

IBM Security Identity Governance and Intelligence
Version 5.2.1

*Administration Topics
for Managers and Employees*



IBM Security Identity Governance and Intelligence
Version 5.2.1

*Administration Topics
for Managers and Employees*



Table of contents

Table list	v	Delegation: processing a request	126
Part 1. Managers	1	Delegation: executing a request	133
Chapter 1. Service Center	3	Authorize escalation	139
Chapter 2. Password management	5	Insert/Update entitlement: generating a request	142
Resetting my forgotten password	5	Insert/Update entitlement: processing a request	155
Resetting account passwords for other users	6	Insert/Updates entitlements: executing a request	163
Chapter 4. Introduction to Access Certifier	11	List of all requests present in the system	168
Campaign Management	11	User access: generating a request	175
Summary of available campaigns	11	User access: processing a request	185
Details - OU Entitlement Review	13	User access: executing a request	193
Details - Entitlement/User	17	Create/Update user: generating a request	198
Details - User Remediation Review	28	Insert/Update user: processing a request	200
Details - Entitlement Review	33	Insert/Update user: executing a request	208
Details - Account Review	38	Chapter 7. Introduction to Business Activity Mapping	209
Details for Supervisor - OU Entitlement	41	Dashboard	209
Details for Supervisor - User Entitlement	46	Permission Perspective	210
Details for Supervisor - User Remediation	50	Activity Perspective	211
Details for Supervisor - Entitlement	55	Chapter 8. Introduction to Report Client	213
Details for Supervisor - Accounts	59	Report	213
Chapter 5. Introduction to User-account matching	65	Request	213
Dashboard	65	Download	214
Chapter 6. Introduction to Access Requests	69	Passphrase	215
ARM Requests Status	70	Part 2. Employees	217
AR functions	71	Chapter 9. Logging in to the Service Center	219
Generating a request to make account changes: selecting the user	72	Chapter 10. Resetting my forgotten password	221
Generating a request to make account changes: answering security questions	73	Chapter 11. Changing my account password	223
Generating a request to make account changes: selecting the accounts	74	Chapter 12. Viewing my requests in the Self Care application	225
Generating a request to make account changes: entering the new password	75	Chapter 13. Updating my security questions	227
Authorizing an account change request	76	Part 3. Appendixes	235
Executing a request of Account change	83	Appendix. Accessibility features for IBM Security Identity Governance and Intelligence	237
Admin Roles: generating a request	88	Index	239
Admin Roles: processing a request	95		
Admin Roles: executing a request	102		
Admin delegation: generating a request	108		
Admin delegation: processing a request	108		
Admin delegation: executing a request	108		
Admin Roles: Catalog	109		
Admin Roles: Shopping Cart	112		
My daily work: list of requests	114		
Delegation: generating a request	120		

Table list

1. Dashboard items controls	4	56. User filters	72
2. Password management tasks	5	57. Users list.	72
3. Summary Attributes.	12	58. User Information tabs	73
4. Details tab note	13	59. Request Status	77
5. Entitlement View details filters.	13	60. Filters	78
6. Campaign Info window	14	61. User Details - Details tab	78
7. Details tab buttons and icons.	15	62. Request Actors	79
8. Details tab note	18	63. User Details - Details tab	80
9. Entitlement View details filters.	18	64. User Details - Entitlements tab	80
10. Campaign Info window	19	65. User Details - Accounts tab	80
11. Details tab buttons and icons.	20	66. User Details - Activities tab	80
12. Columns for Entitlement View	21	67. User Details - Rights	81
13. User Assignments details	22	68. Request attributes	81
14. Note about the entity row of a campaign	22	69. Entitlement info - Structure	81
15. User/Entitlement information	23	70. Request Status	83
16. Filters	24	71. Filters	84
17. Note about UME.	24	72. Request attributes	84
18. Campaign Info window	24	73. User Details - Details tab	84
19. Details tab note	25	74. Request Actors	85
20. Details tab buttons and icons.	25	75. User Details - Details tab	85
21. Note about campaigns	26	76. User Details - Entitlements tab	86
22. Configurable columns for the details of the campaign	26	77. User Details - Accounts tab	86
23. Entitlement View details filters.	28	78. User Details - Activities tab	86
24. Campaign Info window	29	79. User Details - Rights	86
25. Details tab buttons and icons.	30	80. Request attributes	87
26. Risk Violation Mitigation Details	32	81. Entitlement info - Structure	87
27. Note about campaigns	32	82. User filters.	88
28. User/Risk information	33	83. Users list.	88
29. Entitlement View details filters.	33	84. User Details - Details tab	88
30. Note about the UME check box	34	85. User Details - Entitlements tab	89
31. Campaign Info window	34	86. User Details - Accounts tab	89
32. Details tab buttons and icons.	35	87. User Details - Rights	89
33. Entitlement details	36	88. User Details - Activities tab	89
34. Note about campaigns	37	89. Entitlement info - Structure	90
35. User/Entitlement information	37	90. Request Status	96
36. Details Filters	38	91. Filters	98
37. Note about the UME check box	38	92. User Details - Details tab	98
38. Campaign Info window	39	93. Request Actors	99
39. Details tab buttons and icons.	39	94. User Details - Details tab	99
40. Account details	40	95. User Details - Entitlements tab	100
41. Note about campaigns	41	96. User Details - Accounts tab	100
42. User information.	41	97. User Details - Activities tab	100
43. Cert_Campaign_Reviewer_Tab	43	98. User Details - Rights	100
44. Cert_Campaign_Scheduling_Tab	44	99. Request attributes	101
45. Cert_Campaign_Reviewer_Tab	47	100. Entitlement info - Structure	101
46. Cert_Campaign_Scheduling_Tab	48	101. Request Status	103
47. Cert_Campaign_Reviewer_Tab	52	102. Filters	103
48. Cert_Campaign_Scheduling_Tab	52	103. User Details - Details tab.	104
49. Cert_Campaign_Reviewer_Tab	56	104. Request Actors	104
50. Cert_Campaign_Scheduling_Tab	57	105. User Details - Details tab.	105
51. Cert_Campaign_Reviewer_Tab	60	106. User Details - Entitlements tab	105
52. Cert_Campaign_Scheduling_Tab	61	107. User Details - Accounts tab	106
53. User filters.	65	108. User Details - Activities tab	106
54. User/Account attributes	66	109. User Details - Rights	106
55. Request Status	70	110. Request attributes	106
		111. Entitlement info - Structure	107

112.	Request Status	115	173.	User Details - Entitlements tab	160
113.	Filters	116	174.	User Details - Accounts tab	160
114.	User Details - Details tab	116	175.	User Details - Activities tab	160
115.	Request Actors	117	176.	User Details - Rights	161
116.	User Details - Details tab	118	177.	Request attributes	161
117.	User Details - Entitlements tab	118	178.	Entitlement info - Structure	161
118.	User Details - Accounts tab	118	179.	Request Status	163
119.	User Details - Activities tab	118	180.	Filters	163
120.	User Details - Rights	119	181.	User Details - Details tab	164
121.	Request attributes	119	182.	Request Actors	165
122.	Entitlement info - Structure	119	183.	User Details - Details tab	165
123.	User filters	121	184.	User Details - Entitlements tab	166
124.	Users list	121	185.	User Details - Accounts tab	166
125.	User Details - Details tab	121	186.	User Details - Activities tab	166
126.	User Details - Entitlements tab	122	187.	User Details - Rights	166
127.	User Details - Accounts tab	122	188.	Request attributes	167
128.	User Details - Rights	122	189.	Entitlement info - Structure	167
129.	User Details - Activities tab	122	190.	Request Status	169
130.	Entitlement info - Structure	123	191.	Filters	171
131.	Request Status	127	192.	User Details - Details tab	171
132.	Filters	129	193.	Request Actors	172
133.	User Details - Details tab	129	194.	User Details - Details tab	172
134.	Request Actors	130	195.	User Details - Entitlements tab	173
135.	User Details - Details tab	130	196.	User Details - Accounts tab	173
136.	User Details - Entitlements tab	131	197.	User Details - Activities tab	173
137.	User Details - Accounts tab	131	198.	User Details - Rights	173
138.	User Details - Activities tab	131	199.	Entitlement info - Structure	174
139.	User Details - Rights	131	200.	Request attributes	175
140.	Request attributes	132	201.	User filters	175
141.	Entitlement info - Structure	132	202.	Users list	176
142.	Request Status	134	203.	User Details - Details tab	176
143.	Filters	134	204.	User Details - Entitlements tab	176
144.	User Details - Details tab	135	205.	User Details - Entitlements tab (2)	177
145.	Request Actors	135	206.	User Details - Accounts tab	177
146.	User Details - Details tab	136	207.	User Details - Rights	177
147.	User Details - Entitlements tab	136	208.	User Details - Activities tab	177
148.	User Details - Accounts tab	137	209.	Entitlement info - Structure	177
149.	User Details - Activities tab	137	210.	User data	179
150.	User Details - Rights	137	211.	Filters for Current Entitlements	180
151.	Request attributes	137	212.	Business role filters	180
152.	Entitlement info - Structure	138	213.	Application role filters	182
153.	Filters	139	214.	Permission filters	182
154.	User Details - Details tab	140	215.	External roles filters	183
155.	Request attributes	142	216.	Rights property	184
156.	Analysis filters	143	217.	Buttons and Icons	185
157.	User filters	144	218.	Request Status	186
158.	User details	145	219.	Filters	188
159.	Entitlement details	147	220.	User Details - Details tab	188
160.	Entitlement filters	148	221.	Request Actors	189
161.	Entitlement details	148	222.	User Details - Details tab	190
162.	Candidate Role attributes	149	223.	User Details - Entitlements tab	190
163.	User attributes	151	224.	User Details - Accounts tab	190
164.	Candidate Role attributes	151	225.	User Details - Activities tab	190
165.	OU attributes	152	226.	User Details - Rights	191
166.	Dashboard set	153	227.	Request attributes	191
167.	Role statistics filters	154	228.	Entitlement info - Structure	191
168.	Request Status	156	229.	Request Status	193
169.	Filters	158	230.	Filters	193
170.	User Details - Details tab	158	231.	User Details - Details tab	194
171.	Request Actors	159	232.	Request Actors	195
172.	User Details - Details tab	160	233.	User Details - Details tab	195

234. User Details - Entitlements tab	196	244. User Details - Details tab.	205
235. User Details - Accounts tab	196	245. User Details - Entitlements tab	205
236. User Details - Activities tab	196	246. User Details - Accounts tab	205
237. User Details - Rights	196	247. User Details - Activities tab	205
238. Request attributes	197	248. User Details - Rights	206
239. Entitlement info - Structure	197	249. Request attributes	206
240. Request Status	201	250. Entitlement info - Structure	206
241. Filters	203	251. Change My Password.	229
242. User Details - Details tab.	203	252. View Self Care Requests	231
243. Request Actors	204		

Part 1. Managers

Managers are defined in the *Regular Users schema* and can perform tasks in the Service Center. Examples of managers are application managers, user managers, department managers, role managers, and risk managers.

For more information about the tasks that user managers can do, see *Personas and use cases*.

Chapter 1. Service Center

Service Center shows a dashboard and provides access to Identity Governance and Intelligence applications according to roles assigned to you.

Logging in to the Service Center


To log in to Service Center, enter a valid user name and password in the Login window and click **Login**.

Home - Dashboard

When you log in, you see your **Dashboard** home page. It is a dashboard populated with instruments (dashboard items) that report on various aspects of your roles in the system. A dashboard item is configured to be one of the following types:

- Single value, a number with a title.
- Table, with information arranged in rows and columns.
- Graphic chart, one of pie, line, bar, area, or heat map,

Application menu and top bar

To see the application menu, click the application menu icon . The application menu is available from any application or pane in the system. Your menu choices can be constrained by your role in the system. Some choices that are shown in the following list might not be available to your role.






- **Home** - Your home **Dashboard**
- **Access Certifier** - See Chapter 4, "Introduction to Access Certifier," on page 11.
- **Access Requests** - See Chapter 6, "Introduction to Access Requests," on page 69.
- **Reports** - See Chapter 8, "Introduction to Report Client," on page 213.
- **User-Account Matching** - See Chapter 5, "Introduction to User-account matching," on page 65.
- **Business Activity Mapping** - See Chapter 7, "Introduction to Business Activity Mapping," on page 209.
- **Logout** - Logs you out of the system
- **Act as delegate for...** - Click to select a user. You must be configured as a delegate for that user.
- **Terms of Use** - Displays the terms of use for the system.
- **Current Realm: (Realm)** - Read only. The realm that you are working in
- **Last login: (Month) (day), (year) (timestamp)** - Read only. The date and time you last logged in

The top bar also shows the following items:

- Identity Governance and Intelligence
- **(Realm)/(User)** - The realm and login name you are using
- **Help** - Help in the IBM Knowledge Center for your current location in the system.

Dashboard item controls

Table 1. Dashboard items controls

Icon	Label	Description
	Maximize	Click to enlarge the dashboard item. Click again to return to normal size.
	Refresh	Click to refresh the dashboard item. If the underlying data changed, the refresh shows the changes.
	Settings	Click and choose Configure to configure the following settings: <ul style="list-style-type: none"> • Chart Type - Click to choose a chart type from the menu. The chart types available depend on the query for the dashboard item and the configuration of the dashboard item. • Legend - Click to display a dialog for choosing the position of the legend.
	Filter	Click and enter filter criteria in the dialog. Filter fields depend on the dashboard item configuration.
	None. Columns table control	Show or hide columns. Appears only for tables, in the upper right of the table dashboard item. Click to choose which columns to hide or show. The columns available depend on the dashboard item configuration.
Drill down	None. Cursor changes from arrow to select when you move it over an item where you can drill down.	Click to access to additional information that is typically in another application. Depending on the configuration of the dashboard item, you might drill down on the following items: <ul style="list-style-type: none"> • Single-value dashboard item • Graphic chart part - a pie slice, bar section, or line. • Table row
No data available		Read-only message that appears instead of a table or graphic chart if no data returns from the query.

Chapter 2. Password management

Managers and help desk personnel can manage passwords in the Service Center for yourself or for others, depending on how the system is configured.

Password management tasks

You can use the Self Care application to change your own password or reset your password. You can use the Access Request application to change or reset the password for other users.

Use the Service Center to do these tasks:

Table 2. Password management tasks

Task	Refer to
Reset your own password if you have forgotten it.	"Resetting my forgotten password"
Change or reset the account password of other users.	"Resetting account passwords for other users" on page 6

For information about password-related tasks that administrators can do in the Administration Console, see Password administration.

Resetting my forgotten password

If you forgot your Service Center password, you can either specify a new password or have the system generate a new password.

Before you begin

Your security questions must already be set up.

About this task

When you forget your password, you must answer the security questions correctly to reset your password. The new password replaces the old password for your Service Center account. Depending on how your system is configured, you can either specify a new password or use a system-generated password. The new password is sent to the email address that is specified in your personal profile.

If no email address is defined in your personal profile, the system-generated password cannot be sent. Contact the help desk or administrator to add an email address to your profile.

Procedure

1. From the Service Center Login page, type your user ID, and then click **Forgot your password?**
2. On the Forgot Your Password page, answer the security questions, and then click **Continue**. The following scenarios are possible, depending on how a system administrator configured the system:

Option	Description
The questions are answered correctly, and your system is configured for you to specify a new password.	Type your new password in the New Password field, and then type your new password again in the Confirm Password field. Then, click Change Password . When you see a message that indicates a successful password change, click OK .
The questions are answered correctly, and your system is configured to generate a new password and send the password to a predefined email address.	A new system-generated password is automatically sent to the email that is defined in your personal profile. You must use this new password on your next login, and then you can change your password on your next login. Click Return to Login .
The questions are answered correctly, and your system is configured to generate a new password and prompts you to type an email address.	Type the email address where you want the new system-generated password to be sent. You must use this new password on your next login, and then you must change your password on your next login. Click Continue . When you see a message that indicates a successful operation, click Return to Login .
The questions are answered correctly, and your system is configured to generate a new password. However, an email address is not defined in your personal profile.	Contact the help desk or administrator to add your email address to your personal profile. Click Return to Login . After the email address is added to your profile, you can follow the Forgot your password? link again from the Service Center Login page to receive the system-generated password in your email address.
The questions are not answered correctly, and an error message is displayed. Depending on how your system is configured, you might have more attempts to correctly answer the questions.	You cannot access the system unless you remember your password or answer the questions correctly. If you exceed the maximum number of attempts to verify your identity, your Service Center account is locked. Contact your help desk or administrator to unlock your Service Center account or reset your Service Center password.

Related reference:

Chapter 3, “Forgot Your Password,” on page 9

If you forgot your Service Center password, you can reset it.

Resetting account passwords for other users

If you are a manager, or someone entitled with a role that includes this activity, you can change the account passwords for users in the Service Center.

Before you begin

You must be entitled with a role (for example, User Manager, Application Manager, or other) that has the permission to reset the account passwords of other users.

About this task

Depending on how a system administrator configured the system, you can change or reset the passwords of other users in the Access Requests application of Service Center.

Procedure

1. Log in to the Service Center.
2. On the Service Center home page, select **Access Requests**. The Access Requests page is displayed.
3. Select the role that is entitled to reset passwords for others, such as **User Manager** or **Application Manager**.
4. Select the tab that is associated with the password reset task, such as **ManagerPasswordResetGEN** or **HelpDeskPasswordResetGEN**. The first page of a wizard displays the list of users whose password you are entitled to reset. The wizard leads you through the completion of your task.
5. Select a user in the list and click **Next**. Depending on the process that is defined for your role, the next window displays the security questions that verify the identity of the user or the names of the accounts for which the password you are about to reset grants access.
6. If the Security Questions window is displayed, enter the answers to the security questions with the help of the user. The answers must match the answers that were first entered by the user on the first login. The **Identified by other means** check might be available. You can skip the security questions and select this box as an alternative. Click **Next** to proceed to the Accounts window.
7. The Accounts window lists all the accounts that the user is entitled to access. The Ideas account is associated with the Service Center. Select the accounts and click **Next** to proceed to the Account Password Management window where you enter the password or generate the password.
8. The items featured in this window depend on the setup that was done by the administrator. Complete the following items when they are available:
 - a. In the **Applicant** box, enter your own password.
 - b. In the **Beneficiary** box, either type the new password or select **Generate** to have the password created automatically.

If the **Generate** button is available, select it to create the password automatically.

If there is no **Generate** button, type the new password in the **New password** field and the **Confirm password** field. A **Show password characters** check box might be displayed. Select it to see the characters you type. As you type, a list of password requirements on the right shows if you are complying with standards.
 - c. The **New password will be sent to this email address** field displays the email address of the user. Based on the configuration, you might be able to edit it. If the field is not displayed, you must communicate the new password to the user by other means.
9. Click **Submit** to complete the request.

Results

The password is created and emailed to the beneficiary. The request is marked as completed. Depending on the configuration of the process, the request might be

listed with other requests in a report or in another tab available to an Operator or similar role.

Chapter 3. Forgot Your Password

If you forgot your Service Center password, you can reset it.

When you forget your password, you must answer the security questions correctly and change your password. The new password replaces the old password for your Service Center account.

You can reset your password only if you previously set up security questions for the Service Center.

Depending on how a system administrator configured the system, these scenarios are possible:

- You can change your password immediately.
- The system generates a new password and sends it to your email address that is specified in your personal profile.
- The system generates a new password and prompts you to enter an email address to send it to.

If no email address is defined in your personal profile, the new system-generated password cannot be sent. Contact the help desk or administrator to add an email address to your profile.

You cannot access the system unless you remember your password or answer the questions correctly. If you exceed the maximum number of attempts to verify your identity, your Service Center account is locked. Contact your help desk or administrator to unlock your Service Center account or reset your Service Center password.

Related tasks:

“Resetting my forgotten password” on page 5

If you forgot your Service Center password, you can either specify a new password or have the system generate new password.

Chapter 4. Introduction to Access Certifier

The Access Certifier (AC) is the module dedicated to implementing certification for an organization.

The Access Certifier module provides a complete and flexible workflow for certifying permissions that are aggregated to a user through a specific role, according to the RBAC standard and segregation of duty policies that are enforced by the IBM® Security Identity Governance and Intelligence platform.

For example, adding a set of permissions (entitlements) to a role structure might require certification. Mixing old and new entitlements can originate new permissions to be reviewed by an administrator.

Consider the example of fusing two different organization units (OUs) to form a new one: this new situation requires the review of roles that are already aggregated to the old OUs.

The Access Certifier module assists administrators during the role certification workflow by assigning different scopes and responsibilities to several specific certification functions.

User - Assignment Reviewer

To monitor permissions that are joined to a user.

OU - Entitlement Reviewer

To monitor entitlement joined to the OUs.

Entitlement Reviewer

To monitor the structure of a generic entitlement.

Risk Reviewer

To monitor mitigation controls that are joined to the users risks.

Supervisors

To monitor the activities of the reviewers.



Note: The Access Governance Core administrator defines the campaign contents.

Access Certifier users can approve or revoke these contents.

Campaign Management












The following functions for managing the main entities of this module are available:

Summary of available campaigns

In the **Summary** tab, you can view the list of available campaigns.

The following table lists the **Summary** attributes:

Table 3. Summary Attributes


Attribute	Description
Type	<p>Types of campaigns for common reviewers:</p> <ul style="list-style-type: none"> •  User •  OU •  Risk •  Entitlements •  Accounts <p>When a supervisor approves:</p> <ul style="list-style-type: none"> •  User •  OU •  Risk •  Entitlements •  Accounts
Campaign Name	Name of the campaign.
End Date	End date of the campaign.
Status	Status of the campaign.  Stopped shows closed campaigns. If this icon is not present, campaigns are open.
Supervisor	Name of the supervisor of the campaign.
Requested by	Name of the applicant of the campaign.
% Completion	Percentage of the entities that are certified.

The **Details** tab is activated only after the campaign is selected.

- User - Assignment (Reviewer) 
- OU - Entitlement (Reviewer) 
- Risk Violation Mitigation (Reviewer) 
- Entitlements (Reviewer) 
- Account (Reviewer) 
- User - Assignment (Supervisor) 
- OU - Entitlement (Supervisor) 

- Risk Violation Mitigation (Supervisor) 
- Entitlements (Supervisor) 
- Account (Supervisor) 

Table 4. Details tab note

	Note: The Access Governance Core administrator defines the campaign contents and settings. Access Certifier reviewers can have different sets of functional buttons, icons, or tabs available, depending on the configuration of the campaign.
---	---

Details - OU Entitlement Review

After you select the campaign, the **Details** tab shows the list of the entities to be certified.

To search a specific entity, set the filters that are shown in the following table by clicking **Filter/Hide Filter**:

Table 5. Entitlement View details filters.


Context	Filter	Description
User	Org Unit	Click  OU to enter an organizational unit (OU).
	Identity	This field can host the name, the surname, or the User ID of the user.
	Hierarchy	If this check box is selected, the search activity applies to all the hierarchy, starting from the root OU that is indicated in the Org Unit field.
	Only Users with Violations	If this check box is selected, the search activity applies only to users with outstanding violations.
	UME	UME is a digital identity (user) that can have more than one account on the same target system. If this check box is selected, the search activity applies to all the UME involved in the campaign.

Table 5. Entitlement View details filters. (continued)

Context	Filter	Description
Entitlement	Application	Name of the application.
	Search Entitlement (Name or Code)	Name or code of the entitlement.
	User Hierarchy	The user's hierarchy within the organization or group.
	Status	Indicates the status of the certification. <ul style="list-style-type: none"> • Complete • Pending
	Type	Indicate the entitlement type. <ul style="list-style-type: none"> • Permission • IT Role • Business Role • External Role
	Only with Visibility Violations	If this check box is selected, the search activity applies to the entitlements in role alignment violation. That is, entitlements are assigned to a user, but they do not belong to the OU of the user.
	Reviewed	Was the user reviewed? <ul style="list-style-type: none"> • Formerly indicates that the user was reviewed at least one time. • Never indicates that the user was not reviewed.
	Owner	Indicates the owner of the certification activity. <ul style="list-style-type: none"> • Assigned to me • Redirected by me • Redirected to me • Returned

When you click the link **Campaign: Campaign Name** in the upper right part of the page, the Campaign Info window displays the information in the following table:

Table 6. Campaign Info window

Field	Description
Campaign Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Name of the supervisor.
Campaign Type	Type of the campaign.
Allow Redirection	If this check box is selected, the reviewer can redirect to other reviewer entities to be approved or revoked.
Escalation to Supervisor	If this check box is selected, the reviewer can redirect to the supervisor entities to be approved or revoked.
Notes Revocation (Mandatory)	If this check box is selected, inserting a note is mandatory for an entity revocation.

Table 6. Campaign Info window (continued)

Field	Description
Sign Off	The method in which the approval or revocation is validated: Automatic The approval or revocation is immediately signed off. Completed By User The user decides when to sign off on the approval or revocation. End Campaign The approval or revocation is signed off at the end of the campaign.
Start/End Date	Start/end date of the campaign, according to the format established by the administrator.

Depending on the type of the campaign that is selected, the **Details** tab structure can show:

- Different set of attributes
- Different set of icons and buttons

The following table shows the entire superset of buttons and icons of the **Details** tab:

Table 7. Details tab buttons and icons


















Button/Icon	Description
 Inspect	Inspect the entities of the campaign.
 Entity info	Provides information about the entity in the campaign, such as user, OU, entitlement, and risk.
 History	In the Note History window, History displays the information about the previous campaigns in which the entity was involved. When you select a listed item, Note opens automatically, displaying the note for the selected item.
Approve/Revoke	Approve/revoke associations between entities.
 Note	Click to insert a note about the entity.
 Note OK	Click to read a note that was previously inserted through.  .
 Forward	Redirect to another reviewer to be approved or revoked.
 Escalation	Escalate to the supervisor to be approved or revoked.
 Return	Return to the reviewer to be approved or revoked.
 Received	Received directly by another reviewer.
 Received after check	Received by the reviewer after the cycle (return action) was checked.
 Supervisors	This icon indicates that different supervisors are configured for the selected certification. Click this icon to see the entire list of supervisors.
 Sign off	The certifier can decide when to sign off on the approval or revocation.


Table 7. Details tab buttons and icons (continued)

Button/Icon	Description
 Show UME	Identifies the master UME, and you can group UME.
 Stats	Allows the supervisor to monitor by two types of pie charts, the status of the campaign completion.
	Click the colored dot to open a window that displays the following activities: <ul style="list-style-type: none"> The risk activities tree (related to a specific user) into the Risk Info tab The activities that are involved in a specific risk into the Risk Activity tab
Certifying: <i>EntityName</i>	Click Certifying: <i>EntityName</i> in the upper-right part of the page to display information about the entity.
Approve Revoke Redirect Escalate Sign-off	In the upper-right side of the page, which is aligned with Filter/Hide Filter and depending on the previous selection, up to four bulk operations are available. Activate these operations by selecting the check boxes that are associated with each item. You can select all items by clicking the check box on the left side of the upper blue bar.

The following table includes the details of this campaign:

Entitlement/OU Visibility Details		
Type of Campaign	Detail	Description
Entitlement/OU Visibility	Action	Allows the inspection of the entities of the campaign.
	Code	Univocal identifier of the OU.
	Name	Name of the OU.
	% Entity Completion	Percentage of the entities that are certified.

	Note: If an entity row of the campaign is displayed without Approve/Revoke , the entity is no longer available for the reviewer. It can be unavailable for several reasons. For example, the entity was deleted by another process, such as an entitlement, that was originally involved in the certification process.
---	--

When you click the  **OU/Entitlement Info** icon, the OU/Entitlement details window displays the data in the following table:

OU/Entitlement information		
Entity	Detail	Description
OU	Type	Indicates the type that is associated to the OU.
	Name	Name of the OU.
	Code	Univocal identifier of the OU.
	Excluded by SoD Validation	The user is excluded by segregation of duty analysis.
	Owner	Name of the OU owner.
	Description	Brief description of the OU.
Entitlement - Details tab	Type	Type of entitlement: <ul style="list-style-type: none"> • Permission • IT Role • Business Role
	Application	Name of the entitlement application.
	Name	Name of the entitlement.
	Description	Brief description of the entitlement.
	Owner	Name of the entitlement owner.
	Expiration	Expiration date of the entitlement in the dd/mm/yyyy format.
	Last Reviewed Date	Date of the last review in the dd/mm/yyyy format.
Entitlement - Rights tab	Permission	Name of the permission that is involved with the entitlement in the Entitlement tab.
	Right Name	Name of the right that is joined to the permission.
	Value	Value of the right.
Entitlement - Activity tab	Activity Name	Name of the activity.
	Path	Position of the activity relative to the activity tree.
	Description	Brief description of the activity.

Details - Entitlement/User


After the selection of the campaign, the **Details** tab opens and shows specialized views.

Details includes the following specialized views:

- Details - Entitlement View
- Details - User View

This view option can be changed by the administrator.

Table 8. Details tab note

	<p>Note: The Access Governance Core administrator defines the campaign contents and settings. Access Certifier reviewers can have different sets of functional buttons, icons, or tabs available, depending on the configuration of the campaign.</p>
---	--

Details - Entitlement View

After the selection of the Campaign, the Details tab shows the list of the entities to be certified. To search a specific *Entity*, set the filters in the following table by clicking **Filter/Hide Filter**:

Table 9. Entitlement View details filters.


Context	Filter	Description
User	Org Unit	Click  OU to enter an organizational unit (OU).
	Identity	This field can host the name, the surname, or the User ID of the user.
	Hierarchy	If this check box is selected, the search activity applies to all the hierarchy, starting from the root OU that is indicated in the Org Unit field.
	Only Users with Violations	If this check box is selected, the search activity applies only to users with outstanding violations.
	UME	UME is a digital identity (user) that can have more than one account on the same target system. If this check box is selected, the search activity applies to all the UME involved in the campaign.

Table 9. Entitlement View details filters. (continued)

Context	Filter	Description
Entitlement	Application	Name of the application.
	Search Entitlement (Name or Code)	Name or code of the entitlement.
	User Hierarchy	The user's hierarchy within the organization or group.
	Status	Indicates the status of the certification. <ul style="list-style-type: none"> • Complete • Pending
	Type	Indicate the entitlement type. <ul style="list-style-type: none"> • Permission • IT Role • Business Role • External Role
	Only with Visibility Violations	If this check box is selected, the search activity applies to the entitlements in role alignment violation. That is, entitlements are assigned to a user, but they do not belong to the OU of the user.
	Reviewed	Was the user reviewed? <ul style="list-style-type: none"> • Formerly indicates that the user was reviewed at least one time. • Never indicates that the user was not reviewed.
	Owner	Indicates the owner of the certification activity. <ul style="list-style-type: none"> • Assigned to me • Redirected by me • Redirected to me • Returned

Clicking the link **Campaign Campaign Name** in the upper right part of the frame displays the information summarized in the following table in the Campaign Info window:

Table 10. Campaign Info window

Field	Description
Campaign Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Name of the supervisor.
Campaign Type	Type of the campaign.
Allow Redirection	If this check box is selected, the reviewer can redirect to other reviewer entities to be approved or revoked.
Escalation to Supervisor	If this check box is selected, the reviewer can redirect to the supervisor entities to be approved or revoked.
Notes Revocation (Mandatory)	If this check box is selected, inserting a note is mandatory for an entity revocation.

Table 10. Campaign Info window (continued)

Field	Description
Sign Off	The method in which the approval or revocation is validated: Automatic The approval or revocation is immediately signed off. Completed By User The user decides when to sign off on the approval or revocation. End Campaign The approval or revocation is signed off at the end of the campaign.
Start/End Date	Start/end date of the campaign, according to the format established by the administrator.

Details can show different sets of attributes or different sets of icons and buttons. They are based on the type of the campaign you selected.

The following table shows the entire superset of buttons and icons of the **Details** tab:

Table 11. Details tab buttons and icons

















Button/Icon	Description
 Inspect	Inspect the entities of the campaign.
 Entity info	Provides information about the entity in the campaign, such as user, OU, entitlement, and risk.
 History	In the Note History window, History displays the information about the previous campaigns in which the entity was involved. When you select a listed item, Note opens automatically, displaying the note for the selected item.
Approve/Revoke	Approve/revoke associations between entities.
 Note	Click to insert a note about the entity.
 Note OK	Click to read a note that was previously inserted through.  .
 Forward	Redirect to another reviewer to be approved or revoked.
 Escalation	Escalate to the supervisor to be approved or revoked.
 Return	Return to the reviewer to be approved or revoked.
 Received	Received directly by another reviewer.
 Received after check	Received by the reviewer after the cycle (return action) was checked.
 Supervisors	This icon indicates that different supervisors are configured for the selected certification. Click this icon to see the entire list of supervisors.
 Sign off	The certifier can decide when to sign off on the approval or revocation.
 Show UME	Identifies the master UME, and you can group UME.

Table 11. Details tab buttons and icons (continued)

Button/Icon	Description
 Stats	Allows the supervisor to monitor by two types of pie charts, the status of the campaign completion.
	Click the colored dot to open a window that displays the following activities: <ul style="list-style-type: none"> • The risk activities tree (related to a specific user) into the Risk Info tab • The activities that are involved in a specific risk into the Risk Activity tab
Certifying: <i>EntityName</i>	Click Certifying: <i>EntityName</i> in the upper-right part of the page to display information about the entity.
Approve Revoke Redirect Escalate Sign-off	In the upper-right side of the page, which is aligned with Filter/Hide Filter and depending on the previous selection, up to four bulk operations are available. Activate these operations by selecting the check boxes that are associated with each item. You can select all items by clicking the check box on the left side of the upper blue bar.

The following table shows the entire superset of configurable columns for the details of the campaign:

Table 12. Columns for Entitlement View

Column	Description
Attestation buttons	Makes actions visible. <ul style="list-style-type: none"> • Approve • Revoke • Sign Off • Notes • Redirect • Redirect to Supervisors
Master UID	UID of the user.
User First Name	Given name of the user.
User Last Name	Surname of the user.
User info buttons	Makes user information visible. <ul style="list-style-type: none"> • Details • Entitlements • External Data • Accounts • Activities • Rights
OU Name - Code	Name and code of the organizational unit (OU).
OU Owner	Owner of the organizational unit, according to the setting in AGC.
OU Description	Short description of the organizational unit.
Application Name	Name of the application, with the information available about the application.


