

IBM Security Identity Governance and Intelligence
Version 5.2.3.1

*Administration Topics
for Managers and Employees*

IBM

IBM Security Identity Governance and Intelligence
Version 5.2.3.1

*Administration Topics
for Managers and Employees*



Table of contents

Table list	v
Part 1. Managers	1
Chapter 1. Service Center	3
Chapter 2. Password management	7
Resetting my forgotten password	7
Resetting account passwords for other users.	8
Chapter 4. Introduction to Access Certifier	13
Campaign Management	13
Summary of available campaigns	13
Details - OU Entitlement Review	15
Details - Entitlement/User	19
Details - User Remediation Review	33
Details - Entitlement Review.	38
Details - Account Review	44
Details for Supervisor - OU Entitlement	48
Details for Supervisor - User Entitlement	53
Details for Supervisor - User Remediation	58
Details for Supervisor - Entitlement	62
Details for Supervisor - Accounts	67
Chapter 5. Introduction to User-account matching.	73
Dashboard.	73
Chapter 6. Introduction to Access Requests.	77
ARM Requests Status	78
AR functions	79
Account management: generating a request.	80
Generating a request for creating a new account	80
Authorizing an account creation request.	82
Executing a request of account creation	89
Generating a request for updating an account	96
Authorizing an account update request	98
Executing a request of account update	105
Generating a request for managing a password	112
Setting security questions in a new request to make account changes	114
Selecting accounts in a new request to make account changes	114
Entering the new password in a new request to make account changes	116
Authorizing a request for managing a password	117
Executing a request for account change.	125
Account management: authorizing a request	131
Account management: executing a request	131
Selecting users in a new request to assign entitlements and roles	131

Authorizing a request to assign entitlements and roles	138
Executing a request to assign entitlements and roles	146
Generating a request to delegate administrative roles	152
Authorizing a request to delegate administrative roles	153
Executing a request to delegate administrative roles	153
Viewing requests in your Daily Work scope	153
Generating a request to delegate entitlements	160
Authorizing a Delegation request.	164
Executing a Delegation request	172
Authorize escalation	179
Insert/Update entitlement: generating a request	183
Insert/Update entitlement: processing a request	201
Insert/Updates entitlements: executing a request	209
Viewing the requests present in the system	215
Viewing expired requests that require to be approved or rejected	220
Create/Update user: generating a request	222
Insert/Update user: processing a request	224
Insert/Update user: executing a request	233

Chapter 7. Introduction to Business Activity Mapping	235
Dashboard	235
Permission Perspective	236
Business activity Perspective	237

Chapter 8. Introduction to Report Client.	239
Report.	239
Request	239
Download	240
Passphrase	241

Part 2. Employees	243
------------------------------------	------------

Chapter 9. Logging in to the Service Center	245	Appendix. Accessibility features for IBM Security Identity Governance and Intelligence	263
Chapter 10. Resetting my forgotten password	247	Index	265
Chapter 11. Changing my account password	249		
Chapter 12. Viewing my requests in the Self Care application	251		
Chapter 13. Updating my security questions	253		
<hr/> Part 3. Appendixes	261		

Table list

1. Dashboard items controls	4	56. Details of a request	86
2. Password management tasks	7	57. User Details - Details tab	86
3. Summary Attributes.	14	58. User Details - Entitlements tab	87
4. Details tab note	15	59. User Details - Accounts tab	87
5. Filters	15	60. User Details - Activities tab	87
6. Campaign Info window	15	61. User Details - Rights	87
7. Details tab buttons and icons.	16	62. Account details.	88
8. Entity information	18	63. Request Status	90
9. Entitlement View filters.	20	64. Subrequest status	91
10. Campaign Info window	21	65. Filters	91
11. Details tab buttons and icons.	21	66. User Details - Details tab	92
12. Columns for Entitlement View	22	67. Details of a request	93
13. Entity information	25	68. User Details - Details tab	93
14. Filters	27	69. User Details - Entitlements tab	94
15. Campaign Info window	27	70. User Details - Accounts tab	94
16. Details tab buttons and icons.	28	71. User Details - Activities tab	94
17. Configurable columns for the details of the campaign	31	72. User Details - Rights	94
18. Entity information	31	73. Account details.	95
19. Filters	33	74. Account filters	96
20. Campaign Info window	33	75. Account details.	97
21. Details tab buttons and icons.	34	76. Request Status	99
22. Risk Violation Mitigation Details	36	77. Subrequest status	100
23. Entity information	37	78. Filters	100
24. Entitlement View filters.	39	79. User Details - Details tab.	101
25. Note about the UME check box	40	80. Details of a request	102
26. Campaign Info window	40	81. User Details - Details tab.	102
27. Details tab buttons and icons.	40	82. User Details - Entitlements tab	103
28. Entitlement details	42	83. User Details - Accounts tab	103
29. Entity information	42	84. User Details - Activities tab	103
30. Details Filters	44	85. User Details - Rights	103
31. Campaign Info window	45	86. Account details..	104
32. Details tab buttons and icons.	45	87. Request Status	106
33. Account details	46	88. Subrequest status	107
34. Entity information	47	89. Filters	108
35. Cert_Campaign_Reviewer_Tab	50	90. User Details - Details tab.	108
36. Cert_Campaign_Scheduling_Tab	51	91. Details of a request	109
37. Cert_Campaign_Reviewer_Tab	54	92. User Details - Details tab.	109
38. Cert_Campaign_Scheduling_Tab	55	93. User Details - Entitlements tab	110
39. Cert_Campaign_Reviewer_Tab	59	94. User Details - Accounts tab	110
40. Cert_Campaign_Scheduling_Tab	60	95. User Details - Activities tab	110
41. Cert_Campaign_Reviewer_Tab	64	96. User Details - Rights	110
42. Cert_Campaign_Scheduling_Tab	65	97. Account details.	111
43. Cert_Campaign_Reviewer_Tab	68	98. User filters	112
44. Cert_Campaign_Scheduling_Tab	69	99. Attributes in the Users list	113
45. User filters.	73	100. User Information tabs.	113
46. User/Account attributes	74	101. Account details	115
47. Request Status	78	102. Request Status	118
48. Subrequest status	79	103. Subrequest status	119
49. Account filters	80	104. Filters	119
50. Account details.	81	105. User Details - Details tab.	120
51. Password attributes..	82	106. Details of a request - upper section	121
52. Request Status	83	107. User Details - Details tab.	121
53. Subrequest status	84	108. User Details - Entitlements tab	122
54. Filters	84	109. User Details - Accounts tab	122
55. User Details - Details tab	85	110. User Details - Activities tab	122
		111. User Details - Rights	122

112.	Request attributes	123	172.	User Details - Accounts tab	158
113.	Entitlement info - Structure	123	173.	User Details - Activities tab	158
114.	Request Status	126	174.	User Details - Rights	158
115.	Filters	126	175.	Request attributes	158
116.	Request attributes	127	176.	Entitlement info - Structure	159
117.	User Details - Details tab.	127	177.	User filters	160
118.	Details of a request - upper section	128	178.	Attributes in the Users list	161
119.	User Details - Details tab.	128	179.	User Details - Details tab.	161
120.	User Details - Entitlements tab.	129	180.	User Details - Entitlements tab.	162
121.	User Details - Accounts tab	129	181.	User Details - Accounts tab	162
122.	User Details - Activities tab	129	182.	User Details - Rights	162
123.	User Details - Rights	129	183.	User Details - Activities tab	162
124.	Request attributes	130	184.	Entitlement info - Structure	162
125.	Entitlement info - Structure	130	185.	Request Status	165
126.	User filters	131	186.	Subrequest status	166
127.	Attributes in the Users list	131	187.	Filters	167
128.	User Details - Details tab.	132	188.	Request attributes.	167
129.	User Details - Entitlements tab.	132	189.	User Details - Details tab.	167
130.	User Details - Accounts tab	132	190.	Details of a request - upper section	168
131.	User Details - Rights	132	191.	User Details - Details tab.	169
132.	User Details - Activities tab	133	192.	User Details - Entitlements tab.	169
133.	Entitlement info - Structure	133	193.	User Details - Accounts tab	169
134.	Current Entitlement filters.	134	194.	User Details - Activities tab	169
135.	Business Role filters.	135	195.	User Details - Rights	170
136.	Application Role filters.	136	196.	Request attributes	170
137.	Permission filters.	136	197.	Entitlement info - Structure	171
138.	Pushbuttons and Icons in the Shopping Cart page.	138	198.	Request Status	173
139.	Request Status	139	199.	Filters	173
140.	Subrequest status	140	200.	Request attributes.	174
141.	Filters	140	201.	User Details - Details tab.	174
142.	Request details.	141	202.	Details of a request - upper section	175
143.	User Details - Details tab.	141	203.	User Details - Details tab.	176
144.	Details of a request - upper section	142	204.	User Details - Entitlements tab.	176
145.	User Details - Details tab.	142	205.	User Details - Accounts tab	176
146.	User Details - Entitlements tab.	143	206.	User Details - Activities tab	176
147.	User Details - Accounts tab	143	207.	User Details - Rights	177
148.	User Details - Activities tab	143	208.	Request attributes	177
149.	User Details - Rights	143	209.	Entitlement info - Structure	178
150.	Request attributes	144	210.	Filters for requests in Incompatibility status	179
151.	Entitlement info - Structure	144	211.	Request details	179
152.	Request Status	147	212.	User Details - Details tab.	180
153.	Filters	147	213.	Request and request actor details	181
154.	Requests attributes.	148	214.	Request attributes	182
155.	User Details - Details tab.	148	215.	Analysis filters.	184
156.	Details of a request - upper section	149	216.	Role Mining and Data Exploration analyses attributes	184
157.	User Details - Details tab.	149	217.	User filters.	188
158.	User Details - Entitlements tab.	150	218.	User details.	188
159.	User Details - Accounts tab	150	219.	Entitlement details.	190
160.	User Details - Activities tab	150	220.	Entitlement filters	191
161.	User Details - Rights	150	221.	Entitlement details.	192
162.	Request attributes	151	222.	Candidate Role attributes	193
163.	Entitlement info - Structure	151	223.	User attributes	194
164.	Request Status	153	224.	Candidate Role attributes	195
165.	Subrequest status	154	225.	OU attributes.	196
166.	Filters	155	226.	Dashboard set.	196
167.	Request attributes.	155	227.	Role statistics filters.	197
168.	User Details - Details tab.	156	228.	Filters that you can use to search for entitlements.	199
169.	Details of a request - upper section	156	229.	Entitlement attributes in an Update Entitlement request generation.	199
170.	User Details - Details tab.	157			
171.	User Details - Entitlements tab.	158			

230. Request Status	201	256. Request attributes	218
231. Subrequest status	202	257. User Details - Details tab.	218
232. Filters	203	258. Details of a request - upper section	219
233. User Details - Details tab.	204	259. Filters that you can use to search for specific requests	220
234. Details of a request - upper section	204	260. Request attributes	221
235. User Details - Details tab.	205	261. Details of a request - upper section	221
236. User Details - Entitlements tab.	206	262. Request Status	225
237. User Details - Accounts tab	206	263. Subrequest status	226
238. User Details - Activities tab	206	264. Filters	227
239. User Details - Rights	206	265. Requests attributes.	227
240. Request attributes	207	266. User Details - Details tab.	227
241. Entitlement info - Structure	207	267. Details of a request - upper section	228
242. Request Status	210	268. User Details - Details tab.	229
243. Filters	210	269. User Details - Entitlements tab.	230
244. User Details - Details tab.	211	270. User Details - Accounts tab	230
245. Details of a request - upper section	212	271. User Details - Activities tab	230
246. User Details - Details tab.	212	272. User Details - Rights	230
247. User Details - Entitlements tab.	213	273. Request attributes	231
248. User Details - Accounts tab	213	274. Entitlement info - Structure	231
249. User Details - Activities tab	213	275. Dashboard filters	236
250. User Details - Rights	213	276. Dashboard details	236
251. Request attributes	214	277. Configuration steps	240
252. Entitlement info - Structure	214	278. Status labels for reports	240
253. Request Status	216	279. Change My Password.	255
254. Subrequest status	217	280. View Self Care Requests	257
255. Filters	217		

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 13.
- **Access Requests** - See Chapter 6, "Introduction to Access Requests," on page 77.
- **Reports** - See Chapter 8, "Introduction to Report Client," on page 239.
- **User-Account Matching** - See Chapter 5, "Introduction to User-account matching," on page 73.
- **Business Activity Mapping** - See Chapter 7, "Introduction to Business Activity Mapping," on page 235.
- **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 <p>Attention: This control does not work for custom dashboards that are created with the Add from Query action in Report Designer.</p>

Table 1. Dashboard items controls (continued)

Icon	Label	Description
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 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 8

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 new password.

