical Action / Permission
  - Critical Role/Profile

- **Additional Criteria**
  - Show All Objects
  - Executed Transactions Only

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from Saved Variants and the system automatically inserts your values.

You may run the report in the foreground or the background. You can choose Export Set Results to download the data or Print Version to create a PDF file.

**Report Details** – The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

**More Information**

**9.7.6 Transaction Log and Session Details Report**

**Use**

This report captures transaction data from the selected system connector for Firefighter IDs and Firefighters. It displays the number and type of transactions accessed for each Firefighter ID and for each Firefighter.
To run the report, designate values for the following filtering criteria:

- **System**
  You only see the systems for which you are authorized.
- **Firefighter**
- **Firefighter ID**
- **Transaction**
- **Reason Code**
- **Date**
- **Result Set Size**

**Recommendation**

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from *Saved Variants* and the system automatically inserts your values.

You may run the report in the foreground or the background.

You can choose *Export* to download the data or *Print Version* to create a PDF file.

**Report Details**

The application displays only objects that you are authorized to see. For example, on the report results you may only see the data related to North America, if you are only authorized to see North America.

**More Information**

[Reports and Analytics](#) [page 28]

### 9.8 Risk Terminator Log Report

This report provides information on role changes that are directly updated in backend systems.

To run the report, designate values for the following filtering criteria:

- **System**
- **Role/User**
- **Generated By**
- **Generation Date**
- **Generation Time**
- **Reason**
Recommendation

If you frequently run the same report using the same filtering values, define a variant and save it. The next time you want to run that set of values, retrieve the variant from Saved Variants and the system automatically inserts your values.

You may run the report in the foreground or the background.

You can choose Export to download the data or Print Version to create a PDF file.
Important Disclaimers and Legal Information

Coding Samples

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 to 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, unless damages were caused by SAP intentionally or by SAP’s gross negligence.

Accessibility

The information contained in the SAP documentation represents SAP’s current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of willful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with “you”, or a gender-neutral noun (such as “sales person” or “working days”) is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP’s gross negligence or willful misconduct. All links are categorized for transparency (see: http://help.sap.com/disclaimer).