Table 12. Columns for Entitlement View (continued)

Column	Description
Application Owner	Owner of the application, according to the setting in AGC.
Application Description	Short description about the application.
Entitlement Name	Name of the entitlement. If the Entitlement Localization option is active, the entitlement is shown as a localized name.
Entitlement ID Code	ID code of the entitlement.
Entitlement Description	Short description of the entitlement.
Entitlement info button	Makes entitlement information visible. <ul style="list-style-type: none"> • Details • Structure • Activities • Rights
VV	Role Alignment Violation property, which is related to an entitlement assigned to a user but not joined to the organizational unit of the user.
User Type Name	Type of user, according to AGC settings.

Table 13. User Assignments details

Type of Campaign	Detail	Description
User Assignments	Master ID	Univocal identifier of the User.
	Type	Type associated to the User.
	First Name	Name of the User.
	Last Name	Surname of the User.
	Org. Unit	Name of the OU [Univocal identifier of the OU].
	% Entity Completion	Percentage of the Entities certified.

Table 14. Note about the entity row of a campaign

	<p>Note: If an entity row of the campaign is displayed without Approve/Revoke, the entity is no longer available for the reviewer. It can be unavailable for several reasons. For example, the entity was deleted by another process, such as an entitlement, that was originally involved in the certification process.</p>
---	--


Clicking  **User/Entitlement Info** displays the data summarized in the following table in the User/Entitlement details window:

Table 15. User/Entitlement information

Entity	Detail	Description
User	OU	Indicates the type associated to the OU.
	Name	Name of the User.
	Surname	Surname of the User.
	User ID	Univocal identifier of the User.
	User Type	Indicates the type associated to the User.
	Address	Address of the User.
	City	City of the User.
	Email	Email of the User.
	State	Nation of the User.
	Zip code	Postal code of the User.
	Country	Country of the User.
Entitlement - Details tab	Phone	Phone number of the User.
	Type	Type of Entitlement: <ul style="list-style-type: none"> • Permission • IT Role • Business Role
	Application	Name of the Entitlement Application.
	Name	Name of the Entitlement.
	Description	Brief description of the Entitlement.
	Owner	Name of the Entitlement Owner.
	Expiration	Expiration date of the Entitlement in the dd/mm/yyyy format.
Last Reviewed Date	Date of the last review in the dd/mm/yyyy format.	
Entitlement - Rights tab	Permission	Name of the Permission for the entitlement in the Entitlement tab.
	Right Name	Name of the right joined to the permission.
	Value	Value of the right.
Entitlement - Activity tab	Activity Name	Name of the activity.
	Path	Position of the activity into the Activity Tree.
	Description	Brief description of the activity.

Details - User View

The **User View** tab shows the list of the users to be certified. To search a specific user, set the filters in the following table by clicking **Filter/Hide Filter**:

Table 16. Filters




Filter	Description
Org Unit	Use  OU to enter an OU.
Hierarchy	If this check box is ticked, the search activity is on all the hierarchy. It starts from the root OU indicated in Org Unit .
Identity	This field can host the name, the surname, or the ID of the user.
UME	UME is a digital identity (User) that can have more than one account on the same Target System. If this check box is ticked, the search activity is on all the UME in the Campaign.
Status	Indicates the status of the certification. <ul style="list-style-type: none"> • Complete • Pending
Owner	Indicates the owner of the certification activity. <ul style="list-style-type: none"> • Assigned to me • Redirect by me • Redirect to me • Returned
Only Entity with Violation	If this check box is ticked, the search activity is on the entity with Visibility Violation.

Table 17. Note about UME

	Note: If UME is selected, results show the UME for the campaign only. Clicking  Master UME shows all the UME of the selected Master.
---	--

Clicking **Campaign :Campaign Name** in the upper right part of the frame displays the information summarized in the following table in the Campaign Info window:

Table 18. Campaign Info window

Field	Description
Campaign Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Name of the supervisor.
Campaign Type	Type of the campaign.
Allow Redirection	If this check box is selected, the reviewer can redirect to other reviewer entities to be approved or revoked.
Escalation to Supervisor	If this check box is selected, the reviewer can redirect to the supervisor entities to be approved or revoked.
Notes Revocation (Mandatory)	If this check box is selected, inserting a note is mandatory for an entity revocation.


Table 18. Campaign Info window (continued)

Field	Description
Sign Off	The method in which the approval or revocation is validated: Automatic The approval or revocation is immediately signed off. Completed By User The user decides when to sign off on the approval or revocation. End Campaign The approval or revocation is signed off at the end of the campaign.
Start/End Date	Start/end date of the campaign, according to the format established by the administrator.

Details shows a list of rows.

Every row is composed of a different set of attributes and a different set of icons and buttons.

Table 19. Details tab note

	Note: The Access Governance Core administrator defines the campaign contents and settings. Access Certifier reviewers can have different sets of functional buttons, icons, or tabs available, depending on the configuration of the campaign.
---	---

The following table shows the entire superset of buttons and icons for the **Details** tab:

Table 20. Details tab buttons and icons











Button/Icon	Description
 Inspect	Inspect the entities of the campaign.
 Entity info	Provides information about the entity in the campaign, such as user, OU, entitlement, and risk.
 History	In the Note History window, History displays the information about the previous campaigns in which the entity was involved. When you select a listed item, Note opens automatically, displaying the note for the selected item.
Approve/Revoke	Approve/revoke associations between entities.
 Note	Click to insert a note about the entity.
 Note OK	Click to read a note that was previously inserted through.  .
 Forward	Redirect to another reviewer to be approved or revoked.
 Escalation	Escalate to the supervisor to be approved or revoked.
 Return	Return to the reviewer to be approved or revoked.
 Received	Received directly by another reviewer.

Table 20. Details tab buttons and icons (continued)








Button/Icon	Description
 Received after check	Received by the reviewer after the cycle (return action) was checked.
 Supervisors	This icon indicates that different supervisors are configured for the selected certification. Click this icon to see the entire list of supervisors.
 Sign off	The certifier can decide when to sign off on the approval or revocation.
 Show UME	Identifies the master UME, and you can group UME.
 Stats	Allows the supervisor to monitor by two types of pie charts, the status of the campaign completion.
	Click the colored dot to open a window that displays the following activities: <ul style="list-style-type: none"> The risk activities tree (related to a specific user) into the Risk Info tab The activities that are involved in a specific risk into the Risk Activity tab
Certifying: <i>EntityName</i>	Click Certifying: <i>EntityName</i> in the upper-right part of the page to display information about the entity.
Approve Revoke Redirect Escalate Sign-off	In the upper-right side of the page, which is aligned with Filter/Hide Filter and depending on the previous selection, up to four bulk operations are available. Activate these operations by selecting the check boxes that are associated with each item. You can select all items by clicking the check box on the left side of the upper blue bar.

Table 21. Note about campaigns

	Note: If an entity row of the campaign is displayed without Approve/Revoke , the user is no longer available for the reviewer. It can be unavailable for several reasons. For example, the user was deleted by another process.
---	---

The following table shows the entire superset of configurable columns for the details of the campaign:


Table 22. Configurable columns for the details of the campaign

Column	Description
Attestation buttons	Makes for attestations actions available: Approve - Revoke - Sign Off - Notes - Redirect - Redirect to Supervisors , or other. See the entire set.
Master UID	Unique identifier of the user.
Type	Indicates the type of user, according to configurations.
User First Name	Name of the user.
User Last Name	Surname of the user.

Table 22. Configurable columns for the details of the campaign (continued)

Column	Description
User info buttons	Click to see a set of information tabs related to the user: Details - Entitlements - External Data - Accounts - Activities - Rights .
OU Name - Code	Name of the OU and the unique identifier of the OU.

Every row in the **Details** tab is characterized by the % **Entity Completion** progress bar, indicating the percentage of the Entities certified.

Clicking  **User Info** displays the user data, which is organized in different tabs in the User Details window, as summarized in the following table:

Tab	Attributes	Description
Details	OU	Indicates the type associated to the OU.
	Name	Name of the user.
	Last Name	Surname of the user.
	User ID	Univocal identifier of the user.
	User Type	Indicates the type associated to the user.
	Address	Address of the user.
	City	City of the user.
	Email	Email of the user.
	State	Nation of the user.
	Zip/Postal code	Zip/Postal code of the user.
	Country	Country of the user.
Entitlements	Phone	Phone number of the user.
	Type	Type of Entitlement: <ul style="list-style-type: none"> • Permission • IT role • Business role
	Application	Name of the entitlement application.
	Name	Name of the entitlement.
	Description	Brief description of the entitlement.
	Owner	Name of the entitlement owner.
	Expiration	Expiration date of the entitlement, according to the format established by the Administrator.
Last Reviewed Date	Date of the last review, according to the format established by the administrator.	

Tab	Attributes	Description
External Data	The origin of the data is the external target system	
Accounts	The following list is all of the accounts related to the selected user:	
Activities	Activity Name	Name of the activity.
	Path	Position of the activity into the Activity Tree.
	Description	Brief description of the nature of the activity.
Rights	Permission	Name of the permission for the entitlement in the Entitlement tab.
	Right Name	Name of the right joined to the permission.
	Value	Value of the right.

Depending on the configuration, some of tabs might not be present. For example, if the user is not involved in any activity, the **Activity** tab is not in the **User Info**.

Details - User Remediation Review

After you select the campaign, the **Details** tab shows the list of the entities to be certified.

To search a specific entity, set the filters in the following table by clicking **Filter/Hide Filter**:

Table 23. Entitlement View details filters.


Context	Filter	Description
User	Org Unit	Click  OU to enter an organizational unit (OU).
	Identity	This field can host the name, the surname, or the User ID of the user.
	Hierarchy	If this check box is selected, the search activity applies to all the hierarchy, starting from the root OU that is indicated in the Org Unit field.
	Only Users with Violations	If this check box is selected, the search activity applies only to users with outstanding violations.
	UME	UME is a digital identity (user) that can have more than one account on the same target system. If this check box is selected, the search activity applies to all the UME involved in the campaign.

Table 23. Entitlement View details filters. (continued)

Context	Filter	Description
Entitlement	Application	Name of the application.
	Search Entitlement (Name or Code)	Name or code of the entitlement.
	User Hierarchy	The user's hierarchy within the organization or group.
	Status	Indicates the status of the certification. <ul style="list-style-type: none"> • Complete • Pending
	Type	Indicate the entitlement type. <ul style="list-style-type: none"> • Permission • IT Role • Business Role • External Role
	Only with Visibility Violations	If this check box is selected, the search activity applies to the entitlements in role alignment violation. That is, entitlements are assigned to a user, but they do not belong to the OU of the user.
	Reviewed	Was the user reviewed? <ul style="list-style-type: none"> • Formerly indicates that the user was reviewed at least one time. • Never indicates that the user was not reviewed.
	Owner	Indicates the owner of the certification activity. <ul style="list-style-type: none"> • Assigned to me • Redirected by me • Redirected to me • Returned

When you click the link **Campaign: Campaign Name** in the upper right part of the page, the Campaign Info window displays the information summarized in the following table:

Table 24. Campaign Info window

Field	Description
Campaign Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Name of the supervisor.
Campaign Type	Type of the campaign.
Allow Redirection	If this check box is selected, the reviewer can redirect to other reviewer entities to be approved or revoked.
Escalation to Supervisor	If this check box is selected, the reviewer can redirect to the supervisor entities to be approved or revoked.
Notes Revocation (Mandatory)	If this check box is selected, inserting a note is mandatory for an entity revocation.

Table 24. Campaign Info window (continued)

Field	Description
Sign Off	The method in which the approval or revocation is validated: Automatic The approval or revocation is immediately signed off. Completed By User The user decides when to sign off on the approval or revocation. End Campaign The approval or revocation is signed off at the end of the campaign.
Start/End Date	Start/end date of the campaign, according to the format established by the administrator.

Depending on the type of the campaign that is selected, **Details** can show:

- Different set of attributes
- Different set of icons and buttons

The following table shows the entire superset of buttons and icons of the **Details** tab:

Table 25. Details tab buttons and icons

















Button/Icon	Description
 Inspect	Inspect the entities of the campaign.
 Entity info	Provides information about the entity in the campaign, such as user, OU, entitlement, and risk.
 History	In the Note History window, History displays the information about the previous campaigns in which the entity was involved. When you select a listed item, Note opens automatically, displaying the note for the selected item.
Approve/Revoke	Approve/revoke associations between entities.
 Note	Click to insert a note about the entity.
 Note OK	Click to read a note that was previously inserted through.  .
 Forward	Redirect to another reviewer to be approved or revoked.
 Escalation	Escalate to the supervisor to be approved or revoked.
 Return	Return to the reviewer to be approved or revoked.
 Received	Received directly by another reviewer.
 Received after check	Received by the reviewer after the cycle (return action) was checked.
 Supervisors	This icon indicates that different supervisors are configured for the selected certification. Click this icon to see the entire list of supervisors.
 Sign off	The certifier can decide when to sign off on the approval or revocation.

Table 25. Details tab buttons and icons (continued)

Button/Icon	Description
 Show UME	Identifies the master UME, and you can group UME.
 Stats	Allows the supervisor to monitor by two types of pie charts, the status of the campaign completion.
	Click the colored dot to open a window that displays the following activities: <ul style="list-style-type: none"> • The risk activities tree (related to a specific user) into the Risk Info tab • The activities that are involved in a specific risk into the Risk Activity tab
Certifying: <i>EntityName</i>	Click Certifying: <i>EntityName</i> in the upper-right part of the page to display information about the entity.
Approve Revoke Redirect Escalate Sign-off	In the upper-right side of the page, which is aligned with Filter/Hide Filter and depending on the previous selection, up to four bulk operations are available. Activate these operations by selecting the check boxes that are associated with each item. You can select all items by clicking the check box on the left side of the upper blue bar.

The following table includes the details of this campaign:

Table 26. Risk Violation Mitigation Details





Type of Campaign	Detail	Description
Risk Violation Mitigation	Action	Allows the inspection of the entities of the campaign.
	Violation	Risk level:  : Low level  : Medium level  : High level When you click a colored dot, the Risk Info window opens.
	User ID	Univocal identifier of the user.
	User Type	Indicates the type associated with the user.
	Name	Name of the user.
	Surname	Surname of the user.
	OU Name [Code]	Name of the OU [Univocal identifier of the OU].
	% Entity Completion	Percentage of the entities that are certified.

Table 27. Note about campaigns

	<p>Note: If an entity row of the campaign is displayed without Approve/Revoke, the entity is no longer available for the reviewer. It can be unavailable for several reasons. For example, the entity was deleted by another process, such as an entitlement, that was originally involved in the certification process.</p>
---	--


When you click  **User/Risk Info**, the User/Risk details window displays the data summarized in the following table:

Table 28. User/Risk information

Entity	Detail	Description
User	OU	Indicates the type associated with the OU.
	Name	Name of the user.
	Surname	Surname of the user.
	User ID	Univocal identifier of the user.
	User Type	Indicates the type associated with the user.
	Address	Address of the user.
	City	City of the user.
	Email	Email of the user.
	Nation	Nation of the user.
	Zip code	Postal code of the user.
	Country	Country of the user.
Risk	Phone	Phone number of the user.
	Name	Name of the risk.
	Type	Type of risk.
	Level	Risk level: <ul style="list-style-type: none"> • Low level • Medium level • High level
	Description	Brief description of the risk.

Details - Entitlement Review

After you select the campaign, **Details** shows the list of the entities to be certified.

To search a specific entity, set the filters in the following table by clicking **Filter/Hide Filter**:

Table 29. Entitlement View details filters.




Context	Filter	Description
User	Org Unit	Click  OU to enter an organizational unit (OU).
	Identity	This field can host the name, the surname, or the User ID of the user.
	Hierarchy	If this check box is selected, the search activity applies to all the hierarchy, starting from the root OU that is indicated in the Org Unit field.
	Only Users with Violations	If this check box is selected, the search activity applies only to users with outstanding violations.
	UME	UME is a digital identity (user) that can have more than one account on the same target system. If this check box is selected, the search activity applies to all the UME involved in the campaign.

Table 29. Entitlement View details filters. (continued)

Context	Filter	Description
Entitlement	Application	Name of the application.
	Search Entitlement (Name or Code)	Name or code of the entitlement.
	User Hierarchy	The user's hierarchy within the organization or group.
	Status	Indicates the status of the certification. <ul style="list-style-type: none"> • Complete • Pending
	Type	Indicate the entitlement type. <ul style="list-style-type: none"> • Permission • IT Role • Business Role • External Role
	Only with Visibility Violations	If this check box is selected, the search activity applies to the entitlements in role alignment violation. That is, entitlements are assigned to a user, but they do not belong to the OU of the user.
	Reviewed	Was the user reviewed? <ul style="list-style-type: none"> • Formerly indicates that the user was reviewed at least one time. • Never indicates that the user was not reviewed.
	Owner	Indicates the owner of the certification activity. <ul style="list-style-type: none"> • Assigned to me • Redirected by me • Redirected to me • Returned

Table 30. Note about the UME check box

	<p>Note: When the check box UME is selected, results show only the UME in the campaign.</p> <p>When you click  Master UME, it displays all of the UME of the selected master.</p>
---	---

When you click the link **Campaign: Campaign Name** in the upper right part of the page, the Campaign Info window displays the information summarized in the following table:

Table 31. Campaign Info window

Field	Description
Campaign Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Name of the supervisor.
Campaign Type	Type of the campaign.

Table 31. Campaign Info window (continued)

Field	Description
Allow Redirection	If this check box is selected, the reviewer can redirect to other reviewer entities to be approved or revoked.
Escalation to Supervisor	If this check box is selected, the reviewer can redirect to the supervisor entities to be approved or revoked.
Notes Revocation (Mandatory)	If this check box is selected, inserting a note is mandatory for an entity revocation.
Sign Off	The method in which the approval or revocation is validated: Automatic The approval or revocation is immediately signed off. Completed By User The user decides when to sign off on the approval or revocation. End Campaign The approval or revocation is signed off at the end of the campaign.
Start/End Date	Start/end date of the campaign, according to the format established by the administrator.

Depending on the type of the campaign that is selected, **Details** can show:

- Different set of attributes
- Different set of icons and buttons

The following table shows the entire superset of buttons and icons of the **Details** tab:

Table 32. Details tab buttons and icons

















Button/Icon	Description
 Inspect	Inspect the entities of the campaign.
 Entity info	Provides information about the entity in the campaign, such as user, OU, entitlement, and risk.
 History	In the Note History window, History displays the information about the previous campaigns in which the entity was involved. When you select a listed item, Note opens automatically, displaying the note for the selected item.
Approve/Revoke	Approve/revoke associations between entities.
 Note	Click to insert a note about the entity.
 Note OK	Click to read a note that was previously inserted through.  .
 Forward	Redirect to another reviewer to be approved or revoked.
 Escalation	Escalate to the supervisor to be approved or revoked.
 Return	Return to the reviewer to be approved or revoked.
 Received	Received directly by another reviewer.

Table 32. Details tab buttons and icons (continued)


Button/Icon	Description
 Received after check	Received by the reviewer after the cycle (return action) was checked.
 Supervisors	This icon indicates that different supervisors are configured for the selected certification. Click this icon to see the entire list of supervisors.
 Sign off	The certifier can decide when to sign off on the approval or revocation.
 Show UME	Identifies the master UME, and you can group UME.
 Stats	Allows the supervisor to monitor by two types of pie charts, the status of the campaign completion.
	Click the colored dot to open a window that displays the following activities: <ul style="list-style-type: none"> The risk activities tree (related to a specific user) into the Risk Info tab The activities that are involved in a specific risk into the Risk Activity tab
Certifying: <i>EntityName</i>	Click Certifying: <i>EntityName</i> in the upper-right part of the page to display information about the entity.
Approve Revoke Redirect Escalate Sign-off	In the upper-right side of the page, which is aligned with Filter/Hide Filter and depending on the previous selection, up to four bulk operations are available. Activate these operations by selecting the check boxes that are associated with each item. You can select all items by clicking the check box on the left side of the upper blue bar.

The following table includes the details of this campaign:

Table 33. Entitlement details

Type of Campaign	Detail	Description
Entitlement	Action	Allows the inspection of the entities of the campaign.
	Entitlement	Type and name of the entitlement.
	SoD/SA	Click a colored dot to display the following information: <ul style="list-style-type: none"> The risk activities tree (related to a specific user) in Risk Info. The activities that are involved in a specific risk in Risk Activity.
	Description	Brief description of the entitlement.
	Application	Name of the entitlement application.

Table 34. Note about campaigns

	<p>Note: If an entity row of the campaign is displayed without Approve/Revoke, the entity is no longer available for the reviewer. It can be unavailable for several reasons. For example, the entity was deleted by another process, such as an entitlement, that was originally involved in the certification process.</p>
---	--


When you click  **Entitlement Info**, the Entitlement details window displays the data in the following table:

Table 35. User/Entitlement information

Entity	Detail	Description
Entitlement - Details tab	Type	Type of entitlement: <ul style="list-style-type: none"> • Permission • IT Role • Business Role
	Application	Name of the entitlement application.
	Name	Name of the entitlement.
	Description	Brief description of the entitlement.
	Owner	Name of the entitlement owner.
	Expiration	Expiration date of the entitlement in dd/mm/yyyy format.
	Last Reviewed Date	Date of the last review in dd/mm/yyyy format.
	Org. Units	Number of the OUs that the selected entitlement is involved in.
	Users	Number of the users associated with the selected entitlement.
Entitlement - Structure tab	Name	Name of the entitlement.
	Application	Name of the entitlement application.
	Description	Brief description of the entitlement.
Entitlement - Org. Units tab	Name	Name of the OU.
	User ID	Univocal identifier of the user.

Table 35. User/Entitlement information (continued)

Entity	Detail	Description
Entitlement - Users tab	First Name	Name of the user.
	Last Name	Surname of the user.
	Master UID	Univocal identifier of the master user.
	Org. Unit	Name of the OU of the user.

Details - Account Review

After you select the campaign, the **Details** tab shows the list of the entities to be certified.

To search a specific entity, set the filters in the following table by clicking **Filter/Hide Filter**:

Table 36. Details Filters




Filter	Description
Org Unit	Click  OU to enter an organizational unit (OU).
Hierarchy	If this check box is selected, the search activity applies to all the hierarchy, starting from the root OU that is indicated in Org Unit .
Only Users with Violations	
Identity	This field can host the name, the surname, or the ID of the user.
UME	UME is a digital identity (user) that can have more than one account on the same target system. If this check box is selected, the search activity applies to all the UME in the campaign.
Status	The following list shows the status of the certification: <ul style="list-style-type: none"> • Complete • Pending
Owner	The following list shows activity for the owner of the certification: <ul style="list-style-type: none"> • Assigned to me • Redirect by me • Redirect to me • Returned
Account Status	<ul style="list-style-type: none"> • Locked indicates that the account is blocked. • Unlocked indicates that the account is not blocked.
Configuration Name	Name of the configuration joined to the account.
Reviewed	The user can have one of the following review statuses: <ul style="list-style-type: none"> • Formerly indicates that the user was reviewed at least one time. • Never indicates that the user was not reviewed.

Table 37. Note about the UME check box

	<p>Note: When you select UME, it shows only the UME in the campaign. When you click  Master UME, it displays all of the UME of the selected master.</p>
---	---

When you click **Campaign: Campaign Name** in the upper right part of the page, the Campaign Info window displays the information summarized in the following table:

Table 38. Campaign Info window

Field	Description
Campaign Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Name of the supervisor.
Campaign Type	Type of the campaign.
Allow Redirection	If this check box is selected, the reviewer can redirect to other reviewer entities to be approved or revoked.
Escalation to Supervisor	If this check box is selected, the reviewer can redirect to the supervisor entities to be approved or revoked.
Notes Revocation (Mandatory)	If this check box is selected, inserting a note is mandatory for an entity revocation.
Sign Off	The method in which the approval or revocation is validated: Automatic The approval or revocation is immediately signed off. Completed By User The user decides when to sign off on the approval or revocation. End Campaign The approval or revocation is signed off at the end of the campaign.
Start/End Date	Start/end date of the campaign, according to the format established by the administrator.

Depending on the type of the campaign that is selected, the **Details** tab can show:

- Different set of attributes
- Different set of icons and buttons

The following table shows the entire superset of buttons and icons for the **Details** tab:

Table 39. Details tab buttons and icons
















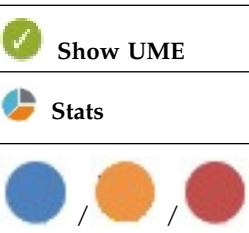
Button/Icon	Description
 Inspect	Inspect the entities of the campaign.
 Entity info	Provides information about the entity in the campaign, such as user, OU, entitlement, and risk.
 History	In the Note History window, History displays the information about the previous campaigns in which the entity was involved. When you select a listed item, Note opens automatically, displaying the note for the selected item.
Approve/Revoke	Approve/revoke associations between entities.
 Note	Click to insert a note about the entity.

Table 39. Details tab buttons and icons (continued)


Button/Icon	Description
 Note OK	Click to read a note that was previously inserted through.  .
 Forward	Redirect to another reviewer to be approved or revoked.
 Escalation	Escalate to the supervisor to be approved or revoked.
 Return	Return to the reviewer to be approved or revoked.
 Received	Received directly by another reviewer.
 Received after check	Received by the reviewer after the cycle (return action) was checked.
 Supervisors	This icon indicates that different supervisors are configured for the selected certification. Click this icon to see the entire list of supervisors.
 Sign off	The certifier can decide when to sign off on the approval or revocation.
 Show UME	Identifies the master UME, and you can group UME.
 Stats	Allows the supervisor to monitor by two types of pie charts, the status of the campaign completion.
	Click the colored dot to open a window that displays the following activities: <ul style="list-style-type: none"> The risk activities tree (related to a specific user) into the Risk Info tab The activities that are involved in a specific risk into the Risk Activity tab
Certifying: <i>EntityName</i>	Click Certifying: <i>EntityName</i> in the upper-right part of the page to display information about the entity.
Approve Revoke Redirect Escalate Sign-off	In the upper-right side of the page, which is aligned with Filter/Hide Filter and depending on the previous selection, up to four bulk operations are available. Activate these operations by selecting the check boxes that are associated with each item. You can select all items by clicking the check box on the left side of the upper blue bar.

The following table includes the details of this campaign:

Table 40. Account details

Type of Campaign	Detail	Description
Account	Application Name	A list of applications joined to the specific account.
	Account setting	The entire set of data that determines the policy of management of the account.

Table 41. Note about campaigns

	<p>Note: If an entity row of the campaign is displayed without Approve/Revoke, the entity is no longer available for the reviewer. It can be unavailable for several reasons. For example, the entity was deleted by another process, such as an entitlement, that was originally involved in the certification process.</p>
---	--


When you click  **Account Info**, the Entitlement details window displays the data summarized in the following table:

Table 42. User information

Tab	Attributes	Description
Details	OU	The type associated to the OU.
	Name	Name of the User.
	Last Name	Surname of the User.
	User ID	Univocal identifier of the User.
	User Type	The type associated to the User.
	Address	Address of the User.
	City	City of the User.
	Email	Email of the User.
	State	Nation of the User.
	Zip/Postal code	Zip/Postal code of the User.
	Country	Country of the User.
Phone	Phone number of the User.	
Accounts	A list of all Accounts related to the selected user.	

Details for Supervisor - OU Entitlement

After you select the campaign, the **Details** tab shows information about the selected campaign. Information about the activities of the reviewers of the campaign is also displayed.

In the upper part of the page, information about the campaign is available. It is summarized in the following table:

Supervisor Campaign	
Detail	Description
Campaign Name (link)	Name of the campaign.
Start Date	Start date of the campaign in the dd/mm/yyyy format.

Supervisor Campaign	
Detail	Description
Sign Off	Validation mode for approval or revocation actions: <ul style="list-style-type: none"> • Automatic: The approval or revocation is immediately signed off. • By User: The user decides when to sign off on the approval or revocation. • End Campaign: The approval or revocation is signed off at the end of the campaign.
Campaign Type	Type of the campaign.
End Date	End date of the campaign in the dd/mm/yyyy format.
% Completion	Percentage of the entities certified.

When you click the link **Campaign: Campaign Name** in the upper right part of the page, the Campaign Info window displays the information summarized in the following table:

Campaign Detail	Description
Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Supervisors of the campaign (at least 1 supervisor).
Campaign Type	Type of campaign. <ul style="list-style-type: none"> • Entitlement • User assignment • Entitlement/OU visibility • Risk violation mitigation
Certification Dataset	Name of the data set that is built to feed or to start the campaign.
Exclude Reviewed Since	If this check box is selected, the entities that were reviewed during the specified time are excluded by revision activity: <ul style="list-style-type: none"> • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year
Notes Revocation (Mandatory)	If this check box is selected, the reviewer is required to specify notes for any revocation.
Allow Bulk Operations	If this check box is selected, the reviewer can use special commands for bulk approval/revocation actions.
Sign Off	Type of sign-off. <ul style="list-style-type: none"> • Automatic • Completed By User • End campaign

Campaign Detail	Description
Activity Details	<p>Attributes for an active campaign.</p> <ul style="list-style-type: none"> • Start Date • End Date • Reviewers Signed Off/Total Reviewers K/N • <i>Entity</i> User Signed Off / Total <i>Entity</i> H/M Users • Working Progress J/TOT-M <ul style="list-style-type: none"> – N is the maximum number of reviewers – M is the maximum number of entities – TOT is the total number of pairs OU-Entitlement or User-Entitlement or User-Risk, depending on the campaign type

Table 43. Cert_Campaign_Reviewer_Tab

Reviewer Detail	Description
Scope	<p>User Hierarchy If enabled, shows the available user hierarchy scope. It is always available for organizational units.</p> <p>Entity If enabled, shows the entity scope.</p>
Default Reviewer	The default reviewer for the campaign.
Allow Redirection	If checked, approvals and revocations can be redirected to another reviewer
Escalation to Supervisor	If checked, approvals and revocations can be escalated to the supervisor of the campaign.
Exclusion list	Defines a list of reviewers that are excluded from the campaign. If enabled, you can use Add and Remove to define the reviewer list.

Fulfillment Detail	Description
Logical deletion	If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are deleted but only logically.
Physical deletion	<p>If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are physically deleted, after a grace period if provided. Before the end of this period, data is available for any usage. For an immediate deletion, set Grace period=0.</p> <p>Campaigns on Account have the following options:</p> <ul style="list-style-type: none"> • Delete the Account • Lock the Account
Physical deletion after workflow	If this option is selected, the entities-joins are deleted after a specified workflow, which is identified through the setting of <i>name Process - name Activity</i> .
Custom Behaviour	The management of the fulfillment involves a set of rules.


Table 44. Cert_Campaign_Scheduling_Tab

Scheduling Detail	Description
Activate On	<p>Start date If checked, enables the workflow processes to define the frequency and length of the campaign.</p> <p>Duration The following values are available:</p> <ul style="list-style-type: none"> • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year • Continuous (never closed)
Execution Frequency	<p>The following values are available:</p> <ul style="list-style-type: none"> • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year • One time <p>The set of values is bounded according to the Duration parameter. If Duration=Continuous, you cannot set values for this parameter.</p>
Time Kept In History (Days)	Number of days to maintain the campaign data in the history.



Notification Type	Description
Campaign Started for Reviewer	<p>If Enable is set, the reviewer receives an email when the campaign begins.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information about the campaign.</p>
Activity Reminder for Reviewer	<p>If Enable is set, the reviewer receives an email at the following times:</p> <ul style="list-style-type: none"> • <i>K</i> days before the end of the campaign. Determined by Days before end date, where <i>K</i> is a value 0 - 32. • When the percentage of activity that is already managed is greater than <i>X</i>%. Determined by Activity percentage <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>
Campaign Reminder for Reviewer	<p>If Enable is set, the reviewer receives an email <i>K days</i> before the end of the campaign. Determined by Days before end date, where <i>K</i> is a value 0 - 32.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>

Notification Type	Description
Campaign Reminder for Supervisor	<p>If Enable is set, the supervisor receives an email <i>K days</i> before the end of the campaign. Determined by Days before end date, <i>K</i> is a value 0 - 32.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>
Continuous Review for Reviewer	<p>If Enable is set, the reviewer receives an email when a continuous campaign begins.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>
Redirect	<p>If Enable is set, the reviewer or supervisor receives an email in response to any action of redirection.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>


To search a specific reviewer, set the filters shown in the following table by clicking **Filter/Hide Filter**:

Reviewer filters	
Filter	Description
Identity	This field can host the Name , the Surname , or the User ID of the user.
Org Unit	Use  OU on the right side of the attribute's box to enter an OU.
Hierarchy	If this box is ticked, the search activity is on all the hierarchy. It starts from the root OU that is indicated in Org Unit .


Results are displayed in the same frame according to the following attributes:

Reviewer details	
Detail	Description
Action	<p> Stats monitors the status of the campaign completion.</p> <p> Inspect inspects the entities of the campaign.</p>
User ID	Univocal identifier of the reviewer.
Name	Name of the reviewer.
Surname	Surname of the reviewer.
OU Name [Code]	Name of the organizational unit of the reviewer.

Reviewer details	
Detail	Description
% Entity Completion	Percentage of the entities certified.

Clicking  **Stats** displays the **Total items** and **Signed Off items** pie charts in the Stats window so you can monitor the campaign completion status.

If **Sign off** is set to **By User** or **Automatic**, the No data to display message is under **Signed Off**.

By clicking  **Inspect**, the Supervisor can view the approved or removed campaigns.

Details for Supervisor - User Entitlement

After the selection of the campaign, the Details tab displays information about the selected campaign and about the activities of the reviewers in the campaign.

The upper part of the frame displays the information about the campaign. It is summarized in the following table:

Supervisor Campaign	
Detail	Description
Campaign Name (link)	Name of the campaign.
Start Date	Start date of the campaign.
Sign Off	Validation mode for approval or revocation actions: <ul style="list-style-type: none"> • Automatic: the approval or revocation is immediately signed off. • By User: the user decides when to sign off the approval or revocation. • End Campaign: the approval or revocation is signed off at the end of the campaign.
Campaign Type	Type of the campaign.
End Date	End date of the campaign.
% Completion	Percentage of the entities certified.

Clicking **Campaign: Campaign Name** in the upper right part of the frame displays the information summarized in the following tab in the Campaign Info window:

Campaign Detail	Description
Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Supervisors of the campaign (at least 1 supervisor).