Before you begin

The administrator must configure the forgotten password service in the Administration Console. Otherwise, the **Forgot your password?** link does not display on the Service Center Login page. For more information, see Configuring password services.

Your security questions must already be set up. For more information, see Chapter 13, "Updating my security questions," on page 253.

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 11

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 or Application Manager) 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.

Related information:

“Entering the new password in a new request to make account changes” on page 116

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

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 7

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. Filters

Filter	Description
Org Unit	Click  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 .
Activity	Click  Browse to choose the Activity associated with the users through the permission associated with the users.
Hierarchy	If this check box is flagged, the search starts from the root that is selected in the Activity field and runs on the hierarchy.
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.

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.

Table 6. 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. By User The user decides when to sign off on the approval or revocation. End Review 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.
 Notes	Click to insert a note about the entity.
 Notes	Click to read a note that was previously inserted through  .
 Redirect	Redirect to another reviewer to be approved or revoked. In the field Redirect to you must set the name of the reviewer.
 Escalation	Escalate to the supervisor to be approved or revoked. The Supervisor can send back the information using  Return .
 Return	Return the information to the sender reviewer.
 Redirect	Received by a reviewer after the checking (see Return).

Table 7. Details tab buttons and icons (continued)

Button/Icon	Description
 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: EntityName	Click Certifying: EntityName 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 no longer be available 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  **Info** icon, you get a set of information related to the data model entity that you are considering:

Table 8. Entity information

Tab	Attributes	Description
User Details	OU	The type that is associated to the Organizational Unit.
	First Name	Name of the User.
	Last Name	Surname of the User.
	Master UID	Unique identifier of the User.
	User Type	The type that is 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.
Entitlement Details	Type	Type of the Entitlement: <ul style="list-style-type: none"> • Business Role • External Role • IT Role • Permission
	Code	Unique identifier of the Entitlement
	Name	Name of the Entitlement
	Description	Short description that is associated to the Entitlement.
	Owner	Owner of the Entitlement.
	Last Reviewed Date	The date of the last certification of the Entitlement.
	Expiration Date	After this date, the Entitlement is not longer active for the User
	Org. Units	Number of Organizational Units where this Entitlement is present. Click the number for opening the tab Org. Units .
Users	List of Users that are associated to the Entitlement.	

Table 8. Entity information (continued)

Tab	Attributes	Description
OU Details	Type	The administrator can set specific values for defining types of OU. For example, a Marketing type can be associated to all Organizational Units involved in marketing.
	Name	Name of the Organizational Unit
	Code	Unique identifier of the Organizational Unit
	Owner	Owner of the Organizational Unit
	Description	Short description that is associated to the Organizational Unit.
Structure	The hierarchical tree view of the selected Entitlement.	
Org. Units	A list of all OU related to the selected Entitlement.	
Activities	A list of all activities that are related to the selected User. If you select an activity, click Actions > Users for getting all the users that are associated to the selected activity.	
Accounts	A list of all accounts that are related to the selected User.	
Rights	A list of all permissions that holds rights and that are related to the selected User.	
Risks	A list of all risks that are related to the selected User.	
Applications	A list of all applications that are related to the selected User.	

Depending on the data model entity, some tabs might not be present.

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 and the contents of the views, can be changed by the administrator.

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 - 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 filters.

Context	Filter	Description
User	Org Unit	Click  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 User 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.
	Activity	Click  Browse to choose the Activity associated with the users through the permission associated with the users.
	Hierarchy	If this check box is flagged, the search starts from the root that is selected in the Activity field and runs on the hierarchy.
	Only Users with Violations	If this check box is ticked, the search activity applies only to users with outstanding violations.
Entitlement	Application	Name of the application.
	Search Entitlement (Name or Code)	Name or code of the entitlement.
	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 ticked, 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
	User Hierarchy	Indicates the group hierarchy for filtering entitlements to be certified.

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.
Sign Off	The method in which the approval or revocation is validated: Automatic The approval or revocation is immediately signed off. By User The user decides when to sign off on the approval or revocation. End Review 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.
 Notes	Click to insert a note about the entity.
 Notes	Click to read a note that was previously inserted through  .

Table 11. Details tab buttons and icons (continued)

Button/Icon	Description
 Redirect	Redirect to another reviewer to be approved or revoked. In the field Redirect to you must set the name of the reviewer.
 Escalation	Escalate to the supervisor to be approved or revoked. The Supervisor can send back the information using  Return .
 Return	Return the information to the sender reviewer.
 Redirect	Received by a reviewer after the checking (see Return).
 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 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.

Table 12. Columns for Entitlement View (continued)

Column	Description
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.
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.
Group Name [Code]	The IGI Administrator can configure several types of hierarchies that are based on user attributes. Every hierarchy can be made by several groups. A group is an element (a node) of the hierarchy, identifies by a name and a specific code. Every group can be associate to a set of entitlements.
Hierarchy Name	Identifier of the hierarchy. The base hierarchy is ORGANIZATIONAL_UNIT hierarchy.

Every row of the campaign host an entitlement to be certified.

You must consider every row as a node of a tree.

You must select and work only one node at the time.

The type of entitlement might be

- Permission
- IT Role

- **Business Role**
- **External Role**

Click the little dark row, on the left of the selected entitlements, for expanding a possible set of subrows that are present if the entitlement is associated to a set of rights.

Note: If the entitlement contains all rights with empty values, it's not possible to expand the structure clicking the dark row.

Note: It's not possible to associate rights to an **External Role**.

If you are considering a permission, the rights that are associated are listed under the permission node.

If you are considering another type of entitlement, the hierarchy of nodes is expanded up to list all permissions and rights that are involved.

If you have a single value right that is associated to a permission, you have only one subrow to manage.

If you have a multi-value right that is associated to a permission, you can have several subrows to manage, in a flat view.

On a row that is related to the value of a right, you can make the following operations:

- **Revoke** deletes the value of a right (the button turns red, like the name of the right).
- **Edit** changes the value of a right (the button turns orange, like the name of the right).


Every value that is not edited keeps its value.

The previous operations are effective and are propagated to the DB of Access Governance Core only if you confirm them, through the button **Approve** related to the selected node.

To click **Approve** is needed for triggering the sign-off action that is configured for the campaign.

It is possible to have several types of sign-off:

- Automatic (after you click **Approve** or **Revoke** for the selected node).
- Manual (after you click **Approve** or **Revoke** for the selected node, the button **Sign off** is enabled).
- At the end of the campaign, automatically.

After the sign-off, you can click  **History** in the row of a specific right, for getting a pop-up with a list of all operations performed.

For required permission with $N > 1$ rights, it is possible to revoke $N - 1$ rights, preserving at least one right (on the last right, the **Revoke** button is disabled).

The **Revoke** button is disabled also for a required permission that has just one right available.

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 no longer available for several reasons. For example, the entity was deleted by another process, such as an entitlement, that was originally involved in the certification process.

Note: In some views, only a subset of the data that is indicated might be shown.


When you click the  **Info** icon, you get a set of information related to the data model entity that you are considering:

Table 13. Entity information

Tab	Attributes	Description
User Details	OU	The type that is associated to the Organizational Unit.
	First Name	Name of the User.
	Last Name	Surname of the User.
	Master UID	Unique identifier of the User.
	User Type	The type that is 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.

Table 13. Entity information (continued)

Tab	Attributes	Description
Entitlement Details	Type	Type of the Entitlement: <ul style="list-style-type: none"> • Business Role • External Role • IT Role • Permission
	Code	Unique identifier of the Entitlement
	Name	Name of the Entitlement
	Description	Short description that is associated to the Entitlement.
	Owner	Owner of the Entitlement.
	Last Reviewed Date	The date of the last certification of the Entitlement.
	Expiration Date	After this date, the Entitlement is not longer active for the User
	Org. Units	Number of Organizational Units where this Entitlement is present. Click the number for opening the tab Org. Units .
Users	List of Users that are associated to the Entitlement.	
OU Details	Type	The administrator can set specific values for defining types of OU. For example, a Marketing type can be associated to all Organizational Units involved in marketing.
	Name	Name of the Organizational Unit
	Code	Unique identifier of the Organizational Unit
	Owner	Owner of the Organizational Unit
	Description	Short description that is associated to the Organizational Unit.
Structure	The hierarchical tree view of the selected Entitlement.	
Org. Units	A list of all OU related to the selected Entitlement.	
Activities	A list of all activities that are related to the selected User. If you select an activity, click Actions > Users for getting all the users that are associated to the selected activity.	
Accounts	A list of all accounts that are related to the selected User.	
Rights	A list of all permissions that holds rights and that are related to the selected User.	

Table 13. Entity information (continued)

Tab	Attributes	Description
Risks		A list of all risks that are related to the selected User.
Applications		A list of all applications that are related to the selected User.

Depending on the data model entity, some tabs might not be present.

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 14. Filters

Filter	Description
Org Unit	Click <input type="text"/> 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.
Activity	Click <input type="text"/> Browse to choose the Activity associated with the users through the permission associated with the users.
Hierarchy	If this check box is flagged, the search starts from the root that is selected in the Activity field and runs on the hierarchy.
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 Users with Violation	If this check box is ticked, the search activity is on the entity with Visibility Violation.

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 15. 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.

Table 15. Campaign Info window (continued)

Field	Description
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. By User The user decides when to sign off on the approval or revocation. End Review 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.

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 16. 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.
 Notes	Click to insert a note about the entity.
 Notes	Click to read a note that was previously inserted through  .
 Redirect	Redirect to another reviewer to be approved or revoked. In the field Redirect to you must set the name of the reviewer.
 Escalation	Escalate to the supervisor to be approved or revoked. The Supervisor can send back the information using  Return .
 Return	Return the information to the sender reviewer.

Table 16. Details tab buttons and icons (continued)

Button/Icon	Description
 Redirect	Received by a reviewer after the checking (see Return).
 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.

Selecting one item, related to a specific user, and clicking on  **Inspect** you can get a table of entitlements related to the selected item.

Every row of the campaign host an entitlement to be certified.

You must consider every row as a node of a tree.

You must select and work only one node at the time.

The type of entitlement might be

- **Permission**
- **IT Role**
- **Business Role**
- **External Role**

Click the little dark row, on the left of the selected entitlements, for expanding a possible set of subrows that are present if the entitlement is associated to a set of rights.

Note: If the entitlement contains all rights with empty values, it's not possible to expand the structure clicking the dark row.

Note: It's not possible to associate rights to an **External Role**.

If you are considering a permission, the rights that are associated are listed under the permission node.

If you are considering another type of entitlement, the hierarchy of nodes is expanded up to list all permissions and rights that are involved.

If you have a single value right that is associated to a permission, you have only one subrow to manage.

If you have a multi-value right that is associated to a permission, you can have several subrows to manage, in a flat view.

On a row that is related to the value of a right, you can make the following operations:


- **Revoke** deletes the value of a right (the button turns red, like the name of the right).
- **Edit** changes the value of a right (the button turns orange, like the name of the right).