Campaign Detail	Description
Campaign Type	Type of campaign. <ul style="list-style-type: none"> • Entitlement • User assignment • Entitlement/OU visibility • Risk violation mitigation
Certification Dataset	Name of the data set that is built to feed or to start the campaign.
Exclude Reviewed Since	If this check box is selected, the entities that were reviewed during the specified time are excluded by revision activity: <ul style="list-style-type: none"> • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year
Notes Revocation (Mandatory)	If this check box is selected, the reviewer is required to specify notes for any revocation.
Allow Bulk Operations	If this check box is selected, the reviewer can use special commands for bulk approval/revocation actions.
Sign Off	Type of sign-off. <ul style="list-style-type: none"> • Automatic • Completed By User • End campaign
Activity Details	Attributes for an active campaign. <ul style="list-style-type: none"> • Start Date • End Date • Reviewers Signed Off/Total Reviewers K/N • <i>Entity</i> User Signed Off / Total <i>Entity</i> H/M Users • Working Progress J/TOT-M <ul style="list-style-type: none"> – N is the maximum number of reviewers – M is the maximum number of entities – TOT is the total number of pairs OU-Entitlement or User-Entitlement or User-Risk, depending on the campaign type

Table 45. Cert_Campaign_Reviewer_Tab

Reviewer Detail	Description
Scope	<p>User Hierarchy If enabled, shows the available user hierarchy scope. It is always available for organizational units.</p> <p>Entity If enabled, shows the entity scope.</p>
Default Reviewer	The default reviewer for the campaign.
Allow Redirection	If checked, approvals and revocations can be redirected to another reviewer
Escalation to Supervisor	If checked, approvals and revocations can be escalated to the supervisor of the campaign.
Exclusion list	Defines a list of reviewers that are excluded from the campaign. If enabled, you can use Add and Remove to define the reviewer list.

Fulfillment Detail	Description
Logical deletion	If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are deleted but only logically.
Physical deletion	<p>If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are physically deleted, after a grace period if provided. Before the end of this period, data is available for any usage. For an immediate deletion, set Grace period=0.</p> <p>Campaigns on Account have the following options:</p> <ul style="list-style-type: none"> • Delete the Account • Lock the Account
Physical deletion after workflow	If this option is selected, the entities-joins are deleted after a specified workflow, which is identified through the setting of <i>name Process - name Activity</i> .
Custom Behaviour	The management of the fulfillment involves a set of rules.

Table 46. Cert_Campaign_Scheduling_Tab

Scheduling Detail	Description
Activate On	<p>Start date If checked, enables the workflow processes to define the frequency and length of the campaign.</p> <p>Duration The following values are available:</p> <ul style="list-style-type: none"> • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year • Continuous (never closed)
Execution Frequency	<p>The following values are available:</p> <ul style="list-style-type: none"> • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year • One time <p>The set of values is bounded according to the Duration parameter. If Duration=Continuous, you cannot set values for this parameter.</p>
Time Kept In History (Days)	Number of days to maintain the campaign data in the history.



Notification Type	Description
Campaign Started for Reviewer	<p>If Enable is set, the reviewer receives an email when the campaign begins.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information about the campaign.</p>


Notification Type	Description
Activity Reminder for Reviewer	<p>If Enable is set, the reviewer receives an email at the following times.</p> <ul style="list-style-type: none"> • <i>K</i> days before the end of the campaign. Determined by Days before end date, where <i>K</i> is a value 0 - 32. • When the percentage of activity that is already managed is greater than <i>X</i>%. Determined by Activity percentage <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>
Campaign Reminder for Reviewer	<p>If Enable is set, the reviewer receives an email <i>K days</i> before the end of the campaign. Determined by Days before end date, where <i>K</i> is a value 0 - 32.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>
Campaign Reminder for Supervisor	<p>If Enable is set, the supervisor receives an email <i>K days</i> before the end of the campaign. Determined by Days before end date, <i>K</i> is a value 0 - 32.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>
Continuous Review for Reviewer	<p>If Enable is set, the reviewer receives an email when a continuous campaign begins.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>
Redirect	<p>If Enable is set, the reviewer or supervisor receives an email in response to any action of redirection.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>

To search a specific reviewer, set the filters in the following table by clicking **Filter/Hide Filter**:


Reviewer filters	
Filter	Description
Identity	This field can host the name, surname, or user ID of the user.
Org Unit	Use <input type="checkbox"/> OU on the right side of the attribute to enter an organizational unit.
Hierarchy	If this box is selected, the search activity is on all the hierarchy. It starts from the root OU in Org Unit .

Results are displayed in the same frame by the following the attributes:

Reviewer details	
Detail	Description
Action	 Stats monitors the status of the campaign completion.  Inspect inspects the entities of the campaign.
Master UID	Univocal identifier of the reviewer.
Name	Name of the reviewer
Last Name	Surname of the reviewer.
OU Name [Code]	Name of the organizational unit of the reviewer.
% Entity Completion	Percentage of the entities certified.

Clicking  **Stats** displays the **Total items** and **Signed Off items** pie charts in the Stats window so you can monitor the status of the Campaign completion.

If the campaign sign-off is in **By User** or **Automatic** mode, the No data to display message is under **Signed Off Items**.

By clicking  **Inspect**, the supervisor can view the approved or removed campaigns.

Details for Supervisor - User Remediation

After the selection of the campaign, the **Details** tab displays information about the selected campaign and about activities of the reviewers in the campaign.

The upper part of the frame displays information about the campaign. It is summarized in the following table:

Supervisor Campaign	
Detail	Description
Campaign Name (link)	Name of the campaign.
Start Date	Start date of the campaign in the dd/mm/yyyy format.
Sign Off	Validation mode for approval or revocation actions: <ul style="list-style-type: none"> • Automatic: the approval or revocation is immediately signed off • By User: the user decides when to sign off the approval or revocation • End Campaign: the approval or revocation is signed off at the end of the campaign.
Campaign Type	Type of the campaign.
End Date	End date of the campaign in the dd/mm/yyyy format.

Supervisor Campaign	
Detail	Description
% Completion	Percentage of the entities certified.

Clicking **Campaign: Campaign Name** in the upper right part of the frame displays the information summarized in following tabs in the Campaign Info window

Campaign Detail	Description
Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Supervisors of the campaign (at least 1 supervisor).
Campaign Type	Type of campaign. <ul style="list-style-type: none"> • Entitlement • User assignment • Entitlement/OU visibility • Risk violation mitigation
Certification Dataset	Name of the data set that is built to feed or to start the campaign.
Exclude Reviewed Since	If this check box is selected, the entities that were reviewed during the specified time are excluded by revision activity: <ul style="list-style-type: none"> • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year
Notes Revocation (Mandatory)	If this check box is selected, the reviewer is required to specify notes for any revocation.
Allow Bulk Operations	If this check box is selected, the reviewer can use special commands for bulk approval/revocation actions.
Sign Off	Type of sign-off. <ul style="list-style-type: none"> • Automatic • Completed By User • End campaign
Activity Details	Attributes for an active campaign. <ul style="list-style-type: none"> • Start Date • End Date • Reviewers Signed Off/Total Reviewers K/N • <i>Entity</i> User Signed Off / Total <i>Entity</i> H/M Users • Working Progress J/TOT-M <ul style="list-style-type: none"> – N is the maximum number of reviewers – M is the maximum number of entities – TOT is the total number of pairs OU-Entitlement or User-Entitlement or User-Risk, depending on the campaign type

Table 47. Cert_Campaign_Reviewer_Tab

Reviewer Detail	Description
Scope	<p>User Hierarchy If enabled, shows the available user hierarchy scope. It is always available for organizational units.</p> <p>Entity If enabled, shows the entity scope.</p>
Default Reviewer	The default reviewer for the campaign.
Allow Redirection	If checked, approvals and revocations can be redirected to another reviewer
Escalation to Supervisor	If checked, approvals and revocations can be escalated to the supervisor of the campaign.
Exclusion list	Defines a list of reviewers that are excluded from the campaign. If enabled, you can use Add and Remove to define the reviewer list.

Fulfillment Detail	Description
Logical deletion	If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are deleted but only logically.
Physical deletion	<p>If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are physically deleted, after a grace period if provided. Before the end of this period, data is available for any usage. For an immediate deletion, set Grace period=0.</p> <p>Campaigns on Account have the following options:</p> <ul style="list-style-type: none"> • Delete the Account • Lock the Account
Physical deletion after workflow	If this option is selected, the entities-joins are deleted after a specified workflow, which is identified through the setting of <i>name Process - name Activity</i> .
Custom Behaviour	The management of the fulfillment involves a set of rules.

Table 48. Cert_Campaign_Scheduling_Tab

Scheduling Detail	Description
Activate On	<p>Start date If checked, enables the workflow processes to define the frequency and length of the campaign.</p> <p>Duration The following values are available:</p> <ul style="list-style-type: none"> • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year • Continuous (never closed)


Table 48. Cert_Campaign_Scheduling_Tab (continued)

Scheduling Detail	Description
Execution Frequency	<p>The following values are available:</p> <ul style="list-style-type: none"> • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year • One time <p>The set of values is bounded according to the Duration parameter. If Duration=Continuous, you cannot set values for this parameter.</p>
Time Kept In History (Days)	Number of days to maintain the campaign data in the history.



Notification Type	Description
Campaign Started for Reviewer	<p>If Enable is set, the reviewer receives an email when the campaign begins.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information about the campaign.</p>
Activity Reminder for Reviewer	<p>If Enable is set, the reviewer receives an email at the following times.</p> <ul style="list-style-type: none"> • <i>K</i> days before the end of the campaign. Determined by Days before end date, where <i>K</i> is a value 0 - 32. • When the percentage of activity that is already managed is greater than <i>X</i>%. Determined by Activity percentage <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>
Campaign Reminder for Reviewer	<p>If Enable is set, the reviewer receives an email <i>K days</i> before the end of the campaign. Determined by Days before end date, where <i>K</i> is a value 0 - 32.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>
Campaign Reminder for Supervisor	<p>If Enable is set, the supervisor receives an email <i>K days</i> before the end of the campaign. Determined by Days before end date, <i>K</i> is a value 0 - 32.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>
Continuous Review for Reviewer	<p>If Enable is set, the reviewer receives an email when a continuous campaign begins.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>


Notification Type	Description
Redirect	<p>If Enable is set, the reviewer or supervisor receives an email in response to any action of redirection.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>

To search a specific *Reviewer*, set the filters in the following table by clicking **Filter/Hide Filter**:


Reviewer filters	
Filter	Description
Identity	This field can host the name, the surname, or the user ID of the user.
Org Unit	Use  OU on the right side of the attribute to enter an OU.
Hierarchy	If this box is selected, the search activity is on all the hierarchy. It starts from the root OU in Org Unit .

Results are displayed in the same frame by the following attributes:

Reviewer details	
Detail	Description
Action	<p> Stats monitors the status of the campaign completion.</p> <p> Inspect inspects the entities of the campaign.</p>
User ID	Univocal identifier of the reviewer.
Name	Name of the reviewer
Surname	Surname of the reviewer.
OU Name [Code]	Name of the Org. Unit the Reviewer belongs to.
% Entity Completion	Percentage of the Entities certified.

Clicking  **Stats** displays the **Total items** and **Signed Off items** pie charts in the Stats window so you can monitor campaign completion status.

If the campaign sign-off is **By User** or **Automatic** mode, the No data to display message is under **Signed Off Items**.

By clicking  **Inspect**, the supervisor can view the approved or removed campaigns.

Details for Supervisor - Entitlement

After you select the campaign, the **Details** tab displays information about it and about the activities of the reviewers in the campaign.

In the upper part of the frame, the information about the campaign is available. It is summarized in the following table:

Supervisor Campaign	
Details	Description
Campaign Name (link)	Name of the campaign.
Start Date	Start date of the campaign.
Sign Off	Validation mode for approval or revocation actions: <ul style="list-style-type: none"> • Automatic: the approval or revocation is immediately signed off • By User: the user decides when to sign off the approval or revocation • End Campaign: the approval or revocation is signed off at the end of the campaign.
Campaign Type	Type of the campaign.
End Date	End date of the campaign.
% Completion	Percentage of the entities certified.

Clicking **Campaign: Campaign Name** in the upper right part of the frame displays the following information in Campaign Info:

Campaign Detail	Description
Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Supervisors of the campaign (at least 1 supervisor).
Campaign Type	Type of campaign. <ul style="list-style-type: none"> • Entitlement • User assignment • Entitlement/OU visibility • Risk violation mitigation
Certification Dataset	Name of the data set that is built to feed or to start the campaign.
Exclude Reviewed Since	If this check box is selected, the entities that were reviewed during the specified time are excluded by revision activity: <ul style="list-style-type: none"> • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year
Notes Revocation (Mandatory)	If this check box is selected, the reviewer is required to specify notes for any revocation.
Allow Bulk Operations	If this check box is selected, the reviewer can use special commands for bulk approval/revocation actions.

Campaign Detail	Description
Sign Off	Type of sign-off. <ul style="list-style-type: none"> • Automatic • Completed By User • End campaign
Activity Details	Attributes for an active campaign. <ul style="list-style-type: none"> • Start Date • End Date • Reviewers Signed Off/Total Reviewers K/N • <i>Entity</i> User Signed Off / Total <i>Entity</i> H/M Users • Working Progress J/TOT-M <ul style="list-style-type: none"> – N is the maximum number of reviewers – M is the maximum number of entities – TOT is the total number of pairs OU-Entitlement or User-Entitlement or User-Risk, depending on the campaign type

Table 49. Cert_Campaign_Reviewer_Tab

Reviewer Detail	Description
Scope	<p>User Hierarchy If enabled, shows the available user hierarchy scope. It is always available for organizational units.</p> <p>Entity If enabled, shows the entity scope.</p>
Default Reviewer	The default reviewer for the campaign.
Allow Redirection	If checked, approvals and revocations can be redirected to another reviewer
Escalation to Supervisor	If checked, approvals and revocations can be escalated to the supervisor of the campaign.
Exclusion list	Defines a list of reviewers that are excluded from the campaign. If enabled, you can use Add and Remove to define the reviewer list.

Fulfillment Detail	Description
Logical deletion	If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are deleted but only logically.
Physical deletion	<p>If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are physically deleted, after a grace period if provided. Before the end of this period, data is available for any usage. For an immediate deletion, set Grace period=0.</p> <p>Campaigns on Account have the following options:</p> <ul style="list-style-type: none"> • Delete the Account • Lock the Account
Physical deletion after workflow	If this option is selected, the entities-joins are deleted after a specified workflow, which is identified through the setting of <i>name Process - name Activity</i> .
Custom Behaviour	The management of the fulfillment involves a set of rules.


Table 50. Cert_Campaign_Scheduling_Tab

Scheduling Detail	Description
Activate On	<p>Start date If checked, enables the workflow processes to define the frequency and length of the campaign.</p> <p>Duration The following values are available:</p> <ul style="list-style-type: none"> • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year • Continuous (never closed)
Execution Frequency	<p>The following values are available:</p> <ul style="list-style-type: none"> • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year • One time <p>The set of values is bounded according to the Duration parameter. If Duration=Continuous, you cannot set values for this parameter.</p>
Time Kept In History (Days)	Number of days to maintain the campaign data in the history.



Notification Type	Description
Campaign Started for Reviewer	<p>If Enable is set, the reviewer receives an email when the campaign begins.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information about the campaign.</p>
Activity Reminder for Reviewer	<p>If Enable is set, the reviewer receives an email at the following times:</p> <ul style="list-style-type: none"> • <i>K</i> days before the end of the campaign. Determined by Days before end date, where <i>K</i> is a value 0 - 32. • When the percentage of activity that is already managed is greater than <i>X</i>%. Determined by Activity percentage <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>
Campaign Reminder for Reviewer	<p>If Enable is set, the reviewer receives an email <i>K days</i> before the end of the campaign. Determined by Days before end date, where <i>K</i> is a value 0 - 32.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>


Notification Type	Description
Campaign Reminder for Supervisor	<p>If Enable is set, the supervisor receives an email <i>K days</i> before the end of the campaign. Determined by Days before end date, <i>K</i> is a value 0 - 32.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>
Continuous Review for Reviewer	<p>If Enable is set, the reviewer receives an email when a continuous campaign begins.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>
Redirect	<p>If Enable is set, the reviewer or supervisor receives an email in response to any action of redirection.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>

To search a specific reviewer, set the filters from the following table by clicking **Filter/Hide Filter**:


Reviewer filters	
Filter	Description
Identity	This field can host the Name , the Surname , or the User ID of the user.
Org Unit	Use  OU on the right side of the attribute's box to enter an OU.
Hierarchy	If this check box is ticked, the search activity is for all the hierarchy. It starts from root OU that is indicated Org Unit .

Results are displayed in the same frame according to the following attributes:

Reviewer details	
Detail	Description
Action	 Stats monitors the status of the campaign completion.  Inspect inspects the entities of the campaign.
Master UID	Univocal identifier of the reviewer.
Name	Name of the reviewer.
Last Name	Surname of the reviewer.
OU Name [Code]	Name of the reviewers organizational unit.
% Entity Completion	Percentage of the Entities certified.

Clicking  **Stats** displays the **Total items** and **Signed Off items** pie charts in the Stats window so you can monitor the campaign completion status.

If **Sign off** is set to **By User** or **Automatic**, the No data to display message is under **Signed Off**.

By clicking  **Inspect**, the Supervisor can view approved or removed *Entities*.

Details for Supervisor - Accounts

Details provides information about the selected campaign and its activities.

The upper part of the frame provides information about the campaign, which is summarized in the following table:

Supervisor Campaign	
Details	Description
Campaign Name (link)	Name of the campaign.
Start Date	Start date of the campaign.
Sign Off	Validation mode for approval or revocation: Automatic The approval or revocation is immediately signed off. By User The user decides when to sign off the approval or revocation. End Campaign The approval or revocation is signed off at the end of the campaign.
Campaign Type	Type of campaign.
End Date	End date of the campaign.
% Completion	Percentage of certified entities.

Clicking **Campaign: Campaign Name** in the upper right part of the frame displays the Campaign Info window. The information is summarized in following tabs:

Campaign Detail	Description
Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Supervisors of the campaign (at least 1 supervisor).
Campaign Type	Type of campaign. <ul style="list-style-type: none"> • Entitlement • User assignment • Entitlement/OU visibility • Risk violation mitigation
Certification Dataset	Name of the data set that is built to feed or to start the campaign.

Campaign Detail	Description
Exclude Reviewed Since	If this check box is selected, the entities that were reviewed during the specified time are excluded by revision activity: <ul style="list-style-type: none"> • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year
Notes Revocation (Mandatory)	If this check box is selected, the reviewer is required to specify notes for any revocation.
Allow Bulk Operations	If this check box is selected, the reviewer can use special commands for bulk approval/revocation actions.
Sign Off	Type of sign-off. <ul style="list-style-type: none"> • Automatic • Completed By User • End campaign
Activity Details	Attributes for an active campaign. <ul style="list-style-type: none"> • Start Date • End Date • Reviewers Signed Off/Total Reviewers K/N • <i>Entity</i> User Signed Off / Total <i>Entity</i> H/M Users • Working Progress J/TOT-M <ul style="list-style-type: none"> – N is the maximum number of reviewers – M is the maximum number of entities – TOT is the total number of pairs OU-Entitlement or User-Entitlement or User-Risk, depending on the campaign type

Table 51. Cert_Campaign_Reviewer_Tab

Reviewer Detail	Description
Scope	<p>User Hierarchy If enabled, shows the available user hierarchy scope. It is always available for organizational units.</p> <p>Entity If enabled, shows the entity scope.</p>
Default Reviewer	The default reviewer for the campaign.
Allow Redirection	If checked, approvals and revocations can be redirected to another reviewer
Escalation to Supervisor	If checked, approvals and revocations can be escalated to the supervisor of the campaign.
Exclusion list	Defines a list of reviewers that are excluded from the campaign. If enabled, you can use Add and Remove to define the reviewer list.

Fulfillment Detail	Description
Logical deletion	If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are deleted but only logically.

Fulfillment Detail	Description
Physical deletion	<p>If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are physically deleted, after a grace period if provided. Before the end of this period, data is available for any usage. For an immediate deletion, set Grace period=0.</p> <p>Campaigns on Account have the following options:</p> <ul style="list-style-type: none"> • Delete the Account • Lock the Account
Physical deletion after workflow	<p>If this option is selected, the entities-joins are deleted after a specified workflow, which is identified through the setting of <i>name Process - name Activity</i>.</p>
Custom Behaviour	<p>The management of the fulfillment involves a set of rules.</p>

Table 52. Cert_Campaign_Scheduling_Tab

Scheduling Detail	Description
Activate On	<p>Start date If checked, enables the workflow processes to define the frequency and length of the campaign.</p> <p>Duration The following values are available:</p> <ul style="list-style-type: none"> • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year • Continuous (never closed)
Execution Frequency	<p>The following values are available:</p> <ul style="list-style-type: none"> • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year • One time <p>The set of values is bounded according to the Duration parameter. If Duration=Continuous, you cannot set values for this parameter.</p>
Time Kept In History (Days)	<p>Number of days to maintain the campaign data in the history.</p>



Notification Type	Description
Campaign Started for Reviewer	<p>If Enable is set, the reviewer receives an email when the campaign begins.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information about the campaign.</p>


Notification Type	Description
Activity Reminder for Reviewer	<p>If Enable is set, the reviewer receives an email at the following times.</p> <ul style="list-style-type: none"> • <i>K</i> days before the end of the campaign. Determined by Days before end date, where <i>K</i> is a value 0 - 32. • When the percentage of activity that is already managed is greater than <i>X</i>%. Determined by Activity percentage <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>
Campaign Reminder for Reviewer	<p>If Enable is set, the reviewer receives an email <i>K days</i> before the end of the campaign. Determined by Days before end date, where <i>K</i> is a value 0 - 32.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>
Campaign Reminder for Supervisor	<p>If Enable is set, the supervisor receives an email <i>K days</i> before the end of the campaign. Determined by Days before end date, <i>K</i> is a value 0 - 32.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>
Continuous Review for Reviewer	<p>If Enable is set, the reviewer receives an email when a continuous campaign begins.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>
Redirect	<p>If Enable is set, the reviewer or supervisor receives an email in response to any action of redirection.</p> <p>The email is constructed according to Email template.</p> <p>If Include campaign details is set, the mail includes additional information on the campaign.</p>

To search a specific Reviewer, set the filters shown in the following table by clicking **Filter/Hide Filter**:


Reviewer filters	
Filter	Description
Identity	Shows the Name , the Surname , or the User ID of the user.
Org Unit	Use <input type="text" value="..."/> OU on the right side of the attribute to enter an OU .
Hierarchy	If selected, the search activity is on the hierarchy, which starts from root OU in Org Unit .

Results are displayed in the same frame by the following attributes:

Reviewer details	
Detail	Description
Action	 Stats monitors the status of the campaign completion.  Inspect inspects the entities of the campaign.
Master UID	Univocal identifier of the Reviewer.
Name	Name of the reviewer.
Last Name	Surname of the reviewer.
OU Name [Code]	Name of the organizational unit of the reviewer
% Entity Completion	Percentage of the Entities certified.

Clicking  **Stats** displays the Stats window with the **Total items** and **Signed Off items** pie charts for campaign completion status monitoring:

If **Sign off** is set to **By User or Automatic**, No data to display is under **Signed Off items**.

By clicking  **Inspect**, the Supervisor can view approved or removed entities.

Chapter 5. Introduction to User-account matching

User-account matching is the module that is dedicated to managing orphan accounts that are currently not matched with company policies.

The User-account matching user can do the following tasks:

- Join orphan accounts with users
- Decouple users and accounts

Dashboard

In this section you can browse a number of Matching Dashboards, one for every target (application or external system) engaged. For example:

Matching Dashboard



Figure 1. Application Accounts: Matching Dashboard

Every Matching Dashboard shows:

Unmatched

The number of accounts that, after the synchronization with the target system, are found not to match with company policies.

Orphan

The number of accounts that are not assigned to any user.

Identity Matched

The number of accounts that were assigned to a user by the action of the logged-in user.

Each of these numbers is shown over the total number of accounts retrieved from the target.


To browse the details of the accounts charted, click **Manage** in the Dashboard you are viewing.

You can use the following filters to search for specific accounts (after clicking **Filter**).

Table 53. User filters

Filter	Description
Application UID	The univocal identifier of the application.

Table 53. User filters (continued)

Filter	Description
Status	The status of the account. It can be: <ul style="list-style-type: none"> • Unmatched • Orphan • Identity Matched
Master UID	The univocal identifier of the user to whom the account is assigned.
Organization Unit	The organization unit associated with the account. Use the  OU button to enter an OU.
Hierarchy	Flag this checkbox to specify that the search is to be made on the entire organizational hierarchy starting from the root OU specified in the OU field.

Note: The filters **Master UID - Organization Unit - Hierarchy** are enabled **ONLY IF** the filter **Status** is set to the value **Identity Matched**

The following details are displayed:

Table 54. User/Account attributes

Attribute	Description
Application UID	The univocal identifier of the application.
Status	The status of the account. It can be: <ul style="list-style-type: none"> • Unmatched • Orphan • Identity Matched
Master UID	The univocal identifier of the user to whom the account is assigned.
Name	The first name of the user to whom the account is assigned.
Surname	The last name of the user to whom the account is assigned.
Email	The email address of the user to whom the account is assigned.
Distinguished Name	The Distinguished Name of the user to whom the account is assigned.
Display Name	The complete name of the application.
Identity UID	An additional univocal identifier of the user to whom the account is assigned.

The **Actions** menu includes the following actions on an account selected from the list:

Permissions

Shows a list of permissions related to the account. If the target is an external system, it displays a list of the latest operations/events involving permissions on the target. This action is not available for matched accounts.

Orphan

Switches a matched account to the **Orphan** status. In other words, removes the association between the account and the user.

Match Switches an **Orphan** or **Unmatched** account to the **Identity Matched** status. It displays the Match User window where you can select a user from the associated OU.

If the user you select has already an account on the application, another window asks if you want to create a secondary account (UME).

Details

Displays the User Details window with system and personal data of the user associated with the account. This action is not available for unmatched accounts.

Click the **Dashboard** tab to return from the detailed view of an application to the general view.

Chapter 6. Introduction to Access Requests

Access Requests (AR) is the module dedicated to running authorization processes.

In the Process Designer (PD) module, the IBM Security Identity Governance and Intelligence administrator defines workflows that implement customized sequences of activities that build authorization flows.

These authorization flows are then managed with Access Requests to assign operating permissions, such as business roles/IT roles/permissions/rights) to the users registered on the system.

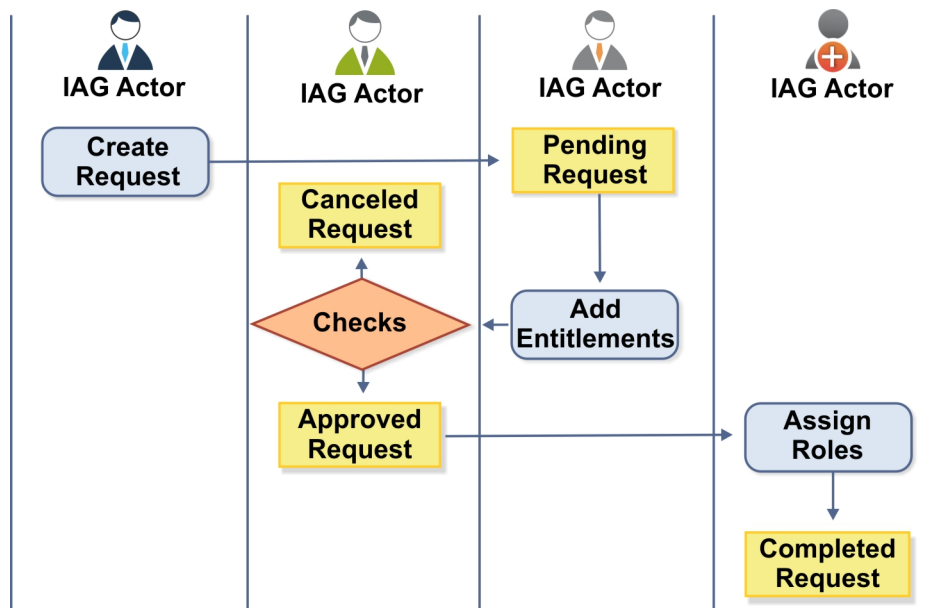


Figure 2. Example of authorization workflow

Access Requests directly communicates with Access Governance Core to execute the assignment/revocation of roles and the propagation of permissions on the target systems.

Access Requests provides the following functions:

- Create user entities
- Manage user accounts (Suspend/Restore account and reset password)
- Assign permissions to users
- Manage the assignment of administration roles
- Manage role delegation

ARM Requests Status

The requests that are generated during the authorization workflow activities can be characterized by various statuses.

They are summarized in the following table:

Table 55. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Rejected	Request can no longer be processed. It is a final status for the request.
In execution	Request waiting for the propagation to the target system.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Pending	Source request is waiting for formalization by one or more approvers.
Escalation	Request contains incompatible roles.
Partially Authorized	Request with some sub requests in authorizable status.
Partially Approved	Request with some sub requests in Approved status.
Partially Executed	Request with some sub requests in executed status.
Partially Completed	Request with all sub requests at end of their lifecycle, some Completed and some in Failed Completion status.
Partially Terminated	Request with some sub requests in Completed and some in progress.
Terminated With Reservation	In this status falls all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request can be split in several sub requests. Every sub request can be characterized by several statuses.

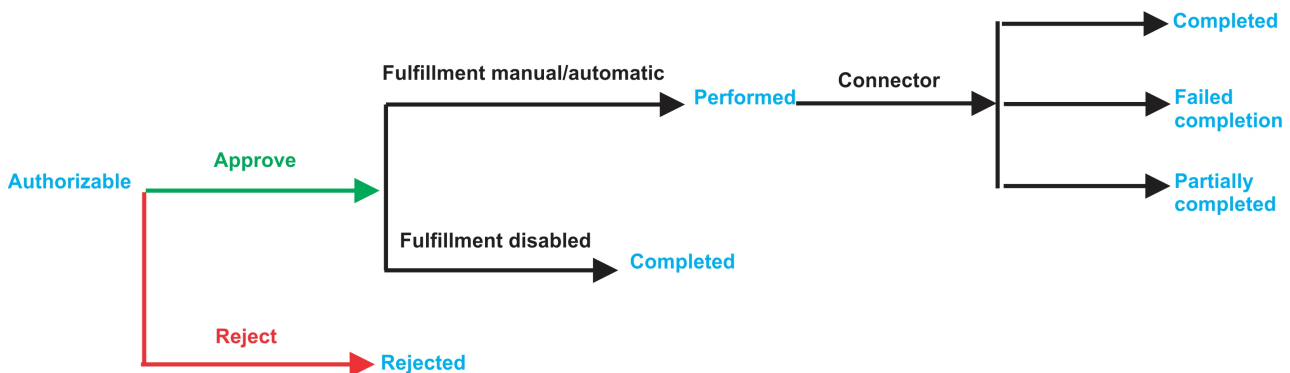


Figure 3. Statuses of a Sub Request

Statuses of a Sub Request	
Status	Description
Rejected	The sub request was rejected by the approver, and it is not fulfilled.
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Manual/Automatic, it means that the connector successfully aligned every permission on the target system.
Performed	The connector did not yet align the permissions on the target system.
Failed Completion	The connector failed to align all permission on the target system.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.

AR functions

Access Requests Manager provides several functions.

This module provides the following set of functions:

- “Generating a request to make account changes: selecting the user” on page 72
- “Authorizing an account change request” on page 76
- “Executing a request of Account change” on page 83
- “Admin Roles: generating a request” on page 88
- “Admin Roles: processing a request” on page 95
- “Admin Roles: executing a request” on page 102
- “Admin delegation: generating a request” on page 108
- “Admin delegation: processing a request” on page 108
- “Admin delegation: executing a request” on page 108
- “My daily work: list of requests” on page 114
- “List of all requests present in the system” on page 168
- “Delegation: generating a request” on page 120
- “Delegation: processing a request” on page 126
- “Delegation: executing a request” on page 133
- “Insert/Update entitlement: generating a request” on page 142
- “Insert/Update entitlement: processing a request” on page 155
- “Insert/Updates entitlements: executing a request” on page 163
- “User access: generating a request” on page 175
- “User access: processing a request” on page 185
- “User access: executing a request” on page 193
- “Create/Update user: generating a request” on page 198
- “Insert/Update user: processing a request” on page 200
- “Insert/Update user: executing a request” on page 208
- “Authorize escalation” on page 139

Generating a request to make account changes: selecting the user

Use this tab to generate a request to reset a user password or to suspend or restore a user account.

This tab starts a wizard that leads you through the steps of a work flow to generate the following types of requests:

- Reset the password of users who forgot their password and are unable to change it. Pre-configured wizards for the User manager and Help Desk administrative roles help you with the process.
- Suspend or restore the account of a selected user.

The Identity Governance and Intelligence Administrator can create similar work flows that respond to other business requirements.


The **User** tab is the first step of the wizard. You select the user on whose password or account you are about to act. You can use filters to search for specific users. The following filters area available:

Table 56. User filters

Filter	Description
User Type	Type of user, for example, Administrative, Business, Employee, Training, External
Full Name/Code	Name and surname of the user or unique identifier of the user
Enabled	When selected, specifiesA flag implies that the user can be assigned entitlements.

Users are displayed in a table that shows the following attributes:

Table 57. Users list.

Field	Description
User details icon	Click the  Info icon to open the User Details window that shows the user's details, assigned entitlements, and assigned accounts.
User ID	Unique identifier of the user.
First Name	Name of the user.
Last Name	Surname of the user.
Group [Code]	Organization Unit [Univocal identifier of the OU] of the user.
User Type	Type of user (for example: Administrative, Business, Employee, Training, External).

To select a user, click a row.



Click  **Info** to show the Details window. The window includes several tabs. Some of the tabs might be present depending on the properties defined for the user:

Table 58. User Information tabs

Tab	Description
Details	User information, including ID, type, organization, name, and address. This tab is always present.
External Data	Information taken from the User Virtual Attributes mapped from external databases in Access Governance Core.
Entitlements	A list of the entitlements assigned to this user. For every entitlement you can click the  Info icon to display more information on the entitlement, its structure, the permissions that compose it, and the list of users and groups entitled to it.
Accounts	The list of accounts that this user can access. This tab is always present. Every user defined in Identity Governance and Intelligence must have access to at least the Ideas account.
Activities	Activities for the user. Activity access is based on assigned rights and entitlements. Click an activity to display a tree view of the hierarchical sequence.
Rights	A list of the rights assigned to this user.