Every value that is not edited keeps its value.

The previous operations are effective and are propagated to the DB of Access Governance Core only if you confirm them, through the button **Approve** related to the selected node.

To click **Approve** is needed for triggering the sign-off action that is configured for the campaign.

It is possible to have several types of sign-off:

- Automatic (after you click **Approve** or **Revoke** for the selected node).
- Manual (after you click **Approve** or **Revoke** for the selected node, the button  **Sign off** is enabled).
- At the end of the campaign, automatically.

After the sign-off, you can click  **History** in the row of a specific right, for getting a pop-up with a list of all operations performed.

For required permission with N>1 rights, it is possible to revoke N-1 rights, preserving at least one right (on the last right, the **Revoke** button is disabled).

The **Revoke** button is disabled also for a required permission that has just one right available.

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 no longer available for several reasons. For example, the entity was deleted by another process, such as an entitlement, that was originally involved in the certification process.

Note: In some views, only a subset of the data that is indicated might be shown.

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

Table 17. Configurable columns for the details of the campaign

Column	Description
Attestation buttons	Makes for attestations actions available: Approve - Revoke - Sign Off - Notes - Redirect - Escalate 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.
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.
% Entitlement Completion	A progressive bar indicates the % of certified entitlements of the user.

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


When you click the  **Info** icon, you get a set of information related to the data model entity that you are considering:

Table 18. Entity information

Tab	Attributes	Description
User Details	OU	The type that is associated to the Organizational Unit.
	First Name	Name of the User.
	Last Name	Surname of the User.
	Master UID	Unique identifier of the User.
	User Type	The type that is 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.

Table 18. Entity information (continued)

Tab	Attributes	Description
Entitlement Details	Type	Type of the Entitlement: <ul style="list-style-type: none"> • Business Role • External Role • IT Role • Permission
	Code	Unique identifier of the Entitlement
	Name	Name of the Entitlement
	Description	Short description that is associated to the Entitlement.
	Owner	Owner of the Entitlement.
	Last Reviewed Date	The date of the last certification of the Entitlement.
	Expiration Date	After this date, the Entitlement is not longer active for the User
	Org. Units	Number of Organizational Units where this Entitlement is present. Click the number for opening the tab Org. Units .
Users	List of Users that are associated to the Entitlement.	
OU Details	Type	The administrator can set specific values for defining types of OU. For example, a Marketing type can be associated to all Organizational Units involved in marketing.
	Name	Name of the Organizational Unit
	Code	Unique identifier of the Organizational Unit
	Owner	Owner of the Organizational Unit
	Description	Short description that is associated to the Organizational Unit.
Structure	The hierarchical tree view of the selected Entitlement.	
Org. Units	A list of all OU related to the selected Entitlement.	
Activities	A list of all activities that are related to the selected User. If you select an activity, click Actions > Users for getting all the users that are associated to the selected activity.	
Accounts	A list of all accounts that are related to the selected User.	
Rights	A list of all permissions that holds rights and that are related to the selected User.	

Table 18. Entity information (continued)

Tab	Attributes	Description
Risks		A list of all risks that are related to the selected User.
Applications		A list of all applications that are related to the selected User.



Depending on the data model entity, some tabs might not be present.

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 19. Filters

Filter	Description
Org Unit	Click  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.
Activity	Click  Browse to choose the Activity associated with the users through the permission associated with the users.
Hierarchy	If this check box is flagged, the search starts from the root that is selected in the Activity field and runs on the hierarchy.
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 Users with Violation	If this check box is ticked, the search activity is on the entity with Visibility Violation.

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 20. Campaign Info window

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

Table 20. Campaign Info window (continued)

Field	Description
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. By User The user decides when to sign off on the approval or revocation. End Review 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 21. 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.
 Notes	Click to insert a note about the entity.
 Notes	Click to read a note that was previously inserted through  .
 Redirect	Redirect to another reviewer to be approved or revoked. In the field Redirect to you must set the name of the reviewer.
 Escalation	Escalate to the supervisor to be approved or revoked. The Supervisor can send back the information using  Return .
 Return	Return the information to the sender reviewer.

Table 21. Details tab buttons and icons (continued)

Button/Icon	Description
 Redirect	Received by a reviewer after the checking (see Return).
 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 22. 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.
	Master UID	Univocal identifier of the user.
	User Type	Indicates the type associated with the user.
	Name	Name of the user.
	Last Name	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.

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 no longer available 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  **Info** icon, you get a set of information related to the data model entity that you are considering:

Table 23. Entity information

Tab	Attributes	Description
User Details	OU	The type that is associated to the Organizational Unit.
	First Name	Name of the User.
	Last Name	Surname of the User.
	Master UID	Unique identifier of the User.
	User Type	The type that is 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.
Entitlement Details	Type	Type of the Entitlement: <ul style="list-style-type: none"> • Business Role • External Role • IT Role • Permission
	Code	Unique identifier of the Entitlement
	Name	Name of the Entitlement
	Description	Short description that is associated to the Entitlement.
	Owner	Owner of the Entitlement.
	Last Reviewed Date	The date of the last certification of the Entitlement.
	Expiration Date	After this date, the Entitlement is not longer active for the User
	Org. Units	Number of Organizational Units where this Entitlement is present. Click the number for opening the tab Org. Units .
Users	List of Users that are associated to the Entitlement.	

Table 23. Entity information (continued)

Tab	Attributes	Description
OU Details	Type	The administrator can set specific values for defining types of OU. For example, a Marketing type can be associated to all Organizational Units involved in marketing.
	Name	Name of the Organizational Unit
	Code	Unique identifier of the Organizational Unit
	Owner	Owner of the Organizational Unit
	Description	Short description that is associated to the Organizational Unit.
Structure	The hierarchical tree view of the selected Entitlement.	
Org. Units	A list of all OU related to the selected Entitlement.	
Activities	A list of all activities that are related to the selected User. If you select an activity, click Actions > Users for getting all the users that are associated to the selected activity.	
Accounts	A list of all accounts that are related to the selected User.	
Rights	A list of all permissions that holds rights and that are related to the selected User.	
Risks	A list of all risks that are related to the selected User.	
Applications	A list of all applications that are related to the selected User.	

Depending on the data model entity, some tabs might not be present.

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 24. Entitlement View filters.





Context	Filter	Description
User	Org Unit	Click  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 User 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.
	Activity	Click  Browse to choose the Activity associated with the users through the permission associated with the users.
	Hierarchy	If this check box is flagged, the search starts from the root that is selected in the Activity field and runs on the hierarchy.
	Only Users with Violations	If this check box is ticked, the search activity applies only to users with outstanding violations.
Entitlement	Application	Name of the application.
	Search Entitlement (Name or Code)	Name or code of the entitlement.
	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 ticked, 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
	User Hierarchy	Indicates the group hierarchy for filtering entitlements to be certified.

Table 25. 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 26. 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: <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 Review 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 27. 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.

Table 27. Details tab buttons and icons (continued)

Button/Icon	Description
 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.
 Notes	Click to insert a note about the entity.
 Notes	Click to read a note that was previously inserted through  .
 Redirect	Redirect to another reviewer to be approved or revoked. In the field Redirect to you must set the name of the reviewer.
 Escalation	Escalate to the supervisor to be approved or revoked. The Supervisor can send back the information using  Return .
 Return	Return the information to the sender reviewer.
 Redirect	Received by a reviewer after the checking (see Return).
 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 28. 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.

Note: If an entity row of the campaign is displayed without **Approve/Revoke**, the entity is no longer available for the reviewer. It can no longer be available 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  **Info** icon, you get a set of information related to the data model entity that you are considering:

Table 29. Entity information

Tab	Attributes	Description
User Details	OU	The type that is associated to the Organizational Unit.
	First Name	Name of the User.
	Last Name	Surname of the User.
	Master UID	Unique identifier of the User.
	User Type	The type that is 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.

Table 29. Entity information (continued)

Tab	Attributes	Description
Entitlement Details	Type	Type of the Entitlement: <ul style="list-style-type: none"> • Business Role • External Role • IT Role • Permission
	Code	Unique identifier of the Entitlement
	Name	Name of the Entitlement
	Description	Short description that is associated to the Entitlement.
	Owner	Owner of the Entitlement.
	Last Reviewed Date	The date of the last certification of the Entitlement.
	Expiration Date	After this date, the Entitlement is not longer active for the User
	Org. Units	Number of Organizational Units where this Entitlement is present. Click the number for opening the tab Org. Units .
Users	List of Users that are associated to the Entitlement.	
OU Details	Type	The administrator can set specific values for defining types of OU. For example, a Marketing type can be associated to all Organizational Units involved in marketing.
	Name	Name of the Organizational Unit
	Code	Unique identifier of the Organizational Unit
	Owner	Owner of the Organizational Unit
	Description	Short description that is associated to the Organizational Unit.
Structure	The hierarchical tree view of the selected Entitlement.	
Org. Units	A list of all OU related to the selected Entitlement.	
Activities	A list of all activities that are related to the selected User. If you select an activity, click Actions > Users for getting all the users that are associated to the selected activity.	
Accounts	A list of all accounts that are related to the selected User.	
Rights	A list of all permissions that holds rights and that are related to the selected User.	

Table 29. Entity information (continued)

Tab	Attributes	Description
Risks		A list of all risks that are related to the selected User.
Applications		A list of all applications that are related to the selected User.



Depending on the data model entity, some tabs might not be present.


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 30. 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 .
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.
Activity	Click  Browse to choose the activity associated with the users through the permission associated with the users.
Hierarchy	If this check box is flagged, the search starts from the root that is selected in the Activity field and runs on the hierarchy.
Only Users with Violations	If this check box is ticked, the search activity is on the entity with Visibility Violation.
Status	The following list shows the status of the certification: <ul style="list-style-type: none"> • Complete • Pending
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.
Account	The identifier of an account.
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
Application	The identifier of an application.
Account Status	<ul style="list-style-type: none"> • Suspend indicates that the account is suspended. • Restore indicates that the account is restored.
Configuration Name	Name of the configuration joined to the account.

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.

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 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.
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. By User The user decides when to sign off on the approval or revocation. End Review 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 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.

Table 32. Details tab buttons and icons (continued)

Button/Icon	Description
 Notes	Click to insert a note about the entity.
 Notes	Click to read a note that was previously inserted through  .
 Redirect	Redirect to another reviewer to be approved or revoked. In the field Redirect to you must set the name of the reviewer.
 Escalation	Escalate to the supervisor to be approved or revoked. The Supervisor can send back the information using  Return .
 Return	Return the information to the sender reviewer.
 Redirect	Received by a reviewer after the checking (see Return).
 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: EntityName	Click Certifying: EntityName 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. 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.

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 no longer available 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  **Info** icon, you get a set of information related to the data model entity that you are considering:

Table 34. Entity information

Tab	Attributes	Description
User Details	OU	The type that is associated to the Organizational Unit.
	First Name	Name of the User.
	Last Name	Surname of the User.
	Master UID	Unique identifier of the User.
	User Type	The type that is 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.
Entitlement Details	Type	Type of the Entitlement: <ul style="list-style-type: none"> • Business Role • External Role • IT Role • Permission
	Code	Unique identifier of the Entitlement
	Name	Name of the Entitlement
	Description	Short description that is associated to the Entitlement.
	Owner	Owner of the Entitlement.
	Last Reviewed Date	The date of the last certification of the Entitlement.
	Expiration Date	After this date, the Entitlement is not longer active for the User
	Org. Units	Number of Organizational Units where this Entitlement is present. Click the number for opening the tab Org. Units .
Users	List of Users that are associated to the Entitlement.	