After you select a user, click **Next**. Depending on the configuration of the work flow, this button opens the Security Questions or the Accounts window.

Related tasks:

“Resetting account passwords for other users” on page 6

If you are a manager, or someone entitled with a role that includes this activity, you can change the account passwords for users in the Service Center.

Generating a request to make account changes: answering security questions

Use this step in the wizard to verify the identity of the user who requested a password reset.

This window displays security questions to use to verify the identity of the beneficiary of the password reset. The items available depend on the choices for questions made by the Identity Governance and Intelligence administrator.

The window displays a number of security questions. A number specifies how many attempts the beneficiary is allowed to make before the account is locked.

A typical scenario for this work flow is one in which you get the answers from the beneficiary and enter them in this window in the user's place.

If the work flow configuration allows, you can also select the **Identified by other means** check box.

Click **Next** to proceed to the Accounts window.

Related tasks:

“Resetting account passwords for other users” on page 6

If you are a manager, or someone entitled with a role that includes this activity, you can change the account passwords for users in the Service Center.



Generating a request to make account changes: selecting the accounts


This step in the wizard is where you select the accounts to work on.

You can perform one of the following actions:

Suspend or restore access of the beneficiary to one or more accounts

The upper part of the window summarizes information on the selected user and provides an entry field for adding request notes.

The rest of the window lists the accounts that the user is entitled to access. Each row corresponds to an account. The  icon means the account is unlocked. The  icon means the account is locked.

You can click on  to view the list of applications associated with the account. Click **Close** to return to the account summary row.

Every account summary row includes a number of check boxes that describe a reason for suspending the access of this user to the account. If the account is unlocked, the check boxes are clear. If the account is locked, one or more check boxes are selected. The check boxes are:

Tech. Suspend

Access suspended for technical reasons

Sec. Suspend

Access suspended for security reasons

Terminated

Access suspended permanently

Auth. Suspend

Access suspended because of authorization conflicts

Expired

The expiration date defined for user was reached

Maint. Suspend

Access is suspended because the account is under maintenance



After you select the entire account, you can take action on the account.

- Select one or more of the check boxes to suspend the user's access to the account or applications selected
- Clear the flagged check boxes to restore the user's access to the account or applications selected

Click **Submit** at the bottom to complete your account suspension/restoration request for the beneficiary.

Provide a new password for the beneficiary to access one or more accounts

The upper part of the window provides information on the user you selected as the beneficiary of your password reset action.

The rest of the window lists the accounts that the user is entitled to access. Each row corresponds to an account. The  symbol means the account is unlocked. The  symbol means the account is locked.

Select the check box in the title bar to select all the accounts listed or select the check box in account summary rows to select specific accounts. When you reset the password in the next step, the new password takes effect.

Click **Next** to proceed to the next step.

Related tasks:

“Resetting account passwords for other users” on page 6

If you are a manager, or someone entitled with a role that includes this activity, you can change the account passwords for users in the Service Center.


Generating a request to make account changes: entering the new password

This final step of the wizard guides you to reset the password.

After you selected the user for this action, verified his/her identity, and selected the accounts to which the new password is to grant access, you are now in the Account Password Management window where you add the new password.

The appearance of the left portion of this window changes based on the configuration options chosen by the Identity Governance and Intelligence administrator for this type of request. This part of this window features the following items:

- **Applicant** section that includes a field named **Your Password** where you are prompted to enter your own password. This box is present if the Administrator configured the request so that your own identity is verified.
- **Beneficiary** section that includes the following items:
 - **New Password** and **Confirm Password** fields.
You might see a **Generate** button on the right side of these fields. You must click this button to have the password generated automatically. If this button is not present, you are required to enter the new password. The password characters you type are hidden. A **Show password characters** check box might be provided to let you view the password you are typing.
 - A **New password will be sent to this email address** field. This field is not shown if the new password is to be communicated to the beneficiary by other means.
If the field is present, you might enter or update the beneficiary's email address.

The right pane shows a checklist of syntax requirements for the new password. If you are entering the password manually, you see green check marks in the list become  if the requirements are ignored.

Click **Submit** to complete the request process. Normally requests for a password reset are complete at this point.

The work flows provided with the product for password reset do complete here. Click the **Request Report** tab to view information about your request, including type of request, the names of the applicant and of the beneficiary, and other information. The status of the request is declared to be completed.

If the work flow is configured to require authorization and other steps, the request is completed after those steps are carried out.

Related tasks:

“Resetting account passwords for other users” on page 6

If you are a manager, or someone entitled with a role that includes this activity, you can change the account passwords for users in the Service Center.

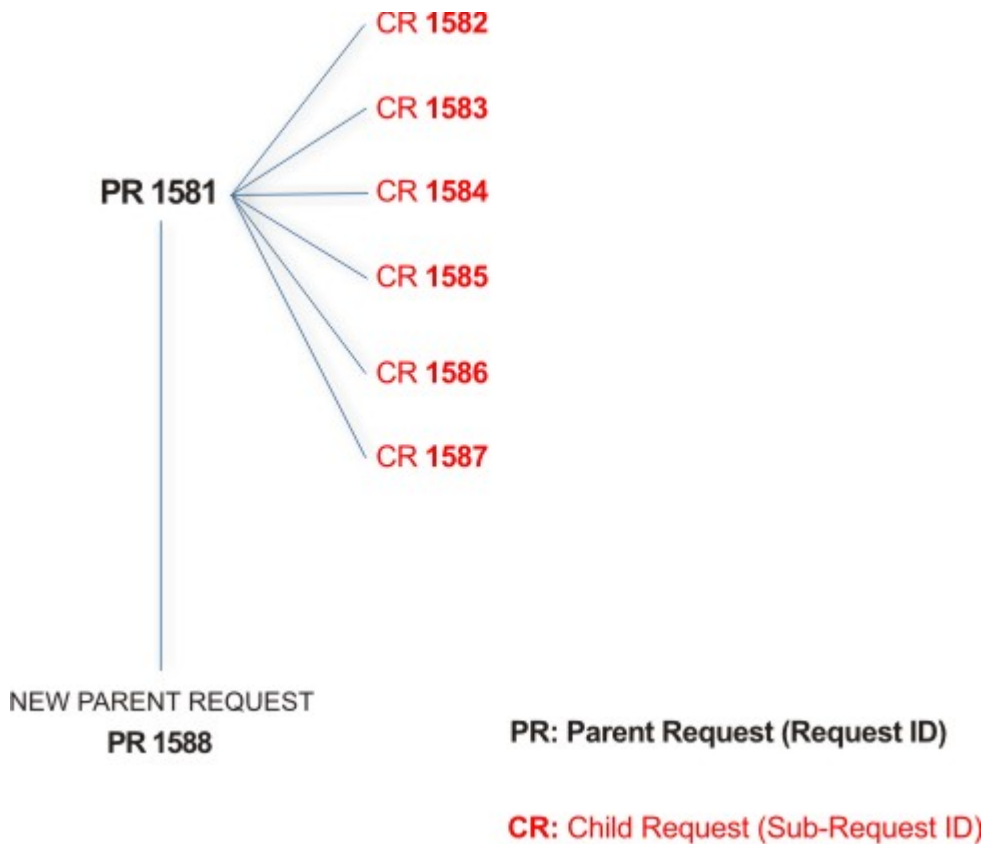
Authorizing an account change request

Authorizing an account change request.

You can view a summary of the generated requests. You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is in black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Requests** and are in red.



In the previous example, **Request ID 1581**, generates six **Sub-Requests**: 1582, 1583, ... and 1587.

There is ALWAYS the possibility to view ALL the requests registered through the REQUEST REPORT EXE activity.

However, when you are logged-in as authorizer, some of the request (and sub-request) listed through the REQUEST REPORT EXE might not be visible because out of the scope defined for the authorizer.

The requests that are generated during the authorization process can be characterized by different statuses, which are summarized in the following table:

Table 59. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Rejected	Request can no longer be processed. It is a final status for the request.
In execution	Request waiting for the propagation to the target system.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Pending	Source request is waiting for formalization by one or more approvers.
Escalation	Request contains incompatible roles.
Partially Authorized	Request with some sub requests in authorizable status.
Partially Approved	Request with some sub requests in Approved status.
Partially Executed	Request with some sub requests in executed status.
Partially Completed	Request with all sub requests at end of their lifecycle, some Completed and some in Failed Completion status.
Partially Terminated	Request with some sub requests in Completed and some in progress.
Terminated With Reservation	In this status falls all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request can be split in several sub requests. Every sub request can be characterized by several statuses.

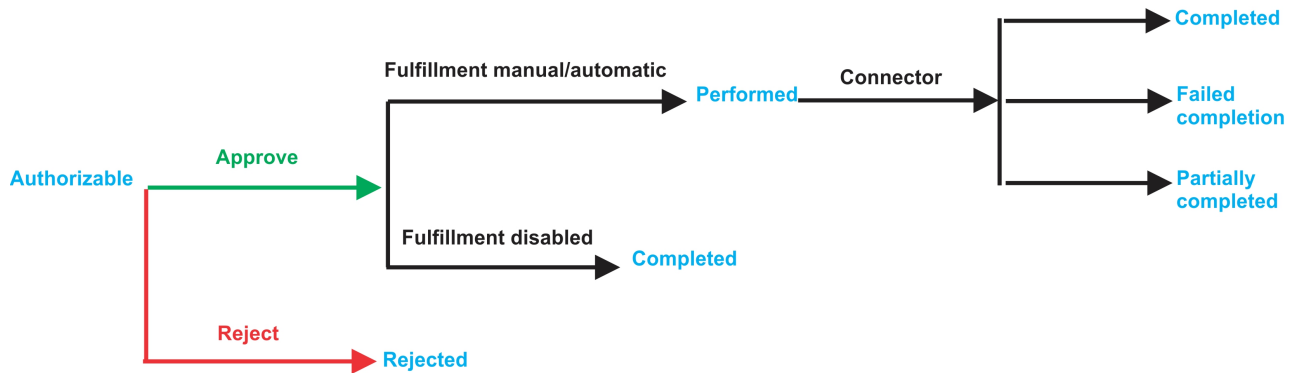


Figure 4. Statuses of a Sub Request

Statuses of a Sub Request	
Status	Description
Rejected	The sub request was rejected by the approver, and it is not fulfilled.

Statuses of a Sub Request	
Status	Description
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Manual/Automatic, it means that the connector successfully aligned every permission on the target system.
Performed	The connector did not yet align the permissions on the target system.
Failed Completion	The connector failed to align all permission on the target system.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.

You can search specific requests with the following filters. Click **Filter/Hide Filter** and then click **Search**.

Table 60. Filters

Filter		Description
Request ID		Unique identifier of the request
Sub Request ID		A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity		Identifier of the IAG actor that generated the request
Beneficiary Identity		Identifier of the beneficiary of the request
Created between	Start Date	Start date of the creation of the request
	End Date	End date of the creation of the request

The results are displayed in the same frame, according to the following attributes:

Requests attributes	
Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (dd/mm/yyyy) and hour (hh:mm) the request was created.
Status	Request Status.

Click **Applicant** and **Beneficiary** to open the User details window and show the following information:

Table 61. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs


Table 61. User Details - Details tab (continued)

Detail	Description
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the frame shows the following information about the **Actors of the Request**:

Table 62. Request Actors

Actor	Detail	Description
Request	ID	Unique identifier of the request
	Type	Type of request
	Status	Status of the Request
	Created on	Date (dd/mm/yyyy) and hour (hh/mm) that the request was created
Applicant/ Beneficiary/ Delegator/	Group	Group of the Applicant/Beneficiary/Delegator
	First Name	Given name of the Applicant/Beneficiary/Delegator
	Last Name	Surname of the Applicant/Beneficiary/Delegator
	User ID	Unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.
Request Notes	Request	Type of request
	to Add	Notes about the add action that was made on the <i>Entity</i> of the request
	to Remove	Notes about the remove action that was made on the <i>Entity</i> of the request
	to Update	Notes about the update action that was made on the <i>Entity</i> of the request
Additional Notes	Request notes can be specified by the author of the request or by a rule. In this field, you can add free text for any reason during the authorization or execution of the request.	

Note: The Request Notes are not mandatory. If there are no notes in the request, the fields of the Request Notes are blank.


Click the  **Info** icon to open the User details window and show the information in a set of tabs:

Table 63. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 64. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement info window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation

Table 65. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 66. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree

Table 66. User Details - Activities tab (continued)


Detail	Description
Description	Brief description of the activity


Table 67. User Details - Rights

Detail	Description
Entitlement	Name of the entitlement
Right	Name of the right
Values	Value of the right

The lower part of the frame shows the following information about the requests:

Table 68. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlement involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the  **Info** icon to open the Entitlement info window and show the summarized information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 69. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement

Table 69. Entitlement info - Structure (continued)

Detail	Description
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.


Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles
- External Roles
- Permissions

The following icons represent these entitlements:



If notes about the considered entitlement are in the request, the  **Note** icon is available. Click it to open the Notes window and show the contents of the note.

In the central side of the frame, you find:

- Elements related to the request to be authorized.
- Elements related to the approver of the request.

In the lower side of the frame, the available buttons are:

- **Back** returns to the summary of the requests.
- **Approve** approves the request.
- **Reject** rejects a request.

Executing a request of Account change

You may get requests to reset a password for a user, suspend an account, restore an account, or other actions.

Account Change requests might include an execution step. Based on the process setup, this step might be executed:

- Automatically through a connector
- Manually

Every request in the list displays two identification numbers:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, in black, is the parent request. Parent requests can have one or more **Sub-Requests** in red.

Depending on how the Account Change process is configured, a request has a Request Status from the following list:

Table 70. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Rejected	Request can no longer be processed. It is a final status for the request.
In execution	Request waiting for the propagation to the target system.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Pending	Source request is waiting for formalization by one or more approvers.
Escalation	Request contains incompatible roles.
Partially Authorized	Request with some sub requests in authorizable status.
Partially Approved	Request with some sub requests in Approved status.
Partially Executed	Request with some sub requests in executed status.
Partially Completed	Request with all sub requests at end of their lifecycle, some Completed and some in Failed Completion status.
Partially Terminated	Request with some sub requests in Completed and some in progress.
Terminated With Reservation	In this status falls all the requests that present an unclear or unexpected behavior. It is a final status for the request.

You can search specific for requests with filters. Click **Filter/Hide Filter** and click **Search**.

Table 71. Filters

Filter		Description
Request ID		Unique identifier of the request
Sub Request ID		A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity		Identifier of the IAG actor that generated the request
Beneficiary Identity		Identifier of the beneficiary of the request
Created between	Start Date	Start date of the creation of the request
	End Date	End date of the creation of the request

Requests are displayed as follows:

Table 72. Request attributes

Attribute	Description
Request ID	Univocal identifier of the parent request
Sub-Request ID	Univocal identifier of the child request
Type	Type of request
Applicant	Name of the applicant of the request
Beneficiary	Name of the beneficiary of the request
Created on	Date (dd/mm/yyyy) and time (hh:mm) the request was created
Status	Request Status

Click **Applicant** or **Beneficiary** to open the User details window.

Table 73. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).


Table 73. User Details - Details tab (continued)

Detail	Description
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the frame shows information about the Request Actors:

Table 74. Request Actors

Actor	Detail	Description
Request	ID	Unique identifier of the request
	Type	Type of request
	Status	Status of the Request
	Created on	Date (dd/mm/yyyy) and hour (hh/mm) that the request was created
Applicant/ Beneficiary/ Delegator/	Group	Group of the Applicant/Beneficiary/Delegator
	First Name	Given name of the Applicant/Beneficiary/Delegator
	Last Name	Surname of the Applicant/Beneficiary/Delegator
	User ID	Unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.
Request Notes	Request	Type of request
	to Add	Notes about the add action that was made on the <i>Entity</i> of the request
	to Remove	Notes about the remove action that was made on the <i>Entity</i> of the request
	to Update	Notes about the update action that was made on the <i>Entity</i> of the request
Additional Notes	Request notes can be specified by the author of the request or by a rule. In this field, you can add free text for any reason during the authorization or execution of the request.	

Note: The Request Notes are not mandatory. If there are no notes in the request, the fields of the Request Notes are blank.

Click the  **Info** icon to open the User details window.

Table 75. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs

Table 75. User Details - Details tab (continued)

Detail	Description
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 76. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement info window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation

Table 77. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 78. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity

Table 79. User Details - Rights


Detail	Description
Entitlement	Name of the entitlement


Table 79. User Details - Rights (continued)

Detail	Description
Right	Name of the right
Values	Value of the right

The lower part of the frame shows additional request attributes.

Table 80. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlement involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy


Click the  **Info** icon to view the details of an entitlement. Information is displayed in a set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 81. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

If notes about the considered entitlement are in the request, the  **Note** icon is available. Click it to open the Notes window.

When you have finished processing a request, click the request and click **Execute** to mark the request as completed.

Admin Roles: generating a request

You can manage request for assigning the Administrative Roles.


The **Users** tab is the first step of the wizard. You can search and select users with the following filters. Click the **Filter/Hide Filter** and then click **Search**.

Table 82. User filters

Filter	Description
User Type	Type of user, for example, Administrative, Business, Employee, Training, External
Full Name/Code	Name and surname of the user or unique identifier of the user
Enabled	When selected, specifies a flag implies that the user can be assigned entitlements.

The results are according to the following attributes:

Table 83. Users list.

Field	Description
User details icon	Click the  Info icon to open the User Details window that shows the user's details, assigned entitlements, and assigned accounts.
User ID	Unique identifier of the user.
First Name	Name of the user.
Last Name	Surname of the user.
Group [Code]	Organization Unit [Univocal identifier of the OU] of the user.
User Type	Type of user (for example: Administrative, Business, Employee, Training, External).

To select the entire list of Users, select the check box on the attributes row; otherwise, select the check box that corresponds to the user row.


Click the  **Info** icon to open the User **details** window show the information in the following set of tabs:

Table 84. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).

Table 84. User Details - Details tab (continued)

Detail	Description
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 85. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement info window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation

Table 86. User Details - Accounts tab


Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 87. User Details - Rights

Detail	Description
Entitlement	Name of the entitlement
Right	Name of the right
Values	Value of the right

Table 88. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity

Click the  **Info** icon to open the Entitlement info window and show the summarized information in the following set of tabs:

- **Details**

- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 89. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

Click **Next** to open the Catalog tab.



This tab is the second step of the wizard.

Admin Roles: Catalog

The Catalog tab is the second step of the wizard.

From the **Catalog** tab you can choose the entitlements and roles for the users selected in the first step of the wizard, Users .

In the upper part of the frame is summarized the information about the selected users:

User data	
Data	Description
 Info	Click the Info icon to open the Entitlement info window.
First Name	Name of the user.
Last Name	Surname of the user.
User ID	Univocal identifier of the user.
Org. Unit [Code]	Name of the organizational unit and [Univocal identifier of the OU].
User Type	Type of user.
Risk Status 	Click the colored dot to open a window that displays: <ul style="list-style-type: none"> • The Risk Activities Tree (related to a specific user) into the Risk Info tab • The Activities involved in a specific risk, into the Mitigations tab

Click the **Refresh** button to update the risk situation of the user.

In the lower part of the frame is a set of tabs:

- **Current Entitlements**
- **Business Roles**
- **Application Roles**
- **Permissions**

According to the configuration of the Activity, some of these tabs might be not present.

Current Entitlements tab


In the **Current Entitlements** tab is the list of the entitlements of the user. From this tab you can search (click the **Filter/Hide Filter** button and click the **Search** button) a specific entitlement through the filters shown below:

Current Entitlements filters	
Filter	Description
Name	Name of the Entitlement.
Family	Family of the Entitlement.
Description	Brief description of the Entitlement.

From the list of Entitlements produced it is possible to **perform two types of operations**:

- **Remove** (Entitlement)
- **Validity** (End date of validity)

To remove the **Current Entitlements** click the **Remove** button (the **Remove** button will be shown in red).

To enter or change the **Validity** of the entitlements click the **Validity** button, the **Date Selection** window opens, click the  **Calendar** button to enter the end date and click **OK** to confirm. The **Validity** button will be highlighted in orange. To remove the end date click on the **Validity** button.



After the desired operations have been performed, click the **Business Roles** tab to assign Business Roles, or click the **Next** button to go to the “Admin Roles: Shopping Cart” on page 94 tab to process the request.

Business Roles tab

In the **Business Roles** tab is the list of available Business Roles (**BRoles**) for the selected user. From this tab you can search (click the **Filter/Hide Filter** button and click the **Search** button) a specific BRole through the filters shown below:

Current Entitlements filters	
Filter	Description
Name	Name of the Entitlement.
Family	Family of the Entitlement.
Description	Brief description of the Entitlement.

From the list of BRoles produced you can add one or more BRoles to the user, click the **Add** button (the **Add** button will be highlighted in green).

If the BRole added has **Dependencies**, the  **Dependencies** button appears, (between the  **Info** button in the BRoles list). Click it to open the **Dependencies** window to add one or more of these.

To add the Dependencies click on the **To Cart** button (the **To Cart** button will be highlighted in green) then click **Ok** to confirm.

Dependencies can be defined and associated with roles. Dependencies are permissions or roles that are necessary, or useful, to other roles.

For example, a role that is named TECHComm, with all the specific permissions for this position, is being defined for an employee who is to take a position as technical writer.

The technical writer reviews the draft documents that are produced by the Product Managers. They are shared in a company repository that is named DraftsOnProducts, which is a dedicated database, linked to a permission named DraftsOnProdcuts_Reader.

The DraftsOnProdcuts_Reader permission can be considered as a dependency of TECHComm.

The **Actions** menu includes the following items:

- **All Roles** Click to choose from the full set of available roles to assign to a selected user.
- **Like Mike** Click to assign to a selected User the same roles of another user that you choose from the full set of users.

Once the desired operations has been performed click on the **Applications Roles** tab to assign Applications Roles, or click on the **Next** button to go to the “Admin Roles: Shopping Cart” on page 94 tab to process the Request.

Applications Roles tab

In this section it is possible to assign the Applications Roles to the User .

In the **Applications Roles** tab, the **Applications** window opens by default, allows to choose a specific Application. From the list displayed, click on an Application to choose it; the **Applications Roles** are immediately displayed in the **Applications Roles** tab. To **exit** from this window, **close it**.

From this tab it is possible to search (clicking on the **Filter/Hide Filter** button) a specific Application also through the filters shown below:

Application Roles filters	
Filter	Description
Application	Name of the Application.
Family	Family of the Entitlement.

Application Roles filters	
Filter	Description
Name	Name of the Entitlement.
Description	Brief description of the Entitlement.

From the list of Roles produced it is possible to add one or more Roles to the User, clicking on the **Add** button (the **Add** button will be highlighted in green).

The **Actions** menu includes the following items:

- **All Roles** Click to choose from the full set of available roles to assign to a selected user.
- **Like Mike** Click to assign to a selected User the same roles of another user that you choose from the full set of users.

Once the desired operations has been performed click on the **Permissionstab** to assign Permissions, or click on the **Next** button to go to the “User Access: Shopping Cart” on page 183tab to process the Request.

Permissions tab

In this section it is possible to assign the Permissions to the User .

In the **Permissions** tab, the **Applications** window opens by default, allows to choose a specific Application. From the list displayed, click on an Application to choose it; the **Permissions** are immediately displayed in the **Permissions** tab. To **exit** from this window, **close it**.

From this tab it is possible to search (clicking on the **Filter/Hide Filter** button) a specific Application also through the filters shown below:

Permissions filters	
Filter	Description
Application	Name of the Application.
Permission Type	Type of Permission.
Name	Name of the Entitlement.
Description	Brief description of the Entitlement.

From the list of Permissions produced it is possible to add one or more Permissions to the User, clicking on the **Add** button (the **Add** button will be highlighted in green).

The **Actions** menu includes the following items:

- **All Roles** Click to choose from the full set of available roles to assign to a selected user.
- **Like Mike** Click to assign to a selected User the same roles of another user that you choose from the full set of users.

After the desired operations have been performed, click the **Next** button to go to the Shopping Cart tab to process the request.


This tab is the third step of the wizard.

Admin Roles: Shopping Cart


The **Shopping Cart** tab hosts a summary tree structure.

The **Operation** column lists the operations performed in the tabs under **Catalog**:

- **Add**
- **Remove**
- **Change** (is referred to the **Validity** change in the Current Entitlements tab)

When you select the  **Clear** button, the operation is revoked and is not taken into consideration when the Request is processed.

The **Application** column lists the names of the Applications of the Entitlements.

The **Name** column lists the Entitlements involved in the performed operation; if the Entitlement is a **Permission**, it may have one or more associated  **Rights** and it is possible to assign a **Value** to each right.

A Right is defined by two attributes: Key (*aaaa* in the example figure) and Value (*v1* in the example figure).


The Key attribute is an identifying name while the Value attribute can be defined each time. A configurable default value can be provided for the Value attribute.


Rights can be either of the following types:

- Single-value
- Single-value with lookup
- Multi-value
- Multi-value with lookup








A single-value Right with lookup allows to choose a single value V_x from a set of several values (V_1, V_2, \dots, V_N)


A multi-value Right with lookup allows to choose a subset of values (V_x, V_y, V_z, \dots) from a larger set of values (V_1, V_2, \dots, V_N).

When a Right is with Lookup, a  **Browse** button is available nearby. Click it to display the **Rights** window, where you can select values.

The presence of the  **Visibility Violation** icon in the **VV** column, denotes an Entitlement in Visibility Violation. An Entitlement is in VV when there is a special reason to assign an Entitlement to a User of that Organization Unit (OU), but you do not want the Entitlement to be available to the other users of the OU.

One or more of the following buttons are enabled for each entitlement: and displayed next to the VV column:

Buttons and Icons	
Button/Icon	Description
	Note: click this button to display the Notes window where you can write notes that will be annexed to the delegation.
	Validity: click this button to display the Date Selection window where you can enter the Start Date and the End Date of the delegation.
Buttons and Icons available only for the Admin Access Request	
	Application Scope: click this button to display the Resource Assign window where you can select one or more Applications to assign.
	Org.Units Scope: click this button to display the Resource Assign window where you can select one or more Org.Units to assign.
	Business Role Scope: click this button to display the Resource Assign window where you can select one or more BRoles to assign.
	Risk Scope: click this button to display the Resource Assign window where you can select one or more Risks to assign.
	Attribute Hierarchy Scope: click this button to display the Resource Assign window where you can select one or more Attribute Hierarchy to assign.

The **New Start Date/New End Date** columns list the dates defined with the  **Validity** button.

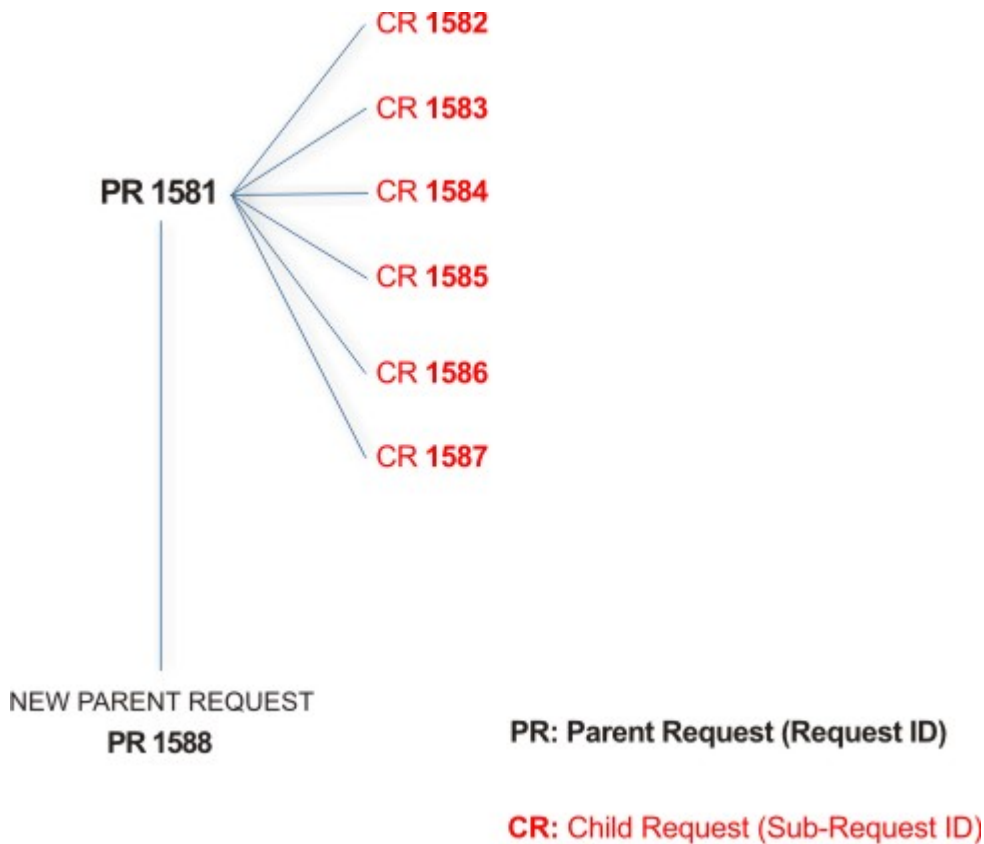
Admin Roles: processing a request

You can view a summary of the generated requests.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is in black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Request ID** and are in red.



In the previous example, **Request ID 1581**, generates six **Sub-Request ID**: 1582, 1583, ... and 1587.

There is ALWAYS the possibility to view ALL the requests registered through the Request Report activity.

However, when you are logged-in as authorizer some of the request (and sub-request) listed through the Request Report activity might not be visible because out of the scope defined for the authorizer.

The requests that are generated during the authorization process can be characterized by different statuses, which are summarized in the following table:

Table 90. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Rejected	Request can no longer be processed. It is a final status for the request.
In execution	Request waiting for the propagation to the target system.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Pending	Source request is waiting for formalization by one or more approvers.

Table 90. Request Status (continued)

Status	Description
Escalation	Request contains incompatible roles.
Partially Authorized	Request with some sub requests in authorizable status.
Partially Approved	Request with some sub requests in Approved status.
Partially Executed	Request with some sub requests in executed status.
Partially Completed	Request with all sub requests at end of their lifecycle, some Completed and some in Failed Completion status.
Partially Terminated	Request with some sub requests in Completed and some in progress.
Terminated With Reservation	In this status falls all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request can be split in several sub requests. Every sub request can be characterized by several statuses.

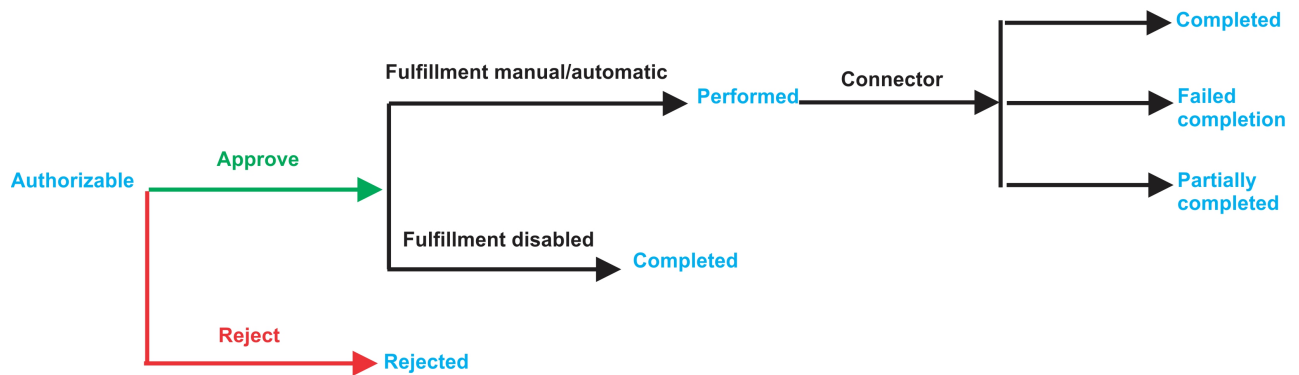


Figure 5. Statuses of a Sub Request

Statuses of a Sub Request	
Status	Description
Rejected	The sub request was rejected by the approver, and it is not fulfilled.
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Manual/Automatic, it means that the connector successfully aligned every permission on the target system.
Performed	The connector did not yet align the permissions on the target system.
Failed Completion	The connector failed to align all permission on the target system.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.

You can search specific requests with the following filters. Click **Filter/Hide Filter** and then click **Search**.

Table 91. Filters

Filter		Description
Request ID		Unique identifier of the request
Sub Request ID		A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity		Identifier of the IAG actor that generated the request
Beneficiary Identity		Identifier of the beneficiary of the request
Created between	Start Date	Start date of the creation of the request
	End Date	End date of the creation of the request

The results are displayed in the same frame, according to the following attributes:

Requests attributes	
Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (dd/mm/yyyy) and hour (hh:mm) the request was created.
Status	Request Status.

Click **Applicant** and **Beneficiary** to open the User details window and show the following information:


Table 92. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the frame shows the following information about the **Actors of the Request**:

Table 93. Request Actors

Actor	Detail	Description
Request	ID	Unique identifier of the request
	Type	Type of request
	Status	Status of the Request
	Created on	Date (dd/mm/yyyy) and hour (hh/mm) that the request was created
Applicant/ Beneficiary/ Delegator/	Group	Group of the Applicant/Beneficiary/Delegator
	First Name	Given name of the Applicant/Beneficiary/Delegator
	Last Name	Surname of the Applicant/Beneficiary/Delegator
	User ID	Unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.
Request Notes	Request	Type of request
	to Add	Notes about the add action that was made on the <i>Entity</i> of the request
	to Remove	Notes about the remove action that was made on the <i>Entity</i> of the request
	to Update	Notes about the update action that was made on the <i>Entity</i> of the request
Additional Notes	Request notes can be specified by the author of the request or by a rule. In this field, you can add free text for any reason during the authorization or execution of the request.	

Note: The Request Notes are not mandatory. If there are no notes in the request, the fields of the Request Notes are blank.