Table 34. Entity information (continued)

Tab	Attributes	Description
OU Details	Type	The administrator can set specific values for defining types of OU. For example, a Marketing type can be associated to all Organizational Units involved in marketing.
	Name	Name of the Organizational Unit
	Code	Unique identifier of the Organizational Unit
	Owner	Owner of the Organizational Unit
	Description	Short description that is associated to the Organizational Unit.
Structure	The hierarchical tree view of the selected Entitlement.	
Org. Units	A list of all OU related to the selected Entitlement.	
Activities	A list of all activities that are related to the selected User. If you select an activity, click Actions > Users for getting all the users that are associated to the selected activity.	
Accounts	A list of all accounts that are related to the selected User.	
Rights	A list of all permissions that holds rights and that are related to the selected User.	
Risks	A list of all risks that are related to the selected User.	
Applications	A list of all applications that are related to the selected User.	

Depending on the data model entity, some tabs might not be present.

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"> • User Assignment • Organization Unit Assignment • Risk Violation Mitigation • Entitlement • Account
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 • By User • End Review

Campaign Detail	Description
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 35. Cert_Campaign_Reviewer_Tab

Reviewer Detail	Description
Scope	User Hierarchy If enabled, shows the available user hierarchy scope. It is always available for organizational units. Entity If enabled, shows the entity scope.
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	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. Campaigns on Account have the following options: <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 36. 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.</p> <p>If Duration=Continuous, you cannot set values for this parameter.</p> <p>In alternative, is shown the check-box Ignore the Dataset at the launch of the Campaign, selected by default.</p> <p>Maintaining the default setting, the campaign works on data that can be feed from several sources (custom rules or Access Optimizer features).</p> <p>If you deselect the check-box, the behavior it's the same but the starting data block is represented by the dataset that is linked to the campaign.</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"> • Daily, starting from K days before the end of the campaign as determined by Days before end date, where K is a value 0 - 32. • When the percentage of activity that is already managed is lower than X% as 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>


Notification Type	Description
Campaign Reminder for Reviewer	<p>If Enable is set, the reviewer receives a daily email starting from <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 a daily email starting from <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 <input type="checkbox"/> 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	 Stats monitors the status of the campaign completion.  Inspect inspects the entities of the campaign.
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.
% 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 Type	Type of campaign. <ul style="list-style-type: none"> • User Assignment • Organization Unit Assignment • Risk Violation Mitigation • Entitlement • Account
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 • By User • End Review
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 37. 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.

Table 37. Cert_Campaign_Reviewer_Tab (continued)

Reviewer Detail	Description
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 38. 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 38. 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.</p> <p>If Duration=Continuous, you cannot set values for this parameter.</p> <p>In alternative, is shown the check-box Ignore the Dataset at the launch of the Campaign, selected by default.</p> <p>Maintaining the default setting, the campaign works on data that can be feed from several sources (custom rules or Access Optimizer features).</p> <p>If you deselect the check-box, the behavior it's the same but the starting data block is represented by the dataset that is linked to the campaign.</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"> • Daily, starting from K days before the end of the campaign as determined by Days before end date, where K is a value 0 - 32. • When the percentage of activity that is already managed is lower than X% as 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 a daily email starting from K days before the end of the campaign. Determined by Days before end date, where K 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 a daily email starting from <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  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	<p> Stats monitors the status of the campaign completion.</p> <p> Inspect inspects the entities of the campaign.</p>
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.

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 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.
% 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 Detail	Description
Campaign Type	Type of campaign. <ul style="list-style-type: none"> • User Assignment • Organization Unit Assignment • Risk Violation Mitigation • Entitlement • Account
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 • By User • End Review
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 39. 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 40. 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.</p> <p>If Duration=Continuous, you cannot set values for this parameter.</p> <p>In alternative, is shown the check-box Ignore the Dataset at the launch of the Campaign, selected by default.</p> <p>Maintaining the default setting, the campaign works on data that can be feed from several sources (custom rules or Access Optimizer features).</p> <p>If you deselect the check-box, the behavior it's the same but the starting data block is represented by the dataset that is linked to the campaign.</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"> • Daily, starting from <i>K</i> days before the end of the campaign as 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 lower than <i>X</i>% as 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 a daily email starting from <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.</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 a daily email starting from <i>K</i> days 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, the surname, or the user ID of the user.


Reviewer filters	
Filter	Description
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	 Stats monitors the status of the campaign completion.  Inspect inspects the entities of the campaign.
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.

Supervisor Campaign	
Details	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 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"> • User Assignment • Organization Unit Assignment • Risk Violation Mitigation • Entitlement • Account
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 • By User • End Review

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 41. 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 42. 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.</p> <p>If Duration=Continuous, you cannot set values for this parameter.</p> <p>In alternative, is shown the check-box Ignore the Dataset at the launch of the Campaign, selected by default.</p> <p>Maintaining the default setting, the campaign works on data that can be feed from several sources (custom rules or Access Optimizer features).</p> <p>If you deselect the check-box, the behavior it's the same but the starting data block is represented by the dataset that is linked to the campaign.</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"> • Daily, starting from K days before the end of the campaign as determined by Days before end date, where K is a value 0 - 32. • When the percentage of activity that is already managed is lower than X% as 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>


Notification Type	Description
Campaign Reminder for Reviewer	<p>If Enable is set, the reviewer receives a daily email starting from <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 a daily email starting from <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 <input type="text"/> 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"> • User Assignment • Organization Unit Assignment • Risk Violation Mitigation • Entitlement • Account
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 • By User • End Review
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 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.

Table 43. Cert_Campaign_Reviewer_Tab (continued)

Reviewer Detail	Description
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)


Table 44. 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.</p> <p>If Duration=Continuous, you cannot set values for this parameter.</p> <p>In alternative, is shown the check-box Ignore the Dataset at the launch of the Campaign, selected by default.</p> <p>Maintaining the default setting, the campaign works on data that can be feed from several sources (custom rules or Access Optimizer features).</p> <p>If you deselect the check-box, the behavior it's the same but the starting data block is represented by the dataset that is linked to the campaign.</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"> • Daily, starting from <i>K</i> days before the end of the campaign as 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 lower than <i>X</i>% as 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 a daily email starting from <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.</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 a daily email starting from <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  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

Reviewer details	
Detail	Description
% 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

You can browse a number of Matching Dashboards, one for every target (application or external system) engaged.

Matching Dashboard

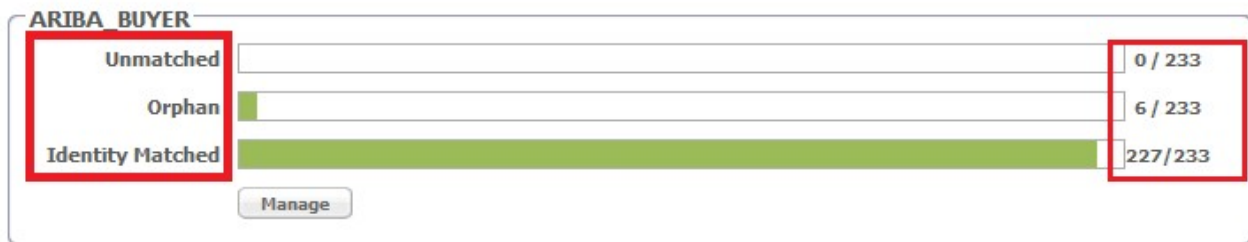


Figure 1. Application Accounts: Matching Dashboard

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 that retrieved from the target.


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

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

Table 45. User filters

Filter	Description
Account ID	The unique identifier of the application.


Table 45. User filters (continued)

Filter	Description
Status	The status of the account. <ul style="list-style-type: none"> • Unmatched • Orphan • Identity Matched
Master UID	The unique identifier of the user to whom the account is assigned.
Organization Unit	The organizational unit that is associated with the account. Click  OU to enter an OU.
Hierarchy	Flag this check-box to specify that the search is to be made on the entire organizational hierarchy that starts 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 46. User/Account attributes

Attribute	Description
Account details	Click  Account details for getting all the details that are related to the account.
Account ID	The unique identifier of the application.
Status	The status of the account. <ul style="list-style-type: none"> • Unmatched • Orphan • Identity Matched
Master UID	The unique identifier of the user to whom the account is assigned.
Name	The name of the user to whom the account is assigned.
Surname	
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	Personal data of the user referred by Master UID .

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

Permissions

Shows a list of permissions that are related to the account. If the target is an external system, it displays a list of the last 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 that is 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.

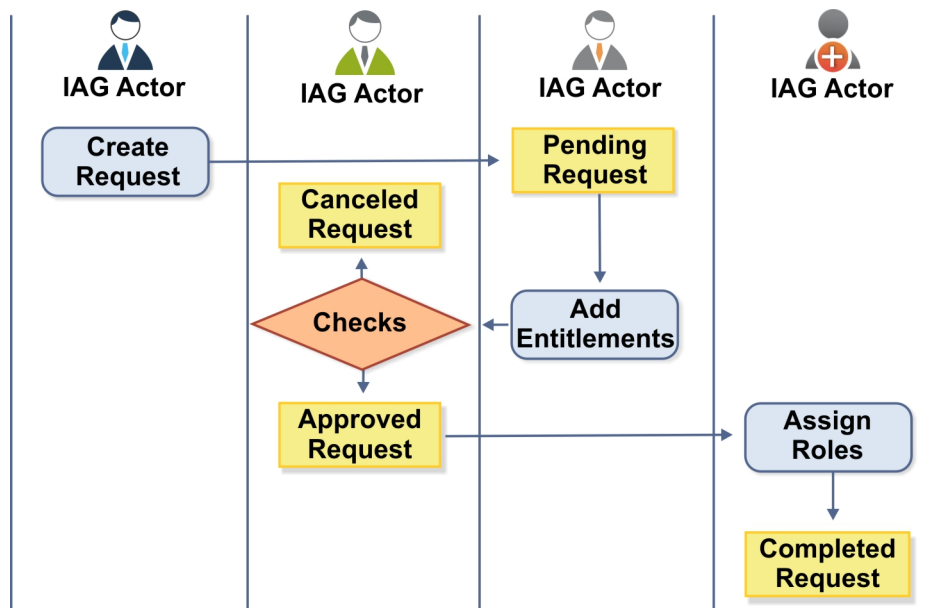


Figure 2. Example of authorization workflow

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 47. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Authorizable	Request is waiting for authorization.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles.
Expired	Request exceeded the time limit that is specified by its Priority without being processed.
In execution	Request is waiting for the propagation to the target system.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in Approved status.
Partially Authorized	Request with some sub requests in Authorizable status.
Partially Completed	Request with all sub requests at end of lifecycle, some of them in Completed status and some of them in Failed Completion status.
Partially Executed	Request with some sub requests in Executed status.
Partially Terminated	Request with some sub requests in Completed status and some in progress.
Pending	Source request is waiting for formalization by one or more approvers.
Rejected	Request can no longer be processed. It is a final status for the request.
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

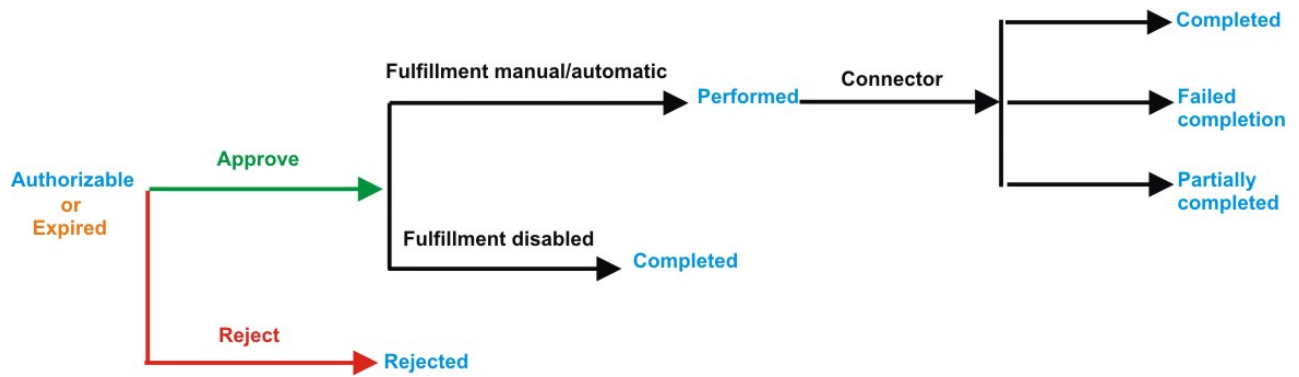


Figure 3. Subrequest status

Table 48. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization.
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Automatic, it means that the connector aligned every permission on the target system. If the fulfillment is on Manual, a human operator aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its Priority without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

AR functions

Access Requests Manager provides several functions.