Click the  **Info** icon to open the User details window and show the information in a set of tabs:

Table 94. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).

Table 94. User Details - Details tab (continued)

Detail	Description
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 95. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement info window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation

Table 96. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 97. User Details - Activities tab


Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity


Table 98. User Details - Rights

Detail	Description
Entitlement	Name of the entitlement
Right	Name of the right
Values	Value of the right

The lower part of the frame shows the following information about the requests:

Table 99. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlement involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the  **Info** icon to open the Entitlement info window and show the summarized information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 100. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.


Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles
- External Roles
- Permissions

The following icons represent these entitlements:



If notes about the considered entitlement are in the request, the  **Note** icon is available. Click it to open the Notes window and show the contents of the note.

In the central side of the frame, you find:

- Elements related to the request to be authorized.
- Elements related to the approver of the request.

In the lower side of the frame, the available buttons are:

- **Back** returns to the summary of the requests.
- **Approve** approves the request.
- **Reject** rejects a request.

Admin Roles: executing a request

You can view a summary of the generated requests.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Requests** and are red.

The requests that are generated during the authorization process can be characterized by different statuses, which are summarized in the following table:

Table 101. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Rejected	Request can no longer be processed. It is a final status for the request.
In execution	Request waiting for the propagation to the target system.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Pending	Source request is waiting for formalization by one or more approvers.
Escalation	Request contains incompatible roles.
Partially Authorized	Request with some sub requests in authorizable status.
Partially Approved	Request with some sub requests in Approved status.
Partially Executed	Request with some sub requests in executed status.
Partially Completed	Request with all sub requests at end of their lifecycle, some Completed and some in Failed Completion status.
Partially Terminated	Request with some sub requests in Completed and some in progress.
Terminated With Reservation	In this status falls all the requests that present an unclear or unexpected behavior. It is a final status for the request.

You can search specific requests with the following filters. Click **Filter/Hide Filter** and then click **Search**.

Table 102. Filters

Filter	Description	
Request ID	Unique identifier of the request	
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.	
Applicant Identity	Identifier of the IAG actor that generated the request	
Beneficiary Identity	Identifier of the beneficiary of the request	
Created between	Start Date	Start date of the creation of the request
	End Date	End date of the creation of the request

The results are displayed in the same frame, according to the following attributes:

Requests attributes	
Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.

Requests attributes	
Attribute	Description
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (dd/mm/yyyy) and hour (hh:mm) the request was created.
Status	Request Status.

Click **Applicant** and **Beneficiary** to open the User details window and show the following information:

Table 103. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	


Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the frame shows the following information about the **Actors of the Request**:

Table 104. Request Actors

Actor	Detail	Description
Request	ID	Unique identifier of the request
	Type	Type of request
	Status	Status of the Request
	Created on	Date (dd/mm/yyyy) and hour (hh/mm) that the request was created

Table 104. Request Actors (continued)

Actor	Detail	Description
Applicant/ Beneficiary/ Delegator/	Group	Group of the Applicant/Beneficiary/Delegator
	First Name	Given name of the Applicant/Beneficiary/Delegator
	Last Name	Surname of the Applicant/Beneficiary/Delegator
	User ID	Unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.
Request Notes	Request	Type of request
	to Add	Notes about the add action that was made on the <i>Entity</i> of the request
	to Remove	Notes about the remove action that was made on the <i>Entity</i> of the request
	to Update	Notes about the update action that was made on the <i>Entity</i> of the request
Additional Notes	Request notes can be specified by the author of the request or by a rule. In this field, you can add free text for any reason during the authorization or execution of the request.	

Note: The Request Notes are not mandatory. If there are no notes in the request, the fields of the Request Notes are blank.


Click the  **Info** icon to open the User details window and show the information in a set of tabs:

Table 105. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 106. User Details - Entitlements tab


Details	Description
	Click Info to open the Entitlement info window

Table 106. User Details - Entitlements tab (continued)


Details	Description
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation

Table 107. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 108. User Details - Activities tab


Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity


Table 109. User Details - Rights

Detail	Description
Entitlement	Name of the entitlement
Right	Name of the right
Values	Value of the right

The lower part of the frame shows the following information about the requests:

Table 110. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlement involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the  **Info** icon to open the Entitlement info window and show the summarized information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 111. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.


Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles
- External Roles
- Permissions

The following icons represent these entitlements:



If notes about the considered entitlement are in the request, the  **Note** icon is available. Click it to open the Notes window and show the contents of the note.

Admin delegation: generating a request

You can submit a request of delegation only for Administrative Roles.

The activity is based on three tabs:

- Delegator
- New Delegation
- Catalog

Note: The scope of this activity is based on Administrative Roles, but it's structure is the same of the activity related to the delegation of common roles (not Administrative Roles)

Admin delegation: processing a request

You can view a summary of the generated delegation requests for Administrative Roles.

The structure of this activity it's the same of:

Delegation: processing a request.

Note: The scope of this activity is based on Administrative Roles, but it's structure is the same of the activity related to the delegation of common roles (not Administrative Roles)

Admin delegation: executing a request

You can view a summary of the authorized requests.

The structure of this activity it's the same of:

Delegation: executing a request



Note: The scope of this activity is based on Administrative Roles, but it's structure is the same of the activity related to the delegation of common roles (not Administrative Roles)

Admin Roles: Catalog

The Catalog tab is the second step of the wizard.

From the **Catalog** tab you can choose the entitlements and roles for the users selected in the first step of the wizard, Users .

In the upper part of the frame is summarized the information about the selected users:

User data	
Data	Description
 Info	Click the Info icon to open the Entitlement info window.
First Name	Name of the user.
Last Name	Surname of the user.
User ID	Univocal identifier of the user.
Org. Unit [Code]	Name of the organizational unit and [Univocal identifier of the OU].
User Type	Type of user.
Risk Status 	Click the colored dot to open a window that displays: <ul style="list-style-type: none"> • The Risk Activities Tree (related to a specific user) into the Risk Info tab • The Activities involved in a specific risk, into the Mitigations tab

Click the **Refresh** button to update the risk situation of the user.

In the lower part of the frame is a set of tabs:

- **Current Entitlements**
- **Business Roles**
- **Application Roles**
- **Permissions**

According to the configuration of the Activity, some of these tabs might be not present.

Current Entitlements tab


In the **Current Entitlements** tab is the list of the entitlements of the user. From this tab you can search (click the **Filter/Hide Filter** button and click the **Search** button) a specific entitlement through the filters shown below:

Current Entitlements filters	
Filter	Description
Name	Name of the Entitlement.
Family	Family of the Entitlement.
Description	Brief description of the Entitlement.

From the list of Entitlements produced it is possible to **perform two types of operations:**

- **Remove** (Entitlement)
- **Validity** (End date of validity)

To remove the **Current Entitlements** click the **Remove** button (the **Remove** button will be shown in red).

To enter or change the **Validity** of the entitlements click the **Validity** button, the **Date Selection** window opens, click the  **Calendar** button to enter the end date and click **OK** to confirm. The **Validity** button will be highlighted in orange. To remove the end date click on the **Validity** button.



After the desired operations have been performed, click the **Business Roles** tab to assign Business Roles, or click the **Next** button to go to the “Admin Roles: Shopping Cart” on page 94 tab to process the request.

Business Roles tab

In the **Business Roles** tab is the list of available Business Roles (**BRoles**) for the selected user. From this tab you can search (click the **Filter/Hide Filter** button and click the **Search** button) a specific BRole through the filters shown below:

Current Entitlements filters	
Filter	Description
Name	Name of the Entitlement.
Family	Family of the Entitlement.
Description	Brief description of the Entitlement.

From the list of BRoles produced you can add one or more BRoles to the user, click the **Add** button (the **Add** button will be highlighted in green).

If the BRole added has **Dependencies**, the  **Dependencies** button appears, (between the  **Info** button in the BRoles list). Click it to open the **Dependencies** window to add one or more of these.

To add the Dependencies click on the **To Cart** button (the **To Cart** button will be highlighted in green) then click **Ok** to confirm.

Dependencies can be defined and associated with roles. Dependencies are permissions or roles that are necessary, or useful, to other roles.

For example, a role that is named TECHComm, with all the specific permissions for this position, is being defined for an employee who is to take a position as technical writer.

The technical writer reviews the draft documents that are produced by the Product Managers. They are shared in a company repository that is named DraftsOnProducts, which is a dedicated database, linked to a permission named DraftsOnProdcuts_Reader.

The DraftsOnProdcuts_Reader permission can be considered as a dependency of TECHComm.

The **Actions** menu includes the following items:

- **All Roles** Click to choose from the full set of available roles to assign to a selected user.
- **Like Mike** Click to assign to a selected User the same roles of another user that you choose from the full set of users.

Once the desired operations has been performed click on the **Applications Roles** tab to assign Applications Roles, or click on the **Next** button to go to the “Admin Roles: Shopping Cart” on page 94 tab to process the Request.

Applications Roles tab

In this section it is possible to assign the Applications Roles to the User .

In the **Applications Roles** tab, the **Applications** window opens by default, allows to choose a specific Application. From the list displayed, click on an Application to choose it; the **Applications Roles** are immediately displayed in the **Applications Roles** tab. To **exit** from this window, **close it**.

From this tab it is possible to search (clicking on the **Filter/Hide Filter** button) a specific Application also through the filters shown below:

Application Roles filters	
Filter	Description
Application	Name of the Application.
Family	Family of the Entitlement.
Name	Name of the Entitlement.
Description	Brief description of the Entitlement.

From the list of Roles produced it is possible to add one or more Roles to the User, clicking on the **Add** button (the **Add** button will be highlighted in green).

The **Actions** menu includes the following items:

- **All Roles** Click to choose from the full set of available roles to assign to a selected user.
- **Like Mike** Click to assign to a selected User the same roles of another user that you choose from the full set of users.

Once the desired operations has been performed click on the **Permission**stab to assign Permissions, or click on the **Next** button to go to the “User Access: Shopping Cart” on page 183tab to process the Request.

Permissions tab

In this section it is possible to assign the Permissions to the User .

In the **Permissions** tab, the **Applications** window opens by default, allows to choose a specific Application. From the list displayed, click on an Application to choose it; the **Permissions** are immediately displayed in the **Permissions** tab. To **exit** from this window, **close it**.

From this tab it is possible to search (clicking on the **Filter/Hide Filter** button) a specific Application also through the filters shown below:

Permissions filters	
Filter	Description
Application	Name of the Application.
Permission Type	Type of Permission.
Name	Name of the Entitlement.
Description	Brief description of the Entitlement.

From the list of Permissions produced it is possible to add one or more Permissions to the User, clicking on the **Add** button (the **Add** button will be highlighted in green).

The **Actions** menu includes the following items:

- **All Roles** Click to choose from the full set of available roles to assign to a selected user.
- **Like Mike** Click to assign to a selected User the same roles of another user that you choose from the full set of users.

After the desired operations have been performed, click the **Next** button to go to the Shopping Cart tab to process the request.


This tab is the third step of the wizard.

Admin Roles: Shopping Cart


The **Shopping Cart** tab hosts a summary tree structure.

The **Operation** column lists the operations performed in the tabs under **Catalog**:

- **Add**
- **Remove**
- **Change** (is referred to the **Validity** change in the Current Entitlements tab)

When you select the  **Clear** button, the operation is revoked and is not taken into consideration when the Request is processed.

The **Application** column lists the names of the Applications of the Entitlements.

The **Name** column lists the Entitlements involved in the performed operation; if the Entitlement is a **Permission**, it may have one or more associated  **Rights** and it is possible to assign a **Value** to each right.

A Right is defined by two attributes: Key (*aaaa* in the example figure) and Value (*v1* in the example figure).

The Key attribute is an identifying name while the Value attribute can be defined each time. A configurable default value can be provided for the Value attribute.


Rights can be either of the following types:


- Single-value

- Single-value with lookup
- Multi-value
- Multi-value with lookup








A single-value Right with lookup allows to choose a single value V_x from a set of several values (V_1, V_2, \dots, V_N)


A multi-value Right with lookup allows to choose a subset of values (V_x, V_y, V_z, \dots) from a larger set of values (V_1, V_2, \dots, V_N).

When a Right is with Lookup, a  **Browse** button is available nearby. Click it to display the **Rights** window, where you can select values.

The presence of the  **Visibility Violation** icon in the **VV** column, denotes an Entitlement in Visibility Violation. An Entitlement is in VV when there is a special reason to assign an Entitlement to a User of that Organization Unit (OU), but you do not want the Entitlement to be available to the other users of the OU.

One or more of the following buttons are enabled for each entitlement: and displayed next to the VV column:

Buttons and Icons	
Button/Icon	Description
	Note: click this button to display the Notes window where you can write notes that will be annexed to the delegation.
	Validity: click this button to display the Date Selection window where you can enter the Start Date and the End Date of the delegation.
Buttons and Icons available only for the Admin Access Request	
	Application Scope: click this button to display the Resource Assign window where you can select one or more Applications to assign.
	Org.Units Scope: click this button to display the Resource Assign window where you can select one or more Org.Units to assign.
	Business Role Scope: click this button to display the Resource Assign window where you can select one or more BRoles to assign.
	Risk Scope: click this button to display the Resource Assign window where you can select one or more Risks to assign.
	Attribute Hierarchy Scope: click this button to display the Resource Assign window where you can select one or more Attribute Hierarchy to assign.

The **New Start Date**/**New End Date** columns list the dates defined with the  **Validity** button.

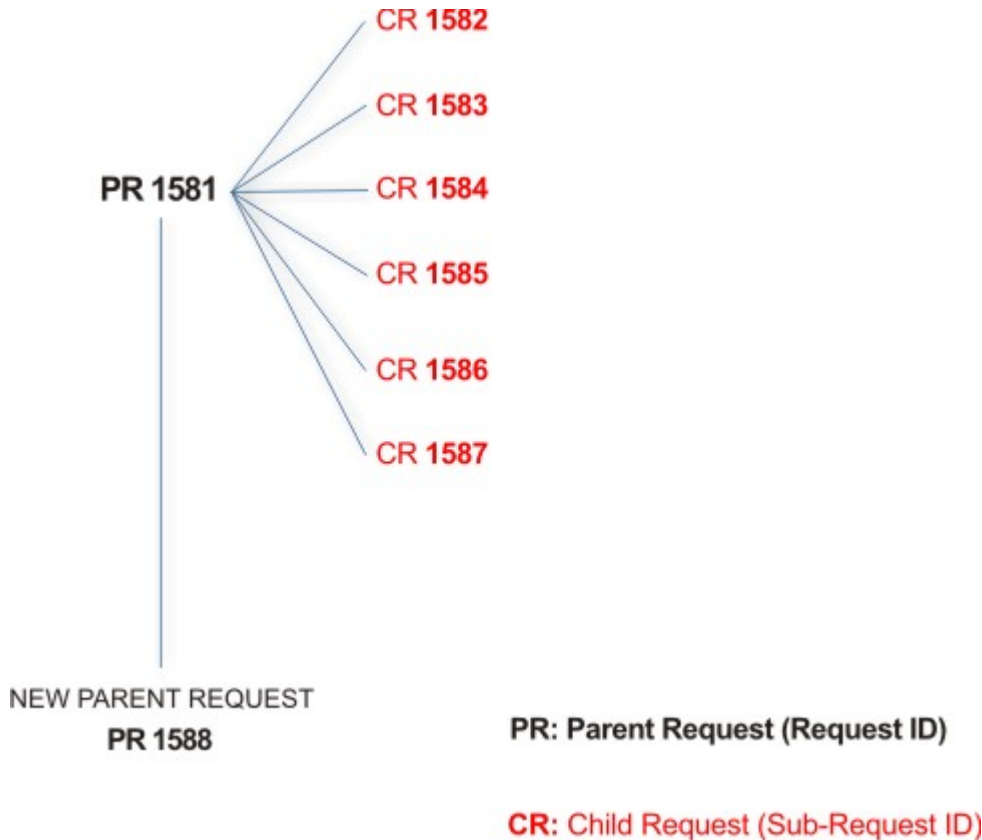
My daily work: list of requests

You can view a summary of the generated requests in your scope.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is in black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Requests** and are in red.



In the previous example, **Request ID 1581**, generates six **Sub-Requests**: 1582, 1583, ... and 1587.

There is ALWAYS the possibility to view ALL the requests registered through the REQUEST REPORT EXE activity.

However, when you are logged-in as authorizer, some of the request (and sub-request) listed through the REQUEST REPORT EXE might not be visible because out of the scope defined for the authorizer.

The requests that are generated during the authorization process can be characterized by different statuses, which are summarized in the following table:

Table 112. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Rejected	Request can no longer be processed. It is a final status for the request.
In execution	Request waiting for the propagation to the target system.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Pending	Source request is waiting for formalization by one or more approvers.
Escalation	Request contains incompatible roles.
Partially Authorized	Request with some sub requests in authorizable status.
Partially Approved	Request with some sub requests in Approved status.
Partially Executed	Request with some sub requests in executed status.
Partially Completed	Request with all sub requests at end of their lifecycle, some Completed and some in Failed Completion status.
Partially Terminated	Request with some sub requests in Completed and some in progress.
Terminated With Reservation	In this status falls all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request can be split in several sub requests. Every sub request can be characterized by several statuses.

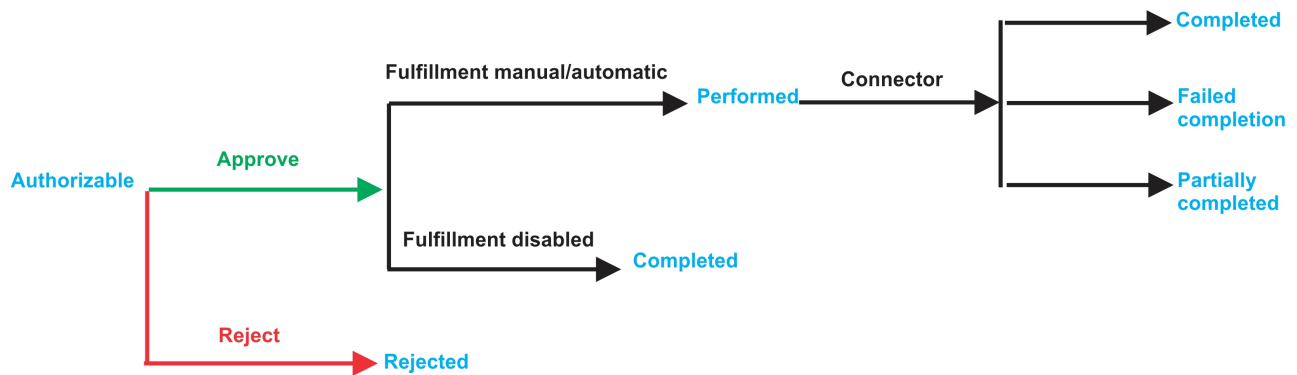


Figure 6. Statuses of a Sub Request

Statuses of a Sub Request	
Status	Description
Rejected	The sub request was rejected by the approver, and it is not fulfilled.

Statuses of a Sub Request	
Status	Description
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Manual/Automatic, it means that the connector successfully aligned every permission on the target system.
Performed	The connector did not yet align the permissions on the target system.
Failed Completion	The connector failed to align all permission on the target system.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.

You can search specific requests with the following filters. Click **Filter/Hide Filter** and then click **Search**.

Table 113. Filters

Filter		Description
Request ID		Unique identifier of the request
Sub Request ID		A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity		Identifier of the IAG actor that generated the request
Beneficiary Identity		Identifier of the beneficiary of the request
Created between	Start Date	Start date of the creation of the request
	End Date	End date of the creation of the request

The results are displayed in the same frame, according to the following attributes:

Requests attributes	
Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (dd/mm/yyyy) and hour (hh:mm) the request was created.
Status	Request Status.

Click **Applicant** and **Beneficiary** to open the User details window and show the following information:

Table 114. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs


Table 114. User Details - Details tab (continued)

Detail	Description
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the frame shows the following information about the **Actors of the Request**:

Table 115. Request Actors

Actor	Detail	Description
Request	ID	Unique identifier of the request
	Type	Type of request
	Status	Status of the Request
	Created on	Date (dd/mm/yyyy) and hour (hh/mm) that the request was created
Applicant/ Beneficiary/ Delegator/	Group	Group of the Applicant/Beneficiary/Delegator
	First Name	Given name of the Applicant/Beneficiary/Delegator
	Last Name	Surname of the Applicant/Beneficiary/Delegator
	User ID	Unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.
Request Notes	Request	Type of request
	to Add	Notes about the add action that was made on the <i>Entity</i> of the request
	to Remove	Notes about the remove action that was made on the <i>Entity</i> of the request
	to Update	Notes about the update action that was made on the <i>Entity</i> of the request
Additional Notes	Request notes can be specified by the author of the request or by a rule. In this field, you can add free text for any reason during the authorization or execution of the request.	

Note: The Request Notes are not mandatory. If there are no notes in the request, the fields of the Request Notes are blank.


Click the  **Info** icon to open the User details window and show the information in a set of tabs:

Table 116. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 117. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement info window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation

Table 118. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 119. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree

Table 119. User Details - Activities tab (continued)


Detail	Description
Description	Brief description of the activity


Table 120. User Details - Rights

Detail	Description
Entitlement	Name of the entitlement
Right	Name of the right
Values	Value of the right

The lower part of the frame shows the following information about the requests:

Table 121. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlement involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the  **Info** icon to open the Entitlement info window and show the summarized information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 122. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement

Table 122. Entitlement info - Structure (continued)

Detail	Description
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.


Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles
- External Roles
- Permissions

The following icons represent these entitlements:



If notes about the considered entitlement are in the request, the  **Note** icon is available. Click it to open the Notes window and show the contents of the note.

Delegation: generating a request

You can require to delegate a set of entitlements to a user.

Note: The **Delegator** tab is available only for the common activity of delegation (delegation of entitlements of a User A to a User B). The "personal delegation" activity, consisting in the action of delegates own entitlements to another user, starts from the Delegated tab.


The **Delegator** tab is the first step of the wizard. You can search and select users by clicking **Filter/Hide Filter** and then **Search**. The following filters area available:

Table 123. User filters

Filter	Description
User Type	Type of user, for example, Administrative, Business, Employee, Training, External
Full Name/Code	Name and surname of the user or unique identifier of the user
Enabled	When selected, specifiesA flag implies that the user can be assigned entitlements.

The results are according to the following attributes:

Table 124. Users list.

Field	Description
User details icon	Click the  Info icon to open the User Details window that shows the user's details, assigned entitlements, and assigned accounts.
User ID	Unique identifier of the user.
First Name	Name of the user.
Last Name	Surname of the user.
Group [Code]	Organization Unit [Univocal identifier of the OU] of the user.
User Type	Type of user (for example: Administrative, Business, Employee, Training, External).

To select the entire list of users, select the check box on the attributes row, otherwise select the check box that corresponds to the user row.


Clicking  **Info** opens the user **details** window, which displays the following information in a set of tabs:

Table 125. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).

Table 125. User Details - Details tab (continued)

Detail	Description
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 126. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement info window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation

Table 127. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 128. User Details - Rights

Detail	Description
Entitlement	Name of the entitlement
Right	Name of the right
Values	Value of the right

Table 129. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity


Clicking  **Info** from the **Entitlement** tab opens the **Entitlement info** window, which displays the information summarized in the **Structure** tab:

Table 130. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.

Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles
- External Roles
- Permissions

The following icons represent these entitlements:



Clicking **Next** opens the Delegated tab.

This tab is the second step of the wizard.

Delegated tab: selecting a user

The New Delegation tab is the second step of the wizard.

From the **Delegated** tab, after selecting the user in the first step of the wizard, Delegator, you can **choose the new users to delegate**.

In the upper part of the frame are summarized the information about the selected users (or about the user logged in for personal delegation).

In the lower part of the frame there is the list of Users that can be choose for to be delegated.

To select the entire list of users, click the check box on the attributes row, otherwise click the check box that corresponds to the user row.

Clicking on the **Next** button, the Catalog tab opens.

This tab is the third step of the wizard.

Catalog tab: selecting entitlements

The Catalog tab is the third step of the wizard.

From the **Catalog** tab you can choose the entitlements of the users selected in the first step of the wizard, Delegator, to delegate to the users selected in the second step of the wizard, New Delegation.


In the upper part of the frame are summarized the information about the selected Users; to left there are the **Delegator Users**, to right there are the **Delegated Users**.

In the lower part of the frame there are two tabs:

- **Assignable Entitlements**
- **Current Entitlements**

Delegation Change: Catalog tab (Personal Delegation request)

The **Catalog** tab it is the second step of the wizard. From here, it is possible to choose the Entitlements, for the Users selected in the first step of the wizard, New Delegation.

	Note: the Entitlements to delegate are those that are assigned to the User logged in.
---	--

In the upper part of the frame are summarized the information about the selected Users; to left there are the **User logged in**, to right there are the **Delegated Users**.




In the lower part of the frame there are two tabs:

- **Assignable Entitlements**
- **Current Entitlements**

Assignable Entitlements tab

In the **Assignable Entitlements** tab, that it is opened by default, there is the list of the **Entitlements**, of the **Delegator Users/User logged in**, that can be possible to delegate to the **Delegated Users**.


From the list of available Entitlements it is possible to **add one or more Entitlements to the Delegated User**, clicking on the **Add** button (the **Add** button will be lighted in green); clicking on the **Add** button, a set of icons, disposed on the selected Entitlement row, will be enabled:

Buttons & Icons	
Button/Icon	Description
	Click Info to display Details , which contains details of the selected entitlement, and Structure , which displays the structure of the selected entitlement, in the Entitlement info window.
	Click Note to open the Notes window so you can write notes that are annexed to the delegation.
	Click Validity so you can enter Start Date and End Date of the delegation in the Date Selection window.

Once the desired operations has been performed it is possible to click on the **Submit** button to process the Request or to go in the **Current Entitlement** tab to perform a set of operations on the delegated Entitlements.

Current Entitlements tab


In the **Current Entitlements** tab there are the list of delegated Entitlement. From this tab it is possible to search (clicking on the **Filter/Hide Filter** button and clicking on the **Search** button) a specific Entitlement through the filters, **Name** (name of the Entitlement) and **Description** (brief description of the Entitlement).



	Note: if the Delegated User has never been involved in a delegation by a specific Delegator User/User logged in, the Current Entitlements tab will be empty.
---	---

From the list of Entitlements produced it is possible to **perform two types of operations:**


- **Remove** (Entitlement)
- **Change** (Delegation date)

To remove the delegated Entitlements click on the **Remove** button (the **Remove** button will be lighted in red). Clicking on it a set of icons, disposed on the selected Entitlement row, will be enabled:

Buttons & Icons	
Button/Icon	Description
	Click Info to display Details , which contains details of the selected entitlement, and Structure , which displays the structure of the selected entitlement, in the Entitlement info window.

Buttons & Icons	
Button/Icon	Description
	Click Note to open the Notes window so you can write notes that are annexed to the delegation.
	Click Validity so you can enter Start Date and End Date of the delegation in the Date Selection window.

Clicking on the **Change** button (the **Change** button will be lighted in green), the **Date Selection** window opens allowing to insert the **End Date** of the delegation.

To insert the date click on the **Calendar** icon, the **Calendar** opens. To clear the field click on the  **Clear** icon.

From the **Current Entitlements** tab it is possible to go in the **Assignable Entitlements** tab or, clicking on the **Submit** button, to process the request.

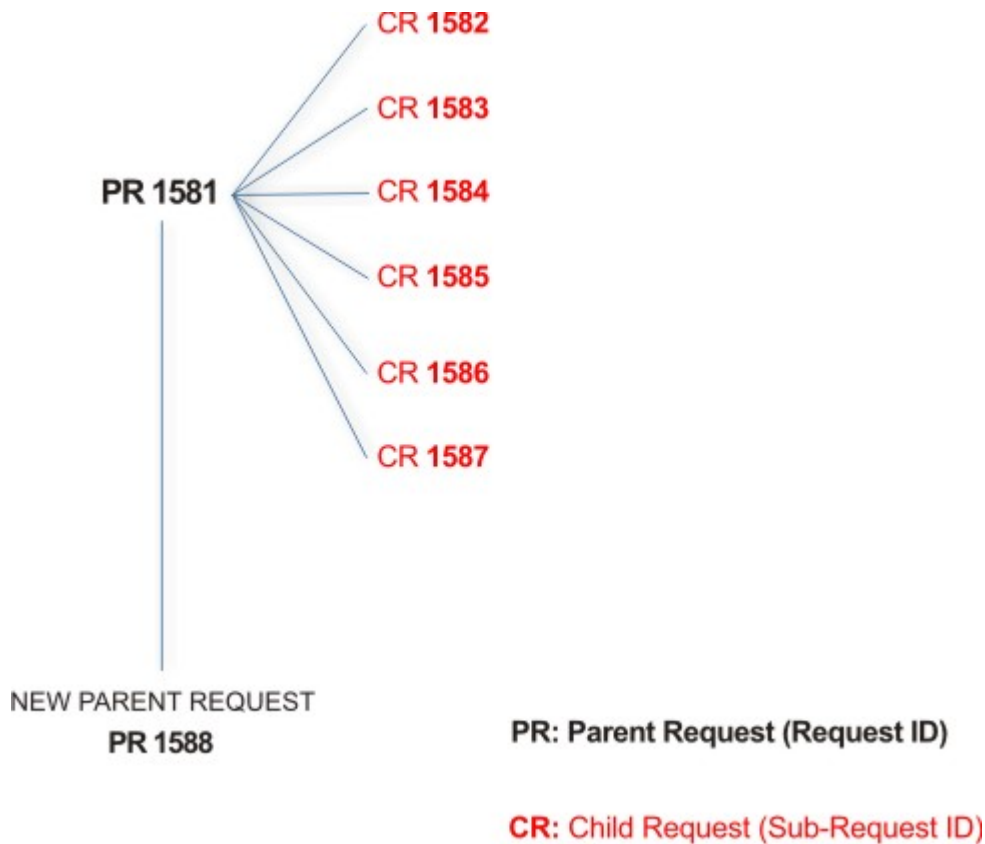
Delegation: processing a request

You can view a summary of the generated requests.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is in black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Request ID** and are in red.



In the previous example, **Request ID 1581**, generates six **Sub-Request ID**: 1582, 1583, ... and 1587.

There is ALWAYS the possibility to view ALL the requests registered through the Request Report activity.

However, when you are logged-in as authorizer some of the request (and sub-request) listed through the Request Report activity might not be visible because out of the scope defined for the authorizer.

The requests that are generated during the authorization process can be characterized by different statuses, which are summarized in the following table:

Table 131. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Rejected	Request can no longer be processed. It is a final status for the request.
In execution	Request waiting for the propagation to the target system.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Pending	Source request is waiting for formalization by one or more approvers.

Table 131. Request Status (continued)

Status	Description
Escalation	Request contains incompatible roles.
Partially Authorized	Request with some sub requests in authorizable status.
Partially Approved	Request with some sub requests in Approved status.
Partially Executed	Request with some sub requests in executed status.
Partially Completed	Request with all sub requests at end of their lifecycle, some Completed and some in Failed Completion status.
Partially Terminated	Request with some sub requests in Completed and some in progress.
Terminated With Reservation	In this status falls all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request can be split in several sub requests. Every sub request can be characterized by several statuses.

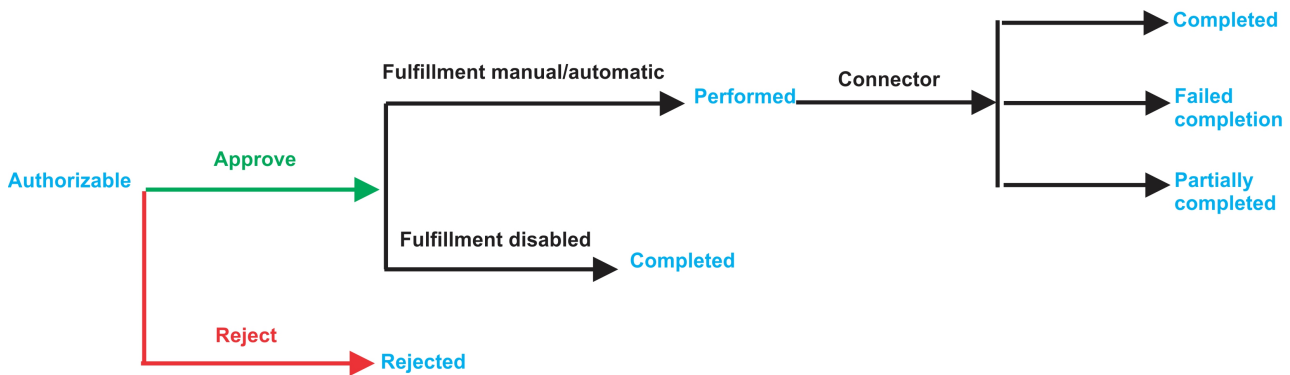


Figure 7. Statuses of a Sub Request

Statuses of a Sub Request	
Status	Description
Rejected	The sub request was rejected by the approver, and it is not fulfilled.
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Manual/Automatic, it means that the connector successfully aligned every permission on the target system.
Performed	The connector did not yet align the permissions on the target system.
Failed Completion	The connector failed to align all permission on the target system.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.

You can search specific requests with the following filters. Click **Filter/Hide Filter** and then click **Search**.

Table 132. Filters

Filter		Description
Request ID		Unique identifier of the request
Sub Request ID		A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity		Identifier of the IAG actor that generated the request
Beneficiary Identity		Identifier of the beneficiary of the request
Created between	Start Date	Start date of the creation of the request
	End Date	End date of the creation of the request

The results are displayed in the same frame, according to the following attributes:

Requests attributes	
Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (dd/mm/yyyy) and hour (hh:mm) the request was created.
Status	Request Status.

Click **Applicant** and **Beneficiary** to open the User details window and show the following information:


Table 133. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the frame shows the following information about the **Actors of the Request**:

Table 134. Request Actors

Actor	Detail	Description
Request	ID	Unique identifier of the request
	Type	Type of request
	Status	Status of the Request
	Created on	Date (dd/mm/yyyy) and hour (hh/mm) that the request was created
Applicant/ Beneficiary/ Delegator/	Group	Group of the Applicant/Beneficiary/Delegator
	First Name	Given name of the Applicant/Beneficiary/Delegator
	Last Name	Surname of the Applicant/Beneficiary/Delegator
	User ID	Unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.
Request Notes	Request	Type of request
	to Add	Notes about the add action that was made on the <i>Entity</i> of the request
	to Remove	Notes about the remove action that was made on the <i>Entity</i> of the request
	to Update	Notes about the update action that was made on the <i>Entity</i> of the request
Additional Notes	Request notes can be specified by the author of the request or by a rule. In this field, you can add free text for any reason during the authorization or execution of the request.	