This module provides the following set of functions:

- “Account management: generating a request” on page 80
- “Account management: authorizing a request” on page 131
- “Account management: executing a request” on page 131
- “Selecting users in a new request to assign entitlements and roles” on page 131
- “Authorizing a request to assign entitlements and roles” on page 138
- “Executing a request to assign entitlements and roles” on page 146
- “Generating a request to delegate administrative roles” on page 152
- “Authorizing a request to delegate administrative roles” on page 153
- “Executing a request to delegate administrative roles” on page 153
- “Viewing requests in your Daily Work scope” on page 153

- “Viewing the requests present in the system” on page 215
- “Generating a request to delegate entitlements” on page 160
- “Authorizing a Delegation request” on page 164
- “Executing a Delegation request” on page 172
- “Insert/Update entitlement: generating a request” on page 183
- “Insert/Update entitlement: processing a request” on page 201
- “Insert/Updates entitlements: executing a request” on page 209
- User access: generating a request
- User access: processing a request
- User access: executing a request
- “Create/Update user: generating a request” on page 222
- “Insert/Update user: processing a request” on page 224
- “Insert/Update user: executing a request” on page 233
- “Authorize escalation” on page 179

Account management: generating a request

You can generate a request for the creation of an account or for updating an existing one. You can also generate a detailed request to reset a user password or to suspend or restore a user account.



- Create Account
- Update Account
- Detailed Request

Generating a request for creating a new account

Use this tab to generate a request to create a new account.

In the **Account Creation** tab, the following filters are available:

Table 49. Account filters

Filter	Description
Priority	<p>Set the level of priority of the request:</p> <ul style="list-style-type: none"> • Low • Medium • High • Unassigned <p>The effect of this setting depends by the configuration of the workflow that is made in Process Designer (see Assigning an expiration reminder policy to a WorkFlow process).</p>
Request Notes	A text field where you can add a free text for commenting the request.
Select a user	<p>Click  Browse to choose the user that is the beneficiary of the account. This selection is mandatory.</p> <p>Note: If the beneficiary of the request is the logged in actor that is managing the request, the field is set and disabled.</p>
Select an account	<p>After the selection of the user, this field is enabled. Click  Browse to choose the account. You can also click on Applications icon to view the applications that are associated with the account configuration.</p>

According to the configuration of Process Designer (see **Process Designer > Manage > Activity**) can be present options for locking the account.

After the filtering, you might decide to create a locked account.

If it is configured, in a single row you find the check-box that describes the reasons for locking an account:

Tech. Suspend

Access that is suspended for technical reasons.

Sec. Suspend

Access that is suspended for security reasons.

Terminated

Access that is suspended permanently.

Auth. Suspend

Access that is suspended because of authorization conflicts.

Expired

The expiration date that is defined for user was reached.

Maint. Suspend

Access is suspended because the account is under maintenance.

After the locking options, the page shows the following attributes:

Table 50. Account details.

Detail	Description
First Name	User name.
Last Name	User surname.
Account ID	Identifies the user on the AG Core module.
Email	Email address of the user. This information is used also from the policies that are related to account expiration.
DN	Distinguished Name of the user.
Display Name	Extra field for future use.
Expiration	After the expiration date, the policies that are configured for the account expiration are enabled (see Access Governance CoreManage > Account). These policies are applied for all the users that are associated to the account that expired.
Target Attributes	<p>A variable subset of account attributes. This subset can be:</p> <ol style="list-style-type: none"> 1. Configured in Access Governance Core > Manage > Accounts > Account Attributes. 2. Additionally filtered in Process Designer > Manage > Activity. <p>This subset might be also an empty set: in this case are not present attributes.</p>

Note: In some views, the type and the number of attributes that are shown, can be dependent by the configuration steps previously indicated.

There is a dedicated section **Password** for managing the password policy settings.

The password policy set in this phase is shared among all the applications that are related to the created account.

For setting the password policy, the following elements are available:

Table 51. Password attributes.

Attribute	Description
New Password	The password for the account to be created. You can write directly the new password or you can click Generate for the automatic provisioning of a random password.
Confirm Password	Repeat the password indicated in New Password . Select the check-box Show password characters if you want to view the password.
Password Requirements	The list of all properties that you must satisfy when you set the New Password . These requirements are related to the account selected in the filters section. The password requirements for the selected account are set in Access Governance Core > Manage > Accounts > Password Creation .

After the definition of all settings, click **Submit** for forwarding the request to the next step, the Authorizing an account creation request.

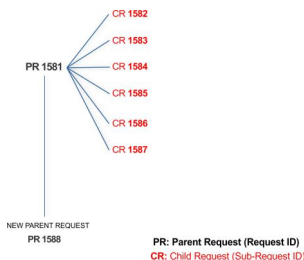
Authorizing an account creation request

Authorizing a creation 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 that are registered through the REQUEST REPORT EXE activity.

When you are logged-in as approver, some of the request (and subrequest) listed through the REQUEST REPORT EXE might not be visible because out of the scope of the approver.

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

Table 52. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Authorizable	Request is waiting for authorization.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles.
Expired	Request exceeded the time limit that is specified by its Priority without being processed.
In execution	Request is waiting for the propagation to the target system.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in Approved status.
Partially Authorized	Request with some sub requests in Authorizable status.
Partially Completed	Request with all sub requests at end of lifecycle, some of them in Completed status and some of them in Failed Completion status.
Partially Executed	Request with some sub requests in Executed status.
Partially Terminated	Request with some sub requests in Completed status and some in progress.
Pending	Source request is waiting for formalization by one or more approvers.
Rejected	Request can no longer be processed. It is a final status for the request.
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

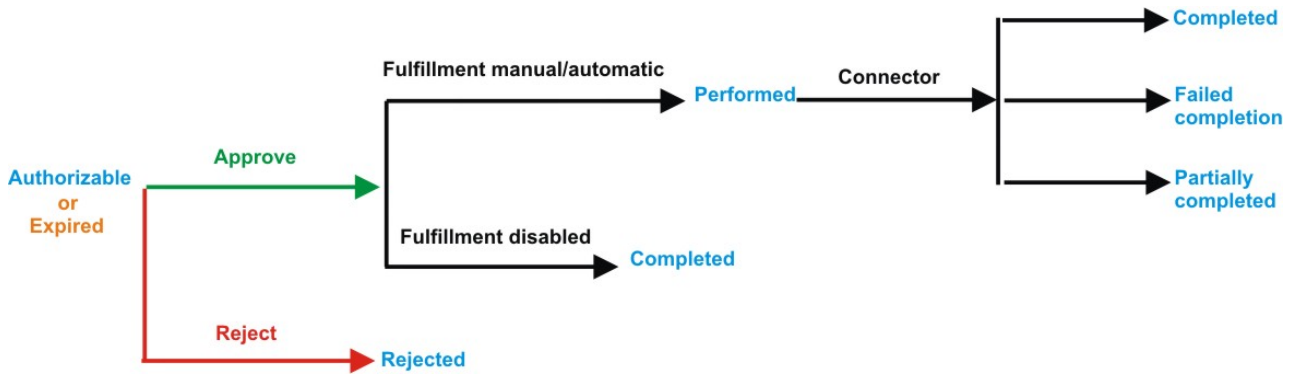


Figure 4. Subrequest status

Table 53. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization.
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Automatic, it means that the connector aligned every permission on the target system. If the fulfillment is on Manual, a human operator aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its Priority without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

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

Table 54. Filters

Filter	Description
Request ID	The 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	The identifier of the IAG actor who generated the request.
Beneficiary Identity	The identifier of the beneficiary of the request.
Type	The action that is requested.
Status	The status of the sub request.

Table 54. Filters (continued)

Filter	Description
Created between	<p>Start Date The start of a time interval when the request was submitted.</p> <p>End Date The end of a time interval when the request was submitted.</p>

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

Requests attributes	
Attribute	Description
Request ID	Unique identifier of the parent request.
Sub-Request ID	Unique 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	The date of creation of the request.
Status	The status of the subrequest.
Priority	The priority that is assigned to the request.

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


Table 55. 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 first part of the frame shows the following information about the **Actors of the Request**:

Table 56. Details of a request

Box	Details
Request	<p>Request ID The unique identifier of the request.</p> <p>Type The type of the request.</p> <p>Status The status of the request. See Table 2 for the different status of a request.</p> <p>Priority The priority that is assigned by the applicant to the request.</p> <p>Created on The date of creation of the request.</p>
Applicant/Beneficiary	<p>Group The group of the Applicant/Beneficiary.</p> <p>First Name The given name of the Applicant/Beneficiary.</p> <p>Last Name The surname of the Applicant/Beneficiary.</p> <p>User ID The unique identifier of the Applicant/Beneficiary. Click  Info to view the user details.</p>


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

Table 57. 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 58. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement information 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 59. User Details - Accounts tab

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

Table 60. 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 61. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

You find also two areas that can contain text:

Request Notes

If the request generated in the previous step doesn't contain notes, this area is empty.

Additional Notes

You can add extra notes for addressing the next step of the flow.

After these two text areas, might be present a row that shows different options for locking the account:

Tech. Suspend

Access that is suspended for technical reasons.

Sec. Suspend

Access that is suspended for security reasons.

Terminated

Access that is suspended permanently.

Auth. Suspend

Access that is suspended because of authorization conflicts.

Expired

The expiration date that is defined for user was reached.

Maint. Suspend

Access is suspended because the account is under maintenance.

Thus you can view several information about the account:

Table 62. Account details.

Detail	Description
First Name	User name.
Last Name	User surname.
Master UID	Identifies the user on the AG Core module.
Email	Email address of the user. This information is used also from the policies that are related to account expiration.
DN	Distinguished Name of the user.
Display Name	Extra field for future use.
Account Expiration Date	After the expiration date, the policies that are configured for the account expiration are enabled (see Access Governance CoreManage > Account). These policies are applied for all the users that are associated to the account that expired.
Applications	Applications that are associated with the account configuration.
Account Attributes	A variable subset of account attributes. This set is defined in the previous step of the workflow.

Note: In some views, the type and the number of attributes that are shown, can be dependent by the configuration steps previously indicated.

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

Requests attributes	
Attribute	Description
Approver	Identifier of the approver that is managing the authorization step.
Status	The status of the request. See Table 2 for the different status of a request.
Last modification date	Date of the last modification.
Approver Details	Extra information that is related to the approver.

Select one of the following options to process the request.

Back Returns you to the list of requests without acting.

Approve
Approves the request.

Reject Rejects the request.

Redirect
Redirects the request to another approver. The Request Redirection window displays a list of candidate users. Select the user to whom you want to redirect the request for approval or rejection.

This option does not change the status of the request.

Send Back
This option is displayed only if the request was redirected to you by the original approver. You can return the request to the original approver, if you determine that you cannot approve or reject it. Write comments in the **Additional Notes** box.

This option does not change the status of the request.

Note:

A request arrives to an approver A with a certain set S of fields; the approver (according to the design of the authorization activity) might add another set S1 of information fields.

Clicking **Approve**, the request sent to the next step of the flow is made up by the fields $S \cup S1$.

Clicking **Redirect**, for sending the request to another approver AR, this last one can see only the set of fields S.

If A edit the information before the redirection, all edited information is lost.

AR might add a set of fields S2; if AR click on **Approve**, the request sent to the next step of the flow, is made up by the fields $S \cup S2$.

If the approver AR click on **Send Back**, the information that are edited by AR is lost.

The **Redirect** and **Send Back** actions are used only to switch requests among approvers, without any update to the request information.

After the **Approve** action, the request is sent to the next step, the Executing an account creation request.

Executing a request of account creation

An account creation request might include an execution step.

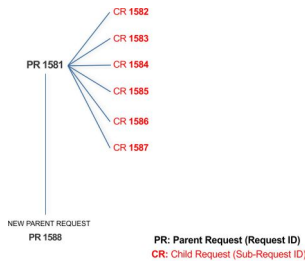
According to the configuration (see **Process Designer > Manage > Activity**), this step might be executed:

- Automatically through a connector
- Manually

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 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.

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

Table 63. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Authorizable	Request is waiting for authorization.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles.
Expired	Request exceeded the time limit that is specified by its Priority without being processed.
In execution	Request is waiting for the propagation to the target system.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in Approved status.
Partially Authorized	Request with some sub requests in Authorizable status.
Partially Completed	Request with all sub requests at end of lifecycle, some of them in Completed status and some of them in Failed Completion status.
Partially Executed	Request with some sub requests in Executed status.
Partially Terminated	Request with some sub requests in Completed status and some in progress.
Pending	Source request is waiting for formalization by one or more approvers.
Rejected	Request can no longer be processed. It is a final status for the request.

Table 63. Request Status (continued)

Status	Description
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

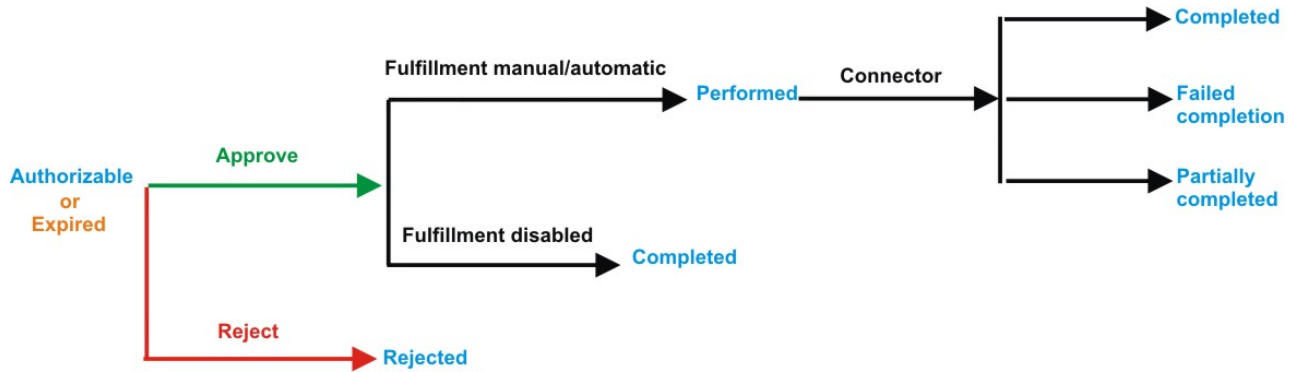


Figure 5. Subrequest status

Table 64. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization.
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Automatic, it means that the connector aligned every permission on the target system. If the fulfillment is on Manual, a human operator aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its Priority without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

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

Table 65. Filters

Filter	Description
Request ID	The Unique identifier of the request.

Table 65. Filters (continued)

Filter	Description
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity	The identifier of the IAG actor who generated the request.
Beneficiary Identity	The identifier of the beneficiary of the request.
Type	The action that is requested.
Status	The status of the sub request.
Created between	<p>Start Date The start of a time interval when the request was submitted.</p> <p>End Date The end of a time interval when the request was submitted.</p>

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

Requests attributes	
Attribute	Description
Request ID	Unique identifier of the parent request.
Sub-Request ID	Unique 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	The date of creation of the request.
Status	The status of the considered request, according to the values indicated in the table 1.
Priority	The priority that is assigned to the request.

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

Table 66. 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 66. 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 first part of the frame shows the following information about the **Actors of the Request**:

Table 67. Details of a request

Box	Details
Request	<p>Request ID The unique identifier of the request.</p> <p>Type The type of the request.</p> <p>Status The status of the request. See Table 2 for the different status of a request.</p> <p>Priority The priority that is assigned by the applicant to the request.</p> <p>Created on The date of creation of the request.</p>
Applicant/Beneficiary	<p>Group The group of the Applicant/Beneficiary.</p> <p>First Name The given name of the Applicant/Beneficiary.</p> <p>Last Name The surname of the Applicant/Beneficiary.</p> <p>User ID The unique identifier of the Applicant/Beneficiary. Click  Info to view the user details.</p>


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

Table 68. 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

Table 68. User Details - Details tab (continued)

Detail	Description
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 69. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement information 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 70. User Details - Accounts tab

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

Table 71. 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 72. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.

Table 72. User Details - Rights (continued)

Detail	Description
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

You find also two areas that can contain text:

Request Notes

If the request generated in the first step doesn't contain notes, this area is empty.

Additional Notes

Extra notes possibly added in the previous authorization step of the flow.

After these two text areas, might be present a row that shows different options for locking the account:

Tech. Suspend

Access that is suspended for technical reasons.

Sec. Suspend

Access that is suspended for security reasons.

Terminated

Access that is suspended permanently.

Auth. Suspend

Access that is suspended because of authorization conflicts.

Expired

The expiration date that is defined for user was reached.

Maint. Suspend

Access is suspended because the account is under maintenance.

Thus you can view several information about the account:

Table 73. Account details.

Detail	Description
First Name	User name.
Last Name	User surname.
Master UID	Identifies the user on the AG Core module.
Email	Email address of the user. This information is used also from the policies that are related to account expiration.
DN	Distinguished Name of the user.
Display Name	Extra field for future use.
Account Expiration Date	After the expiration date, the policies that are configured for the account expiration are enabled (see Access Governance CoreManage > Account). These policies are applied for all the users that are associated to the account that expired.
Applications	Applications that are associated with the account configuration.


Table 73. Account details. (continued)

Detail	Description
Account Attributes	A variable subset of account attributes. This set is defined in the previous step of the workflow.

Note: In some views, the type and the number of attributes that are shown, can be dependent by the configuration steps previously indicated.

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

Requests attributes	
Attribute	Description
Approver	Identifier of the approver that is managing the authorization step.
Status	The status of the request. See Table 2 for the different status of a request.
Last modification date	Date of the last modification.
Approver Info	Extra information that is related to the approver.

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

When you finished to process a request, click **Execute** to mark the request as completed.

Generating a request for updating an account

Use this tab to generate a request to update an existing account.

In the **Account Update** tab, the following filters are available:

Table 74. Account filters



Filter	Description
Priority	Set the level of priority of the request: <ul style="list-style-type: none"> • Low • Medium • High • Unassigned <p>The effect of this setting depends by the configuration of the workflow that is made in Process Designer (see Assigning an expiration reminder policy to a WorkFlow process).</p>
Request Notes	A text field where you can add a free text for commenting the request.
Select a user	Click  Browse to choose the user that is the beneficiary of the account. This selection is mandatory. Note: If the beneficiary of the request is the logged in actor that is managing the request, the field is set and disabled.

Table 74. Account filters (continued)

Filter	Description
Select an account	After the selection of the user, this field is enabled. Click  Browse to choose the account. You can also click on Applications icon to view the applications that are associated with the account configuration.

If available, you can select the check-box **Remove this account** for deleting the account that you are considering. In this case, all the fields present in the page are disabled.

According to the configuration of Process Designer (see **Process Designer > Manage > Activity**) can be present options for locking the account.

After the filtering, you might decide to create a locked account.

In a single row you find the check-box that describes the reasons for locking an account:

Tech. Suspend

Access that is suspended for technical reasons.

Sec. Suspend

Access that is suspended for security reasons.

Terminated

Access that is suspended permanently.

Auth. Suspend

Access that is suspended because of authorization conflicts.

Expired

The expiration date that is defined for user was reached.

Maint. Suspend

Access is suspended because the account is under maintenance.

After the locking options, the page shows the following attributes:

Table 75. Account details.

Detail	Description
First Name	User name.
Last Name	User surname.
Account ID	Identifies the user on the AG Core module.
Email	Email address of the user. This information is used also from the policies that are related to account expiration.
DN	Distinguished Name of the user.
Display Name	Extra field for future use.
Expiration	After the expiration date, the policies that are configured for the account expiration are enabled (see Access Governance CoreManage > Account). These policies are applied for all the users that are associated to the account that expired.

Table 75. Account details. (continued)

Detail	Description
Target Attributes	<p>A variable subset of account attributes. This subset can be:</p> <ol style="list-style-type: none"> 1. Configured in Access Governance Core > Manage > Accounts > Account Attributes. 2. Additionally filtered in Process Designer > Manage > Activity. <p>This subset might be also an empty set: in this case are not present attributes.</p>

Note: In some views, the type and the number of attributes that are shown, can be dependent by the configuration steps previously indicated.

After the definition of all settings, click **Submit** for forwarding the request to the next step, the Authorizing an account update request.

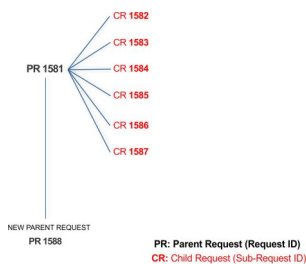
Authorizing an account update request

Authorizing an update 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 that are registered through the REQUEST REPORT EXE activity.

When you are logged-in as approver, some of the request (and subrequest) listed through the REQUEST REPORT EXE might not be visible because out of the scope of the approver.

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

Table 76. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Authorizable	Request is waiting for authorization.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles.
Expired	Request exceeded the time limit that is specified by its Priority without being processed.
In execution	Request is waiting for the propagation to the target system.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in Approved status.
Partially Authorized	Request with some sub requests in Authorizable status.
Partially Completed	Request with all sub requests at end of lifecycle, some of them in Completed status and some of them in Failed Completion status.
Partially Executed	Request with some sub requests in Executed status.
Partially Terminated	Request with some sub requests in Completed status and some in progress.
Pending	Source request is waiting for formalization by one or more approvers.
Rejected	Request can no longer be processed. It is a final status for the request.
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

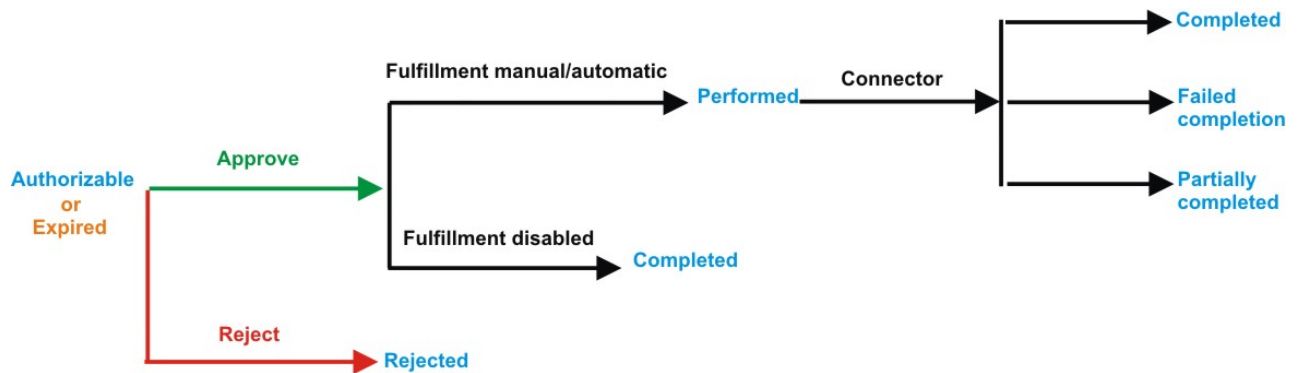


Figure 6. Subrequest status

Table 77. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization.
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Automatic, it means that the connector aligned every permission on the target system. If the fulfillment is on Manual, a human operator aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its Priority without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

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

Table 78. Filters

Filter	Description
Request ID	The 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	The identifier of the IAG actor who generated the request.
Beneficiary Identity	The identifier of the beneficiary of the request.
Type	The action that is requested.
Status	The status of the sub request.
Created between	<p>Start Date The start of a time interval when the request was submitted.</p> <p>End Date The end of a time interval when the request was submitted.</p>

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

Requests attributes	
Attribute	Description
Request ID	Unique identifier of the parent request.
Sub-Request ID	Unique 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	The date of creation of the request.
Status	
Priority	The priority that is assigned to the request.