Note: The Request Notes are not mandatory. If there are no notes in the request, the fields of the Request Notes are blank.


Click the  **Info** icon to open the User details window and show the information in a set of tabs:

Table 135. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).

Table 135. User Details - Details tab (continued)

Detail	Description
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 136. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement info window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation

Table 137. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 138. User Details - Activities tab


Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity


Table 139. User Details - Rights

Detail	Description
Entitlement	Name of the entitlement
Right	Name of the right
Values	Value of the right

The lower part of the frame shows the following information about the requests:

Table 140. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlement involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the  **Info** icon to open the Entitlement info window and show the summarized information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 141. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.


Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles
- External Roles
- Permissions

The following icons represent these entitlements:



If notes about the considered entitlement are in the request, the  **Note** icon is available. Click it to open the Notes window and show the contents of the note.

In the central side of the frame, you find:

- Elements related to the request to be authorized.
- Elements related to the approver of the request.

In the lower side of the frame, the available buttons are:

- **Back** returns to the summary of the requests.
- **Approve** approves the request.
- **Reject** rejects a request.

Delegation: executing a request

You can view a summary of the authorized requests.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Requests** and are red.

The requests that are generated during the authorization process can be characterized by different statuses, which are summarized in the following table:

Table 142. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Rejected	Request can no longer be processed. It is a final status for the request.
In execution	Request waiting for the propagation to the target system.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Pending	Source request is waiting for formalization by one or more approvers.
Escalation	Request contains incompatible roles.
Partially Authorized	Request with some sub requests in authorizable status.
Partially Approved	Request with some sub requests in Approved status.
Partially Executed	Request with some sub requests in executed status.
Partially Completed	Request with all sub requests at end of their lifecycle, some Completed and some in Failed Completion status.
Partially Terminated	Request with some sub requests in Completed and some in progress.
Terminated With Reservation	In this status falls all the requests that present an unclear or unexpected behavior. It is a final status for the request.

You can search specific requests with the following filters. Click **Filter/Hide Filter** and then click **Search**.

Table 143. Filters

Filter	Description	
Request ID	Unique identifier of the request	
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.	
Applicant Identity	Identifier of the IAG actor that generated the request	
Beneficiary Identity	Identifier of the beneficiary of the request	
Created between	Start Date	Start date of the creation of the request
	End Date	End date of the creation of the request

The results are displayed in the same frame, according to the following attributes:

Requests attributes	
Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.

Requests attributes	
Attribute	Description
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (dd/mm/yyyy) and hour (hh:mm) the request was created.
Status	Request Status.

Click **Applicant** and **Beneficiary** to open the User details window and show the following information:

Table 144. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	


Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the frame shows the following information about the **Actors of the Request**:

Table 145. Request Actors

Actor	Detail	Description
Request	ID	Unique identifier of the request
	Type	Type of request
	Status	Status of the Request
	Created on	Date (dd/mm/yyyy) and hour (hh/mm) that the request was created

Table 145. Request Actors (continued)

Actor	Detail	Description
Applicant/ Beneficiary/ Delegator/	Group	Group of the Applicant/Beneficiary/Delegator
	First Name	Given name of the Applicant/Beneficiary/Delegator
	Last Name	Surname of the Applicant/Beneficiary/Delegator
	User ID	Unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.
Request Notes	Request	Type of request
	to Add	Notes about the add action that was made on the <i>Entity</i> of the request
	to Remove	Notes about the remove action that was made on the <i>Entity</i> of the request
	to Update	Notes about the update action that was made on the <i>Entity</i> of the request
Additional Notes	Request notes can be specified by the author of the request or by a rule. In this field, you can add free text for any reason during the authorization or execution of the request.	

Note: The Request Notes are not mandatory. If there are no notes in the request, the fields of the Request Notes are blank.


Click the  **Info** icon to open the User details window and show the information in a set of tabs:

Table 146. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 147. User Details - Entitlements tab


Details	Description
	Click Info to open the Entitlement info window

Table 147. User Details - Entitlements tab (continued)


Details	Description
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation

Table 148. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 149. User Details - Activities tab


Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity


Table 150. User Details - Rights

Detail	Description
Entitlement	Name of the entitlement
Right	Name of the right
Values	Value of the right

The lower part of the frame shows the following information about the requests:

Table 151. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlement involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the  **Info** icon to open the Entitlement info window and show the summarized information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 152. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.


Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles
- External Roles
- Permissions

The following icons represent these entitlements:



If notes about the considered entitlement are in the request, the  **Note** icon is available. Click it to open the Notes window and show the contents of the note.

Authorize escalation

The Risk Manager provides several operations for user risks.

After you make a request, the Risk Manager processes the user risk that is generated by a request.

In the **Authorize Escalation** tab, you can view a summary of the generated risk requests.

You can search specific requests with the following filters by clicking **Filter/Hide Filter** and then **Search**:

Table 153. Filters

Filter		Description
Request ID		Unique identifier of the request
Sub Request ID		A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity		Identifier of the IAG actor that generated the request
Beneficiary Identity		Identifier of the beneficiary of the request
Created between	Start Date	Start date of the creation of the request
	End Date	End date of the creation of the request

The results are displayed in the same frame, according to the following attributes:

Requests attributes	
Attribute	Description
Request ID	Univocal identifier of the parent request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (dd/mm/yyyy) and hour (hh:mm) the request was created.


Clicking **Applicant** and **Beneficiary** opens the User details window, which shows the following information:



Table 154. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	


Click **Request ID** to view the details.

The upper part of the frame displays the following information about the **Actors of the Request**:

Request Actors		
Actor	Detail	Description
Request	ID	Univocal identifier of the Request.
	Status	Status of the Request.
	Created on	Date (dd/mm/yyyy) and hour (hh:mm) of creation of the request.
	Type	Type of request.
	New Risk	Clicking the  Info icon opens a window that shows: <ul style="list-style-type: none"> The Risk Activities Tree, which is related to a specific user, in the Risk Info tab. The Activities for a specific risk in the Mitigations tab.

Request Actors		
Actor	Detail	Description
Applicant/ Beneficiary/ Delegator	Organization Unit	Organization Unit (OU) of the Applicant, Beneficiary, or Delegator .
	First Name	Given name of the Applicant, Beneficiary, or Delegator .
	Last Name	Surname of the Applicant, Beneficiary, or Delegator .
	User ID	Univocal identifier of the Applicant, Beneficiary, or Delegator . Click the  Info icon to view the User details.
	Current Risk 	Clicking the colored dot opens a window that shows: <ul style="list-style-type: none"> • The Risk Activities Tree, which is related to a specific user, in the Risk Info tab. • The Activities for a specific risk in the Mitigations tab.
Request Notes	Request	Type of request.
	to Add	Notes about what addition was made on the <i>Entity</i> of the request.
	to Remove	Notes about what was removed from the <i>Entity</i> of the request.
	to Update	Notes about what update was made on the <i>Entity</i> of the request.
Additional Notes	The Risk Manager can write more notes about the request.	

Note: The Request Notes are not mandatory. When there aren't notes in the request, the fields of the Request Notes are empty.

Clicking the  **Info** icon in the Request box in the upper part of the frame opens the Incompatibility Info window. It has the following tabs:

- **Risk Info**
- **Mitigation**


The **Mitigation** tab in the lower part of the frame shows the mitigations that are already assigned to the user.


- At the first level, there is a set of risks.
- At the second level for every risk, there is the set of At-Risk Activities in which the user is involved; it might also display aggregated mitigations.

For information related to the Service Center mitigation configuration user interface, see How to read the tree of the risks of a user.

In the lower left part of the frame, the following information about the requests is summarized:


Table 155. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlement involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Clicking the  **Info** icon opens the Entitlement info window, which summarizes the following information in a set of tabs:

- **Structure**
- **Dependencies**
- **Activity**
- **Rights**

The **Structure** tab is always available. It shows the structure of the Entitlement of the Request. The other tabs are available only when the Entitlement is characterized by **Dependencies**, **Activities**, or **Rights**.

If notes about entitlements are in the request, the  **Note** icon is available. Click it to open the **Notes** window and show the contents of the note.

The lower right part of the frame shows information about the mitigations that are assigned to the user by the Risk Manager. **Control Name** is the name of the mitigation; **Description** is brief description of the mitigation.

The following operations are available from this frame:

- **Back** returns to the summary of the generated Risk Requests.
- **Approve** approves a request.
- **Reject** rejects a request.
- **Viol. Info** displays the Risk tree, and you can assign the appropriate mitigation to the risk.

After the appropriate mitigation is assigned to the user risk, it is visible in the lower right part of the frame.

Insert/Update entitlement: generating a request

You can insert a new user or update information for a registered user.

- Insert Entitlement

- Update Entitlement

Insert entitlements: generating a request

Use this workflow to create roles.

From the **Create Role** tab, you can select two more tabs:

Role Mining

Use it to discover roles

Data Exploration







Use it to collect information on the current status of User-Entitlements associations

If you first select **Data Exploration**, you are then lead to select the **Role Mining** tab.

In the **Role Mining** tab, every role mining analysis is described by fields arranged in a row.

Click **Filter** and use the items described in the next table to find one or more analyses:

Table 156. Analysis filters.

Filter	Description
Analysis Description	A descriptive text of the analysis.
Organization Unit	Click  Browse to choose the OU in the analysis.
Application	Click  Browse to choose the Application in the analysis.
Entitlement Type	Indicates the entitlement types. <ul style="list-style-type: none"> • Permission • IT Role • Business Role • External Role
Status	Indicates the status of the analysis. <ul style="list-style-type: none"> •  Indicates in progress. •  Indicates complete. •  Indicates an error. •  Indicates invalidated due to a new bulk load.
User/Entitlement Attributes	If present, according to the current configuration.

The details provided in each row of data belonging to an analysis are the totality of the ones described in the preceding table, with two important additions.

Click  **Info** to get the complete set of analysis information.

Use the **Actions** menu to run the following actions in this context:

Add To define a role mining analysis.

Remove

To delete a selected role mining analysis row.

Follow these steps to create a role after selecting an analysis:

1. Click **Next** to access the next wizard step in the **Candidate Roles** pane.

The left frame includes the following tabs:

- Roles
- Entitlements
- Users
- Statistics tab

The selection of one of these tabs displays in turn another set of tabs in the right frame.

The main task that you can run in this step is to choose a candidate role of preference.

2. Click **Next** to gain access to the next wizard step in the **Impact Analysis** pane.

The main functionality (**Structure - Permission - Users - Risk Info** tabs) available in the **Impact Analysis** pane allows you to:

- Modify the selected candidate role to match OU needs
- Simulate the effect of a candidate role after being imported into an organization.

3. Click **Next** to gain access to the next wizard step in the **Entitlements Details** pane.

4. Finally, select **Summary** to display the candidate role that you can submit to the authorization process by clicking the **Submit** button.




User analysis: This section provides several ways of investigating the nature and structure of Candidate Roles from a User approach.

You can use the filters shown in the table below to help you find Users (click on **Filter**):

Table 157. User filters.

Attribute	Description
Master UID	Univocal identifier of the User
Last Name	Surname of the User.
First Name	Name of the User.
Organization Unit	Indicates the OU in which the User is registered.
Hier.	Flag this check box to get the tree view of the Organization unit.

Table 157. User filters. (continued)

Attribute	Description
Entitlement Coverage	<p>This filter can assume three distinct values:</p> <ul style="list-style-type: none">  Out of Role: the User is not aggregated to any Entitlement through the Candidate Roles.  Partially covered: the User is aggregated only to a subset of Entitlements through the Candidate Roles.  Covered: the User is aggregated to ALL Entitlements through the Candidate Roles.

Upon selecting a User in the **Users** tab on the left, the **User Details** tab, on the right, is shown by default with the relevant information, distinguished in the following groups: **User - Entitlements - Applications**.

Table 158. User details.

User	
Attribute	Description
Last Name	Indicates the User's last name
Name	Indicates the User's name
User ID	Indicates the User's User ID
Organization Unit	Indicates the OU in which the User is registered
Entitlements	
Entitlements	Indicates the number of Entitlements assigned to the selected User
Entitlement Support (%)	Indicates the percentage of Entitlements that should be assigned to the User from the entire set of Entitlements involved in the Request
Covered Entitlements	Indicates the number of Entitlements assigned to the User
Entitlement Coverage (%)	Indicates the percentage of Entitlements actually assigned to the User from the entire set of Entitlements that should be assigned to the User
Applications	
Applications	Indicates the number of Applications involving the selected User
Application Support (%)	Indicates the percentage of Applications that should be assigned to the User from the entire set of Applications involved in the Request
Covered Applications	Indicates the number of Applications assigned to the User

Table 158. User details. (continued)

User	
Attribute	Description
Application Coverage(%)	Indicates the percentage of Applications actually assigned to the User from the entire set of Applications that should be assigned to the User

The other operations for User analysis are:

- Entitlements assigned to the selected User
- Applications assigned to the selected User

Role analysis:

The Role Mining tab contains many features for investigating the structure of the candidate roles indicated by the analysis.

The left frame contains four tabs:

- Roles (default active tab)
- Entitlements
- Users
- Statistics

In the **Roles** tab, the candidate roles are characterized by a set of statuses, according to the role position in the operational flow managed by the role engineer.

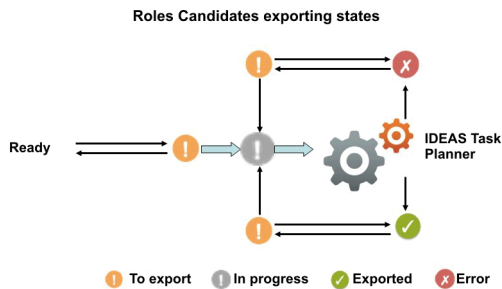


Figure 8. Possible states of candidate roles.

The main goal of Role Mining activity is to identify and import candidate roles, into "Enterprise" roles set (AG Core database).

Click **Filter** to filter candidate roles according to their names.

Each candidate role row presents the attributes shown below:

For any candidate role selected in the **Roles** tab, in the right pane you can select several tabs.

In particular, in **Roles Details** tab are shown all the characteristics of the candidate role, grouped for entity:

Table 159. Entitlement details.

Detail	Description
Role Name	Name of role
Rep. Status	Status of the role
Application	Name of the application.
Application Support (%)	Percentage of application to be assigned to the candidate roles, from the entire set of entitlements involved in the analysis.
Entitlements	Name of the entitlement.
Entitlements Support (%)	Percentage of entitlements to be assigned to the candidate roles, from the entire set of entitlements involved in the analysis.
Users	Number of users assigned to the selected role.
User Support (%)	Percentage of users to be assigned to the role, from the entire set of users involved in the analysis.
Org Units	Number of organization units involved in the selected role.
Org Unit Support (%)	Percentage of organization units to be assigned to the role, from the entire set of organization units involved in the analysis.
OU Spread	OU Spread indicates the inclination towards obtaining a very scattered or localized entitlement distribution in the OU hierarchy. See Spread.
Minimum Farness	Minimum distance between an OU and the centroid of distribution, rather than between an OU and a particular attribute such as an entitlement. See Farness.
Average Farness	Average distance of all OUs from the centroid of distribution. See Farness.
Average Coverage (%)	Average percentage of OUs assigned with the entitlement.
Maximum Coverage (%)	Maximum percentage of OUs assigned with the entitlement.
Attribute 0... Attribute 9 (for Entitlements)	Attributes configured in the section Entitlement attributes.

In the Role map, is shown the map of the candidate role.

Four other tabs (**Entitlements**, **Applications**, **Users**, **Organization Units**) can be selected for showing the related entities involved with the candidate role selected.

Finally, the **Impact Analysis** tab allows you to evaluate the changes involved in the organization if you are going to import the candidate role into "Enterprise" roles set (AG Core database).

Entitlements analysis:

This section contains many useful features for investigating the structure of the Candidate Roles from an Entitlement approach.











Entitlements are characterized by the following icons (, , ) related to the concept of "User coverage". Entitlements can be filtered (clicking **Filter**) using the filters described in the table below:

Table 160. Entitlement filters

Attribute	Description
Name	Indicates the name of the entitlement.
Entitlement Type	The entitlement can be one of the following: <ul style="list-style-type: none">  : Permission  : IT role  : Business role  : External role
Application	Name of the application.
User Coverage	This filter can assume three different values: <ul style="list-style-type: none">  Out of Role: the entitlement cannot be assigned to any qualified user using the candidate roles.  Partially covered: the entitlement can be assigned only to a subset of qualified users using the candidate roles.  Covered: the entitlement can be assigned to all qualified users using the candidate roles.

Upon selecting an entitlement in the **Entitlements** tab on the left, the **Entitlements Details** tab is by default shown on the right with the relevant information. The information is organized in the following groups: **Entitlements - Users - Organization Units**.

Table 161. Entitlement details

Attribute	Description
Application	Name of the application.
Entitlement Name	Name of the entitlement.
Users	Number of users assigned to the selected entitlement.
User Support (%)	Percentage of users that have the entitlement from the entire set of users that must have the entitlement.
Covered Users	Number of users covered with the entitlement.
User Coverage (%)	Percentage of users in the OU who are assigned to the entitlement.

Table 161. Entitlement details (continued)

Attribute	Description
Org Units	Number of organization units involved in the selected entitlement.
Org Unit Support (%)	Percentage of organization units to be assigned to the entitlement, from the entire set of organization units involved in the analysis.
Covered Org Units	Number of organization units covered with the Role entitlement.
Org Unit Coverage(%)	Percentage of organization units that are assigned with the entitlement, from the entire set of organization units that must be assigned with the entitlement.
OU Spread	OU Spread indicates the inclination towards obtaining a very scattered or localized entitlement distribution in the OU hierarchy. See Spread.
Minimum Farness	Minimum distance between an OU and the centroid of distribution, rather than between an OU and a particular attribute such as an entitlement. See Farness.
Average Farness	Average distance of all OUs from the centroid of distribution. See Farness.
Average Coverage (%)	Average percentage of OUs assigned with the entitlement.
Maximum Coverage (%)	Maximum percentage of OUs assigned with the entitlement.
Attribute 0... Attribute 9 (for Entitlements)	Attributes configured in the Entitlement attributes section.

The other operations for Entitlements analysis are:

- Users aggregated with the selected Entitlement
- OUs aggregated with the selected Entitlement

Users aggregated with the selected entitlement









The **Users** tab lists all candidate roles containing the entitlement previously selected in the **Entitlementstab**.

For each candidate role, the data set in the table below is displayed:

Table 162. Candidate Role attributes

Attribute	Description
Role Name	Indicates the name of the role.



Table 162. Candidate Role attributes (continued)

Attribute	Description
Exportation (Report/Release)	The role can have one of the following statuses: <ul style="list-style-type: none"> •  Scheduled to be exported •  Exportation in progress •  Successfully exported •  Error
Users	Indicates the number of users for the selected candidate role.
Entitlements	Indicates the number of entitlements for the selected candidate role.
Assignments	Indicates the number of user-entitlement assignments for the selected candidate role.
OU Spread	../CrossIdeas_Topics/AA/Role_Mining_Guidelines_Spread.dita is a numeric index that provides an estimate of the “homogeneous diffusion” of a role in the hierarchical structure of an organization. OU spread indicates the tendency towards a scattered/localized role distribution in the OU hierarchy.
Org Units	Indicates the number of OUs for the selected candidate role.
Applications	Indicates the number of applications for the selected candidate role.
Entitlement Type	Entitlement types include the following ones: <ul style="list-style-type: none"> •  Permission •  IT role •  Business role •  External role
Attribute 0...	Attributes that are configured in the User Attributes section.
Attribute 9	
(for Users)	
Attribute 0...	Attributes that are configured in the Entitlements Attributes section.
Attribute 9	
(for Entitlements)	

When you select a candidate role from the central pane, the users joined to the candidate role are automatically highlighted in the **Users** tab in the far right.

Listed Users are characterized by the attributes shown in the table below:

Table 163. User attributes

Attribute	Description
In/Out	The user status can be one of the following: <ul style="list-style-type: none">  In Role (Role aggregated to the User)  Out of Role (Role not aggregated to the User)
Last Name	Surname of the user.
Name	Name of the user.
User ID	Unique ID assigned to the user.
Organization Units	Name of the OU, in which the user is registered.
Attribute 0... Attribute 9 (for Users)	Attributes configured in the User attributes section.

When you select a user from the **Users** tab in the far right, all aggregated candidate roles are automatically highlighted in the central pane.

OUs aggregated with the selected entitlement

The **Organization Units** tab lists all candidate roles containing the entitlement previously selected in the **Entitlements** tab .

The attributes described in the table below are displayed for each candidate role:

Table 164. Candidate Role attributes









Attribute	Description
Role Name	Indicates the name of the role.
Exportation (Report/Release)	The role can have one of the following statuses: <ul style="list-style-type: none">  Scheduled to be exported  Exportation in progress  Successfully exported  Error
Users	Indicates the number of users for the selected candidate role.
Entitlements	Indicates the number of entitlements for the selected candidate role.
Assignments	Indicates the number of user-entitlement assignments for the selected candidate role.
OU Spread	../CrossIdeas_Topics/AA/Role_Mining_Guidelines_Spread.dita is a numeric index that provides an estimate of the “homogeneous diffusion” of a role in the hierarchical structure of an organization. OU spread indicates the tendency towards a scattered/localized role distribution in the OU hierarchy.
Org Units	Indicates the number of OUs for the selected candidate role.



Table 164. Candidate Role attributes (continued)

Attribute	Description
Applications	Indicates the number of applications for the selected candidate role.
Entitlement Type	Entitlement types include the following ones: <ul style="list-style-type: none">  Permission  IT role  Business role  External role
Attribute 0... Attribute 9 (for Users)	Attributes that are configured in the User Attributes section.
Attribute 0... Attribute 9 (for Entitlements)	Attributes that are configured in the Entitlements Attributes section.

When you select a candidate role in the central pane, the OUs joined to the candidate role are automatically highlighted in the **Organization Units** tab in the far right.

The listed OUs are characterized by the attributes shown in the table below:

Table 165. OU attributes.

Attribute	Description
In/Out	The OU status can be one of the following: <ul style="list-style-type: none">  In Role (Role aggregated to the OU)  Out of Role (Role not aggregated to the OU)
Code	Code assigned to the OU.
Name	Name of the OU, in which the user is registered.
Farness	Farness is a numeric index that provides an estimate of the virtual distance between OUs having the same entitlement/candidate role. It can measure the distance between OUs in which different registered users are assigned the same entitlement/candidate role.
Coverage (%)	Percentage of users in the OU who are assigned to the entitlement.
Users	Number of users assigned to the selected entitlement.

When you select an OU from the **OU** tab in the far right, all the aggregated candidate roles are automatically highlighted in the central pane.

Statistics:


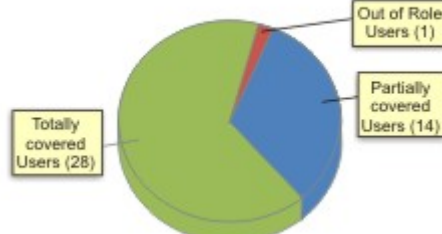
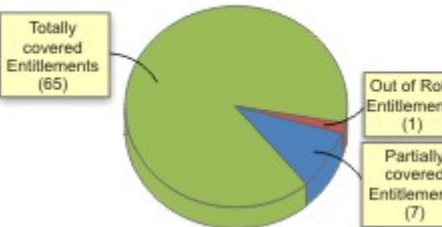
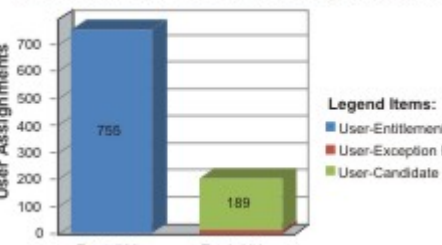
The Statistics tab provides a set of graphical dashboards for the selected analysis.

The available dashboards are structured into two tabs:

- Analysis Statistics
- Role Statistics

Analysis Statistics

Table 166. Dashboard set.





Dashboard	Description
<p style="text-align: center;">Total Roles (37)</p> 	<ul style="list-style-type: none"> • The green zone represents the collection of candidate roles, for example roles whose adoption into the organization can be considered useful. • The red zone represents exception roles, for example those built with entitlements that are not aggregated to the set of candidate roles. Every exception role is composed of a single entitlement.
<p style="text-align: center;">Analyzed Users (43)</p> 	<ul style="list-style-type: none"> • Users in the green zone: each of their assigned entitlements is involved in at least one candidate role. • Users in the blue zone: some of their assigned entitlements are not involved in any candidate role. • Users in the red zone: none of their assigned entitlements belong to any candidate role.
<p style="text-align: center;">Analyzed Entitlements (73)</p> 	<ul style="list-style-type: none"> • Entitlements in the green zone: each user assigned to these entitlements is involved in at least one candidate role. • Entitlements in the blue zone: some users assigned to these entitlements are not involved in any candidate role. • Entitlements in the red zone: none of the users assigned to these entitlements are involved in any candidate role.
<p style="text-align: center;">User Assignments (Saving 72.98%)</p> 	<ul style="list-style-type: none"> • The blue histogram shows all entitlements assigned to the considered users. • The green histogram shows all candidate roles assigned to the considered users. • The red histogram shows all exception roles assigned to the considered users.

Role statistics

The **Role Statistics** tab provides a set of histograms for a selected request.

Different filters can be chosen as described in the table below:

Table 167. Role statistics filters.

Filter	Description
Name	Name(s) of role(s) involved in the request.
Order By	You can sort the displayed data in ascending or descending order, based on the data elements provided. You can start with Users .
<i>Listed in the rows below are all the algorithm parameters involved in the request, selectable by selecting the appropriate check box. The related histogram will be displayed only if the check box is selected.</i>	
Users	Users involved in the request
Entitlements	Entitlements involved in the request
Spread	OU spread
Org Units	OUs involved in the request
Entitlement Types	The entitlement can be one of the following: <ul style="list-style-type: none"> •  : Permission •  : IT role •  : Business role •  : External role
Applications	Applications involved in the request
User Attribute 0 ... Attribute 9	Only user attributes specified in the request are available
Entitlement Attribute 0 ... Attribute 9	Only entitlement attributes specified in the request are available
Role Attribute 0 ... Attribute 9	Only role attributes specified in the request are available

The next figure shows an example with the **User** and **Entitlements** check boxes selected, where statistics are listed by entitlement in descending order.



Figure 9. Example of Statistics with User and Entitlements check boxes selected.

Update entitlements: generating a request

For information about this topic, see the IBM Security Identity Governance and Intelligence Knowledge Center at http://www.ibm.com/support/knowledgecenter/SSGHJR_5.2.1.

In the knowledge center, type the title of the user interface page in the **Search** field and press Enter. For example, if you are viewing the Manage Targets page, type manage targets in the **Search** field and press Enter.

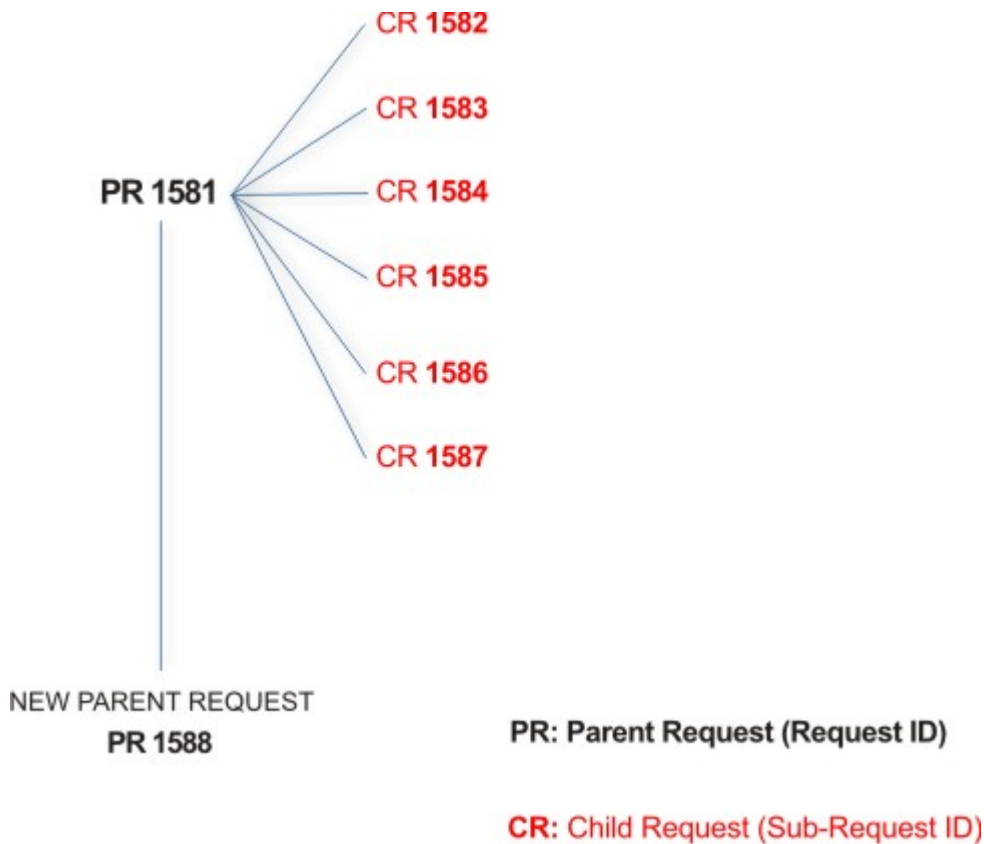
Insert/Update entitlement: processing a request

You can view a summary of the generated requests.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is in black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Request ID** and are in red.



In the previous example, **Request ID 1581**, generates six **Sub-Request ID**: 1582, 1583, ... and 1587.

There is ALWAYS the possibility to view ALL the requests registered through the Request Report activity.

However, when you are logged-in as authorizer some of the request (and sub-request) listed through the Request Report activity might not be visible because out of the scope defined for the authorizer.

The requests that are generated during the authorization process can be characterized by different statuses, which are summarized in the following table:

Table 168. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Rejected	Request can no longer be processed. It is a final status for the request.
In execution	Request waiting for the propagation to the target system.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Pending	Source request is waiting for formalization by one or more approvers.

Table 168. Request Status (continued)

Status	Description
Escalation	Request contains incompatible roles.
Partially Authorized	Request with some sub requests in authorizable status.
Partially Approved	Request with some sub requests in Approved status.
Partially Executed	Request with some sub requests in executed status.
Partially Completed	Request with all sub requests at end of their lifecycle, some Completed and some in Failed Completion status.
Partially Terminated	Request with some sub requests in Completed and some in progress.
Terminated With Reservation	In this status falls all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request can be split in several sub requests. Every sub request can be characterized by several statuses.

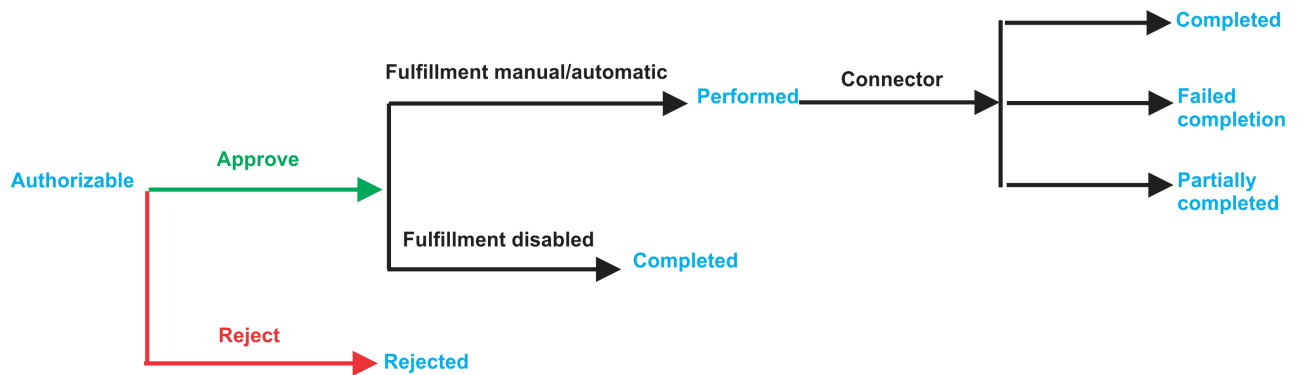


Figure 10. Statuses of a Sub Request

Statuses of a Sub Request	
Status	Description
Rejected	The sub request was rejected by the approver, and it is not fulfilled.
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Manual/Automatic, it means that the connector successfully aligned every permission on the target system.
Performed	The connector did not yet align the permissions on the target system.
Failed Completion	The connector failed to align all permission on the target system.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.

You can search specific requests with the following filters.

Click **Filter/Hide Filter** and then click **Search**.

Table 169. Filters

Filter		Description
Request ID		Unique identifier of the request
Sub Request ID		A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity		Identifier of the IAG actor that generated the request
Beneficiary Identity		Identifier of the beneficiary of the request
Created between	Start Date	Start date of the creation of the request
	End Date	End date of the creation of the request

The results are displayed in the same frame, according to the following attributes:

Requests attributes	
Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (dd/mm/yyyy) and hour (hh:mm) the request was created.
Status	The status of the sub-requests (Sub-Request ID column).

Click an item under **Applicant** or **Beneficiary** to open the related User details window and show the following information:


Table 170. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click an item under **Request ID** to view the details.

The upper part of the frame shows the following information about the **Actors of the Request**:

Table 171. Request Actors

Actor	Detail	Description
Request	ID	Unique identifier of the request
	Type	Type of request
	Status	Status of the Request
	Created on	Date (dd/mm/yyyy) and hour (hh/mm) that the request was created
Applicant/ Beneficiary/ Delegator/	Group	Group of the Applicant/Beneficiary/Delegator
	First Name	Given name of the Applicant/Beneficiary/Delegator
	Last Name	Surname of the Applicant/Beneficiary/Delegator
	User ID	Unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.
Request Notes	Request	Type of request
	to Add	Notes about the add action that was made on the <i>Entity</i> of the request
	to Remove	Notes about the remove action that was made on the <i>Entity</i> of the request
	to Update	Notes about the update action that was made on the <i>Entity</i> of the request
Additional Notes	Request notes can be specified by the author of the request or by a rule. In this field, you can add free text for any reason during the authorization or execution of the request.	