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


Table 79. 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 first part of the frame shows the following information about the **Actors of the Request**:

Table 80. Details of a request

Box	Details
Request	<p>Request ID The unique identifier of the request.</p> <p>Type The type of the request.</p> <p>Status The status of the request. See Table 2 for the different status of a request.</p> <p>Priority The priority that is assigned by the applicant to the request.</p> <p>Created on The date of creation of the request.</p>
Applicant/Beneficiary	<p>Group The group of the Applicant/Beneficiary.</p> <p>First Name The given name of the Applicant/Beneficiary.</p> <p>Last Name The surname of the Applicant/Beneficiary.</p> <p>User ID The unique identifier of the Applicant/Beneficiary. Click  Info to view the user details.</p>


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

Table 81. 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 82. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement information 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 83. User Details - Accounts tab

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

Table 84. 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 85. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

You find also two areas that can contain text:

Request Notes

If the request generated in the previous step doesn't contain notes, this area is empty.

Additional Notes

You can add extra notes for addressing the next step of the flow.

After these two text areas, might be present a row that shows different options for locking the account:

Tech. Suspend

Access that is suspended for technical reasons.

Sec. Suspend

Access that is suspended for security reasons.

Terminated

Access that is suspended permanently.

Auth. Suspend

Access that is suspended because of authorization conflicts.

Expired

The expiration date that is defined for user was reached.

Maint. Suspend

Access is suspended because the account is under maintenance.

Thus you can view several information about the account:

Table 86. Account details.

Detail	Description
First Name	User name.
Last Name	User surname.
Master UID	Identifies the user on the AG Core module.
Email	Email address of the user. This information is used also from the policies that are related to account expiration.
DN	Distinguished Name of the user.
Display Name	Extra field for future use.
Account Expiration Date	After the expiration date, the policies that are configured for the account expiration are enabled (see Access Governance CoreManage > Account). These policies are applied for all the users that are associated to the account that expired.
Applications	Applications that are associated with the account configuration.
Account Attributes	A variable subset of account attributes. This set is defined in the previous step of the workflow.

Note: In some views, the type and the number of attributes that are shown, can be dependent by the configuration steps previously indicated.

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

Requests attributes	
Attribute	Description
Approver	Identifier of the approver that is managing the authorization step.
Status	The status of the request. See Table 2 for the different status of a request.
Last modification date	Date of the last modification.
Approver Details	Extra information that is related to the approver.

Select one of the following options to process the request.

Back Returns you to the list of requests without acting.

Approve
Approves the request.

Reject Rejects the request.

Redirect
Redirects the request to another approver. The Request Redirection window displays a list of candidate users. Select the user to whom you want to redirect the request for approval or rejection.

This option does not change the status of the request.

Send Back
This option is displayed only if the request was redirected to you by the original approver. You can return the request to the original approver, if you determine that you cannot approve or reject it. Write comments in the **Additional Notes** box.

This option does not change the status of the request.

Note:

A request arrives to an approver A with a certain set S of fields; the approver (according to the design of the authorization activity) might add another set S1 of information fields.

Clicking **Approve**, the request sent to the next step of the flow is made up by the fields $S \cup S1$.

Clicking **Redirect**, for sending the request to another approver AR, this last one can see only the set of fields S.

If A edit the information before the redirection, all edited information is lost.

AR might add a set of fields S2; if AR click on **Approve**, the request sent to the next step of the flow, is made up by the fields $S \cup S2$.

If the approver AR click on **Send Back**, the information that are edited by AR is lost.

The **Redirect** and **Send Back** actions are used only to switch requests among approvers, without any update to the request information.

After the **Approve** action, the request is sent to the next step, the Executing an account creation request.

Executing a request of account update

Executing an account update request.

An account update request might include an execution step.

According to the configuration (see **Process Designer > Manage > Activity**), this step might be executed:

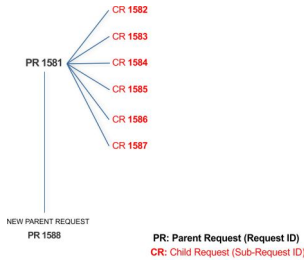
- Automatically through a connector

- Manually

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 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.

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

Table 87. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Authorizable	Request is waiting for authorization.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles.
Expired	Request exceeded the time limit that is specified by its Priority without being processed.
In execution	Request is waiting for the propagation to the target system.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in Approved status.
Partially Authorized	Request with some sub requests in Authorizable status.
Partially Completed	Request with all sub requests at end of lifecycle, some of them in Completed status and some of them in Failed Completion status.
Partially Executed	Request with some sub requests in Executed status.
Partially Terminated	Request with some sub requests in Completed status and some in progress.
Pending	Source request is waiting for formalization by one or more approvers.

Table 87. Request Status (continued)

Status	Description
Rejected	Request can no longer be processed. It is a final status for the request.
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

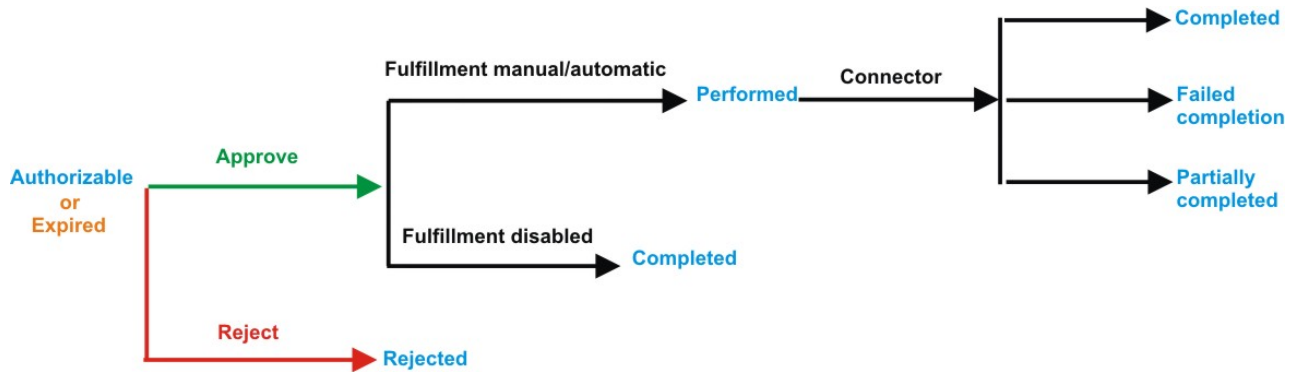


Figure 7. Subrequest status

Table 88. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization.
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Automatic, it means that the connector aligned every permission on the target system. If the fulfillment is on Manual, a human operator aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its Priority without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

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

Table 89. Filters

Filter	Description
Request ID	The 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	The identifier of the IAG actor who generated the request.
Beneficiary Identity	The identifier of the beneficiary of the request.
Type	The action that is requested.
Status	The status of the sub request.
Created between	<p>Start Date The start of a time interval when the request was submitted.</p> <p>End Date The end of a time interval when the request was submitted.</p>

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

Requests attributes	
Attribute	Description
Request ID	Unique identifier of the parent request.
Sub-Request ID	Unique 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	The date of creation of the request.
Status	The status of the considered request, according to the values indicated in the table 1.
Priority	The priority that is assigned to the request.

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

Table 90. 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 90. 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 first part of the frame shows the following information about the **Actors of the Request**:

Table 91. Details of a request

Box	Details
Request	<p>Request ID The unique identifier of the request.</p> <p>Type The type of the request.</p> <p>Status The status of the request. See Table 2 for the different status of a request.</p> <p>Priority The priority that is assigned by the applicant to the request.</p> <p>Created on The date of creation of the request.</p>
Applicant/Beneficiary	<p>Group The group of the Applicant/Beneficiary.</p> <p>First Name The given name of the Applicant/Beneficiary.</p> <p>Last Name The surname of the Applicant/Beneficiary.</p> <p>User ID The unique identifier of the Applicant/Beneficiary. Click  Info to view the user details.</p>


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

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

Table 92. User Details - Details tab (continued)

Detail	Description
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 93. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement information 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 94. User Details - Accounts tab

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

Table 95. 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 96. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.

Table 96. User Details - Rights (continued)

Detail	Description
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

You find also two areas that can contain text:

Request Notes

If the request generated in the first step doesn't contain notes, this area is empty.

Additional Notes

Extra notes possibly added in the previous authorization step of the flow.

After these two text areas, might be present a row that shows different options for locking the account:

Tech. Suspend

Access that is suspended for technical reasons.

Sec. Suspend

Access that is suspended for security reasons.

Terminated

Access that is suspended permanently.

Auth. Suspend

Access that is suspended because of authorization conflicts.

Expired

The expiration date that is defined for user was reached.

Maint. Suspend

Access is suspended because the account is under maintenance.

Thus you can view several information about the account:

Table 97. Account details.

Detail	Description
First Name	User name.
Last Name	User surname.
Master UID	Identifies the user on the AG Core module.
Email	Email address of the user. This information is used also from the policies that are related to account expiration.
DN	Distinguished Name of the user.
Display Name	Extra field for future use.
Account Expiration Date	After the expiration date, the policies that are configured for the account expiration are enabled (see Access Governance CoreManage > Account). These policies are applied for all the users that are associated to the account that expired.
Applications	Applications that are associated with the account configuration.


Table 97. Account details. (continued)

Detail	Description
Account Attributes	A variable subset of account attributes. This set is defined in the previous step of the workflow.

Note: In some views, the type and the number of attributes that are shown, can be dependent by the configuration steps previously indicated.

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

Requests attributes	
Attribute	Description
Approver	Identifier of the approver that is managing the authorization step.
Status	The status of the request. See Table 2 for the different status of a request.
Last modification date	Date of the last modification.
Approver Info	Extra information that is related to the approver.

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

When you finished to process a request, click **Execute** to mark the request as completed.

Generating a request for managing a password

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 are available:

Table 98. User filters


Filter	Description
User Type	The type of user. For example, Administrative, Business, Employee, Training, External.

Table 98. User filters (continued)

Filter	Description
First Name/Last Name/Master UID	The name or surname or the unique identifier of the user.
Enabled	The user is enabled to receive assignments of entitlements.
Activity	The business activity that the user is involved with. After the selection of the activity, you can flag Hierarchy to search also all the activities that are defined from this point down in the hierarchical structure.

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

Table 99. Attributes in the Users list

Attribute	Description
User Details	Click  User Details to open the User details window. This window shows several user details like external data, assigned entitlements, assigned accounts, and rights.
First Name	The name of the user
Last Name	The surname of the user
User ID	The Unique identifier of the user
User Type	The type of user. For example, Administrative, Business, Employee, Training, External.
Group [Code]	The Organization Unit [Univocal identifier of the OU] to which the user belongs

To select a user, click a row.