Note: The Request Notes are not mandatory. If there are no notes in the request, the fields of the Request Notes are blank.

The lower part of the frame shows a sub-set of fields related to the request submitted during the generation phase.

This subset depends by the configuration set by the Administrator through Process Designer module.

Click an item under **Sub-Request ID** to view the details.

The upper part of the frame shows the same information set shown in the above table, but related to the selected sub request.

The lower part of the frame shows a sub-set of fields related to the sub request associated to a request submitted during the generation phase.

This subset depends by the configuration set by the Administrator through Process Designer module.


Click the  **Info** icon to open the User details window and show the information in a set of tabs:

Table 172. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 173. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement info window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation

Table 174. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 175. User Details - Activities tab


Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity


Table 176. User Details - Rights

Detail	Description
Entitlement	Name of the entitlement
Right	Name of the right
Values	Value of the right

The lower part of the frame shows the following information about the requests:

Table 177. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlement involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the  **Info** icon to open the Entitlement info window and show the summarized information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 178. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.


Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles
- External Roles
- Permissions

The following icons represent these entitlements:



If notes about the considered entitlement are in the request, the  **Note** icon is available. Click it to open the Notes window and show the contents of the note.

In the central side of the frame, you find:

- Elements related to the request to be authorized.
- Elements related to the approver of the request.

In the lower side of the frame, the available buttons are:

- **Back** returns to the summary of the requests.
- **Approve** approves the request.
- **Reject** rejects a request.

Insert/Updates entitlements: executing a request

You can view a summary of the generated requests.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Requests** and are red.

The requests that are generated during the authorization process can be characterized by different statuses, which are summarized in the following table:

Table 179. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Rejected	Request can no longer be processed. It is a final status for the request.
In execution	Request waiting for the propagation to the target system.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Pending	Source request is waiting for formalization by one or more approvers.
Escalation	Request contains incompatible roles.
Partially Authorized	Request with some sub requests in authorizable status.
Partially Approved	Request with some sub requests in Approved status.
Partially Executed	Request with some sub requests in executed status.
Partially Completed	Request with all sub requests at end of their lifecycle, some Completed and some in Failed Completion status.
Partially Terminated	Request with some sub requests in Completed and some in progress.
Terminated With Reservation	In this status falls all the requests that present an unclear or unexpected behavior. It is a final status for the request.

You can search specific requests with the following filters. Click **Filter/Hide Filter** and then click **Search**.

Table 180. Filters

Filter	Description
Request ID	Unique identifier of the request
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity	Identifier of the IAG actor that generated the request

Table 180. Filters (continued)

Filter		Description
Beneficiary Identity		Identifier of the beneficiary of the request
Created between	Start Date	Start date of the creation of the request
	End Date	End date of the creation of the request

The results are displayed in the same frame, according to the following attributes:

Requests attributes	
Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (dd/mm/yyyy) and hour (hh:mm) the request was created.
Status	Request Status.

Click **Applicant** and **Beneficiary** to open the User details window and show the following information:


Table 181. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the frame shows the following information about the **Actors of the Request**:

Table 182. Request Actors

Actor	Detail	Description
Request	ID	Unique identifier of the request
	Type	Type of request
	Status	Status of the Request
	Created on	Date (dd/mm/yyyy) and hour (hh/mm) that the request was created
Applicant/ Beneficiary/ Delegator/	Group	Group of the Applicant/Beneficiary/Delegator
	First Name	Given name of the Applicant/Beneficiary/Delegator
	Last Name	Surname of the Applicant/Beneficiary/Delegator
	User ID	Unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.
Request Notes	Request	Type of request
	to Add	Notes about the add action that was made on the <i>Entity</i> of the request
	to Remove	Notes about the remove action that was made on the <i>Entity</i> of the request
	to Update	Notes about the update action that was made on the <i>Entity</i> of the request
Additional Notes	Request notes can be specified by the author of the request or by a rule. In this field, you can add free text for any reason during the authorization or execution of the request.	

Note: The Request Notes are not mandatory. If there are no notes in the request, the fields of the Request Notes are blank.


Click the  **Info** icon to open the User details window and show the information in a set of tabs:

Table 183. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).

Table 183. User Details - Details tab (continued)

Detail	Description
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 184. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement info window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation

Table 185. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 186. User Details - Activities tab


Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity


Table 187. User Details - Rights

Detail	Description
Entitlement	Name of the entitlement
Right	Name of the right
Values	Value of the right

The lower part of the frame shows the following information about the requests:

Table 188. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlement involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the  **Info** icon to open the Entitlement info window and show the summarized information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 189. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.


Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles
- External Roles
- Permissions

The following icons represent these entitlements:



If notes about the considered entitlement are in the request, the  **Note** icon is available. Click it to open the Notes window and show the contents of the note.

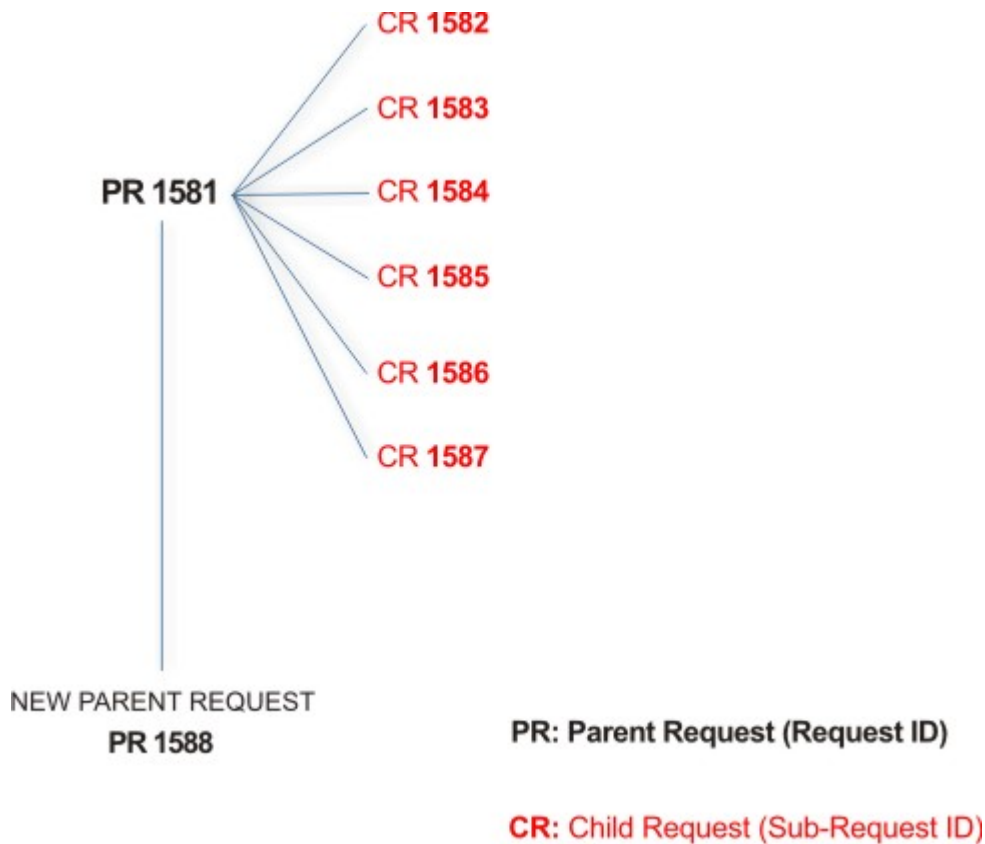
List of all requests present in the system

You can view a summary of the generated requests.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is in black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Request ID** and are in red.



In the previous example, **Request ID 1581**, generates six **Sub-Request ID**: 1582, 1583, ... and 1587.

There is ALWAYS the possibility to view ALL the requests registered through the Request Report activity.

However, when you are logged-in as authorizer some of the request (and sub-request) listed through the Request Report activity might not be visible because out of the scope defined for the authorizer.

The requests that are generated during the authorization process can be characterized by different statuses, which are summarized in the following table:

Table 190. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Rejected	Request can no longer be processed. It is a final status for the request.
In execution	Request waiting for the propagation to the target system.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Pending	Source request is waiting for formalization by one or more approvers.

Table 190. Request Status (continued)

Status	Description
Escalation	Request contains incompatible roles.
Partially Authorized	Request with some sub requests in authorizable status.
Partially Approved	Request with some sub requests in Approved status.
Partially Executed	Request with some sub requests in executed status.
Partially Completed	Request with all sub requests at end of their lifecycle, some Completed and some in Failed Completion status.
Partially Terminated	Request with some sub requests in Completed and some in progress.
Terminated With Reservation	In this status falls all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request can be split in several sub requests. Every sub request can be characterized by several statuses.

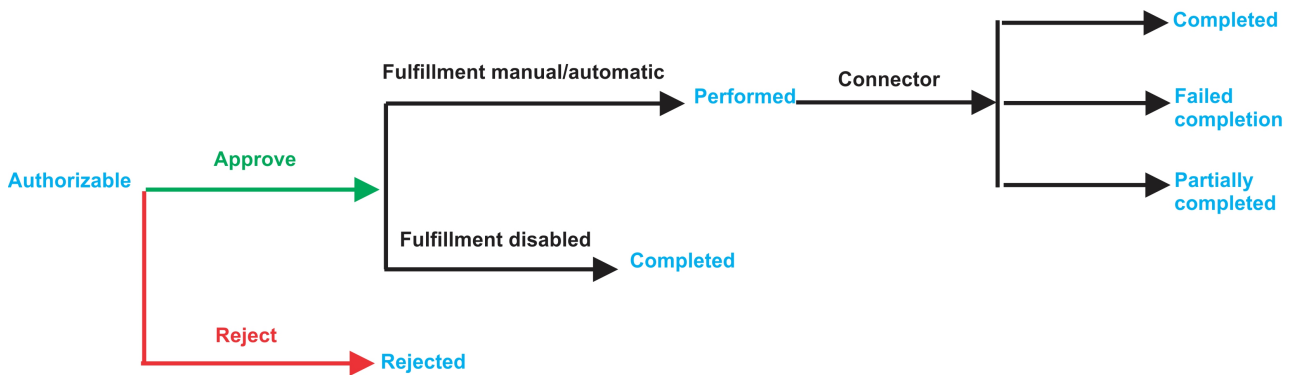


Figure 11. Statuses of a Sub Request

Statuses of a Sub Request	
Status	Description
Rejected	The sub request was rejected by the approver, and it is not fulfilled.
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Manual/Automatic, it means that the connector successfully aligned every permission on the target system.
Performed	The connector did not yet align the permissions on the target system.
Failed Completion	The connector failed to align all permission on the target system.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.

You can search specific requests with the following filters. Click **Filter/Hide Filter** and then click **Search**.

Table 191. Filters

Filter		Description
Request ID		Unique identifier of the request
Sub Request ID		A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity		Identifier of the IAG actor that generated the request
Beneficiary Identity		Identifier of the beneficiary of the request
Created between	Start Date	Start date of the creation of the request
	End Date	End date of the creation of the request

The results are displayed in the same frame, according to the following attributes:

Requests attributes	
Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (dd/mm/yyyy) and hour (hh:mm) the request was created.
Status	Request Status.

Click **Applicant** and **Beneficiary** to open the User details window and show the following information:


Table 192. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the frame shows the following information about the **Actors of the Request**:

Table 193. Request Actors

Actor	Detail	Description
Request	ID	Unique identifier of the request
	Type	Type of request
	Status	Status of the Request
	Created on	Date (dd/mm/yyyy) and hour (hh/mm) that the request was created
Applicant/ Beneficiary/ Delegator/	Group	Group of the Applicant/Beneficiary/Delegator
	First Name	Given name of the Applicant/Beneficiary/Delegator
	Last Name	Surname of the Applicant/Beneficiary/Delegator
	User ID	Unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.
Request Notes	Request	Type of request
	to Add	Notes about the add action that was made on the <i>Entity</i> of the request
	to Remove	Notes about the remove action that was made on the <i>Entity</i> of the request
	to Update	Notes about the update action that was made on the <i>Entity</i> of the request
Additional Notes	Request notes can be specified by the author of the request or by a rule. In this field, you can add free text for any reason during the authorization or execution of the request.	

Note: The Request Notes are not mandatory. If there are no notes in the request, the fields of the Request Notes are blank.


Click the  **Info** icon to open the User details window and show the information in a set of tabs:

Table 194. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).

Table 194. User Details - Details tab (continued)

Detail	Description
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 195. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement info window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation

Table 196. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 197. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity

Table 198. User Details - Rights

Detail	Description
Entitlement	Name of the entitlement
Right	Name of the right
Values	Value of the right

From the **Entitlement** tab, click the  **Info** icon to open the Entitlement info window and show the following information in the **Structure** tab:

Table 199. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

The following figure shows the generic hierarchical structure of an entitlement:

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.

Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles
- External Roles
- Permissions


The following icons represent these entitlements:




Structure of a generic entitlement

The lower part of the frame shows the following information about the requests:


Table 200. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlement involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the  **Info** icon to open the Entitlement info window and show the summarized information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

If notes about the considered entitlement are in the request, the  **Note** icon is available. Click it to open the Notes window and show the contents of the note.

User access: generating a request

Select this tab to add role access to one or more selected users.

The **Users** tab is the first step of a wizard that guides you to select users and grant them access to entitlements.


Use the following filters to search specific users and then click **Search**.

Table 201. User filters

Filter	Description
User Type	Type of user, for example, Administrative, Business, Employee, Training, External
Full Name/Code	Name and surname of the user or unique identifier of the user
Enabled	When selected, specifies a flag implies that the user can be assigned entitlements.

Users are displayed with the following attributes:

Table 202. Users list.

Field	Description
User details icon	Click the  Info icon to open the User Details window that shows the user's details, assigned entitlements, and assigned accounts.
User ID	Unique identifier of the user.
First Name	Name of the user.
Last Name	Surname of the user.
Group [Code]	Organization Unit [Univocal identifier of the OU] of the user.
User Type	Type of user (for example: Administrative, Business, Employee, Training, External).

To select the entire list of users, select the check box on the attributes row; otherwise, select the check box in the user's row.


Click the  **Info** icon to open the **details** window. This window displays user information in the following tabs:

Table 203. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 204. User Details - Entitlements tab


Details	Description
	Click Info to open the Entitlement info window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user

Table 204. User Details - Entitlements tab (continued)


Details	Description
End Date	End date of the assignation of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation

Table 205. User Details - Entitlements tab (2).



Details	Description
	Click the Info icon to open the Entitlement info window.
Name	Name of the entitlement
VV	This  icon denotes an entitlement in Visibility Violation.
Application	Type of application.
Start Date	Start date when the entitlement was assigned to the user.
End Date	End Date when the entitlement was assigned to the user.

Table 206. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 207. User Details - Rights

Detail	Description
Entitlement	Name of the entitlement
Right	Name of the right
Values	Value of the right

Table 208. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity

From the **Entitlement** tab, click the  **Info** icon to open the **Entitlement info** and show the information in the **Structure** tab

Table 209. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement

Table 209. Entitlement info - Structure (continued)

Detail	Description
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.


Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles
- External Roles
- Permissions

The following icons represent these entitlements:



Click the  **Info** icon to open the **Entitlement info** window and show the information in the following set of tabs:

- **Structure**
- **Dependencies**
- **Activity**
- **Rights**

The **Structure** tab is always available and shows the structure of the entitlement of the request; the other tabs are available only when the entitlement it is characterized by **Dependencies**, **Activities**, or **Rights**.

Click **Next** to open the “Admin Roles: Catalog” on page 90 tab.






User Access: Catalog

The Catalog tab is the second step of the wizard.

With the **Catalog** tab you can choose the entitlements and roles for the users selected in the first step of the wizard, Users .

The upper part of the frame summarizes the information about the selected users:

Table 210. User data.

Data	Description
 Info	Click the Info icon to open the Entitlement info window.
User ID	Univocal identifier of the user.
First Name	Name of the user.
Last Name	Surname of the user.
Group [Code]	Name of the organization unit or univocal identifier of the OU.
User Type	Type of user.
Risk Status	<p>The risk status associated with the user is displayed by a symbol:</p> <ul style="list-style-type: none">  There is no risk.  The risk level is low.  The risk level is medium.  The risk level is high. <p>Click the colored dot to open a window that displays:</p> <ul style="list-style-type: none"> • The Risk Activities Tree (related to a specific user) in the Risk Info tab • The Activities involved in a specific risk, in the Mitigations tab

Click the **Refresh** button to update the risk situation of the user.

The lower part of the frame includes the following tabs:

- **Current Entitlements**
- **Business Roles**
- **Application Roles**
- **Permissions**

- **External Roles**

Depending on the configuration of the activity, some of these tabs may not be present.

Current Entitlements tab

The **Current Entitlements** tab lists the entitlements assigned to the selected users. From here you can use the following filters to search specific entitlements (click **Filter > Search**):

Table 211. Filters for Current Entitlements.


Filter	Description
Application	The name of the parent application.
Name or code	The name or identification code of the entitlement.
Type	It can be: Permission, IT role, Business role, or External role.
Description	A brief description of the entitlement.
Group	The Organization unit with which the entitlement is associated.

You can start the following actions from the list of entitlements displayed :

- **Remove** (Entitlement)
- **Validity** (End date of validity)

To remove the **Current Entitlements**, click the **Remove** button (the **Remove** button will be shown in red).

To enter or change the **Validity** of the entitlements:

1. Click **Validity** to display the **Date Selection** window.
2. Click  **Calendar** to enter the end date and click **OK** to confirm.
The **Validity** button will be highlighted in orange.

To remove the end date, click the **Validity** button.

When you are done, click the **Business Roles** tab to assign Business roles, or click **Next** to go to the “User Access: Shopping Cart” on page 183tab to process the Create Access request.

Business Roles tab

The **Business Roles** tab displays the list of available Business roles for the selected users. From here you can use the following filters to search specific Business roles (click **Filter > Search**):

Table 212. Business role filters.

Filter	Description
Name or Code	The name or identification code of the Business role.
Description	A brief description of the Business role.

Table 212. Business role filters. (continued)

Filter	Description
Family	The family of the Business role.
Group	The Organization unit with which the Business role is associated.

From the list of Business roles, you can assign one or more roles to the selected users. Click **Add** (the **Add** button is highlighted in green).

If the added role has **Dependencies**, the  **Dependencies** button appears near the  **Info** button in the Business Roles list).

1. Click this button to open the **Dependencies** window and add one or more of these.
2. Click **To Cart** (the **To Cart** button is highlighted in green) to add the dependencies.
3. Click **Ok** to confirm.

Dependencies can be defined and associated with roles. Dependencies are permissions or roles that are necessary, or useful, to other roles.

For example, a role that is named TECHComm, with all the specific permissions for this position, is being defined for an employee who is to take a position as technical writer.

The technical writer reviews the draft documents that are produced by the Product Managers. They are shared in a company repository that is named DraftsOnProducts, which is a dedicated database, linked to a permission named DraftsOnProdcuts_Reader.

The DraftsOnProdcuts_Reader permission can be considered as a dependency of TECHComm.

The **Actions** menu includes the following items:

All Roles

Select this action to choose roles to assign to a selected user from the full set of available roles.

Like Mike

Select this action to assign to a selected user the same roles of another user chosen from the full set of users.


When you are done, click the **Application Roles** tab to assign Application roles, or click **Next** to go to the “User Access: Shopping Cart” on page 183 tab to process the Create Access request.

Application Roles tab

The **Application Roles** tab displays the list of available IT roles ordered by parent application. From here you can use the following filters to search specific entitlements (click **Filter** > **Search**):

Table 213. Application role filters.

Filter	Description
Application	The name of the parent application.
Name or Code	The name or identification code of the IT role.
Family	The family of the IT role.
Description	A brief description of the IT role.
Group	The Organization unit with which the entitlement is associated.

Each row of the list includes two **Info** icons (). Click the one under the **Application** heading to view details of the parent application. Click the one on the far right to view details of the entitlement.

From the list of entitlements, you can assign one or more roles to the selected users. Click **Add** (the **Add** button is highlighted in green).

The **Actions** menu includes the following items:

All Roles

Select this action to choose roles to assign to a selected user from the full set of available roles.

Like Mike

Select this action to assign to a selected user the same roles of another user chosen from the full set of users.


When you are done, click the **Permissions** tab to assign Permissions, or click **Next** to go to the “User Access: Shopping Cart” on page 183 tab to process the Create Access request.

Permissions tab

The **Permissions** tab displays the list of available permissions ordered by parent application. From here you can use the following filters to search specific permissions (click **Filter** > **Search**):

Table 214. Permission filters.

Filter	Description
Application	The name of the parent application.
Name or Code	The name or identification code of the permission.
Family	The family of the permission.
Description	A brief description of the permission.
Group	The Organization unit with which the permission is associated.

Each row of the list includes two **Info** icons (). Click the one under the **Application** heading to view details of the parent application. Click the one on the far right to view details of the entitlement.

From the list of entitlements, you can assign one or more permissions to the selected users. Click **Add** (the **Add** button is highlighted in green).

The **Actions** menu includes the following items:

All Roles

Select this action to choose roles to assign to a selected user from the full set of available roles.

Like Mike

Select this action to assign to a selected user the same roles of another user chosen from the full set of users.


When you are done, click the **External Roles** tab to assign external roles, or click **Next** to go to the “User Access: Shopping Cart” tab to process the Create Access request.

External Roles tab

The **External Roles** tab displays the list of available External roles ordered by parent application. From here you can use the following filters to search specific External roles (click **Filter** > **Search**):

Table 215. External roles filters.

Filter	Description
Application	The name of the parent application.
Name or Code	The name or identification code of the External role.
Family	The family of the External role.
Description	A brief description of the External role.
Group	The Organization unit with which the External role is associated.

Each row of the list includes two **Info** icons (). Click the one under the **Application** heading to view details of the parent application. Click the one on the far right to view details of the entitlement.

From the list of entitlements, you can assign one or more External Roles to the selected users. Click **Add** (the **Add** button is highlighted in green).

The **Actions** menu includes the following items:

All Roles

Select this action to choose roles to assign to a selected user from the full set of available roles.

Like Mike

Select this action to assign to a selected user the same roles of another user chosen from the full set of users.

When you are done, click **Next** to go to the “User Access: Shopping Cart” tab to process the Create Access request.

User Access: Shopping Cart

This is the third step of the Create Access Request wizard.


The Shopping Cart tab hosts a summary tree structure:

Operation	Name	Value	Application	Group [Code]	Hierarchy	Description	VV	Scope	New Start Date	New End Date
▼ Add	LucaBR						1			
▼ Add	SAP-HRP025_Z-PY_CSP		SAP-HR				1			
▼ Add	ALPHA1		ALPHA				1			
▶	aaaa	<input type="text"/>								
▶	bbbb	<input type="text"/>								
▶	fourth	<input type="text"/>								
▼ Change	LOGIN		Gamma	ACME Corp. [root]	ORGANIZATIONAL_UNIT		1			Mar 15, 2016
▼ Remove	AGOV_INSERT/TELEPHONY R		AGOV	ACME Corp. [root]	ORGANIZATIONAL_UNIT		1			


Figure 12. Shopping Cart summary tree structure.

The **Operation** column lists the operations performed in the tabs under **Catalog**:

- **Add**
- **Remove**
- **Change** (is referred to the **Validity** change in the “User Access: Catalog” on page 179 tab)

When you select the  **Clear** button, the operation is revoked and is not taken into consideration when the Request is processed.

The **Application** column lists the names of the Applications of the Entitlements.

The **Name** column lists the Entitlements involved in the performed operation; if the Entitlement is a **Permission**, it may have one or more associated  **Rights** and it is possible to assign a **Value** to each right.

A Right is defined by two attributes: Key (*aaaa* in the example figure) and Value (*v1* in the example figure).

The Key attribute is an identifying name while the Value attribute can be defined each time. A configurable default value can be provided for the Value attribute.


Rights can be:


- single-value
- multi-value

In either case (single/multi value) you can choose from a predefined set of values found in **Rights Single/Multi Value with Look up**.

Table 216. Rights property.








Value	Look up	No Look up
Single	A single-value Right with lookup allows to choose a single value Vx from a set of several values (V1,V2, ... VN)	It is not possible to choose from a set of values.
Multi	A multi-value Right with lookup allows to choose a subset of values (Vx,Vy,Vz,...) from a larger set of values (V1,V2, ... VN).	It is not possible to choose from a set of values.


When a Right is with Lookup, a  **Browse** button is available nearby. Click it to display the **Rights** window, where you can pick values.

The presence of the  **Role Alignment Violation** icon in the **VV** column, denotes an Entitlement in Role Alignment Violation. An Entitlement is in VV when there is a special reason to assign an Entitlement to a User of that OU but you do not want the Entitlement to be available to the other users of the OU.

One or more of the following buttons are enabled for each entitlement: and displayed next to the VV column:

Table 217. Buttons and Icons.

Button/Icon	Description
	Note: click this button to display the Notes window where you can write notes that will be annexed to the delegation.
	Validity: click this button to display the Date Selection window where you can enter the Start Date and the End Date of the delegation.
Buttons and Icons available only for the Admin Access Request	
	Application Scope: click this button to display the Resource Assign window where you can select one or more Applications to assign.
	Org.Units Scope: click this button to display the Resource Assign window where you can select one or more Org.Units to assign.
	Business Role Scope: click this button to display the Resource Assign window where you can select one or more BRoles to assign.
	Risk Scope: click this button to display the Resource Assign window where you can select one or more Risks to assign.
	Attribute Hierarchy Scope: click this button to display the Resource Assign window where you can select one or more Attribute Hierarchy to assign.

The **New Start Date**/**New End Date** columns list the dates defined with the  **Validity** button.

User access: processing a request

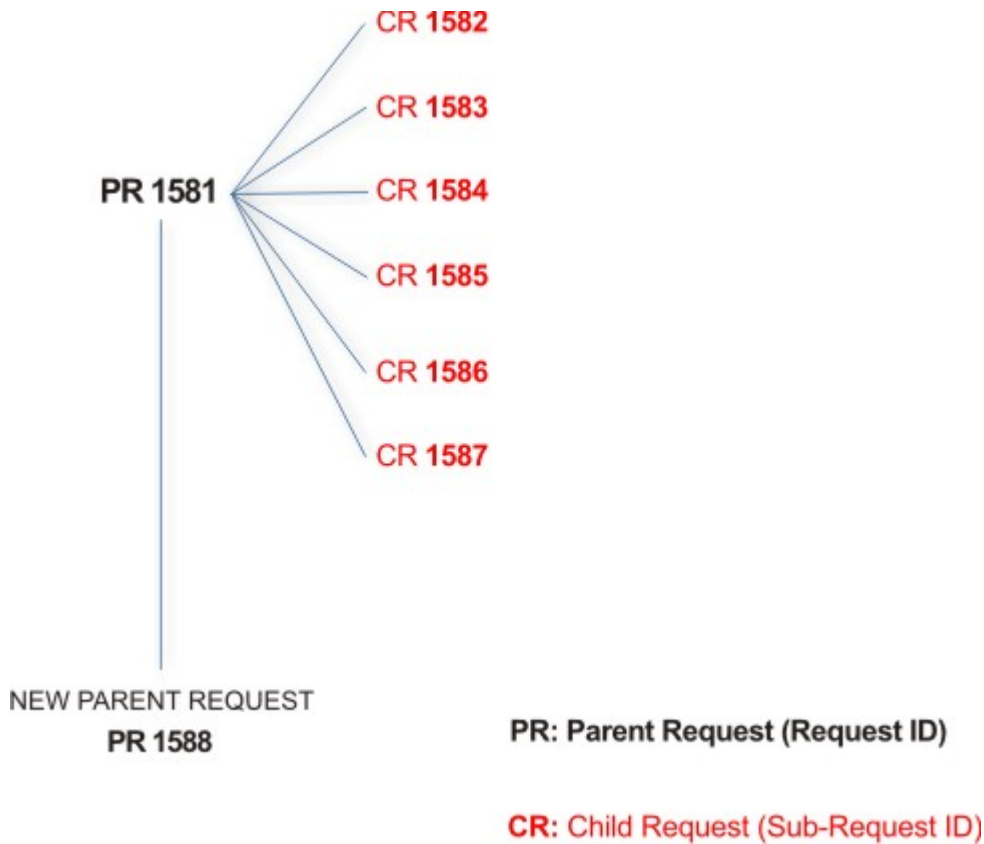
You can view a summary of the generated requests.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is in black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Request ID**

and are in red.



In the previous example, **Request ID 1581**, generates six **Sub-Request ID**: 1582, 1583, ... and 1587.

There is ALWAYS the possibility to view ALL the requests registered through the Request Report activity.

However, when you are logged-in as authorizer some of the request (and sub-request) listed through the Request Report activity might not be visible because out of the scope defined for the authorizer.

The requests that are generated during the authorization process can be characterized by different statuses, which are summarized in the following table:

Table 218. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Rejected	Request can no longer be processed. It is a final status for the request.
In execution	Request waiting for the propagation to the target system.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.

Table 218. Request Status (continued)

Status	Description
Pending	Source request is waiting for formalization by one or more approvers.
Escalation	Request contains incompatible roles.
Partially Authorized	Request with some sub requests in authorizable status.
Partially Approved	Request with some sub requests in Approved status.
Partially Executed	Request with some sub requests in executed status.
Partially Completed	Request with all sub requests at end of their lifecycle, some Completed and some in Failed Completion status.
Partially Terminated	Request with some sub requests in Completed and some in progress.
Terminated With Reservation	In this status falls all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request can be split in several sub requests. Every sub request can be characterized by several statuses.

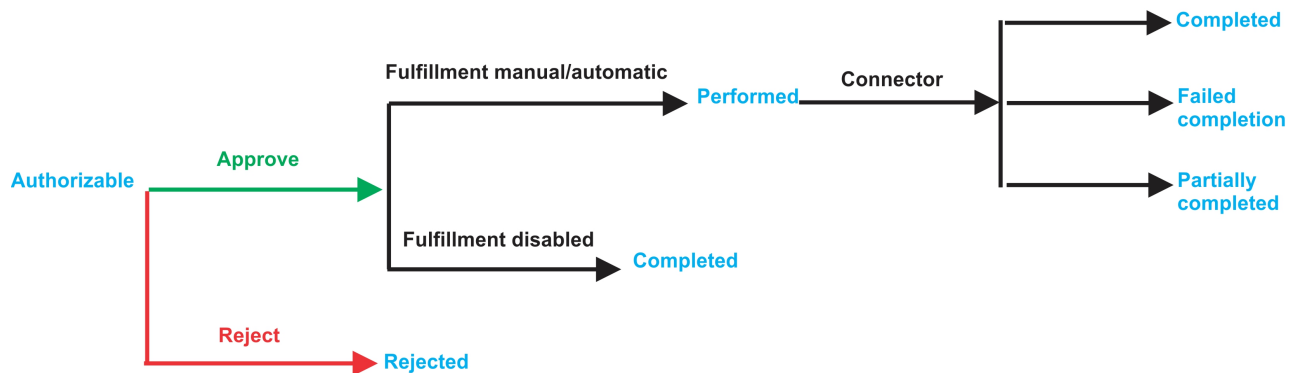


Figure 13. Statuses of a Sub Request

Statuses of a Sub Request	
Status	Description
Rejected	The sub request was rejected by the approver, and it is not fulfilled.
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Manual/Automatic, it means that the connector successfully aligned every permission on the target system.
Performed	The connector did not yet align the permissions on the target system.
Failed Completion	The connector failed to align all permission on the target system.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.

You can search specific requests with the following filters. Click **Filter/Hide Filter** and then click **Search**.

Table 219. Filters

Filter		Description
Request ID		Unique identifier of the request
Sub Request ID		A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity		Identifier of the IAG actor that generated the request
Beneficiary Identity		Identifier of the beneficiary of the request
Created between	Start Date	Start date of the creation of the request
	End Date	End date of the creation of the request

The results are displayed in the same frame, according to the following attributes:

Requests attributes	
Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (dd/mm/yyyy) and hour (hh:mm) the request was created.
Status	Request Status.

Click **Applicant** and **Beneficiary** to open the User details window and show the following information:

Table 220. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).


Table 220. User Details - Details tab (continued)

Detail	Description
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the frame shows the following information about the **Actors of the Request**:

Table 221. Request Actors

Actor	Detail	Description
Request	ID	Unique identifier of the request
	Type	Type of request
	Status	Status of the Request
	Created on	Date (dd/mm/yyyy) and hour (hh/mm) that the request was created
Applicant/ Beneficiary/ Delegator/	Group	Group of the Applicant/Beneficiary/Delegator
	First Name	Given name of the Applicant/Beneficiary/Delegator
	Last Name	Surname of the Applicant/Beneficiary/Delegator
	User ID	Unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.
Request Notes	Request	Type of request
	to Add	Notes about the add action that was made on the <i>Entity</i> of the request
	to Remove	Notes about the remove action that was made on the <i>Entity</i> of the request
	to Update	Notes about the update action that was made on the <i>Entity</i> of the request
Additional Notes	Request notes can be specified by the author of the request or by a rule. In this field, you can add free text for any reason during the authorization or execution of the request.	

Note: The Request Notes are not mandatory. If there are no notes in the request, the fields of the Request Notes are blank.


Click the  **Info** icon to open the User details window and show the information in a set of tabs:

Table 222. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 223. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement info window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation

Table 224. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 225. User Details - Activities tab


Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity


Table 226. User Details - Rights

Detail	Description
Entitlement	Name of the entitlement
Right	Name of the right
Values	Value of the right

The lower part of the frame shows the following information about the requests:

Table 227. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlement involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the  **Info** icon to open the Entitlement info window and show the summarized information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 228. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.


Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles
- External Roles
- Permissions

The following icons represent these entitlements:



If notes about the considered entitlement are in the request, the  **Note** icon is available. Click it to open the Notes window and show the contents of the note.

In the central side of the frame, you find:

- Elements related to the request to be authorized.
- Elements related to the approver of the request.

In the lower side of the frame, the available buttons are:

- **Back** returns to the summary of the requests.
- **Approve** approves the request.
- **Reject** rejects a request.

User access: executing a request

You can view a summary of the generated requests.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Requests** and are red.

The requests that are generated during the authorization process can be characterized by different statuses, which are summarized in the following table:

Table 229. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Rejected	Request can no longer be processed. It is a final status for the request.
In execution	Request waiting for the propagation to the target system.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Pending	Source request is waiting for formalization by one or more approvers.
Escalation	Request contains incompatible roles.
Partially Authorized	Request with some sub requests in authorizable status.
Partially Approved	Request with some sub requests in Approved status.
Partially Executed	Request with some sub requests in executed status.
Partially Completed	Request with all sub requests at end of their lifecycle, some Completed and some in Failed Completion status.
Partially Terminated	Request with some sub requests in Completed and some in progress.
Terminated With Reservation	In this status falls all the requests that present an unclear or unexpected behavior. It is a final status for the request.

You can search specific requests with the following filters. Click **Filter/Hide Filter** and then click **Search**.

Table 230. Filters

Filter	Description
Request ID	Unique identifier of the request
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity	Identifier of the IAG actor that generated the request

Table 230. Filters (continued)

Filter		Description
Beneficiary Identity		Identifier of the beneficiary of the request
Created between	Start Date	Start date of the creation of the request
	End Date	End date of the creation of the request

The results are displayed in the same frame, according to the following attributes:

Requests attributes	
Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (dd/mm/yyyy) and hour (hh:mm) the request was created.
Status	Request Status.

Click **Applicant** and **Beneficiary** to open the User details window and show the following information:


Table 231. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the frame shows the following information about the **Actors of the Request**:

Table 232. Request Actors

Actor	Detail	Description
Request	ID	Unique identifier of the request
	Type	Type of request
	Status	Status of the Request
	Created on	Date (dd/mm/yyyy) and hour (hh/mm) that the request was created
Applicant/ Beneficiary/ Delegator/	Group	Group of the Applicant/Beneficiary/Delegator
	First Name	Given name of the Applicant/Beneficiary/Delegator
	Last Name	Surname of the Applicant/Beneficiary/Delegator
	User ID	Unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.
Request Notes	Request	Type of request
	to Add	Notes about the add action that was made on the <i>Entity</i> of the request
	to Remove	Notes about the remove action that was made on the <i>Entity</i> of the request
	to Update	Notes about the update action that was made on the <i>Entity</i> of the request
Additional Notes	Request notes can be specified by the author of the request or by a rule. In this field, you can add free text for any reason during the authorization or execution of the request.	

Note: The Request Notes are not mandatory. If there are no notes in the request, the fields of the Request Notes are blank.


Click the  **Info** icon to open the User details window and show the information in a set of tabs:

Table 233. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).

Table 233. User Details - Details tab (continued)

Detail	Description
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 234. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement info window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation

Table 235. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 236. User Details - Activities tab


Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity


Table 237. User Details - Rights

Detail	Description
Entitlement	Name of the entitlement
Right	Name of the right
Values	Value of the right

The lower part of the frame shows the following information about the requests:

Table 238. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlement involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the  **Info** icon to open the Entitlement info window and show the summarized information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 239. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.


Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles
- External Roles
- Permissions

The following icons represent these entitlements:



If notes about the considered entitlement are in the request, the  **Note** icon is available. Click it to open the Notes window and show the contents of the note.

Create/Update user: generating a request

You can insert a new user or update information for a registered user.

- Create User
- Update User

Insert user: generating a request

You can insert or update a new user.



Insert User

From the **User Creation** tab, you can complete the form for the **User Create Request**.

The structure and the contents of the form depend by the configuration provided through:

- the Access Governance Core module, in **Settings > Core Configurations > User Virtual Attributes** panel.
- the Process Designer module, in **Manage > Activity** panel.

An example of a possible form it's indicated in the table below:

User Creation field	
Field	Description
Code	Univocal identifier of the user.
First Name	Name of the user.
Last Name	Surname of the user.
Email	Email of the user.
User Type	Type of user.
ID External Table	Univocal identifier of the External Table.
Address	Address of the user.
City	City of the user.
State	State of the user.
Country	Country of the user.
Phone Number	Phone number of the user.
Gender	Gender of the user.
Date of Birth	Date of birth of the user. Click  Calendar to choose the date. Click  Clear to delete the date of birth.

The fields mandatory are indicated with the presence of an *.

Click **Submit** to process the request.

Note: **Previous** and **Next** are disabled. The request has one step.

Update user: generating a request

You can update information about a registered user.

Update User

From the **Users** tab, you can view a list of users.

You have to select the user that you want to manage in the next step.

Clicking on the blue icon on the left, you can view the details related to the user.

Click **Next** button to proceed.



Note: **Previous** is disabled.

From the **User Update** tab, you can complete the form for the **User Update Request**.

The structure and the contents of the form depend by the configuration provided through:

- the Access Governance Core module, in **Settings > Core Configurations > User Virtual Attributes** panel.
- the Process Designer module, in **Manage > Activity** panel.

An example of a possible form it's indicated in the table below:

User Creation field	
Field	Description
Code	Univocal identifier of the user.
First Name	Name of the user.
Last Name	Surname of the user.
Email	Email of the user.
User Type	Type of user.
ID External Table	Univocal identifier of the External Table.
Address	Address of the user.
City	City of the user.
State	State of the user.
Country	Country of the user.
Phone Number	Phone number of the user.
Gender	Gender of the user.
Date of Birth	Date of birth of the user. Click  Calendar to choose the date. Click  Clear to delete the date of birth.

The fields mandatory are indicated with the presence of an *.

Click **Submit** to process the request.

Note: **Previous** and **Next** are disabled.

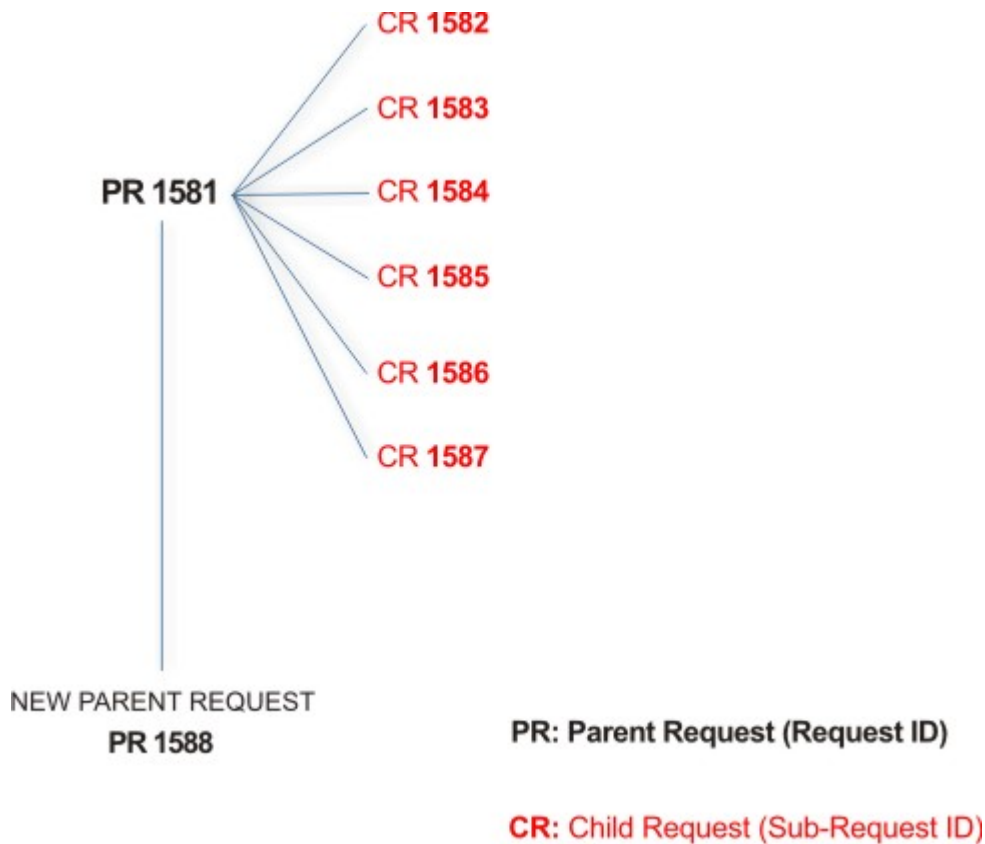
Insert/Update user: processing a request

You can view a summary of the generated requests.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is in black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Request ID** and are in red.



In the previous example, **Request ID 1581**, generates six **Sub-Request ID**: 1582, 1583, ... and 1587.

There is ALWAYS the possibility to view ALL the requests registered through the Request Report activity.

However, when you are logged-in as authorizer some of the request (and sub-request) listed through the Request Report activity might not be visible because out of the scope defined for the authorizer.

The requests that are generated during the authorization process can be characterized by different statuses, which are summarized in the following table:

Table 240. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Rejected	Request can no longer be processed. It is a final status for the request.
In execution	Request waiting for the propagation to the target system.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Pending	Source request is waiting for formalization by one or more approvers.

Table 240. Request Status (continued)

Status	Description
Escalation	Request contains incompatible roles.
Partially Authorized	Request with some sub requests in authorizable status.
Partially Approved	Request with some sub requests in Approved status.
Partially Executed	Request with some sub requests in executed status.
Partially Completed	Request with all sub requests at end of their lifecycle, some Completed and some in Failed Completion status.
Partially Terminated	Request with some sub requests in Completed and some in progress.
Terminated With Reservation	In this status falls all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request can be split in several sub requests. Every sub request can be characterized by several statuses.

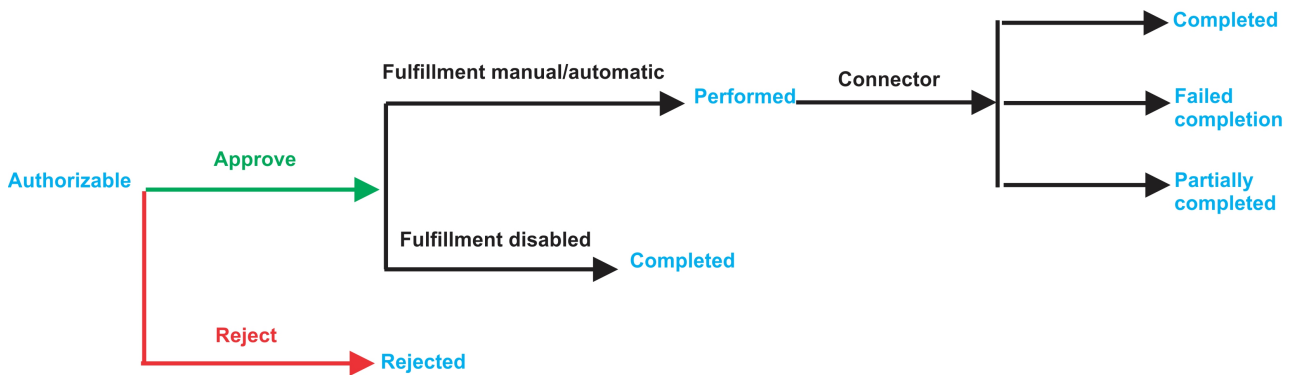


Figure 14. Statuses of a Sub Request

Statuses of a Sub Request	
Status	Description
Rejected	The sub request was rejected by the approver, and it is not fulfilled.
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Manual/Automatic, it means that the connector successfully aligned every permission on the target system.
Performed	The connector did not yet align the permissions on the target system.
Failed Completion	The connector failed to align all permission on the target system.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.

You can search specific requests with the following filters.

Click **Filter/Hide Filter** and then click **Search**.

Table 241. Filters

Filter		Description
Request ID		Unique identifier of the request
Sub Request ID		A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity		Identifier of the IAG actor that generated the request
Beneficiary Identity		Identifier of the beneficiary of the request
Created between	Start Date	Start date of the creation of the request
	End Date	End date of the creation of the request

The results are displayed in the same frame, according to the following attributes:

Requests attributes	
Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (dd/mm/yyyy) and hour (hh:mm) the request was created.
Status	The status of the sub-requests (Sub-Request ID column).

Click an item under **Applicant** or **Beneficiary** to open the related User details window and show the following information:


Table 242. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click an item under **Request ID** to view the details.

The upper part of the frame shows the following information about the **Actors of the Request**:

Table 243. Request Actors

Actor	Detail	Description
Request	ID	Unique identifier of the request
	Type	Type of request
	Status	Status of the Request
	Created on	Date (dd/mm/yyyy) and hour (hh/mm) that the request was created
Applicant/ Beneficiary/ Delegator/	Group	Group of the Applicant/Beneficiary/Delegator
	First Name	Given name of the Applicant/Beneficiary/Delegator
	Last Name	Surname of the Applicant/Beneficiary/Delegator
	User ID	Unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.
Request Notes	Request	Type of request
	to Add	Notes about the add action that was made on the <i>Entity</i> of the request
	to Remove	Notes about the remove action that was made on the <i>Entity</i> of the request
	to Update	Notes about the update action that was made on the <i>Entity</i> of the request
Additional Notes	Request notes can be specified by the author of the request or by a rule. In this field, you can add free text for any reason during the authorization or execution of the request.	

Note: The Request Notes are not mandatory. If there are no notes in the request, the fields of the Request Notes are blank.

The lower part of the frame shows a sub-set of fields related to the request submitted during the generation phase.

This subset depends by the configuration set by the Administrator through Process Designer module.

Click an item under **Sub-Request ID** to view the details.

The upper part of the frame shows the same information set shown in the above table, but related to the selected sub request.

The lower part of the frame shows a sub-set of fields related to the sub request associated to a request submitted during the generation phase.

This subset depends by the configuration set by the Administrator through Process Designer module.


Click the  **Info** icon to open the User details window and show the information in a set of tabs:

Table 244. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 245. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement info window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation

Table 246. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 247. User Details - Activities tab


Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity


Table 248. User Details - Rights

Detail	Description
Entitlement	Name of the entitlement
Right	Name of the right
Values	Value of the right

The lower part of the frame shows the following information about the requests:

Table 249. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlement involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The  icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the  **Info** icon to open the Entitlement info window and show the summarized information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 250. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.


Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles
- External Roles
- Permissions

The following icons represent these entitlements:



If notes about the considered entitlement are in the request, the  **Note** icon is available. Click it to open the Notes window and show the contents of the note.

In the central side of the frame, you find:

- Elements related to the request to be authorized.
- Elements related to the approver of the request.

In the lower side of the frame, the available buttons are:

- **Back** returns to the summary of the requests.
- **Approve** approves the request.
- **Reject** rejects a request.

Insert/Update user: executing a request

For this type of authorization workflow the execution step is an empty step.

For technical reasons of compatibility, this workflow is ended by an empty execution step, that don't requires any action.

Chapter 7. Introduction to Business Activity Mapping

Business Activity Mapping (TT) module aimed at managing relations between permissions and activities

The Business Activity Mapping module allows the user to act on these relations from two perspectives:

- Permissions-Activities
- Activities-Permissions

Dashboard

The upper part of the Dashboard contains a summary of the following permission statuses:

Linked

The permission is joined to an activity.

Ignored

The permission is not joined to any activity.

Missing Activity

The operator does not know to which activities to join the permission.

To be Defined (TBD)

The permission is not joined to any activity but is not in the **Ignored** or **Missing Activity** status.

The green status bar and the numbers X/Y change according to the number of permissions processed.

For example, the following figure shows 342 permissions to process, where 90 are **Linked**, 0 are **Ignored** or in **Missing Activity**, and 252 are **To be Defined**.





Figure 15. Summary of permissions statuses

The upper right part of the page contains information about **Last Changed** and about the user who made them.



Note: The data beyond the green status bar refers to the number of the permissions and not to the association between entities.

The following filters are available by clicking **Filter/Hide Filter**:




Dashboard Filters	
Filter	Description
Application	Clicking  Application opens the Applications window. You can select the available application from the list. The list of available applications changes, depending on the visibility of the user.
Activity	Clicking  Activity opens the Activities window. You can select activities from the Activity tree tab or search from the Activity tab.
Permission	Name of the permission.
Status	Status of the permission <ul style="list-style-type: none"> • To be Defined • Linked • Ignored • Missing Activity

The results are displayed in the same page and summarize the associations made according to the following attributes:

Dashboard Details	
Detail	Description
Application	Name of the application.
Permission	Name of the permission.
Status	Status of the permission.
Activity	Activity that is associated with the permission.

If the same permission is joined to more than one activity, the permission is displayed several times.


Figure 16. Permission-activity relationship

Application	Permission	Status	Activity
Hyperion-GRS	 cn=GG-SH-GRS-GRS_ADMIN,OU=GroupsIAM,OU=InfrastructureServices,DC=IAMresources,DC=ACMEiam	Linked	Consolidation Rectification
ACME Portal	 ing_administrators	Linked	Accounts payable
ACME Portal	 ing_administrators	Linked	Market Analysis2

Permission Perspective

On this tab, you can associate Permissions with one or more Activities.

On the **Permission** tab (left), you can search a specific Permission with the following filters. (Click **Filter/Hide Filter**.)

Permission filters	
Filter	Description
Application	Name of the Application. Click  Application to open the Applications window. You can choose the available Application from the list. The list changes depending on the User's visibility.
Permission	Name of the Permission.
Status	Status of the Permission.

Results are displayed in the same frame according to the following attributes:

Permission attributes	
Attribute	Description
Status	Status of the Permission.
Permission	Name of the Permission.
Application	Name of the Application.

On the **Permission** tab, click a Permission to enable the **Details** tab (right).

The upper part of this frame displays information about the selected Permission. It also displays two radio-buttons to switch the status of the selected Permission from **TBD** to **Ignore** or **Missing Activity**.

Permission details	
Detail	Description
Name	Name of the Permission.
Application	Name of the Application.
Description	Brief description of the Permission.

The **Actions** menu provides the following functions:

- **Add** assigns an Activity to the selected Permission.
- **Remove** removes an Activity from the selected Permission.

When the Permission-Activity association is removed, the status of the Permission returns to **To be Defined**.

When you finish, click **Save** on the lower right side of the frame.

Note: When a Permission is in **Linked** status, you cannot change to any other status. To switch the status of the Linked permission, you must remove the joined Activity.

Activity Perspective

You can join activities to one or more permissions or groups.

On the **Activity tree** tab, you can browse the activity tree for the required activity. On the **Activity** tab, the Name (name of the activity) and the Identifier (univocal identifier of the activity) filters for search activity are indicated. Click the **Filter/Hide Filter**.

On the **Actions** menu, **View** switches from the Activities flat view to the hierarchical view (**Activity tree** tab).

By selecting an activity from the list, the **Details** tab is enabled and shows the permissions and groups that are joined to the selected activity.

The **Actions** menu provides the following functions:

- **Add Group** adds a root level group that is identified as **PROFILE_GROUP_random_number**
Where
PROFILE_GROUP is a fixed string.
random_number is a random label that is composed of five ciphers. You cannot modify this name. A root level group can include permissions and groups. The groups included in the root level group are identified by the **Group** icon.
- **Add Perm** (permission) adds a permission directly to the selected activities or to a group.
- **Add Rights** is enabled only if the activity is joined to a permission with rights, and it can define the values for the rights.
- **Remove** removes permissions and groups. Removing a group instantly removes everything that is joined with the group.
- **And/Or** inverts the value of the Boolean condition of the selected node (Groups, Permissions, and Rights).

Note: The **AND/OR** condition is applied to all properties of permissions and groups and to everything contained in the groups. This condition is useful for the segregation of duty analysis.

Chapter 8. Introduction to Report Client

Report Client (RC) module allows to configure and run reports designed by the administrator through Report Designer.

IBM Security Identity Governance and Intelligence Report Designer module's front-end component, provides a modeler that can outline every type of report. Using this modeler, the administrator can visually describe the entire report creation process.

Configuring a report determines:

- The data model entities that are in the report
- The output format of the report
- The scheduling of the effective run of the report

These three main actions are supported by a wizard.

Users can configure all the aspects of the report with a discrete number of steps, which vary according to the report.

Report

The following functions for managing the main entities of this module are available:

- Request
- Download
- Passphrase

Note: For unauthorized users, the **Reports** menu is not active. If the menu is active but the **Request** tab is empty, no reports are assigned to or available for the user who is logged in.

Request

The left side of the Reports page is tree-structured and contains the assigned reports. Reports are always the leafs of the hierarchy.

All elements of the report set are represented as leaf nodes. Every node is labeled with the report name that was created by an administrator of the Report Designer (RD) module.

The Report Designer administrator can classify the available reports into a hierarchy of folders that are labeled with specific names. Every folder can contain specific set of reports. A folder can contain a set of report (leaves of the hierarchy) or other folders. You can recursively repeat this structure for each folder.

When the authorized user considers a report, that user can configure some settings, which are organized into a wizard that has several steps. The available settings are outlined by the administrator of the Report Designer module.

If the user does not add an item to the **Assigned Applications** page, all the **Visibility-Entities** are selected for the report.

After the report is configured, click **Execute** as the last step.

The Report Configuration wizard: how to configure a report

The configuration of a report is managed with a wizard, which is an interactive utility that guides users through a multistep process.

In every step of the wizard, the user can configure a specific tab, which is dedicated to a limited subset of information.

The user can navigate back and forward through the sequence of steps in the wizard.

See the sequence of steps for the configuration wizard in the following table:

Configuration Steps		
Step (tab)	Description	Always/Optional
Details tab	Shows the description of the report (read-only).	Always present
Visibility - Users tab	Specifies which users are considered in the report generation.	Optional
Visibility - Applications tab	Specifies which application is considered in the report generation.	Optional
Visibility - Entitlements tab	Specifies which entitlements are considered in the report generation.	Optional
Visibility - Organization Units tab	Specifies which organization units are considered in the report generation.	Optional
Visibility - Activities tab	Specifies which activities are considered in the report generation.	Optional
Visibility - Configurations tab	Specifies which type of account configurations are considered in the report generation.	Optional
Filters tab	Specifies which type of filters are used for the report generation.	Always present
Schedule tab	Specifies the scheduling parameters for the report.	Always present

Download

After you run a report, you can check its status or download it.

The following table describes the various status labels for reports:

Report Status	
Status	Description
Pending	The report is waiting to run.

Report Status	
Status	Description
Running	The report is running.
Download	The report can be downloaded by the user.
Error	An error occurred while the report was running.

Note: When the report is in the Download status, you can download it so it cannot be deleted.

The following figure shows a sample report in XLSX file format (User Imported report):

ID	IDEAS ID	Deleted	User ID	First Name	Surname	Employment type	User Status	User type	Position
51164	83491	0	s25140	Sandra	Strecher	I	A	primary	staff@34-34000-50037990
51165	83492	0	s25488	Oi Yan	Fung	I	A	primary	staff@34-34000-50037837

Figure 17. Report sample: User Imported

If provided by the Report Designer administrator, the report can have either a cake or bar chart, as shown in the following example:

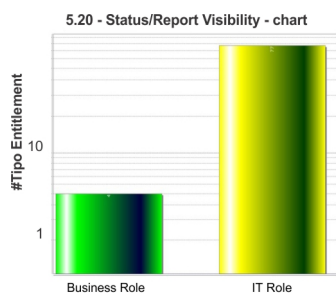


Figure 18. Chart: Bar type

Passphrase

A report console user can receive an email that contains a passphrase so that the user can download a report that was run by another user.

Set the received passphrase in the Download Report window and follow the system dialog window to download the report.

Use this method to obtain a report that is not in the set of available reports for the logged in user. See the **Request** tab.

Part 2. Employees

Employees are defined in the *Regular Users schema* and can perform tasks in the Service Center.

For more information about the tasks that employees can do, see Personas and use cases.

Chapter 9. Logging in to the Service Center

When you log in to the Service Center for the first time, you are prompted to provide answers to security questions.

Before you begin

You must have your user ID and password from your system administrator.

About this task

The Service Center includes applications that are intended for users who are not administrators. Business users, such as managers and employees can do tasks in the Service Center, depending on the access that is granted to them by an administrator.

The Self Care application is available in the Service Center. Within the Self Care application, employees can change their account passwords, view their password change requests, and update their security questions.

Be sure to change your password after you log in to the Service Center for the first time.

Procedure

1. From the Service Center Login page, type your user ID and password, and then click **Log In**.
2. Select the security questions and provide answers that you can easily remember. The answers are not case-sensitive.
3. On the Service Center home page, click the application menu icon, and select **Self Care**.

What to do next

You can change your account password, view your requests, and update your security questions from the Self Care application.

“Resetting my forgotten password” on page 5

If you forgot your Service Center password, you can either specify a new password or have the system generate new password.

Chapter 11, “Changing my account password,” on page 223

Employees can change their own passwords by using the Self Care application in the Service Center.

Chapter 12, “Viewing my requests in the Self Care application,” on page 225

You can view your requests by using the Self Care application in the Service Center.

Chapter 13, “Updating my security questions,” on page 227

You can set up your account recovery security questions and answers by using the Self Care application in the Service Center.

Chapter 10. Resetting my forgotten password

If you forgot your Service Center password, you can either specify a new password or have the system generate new password.

Before you begin

Your security questions must already be set up.

About this task

When you forget your password, you must answer the security questions correctly to reset your password. The new password replaces the old password for your Service Center account. Depending on how your system is configured, you can either specify a new password or use a system-generated password. The new password is sent to the email address that is specified in your personal profile.

If no email address is defined in your personal profile, the system-generated password cannot be sent. Contact the help desk or administrator to add an email address to your profile.

Procedure

1. From the Service Center Login page, type your user ID, and then click **Forgot your password?**
2. On the Forgot Your Password page, answer the security questions, and then click **Continue**. The following scenarios are possible, depending on how a system administrator configured the system:

Option	Description
The questions are answered correctly, and your system is configured for you to specify a new password.	Type your new password in the New Password field, and then type your new password again in the Confirm Password field. Then, click Change Password . When you see a message that indicates a successful password change, click OK .
The questions are answered correctly, and your system is configured to generate a new password and send the password to a predefined email address.	A new system-generated password is automatically sent to the email that is defined in your personal profile. You must use this new password on your next login, and then you can change your password on your next login. Click Return to Login .
The questions are answered correctly, and your system is configured to generate a new password and prompts you to type an email address.	Type the email address where you want the new system-generated password to be sent. You must use this new password on your next login, and then you must change your password on your next login. Click Continue . When you see a message that indicates a successful operation, click Return to Login .

Option	Description
<p>The questions are answered correctly, and your system is configured to generate a new password. However, an email address is not defined in your personal profile.</p>	<p>Contact the help desk or administrator to add your email address to your personal profile. Click Return to Login. After the email address is added to your profile, you can follow the Forgot your password? link again from the Service Center Login page to receive the system-generated password in your email address.</p>
<p>The questions are not answered correctly, and an error message is displayed. Depending on how your system is configured, you might have more attempts to correctly answer the questions.</p>	<p>You cannot access the system unless you remember your password or answer the questions correctly. If you exceed the maximum number of attempts to verify your identity, your Service Center account is locked. Contact your help desk or administrator to unlock your Service Center account or reset your Service Center password.</p>

Related reference:

Chapter 3, “Forgot Your Password,” on page 9

If you forgot your Service Center password, you can reset it.

Chapter 11. Changing my account password

Employees can change their own passwords by using the Self Care application in the Service Center.

Before you begin

If single sign-on is not enabled, you must know your current Service Center password.

About this task

Depending on how a system administrator configured the system, you can change your password by using the Self Care application in the Service Center.

Procedure

1. From the Service Center Login page, type your user ID and password, and then click **Log In**. The Service Center home page is displayed.
2. On the Service Center home page, click the application menu icon, and then select **Self Care**. The Self Care page is displayed.
3. On the Self Care page, click the **Change My Password** tab.
4. Select the accounts that you want to change the password for, and click **Change Password**. Click **Filter** to show options for filtering the list of accounts. You can search for accounts by name or user ID. To toggle the filter off, click **Hide Filter**. The Change Password window is displayed.
5. In the **Current password** field, enter your current Service Center password. This field is displayed only if single sign-on is *not* enabled.
6. In the **New password** field, type a new password, and then type the new password again in the **Confirm password** field. Then, click **Change Password**. Your new password must conform to the rules that are indicated on the Change Password window. The system administrator configured the rules in the Administration Console.
7. When an information message is displayed, which indicates that the request was successfully submitted, click **OK**.
8. Check the status of your password change request. See Chapter 12, “Viewing my requests in the Self Care application,” on page 225. Some requests are immediately completed, while other requests might take more time to complete. Even when the password change request is submitted successfully, it might take time for the password change operation to be complete.

Results

The password is changed, and the Change My Password page is displayed.

What to do next

You can change the password for another account, or do a different task in the Service Center.

Related reference:

Chapter 14, "Change My Password," on page 229
You can change the password for one or more of your own accounts.

Chapter 12. Viewing my requests in the Self Care application

You can view your requests by using the Self Care application in the Service Center.

About this task

Depending on how a system administrator configured the system, you can do these tasks:

- Check the status of a change password request for your account.
- Check the status of a change password request that a manager or help desk administrator submitted for your account.
- See which requests are complete and which requests are not complete.
- Search for requests that are based on the filter criteria that you specify.

Procedure

1. From the Service Center Login page, type your user ID and password, and then click **Log In**. The Service Center home page is displayed.
2. On the Service Center home page, click the application menu icon, and then select **Self Care**. The Self Care page is displayed.
3. On the Self Care page, click the **View Self Care Requests** tab.
4. Optional: Click **Filter** to show options for filtering the list of requests. For example, you can view the requests that are completed in the last 30 days. To toggle the filter off, click **Hide Filter**.

What to do next

You can do a different task in the Service Center.

Related reference:

Chapter 15, “View Self Care Requests,” on page 231

You can view the requests that you submitted by using the Self Care application in the Service Center.

Chapter 13. Updating my security questions

You can set up your account recovery security questions and answers by using the Self Care application in the Service Center.

Before you begin

You must know your current Service Center password.

About this task

You are required to provide answers to the security questions when you log in to the Service Center for the first time, or when the system administrator changes the security question configuration.

You can update the answers to the security questions whenever you would like to. The steps for changing the account recovery settings are included below.

Procedure

1. From the Service Center Login page, type your user ID and password, and then click **Log In**. The Service Center home page is displayed.
2. On the Service Center home page, click the application menu icon, and then select **Self Care**. The Self Care page is displayed.
3. On the Self Care page, click the **Account Recovery Setup** tab.
4. In the **Security Questions** tab, select the questions from the list and provide answers. Then click **Save**. The account recovery settings are saved.
5. Optional: In the **Contact Information** tab, you can view your email address in the **Primary email address** field.

What to do next

You can do a different task in the Self Care application, such as changing your password or viewing your password change requests.

Related reference:

Chapter 16, "Account Recovery Setup," on page 233

You can configure your security questions in case you need to recover your forgotten password or reset your password in the Service Center Self Care application.

Chapter 14. Change My Password

You can change the password for one or more of your own accounts.

Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests and then click **Search**.

Select the check box next to one or more of your accounts, and then click **Change Password**.

On the Change Password window, if single sign-on is enabled, you are not prompted to enter your current password. If single sign-on is *not* enabled, then you must enter your current Service Center password in the **Current password** field.

Table 251. Change My Password

Column Name	Description
Active	Indicates whether the account is active.
Name	The account configuration name that is associated with the user ID.
User ID	The user ID of the account.

You can display the results in different ways by using the controls at the bottom of the page:

- Click the drop-down list next to the **Items Per Page** field and select the number of items you want to display on the page.
- Click the arrows to move backward or forward through multiple pages.

Related tasks:

Chapter 11, “Changing my account password,” on page 223

Employees can change their own passwords by using the Self Care application in the Service Center.

Chapter 15. View Self Care Requests

You can view the requests that you submitted by using the Self Care application in the Service Center.

Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests and then click **Search**.

Table 252. View Self Care Requests

Column Name	Description
Status	Status of the password change request. The following statuses are valid: Failed The request failed. Pending The request is waiting for approval. Performed The request is in the queue to be completed. Successful The request is successful and complete.
User ID	Account user ID.
Name	Account configuration name.
Requester Last Name	The surname of the person who requested the password change.
Requester First Name	The given name of the person who requested the password change.
Submitted	Date that the request was submitted.
Completed	Date that the request was completed.
Request ID	System-generated ID for the request.

You can display the results in different ways by using the controls at the bottom of the page:

- Click the drop-down list next to the **Items Per Page** field and select the number of items you want to display on the page.
- Click the arrows to move backward or forward through multiple pages.

Related tasks:

Chapter 12, “Viewing my requests in the Self Care application,” on page 225

You can view your requests by using the Self Care application in the Service Center.

Chapter 16. Account Recovery Setup

You can configure your security questions in case you need to recover your forgotten password or reset your password in the Service Center Self Care application.

You are required to provide answers to the security questions when you log in to the Service Center for the first time, or when the system administrator changes the security question configuration.

You can also update the answers to the security questions whenever you would like to.

The Account Recovery Setup page includes two tabs:

Security Questions

For each question, select a question from the list and then provide an answer that you can easily remember. The answers are not case sensitive.

Contact Information

View your contact information that is configured in the system. If you forget your login credentials, you will be contacted using this information. If this information is incorrect, you cannot recover your credentials. If necessary, ensure that changes are made to this information in your user profile.

Related tasks:

Chapter 13, “Updating my security questions,” on page 227

You can set up your account recovery security questions and answers by using the Self Care application in the Service Center.

Part 3. Appendixes

Appendix. Accessibility features for IBM Security Identity Governance and Intelligence

Accessibility features assist users who have a disability, such as restricted mobility or limited vision, to use information technology content successfully.

Accessibility features

IBM Security Identity Governance and Intelligence Version 5.2.1 is not tested for accessibility.

The online product documentation in IBM Knowledge Center is enabled for accessibility. The accessibility features of IBM Knowledge Center are described at http://www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility.

Related accessibility information

In addition to standard IBM help desk and support websites, IBM has established a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:

TTY service
800-IBM-3383 (800-426-3383)
(within North America)

IBM and accessibility

For more information about the commitment that IBM has to accessibility, see (www.ibm.com/able).

Index

A

accessibility features for this
product 237

D

Dashboard
home in Service Center 3

H

Home
Service Center 3

S

Service Center
home page 3



Printed in USA