Click  **Info** to show the Details window. The window includes several tabs. Some of the tabs might not be present depending on the properties that were defined for the user:

Table 100. User Information tabs

Tab	Description
Details	User information, including ID, type, organization, name, and address. This tab is always present.
External Data	Information that is taken from the User Virtual Attributes that are mapped from external databases in Access Governance Core.
Entitlements	A list of the entitlements that are assigned to this user. Click  Info for more information on an entitlement, its structure, the permissions that compose it, and the list of users and groups that are entitled to it.
Accounts	The list of accounts that this user can access. This tab is always present. Every user that is 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 that are assigned to this user.

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

Related tasks:

“Resetting account passwords for other users” on page 8

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.

Setting security questions in a new request to make account changes

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 that were 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 8

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.

Selecting accounts in a new request to make account changes



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

You can do 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.

Priority declares the priority level that is assigned to this request. If the field is enabled, you can change the priority level. Select the field to display the available priority levels to which you can move the request.

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


You can click  to view the list of applications that are associated with the account and the details that are related to the account:

Table 101. Account details

Detail	Description
Applications	Applications that are associated with the account configuration.
Account ID	Identifies the user on the AG Core module.
First Name	User name.
Last Name	User surname.
Email	Email address of the user. This information is used also from the policies that are related to account expiration.
DN	Distinguished Name of the user.
Display Name	Distinguished Name of the user.
Account Expiration Date	After the expiration date, the policies that are configured for the account expiration are enabled (see Manage > Account). These policies are applied for all the users that are associated to the account that expired.
Last Login	Date of the last login.
Last Login Error	Date of the last login error.
Number of Login Errors	Number of consecutive login errors. This value is reset to zero when a correct login is made.
Last Password Change	Date of the last password change.
Target Attributes	A variable subset of account attributes. This subset is configured in Manage > Accounts > Target Attributes . This subset might be also an empty set: in this case are not present attributes.

Note: In some views, the type and the number of attributes that are shown can be dependent by the configuration set in **Manage > Account > Target Attributes**. In particular, see the following conditions:

- Only a subset of data might be shown (see **Visible** column).
- Only a subset of data might be mandatory (indicated by *) (see **Required** column).
- Only a subset of data might be editable (see **Editable** column).
- Only a subset of data might be set with a default value (see **Default Value** column).

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 that is suspended for technical reasons.

Sec. Suspend

Access that is suspended for security reasons.

Terminated

Access that is suspended permanently.

Auth. Suspend

Access that is suspended because of authorization conflicts.

Expired

The expiration date that is defined for user was reached.

Maint. Suspend

Access is suspended because the account is under maintenance.

After you select the entire account, you can act 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.

Priority declares the priority level that is assigned to this request. If the field is enabled, you can change the priority level. Select the field to display the available priority levels to which you can move the request.

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

The  symbol means that this account is unlocked.

The  symbol means that this account is locked.

Select the check box in the title bar to select all the accounts that are 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 8

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.


Entering the new password in a new request to make account changes

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

You are now in the Account Password Management window where you add the new password for the beneficiary. This step follows the steps where you selected the user for this action, verified the user's identity, and selected the accounts to which the new password is to grant access,

The appearance of the left portion of this window changes based on the configuration options that were 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 the **Your Password** field, 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** pushbutton on the right side of these fields. Select it to generate the password automatically. If **Generate** is not present, you are required to enter the new password. The password characters that you type are hidden. A **Show password characters** check box might be provided to help you view the password that 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.

The work flows that are provided with the product for password reset 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 8

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.

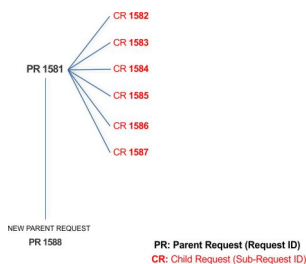
Authorizing a request for managing a password

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 that are registered through the REQUEST REPORT EXE activity.

When you are logged-in as approver, some of the request (and subrequest) listed through the REQUEST REPORT EXE might not be visible because out of the scope of the approver.

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

Table 102. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Authorizable	Request is waiting for authorization.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles.
Expired	Request exceeded the time limit that is specified by its Priority without being processed.
In execution	Request is waiting for the propagation to the target system.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in Approved status.
Partially Authorized	Request with some sub requests in Authorizable status.
Partially Completed	Request with all sub requests at end of lifecycle, some of them in Completed status and some of them in Failed Completion status.
Partially Executed	Request with some sub requests in Executed status.
Partially Terminated	Request with some sub requests in Completed status and some in progress.
Pending	Source request is waiting for formalization by one or more approvers.
Rejected	Request can no longer be processed. It is a final status for the request.
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

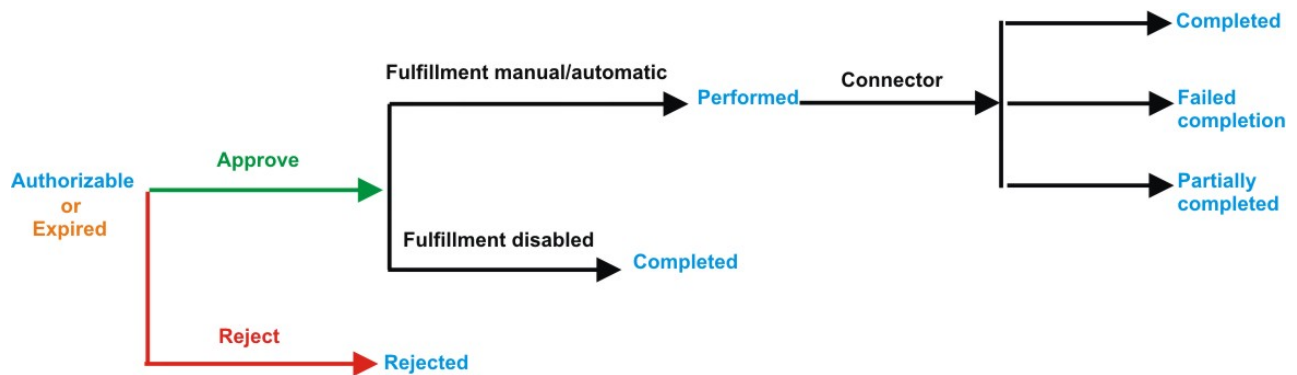


Figure 8. Subrequest status

Table 103. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization.
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Automatic, it means that the connector aligned every permission on the target system. If the fulfillment is on Manual, a human operator aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its Priority without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

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

Table 104. Filters

Filter	Description
Request ID	The 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	The identifier of the IAG actor who generated the request.
Beneficiary Identity	The identifier of the beneficiary of the request.

Table 104. Filters (continued)

Filter	Description
Type	The action that is requested.
Status	The status of the sub request.
Created between	<p>Start Date The start of a time interval when the request was submitted.</p> <p>End Date The end of a time interval when the request was submitted.</p>

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.
Priority	The priority that is assigned to the request.

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


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	

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 106. Details of a request - upper section

Box	Details
Request	<p>ID The unique identifier of the request.</p> <p>Type The type of the request.</p> <p>Status The status of the request.</p> <p>Priority The priority that is assigned by the applicant to the request.</p> <p>Created on The date (dd/mm/yyyy) and time (hh/mm) that the request was created.</p>
Applicant/ Beneficiary/ Delegator/	<p>Group The group of the Applicant/Beneficiary/Delegator.</p> <p>First Name The given name of the Applicant/Beneficiary/Delegator.</p> <p>Last Name The surname of the Applicant/Beneficiary/Delegator.</p> <p>User ID The unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.</p>
Modified Entitlement	<p>Application The application with which the entitlement is associated.</p> <p>Name The name of the entitlement.</p> <p>Description A description of the entitlement.</p> <p>Publishing Status The Publishing Status of the entitlement. Can be Published or Unpublished.</p>

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 107. 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

Table 107. User Details - Details tab (continued)

Detail	Description
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 108. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement information 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 109. User Details - Accounts tab

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

Table 110. 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 111. User Details - Rights


Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.


Table 111. User Details - Rights (continued)

Detail	Description
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

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

Table 112. Request attributes

Attribute	Description
Application	Type of application.
Name	Name of the entitlement.
Description	Brief description of the entitlement.
Owner	Owner of the entitlements that are 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.
Details	For a selected entitlement, click: <ul style="list-style-type: none"> • Information icon for getting the Entitlement Details. • Notes icon for reading a possible note that is specified in the previous step.

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 113. 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 (Application 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 (Application 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 that are related to the request to be authorized.
- Elements that are related to the approver of the request.

Select an option at the bottom to process the request.

Back Returns you to the list of requests without acting.

Approve

Approves the request.

Reject Rejects the request.

Redirect

Redirects the request to another approver. The Request Redirection window displays a list of candidate users. Select the user to whom you want to redirect the request for approval or rejection.

This option does not change the status of the request.

Send Back

This option is displayed only if the request was redirected to you by the original approver. You can return the request to the original approver, if you determine that you cannot approve or reject it. Write comments in the **Additional Notes** box.

This option does not change the status of the request.

Note:

A request arrives to an approver A with a certain set S of fields; the approver (according to the design of the authorization activity) might add another set S1 of information fields.

Clicking **Approve**, the request sent to the next step of the flow is made up by the fields $S \cup S1$.

Clicking **Redirect**, for sending the request to another approver AR, this last one can see only the set of fields S.

If A edit the information before the redirection, all edited information is lost.

AR might add a set of fields S2; if AR click on **Approve**, the request sent to the next step of the flow, is made up by the fields $S \cup S2$.

If the approver AR click on **Send Back**, the information that are edited by AR is lost.

The **Redirect** and **Send Back** actions are used only to switch requests among approvers, without any update to the request information.

Executing a request for account change

You might get requests to reset a password for a user, to suspend or 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 114. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Authorizable	Request is waiting for authorization.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles.
Expired	Request exceeded the time limit that is specified by its Priority without being processed.
In execution	Request is waiting for the propagation to the target system.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in Approved status.
Partially Authorized	Request with some sub requests in Authorizable status.
Partially Completed	Request with all sub requests at end of lifecycle, some of them in Completed status and some of them in Failed Completion status.
Partially Executed	Request with some sub requests in Executed status.
Partially Terminated	Request with some sub requests in Completed status and some in progress.
Pending	Source request is waiting for formalization by one or more approvers.
Rejected	Request can no longer be processed. It is a final status for the request.
Terminated With Reservation	This status includes 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 115. Filters

Filter	Description
Request ID	The 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	The identifier of the IAG actor who generated the request.
Beneficiary Identity	The identifier of the beneficiary of the request.
Type	The action that is requested.
Status	The status of the sub request.

Table 115. Filters (continued)

Filter	Description
Created between	<p>Start Date The start of a time interval when the request was submitted.</p> <p>End Date The end of a time interval when the request was submitted.</p>

Requests are displayed with the following attributes:

Table 116. 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	The status of the considered request, according to the values indicated in the table 1.
Priority	The priority that is assigned to the request

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


Table 117. 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 information about the Request Actors:

Table 118. Details of a request - upper section

Box	Details
Request	<p>ID The unique identifier of the request.</p> <p>Type The type of the request.</p> <p>Status The status of the request.</p> <p>Priority The priority that is assigned by the applicant to the request.</p> <p>Created on The date (dd/mm/yyyy) and time (hh/mm) that the request was created.</p>
Applicant/ Beneficiary/ Delegator/	<p>Group The group of the Applicant/Beneficiary/Delegator.</p> <p>First Name The given name of the Applicant/Beneficiary/Delegator.</p> <p>Last Name The surname of the Applicant/Beneficiary/Delegator.</p> <p>User ID The unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.</p>
Modified Entitlement	<p>Application The application with which the entitlement is associated.</p> <p>Name The name of the entitlement.</p> <p>Description A description of the entitlement.</p> <p>Publishing Status The Publishing Status of the entitlement. Can be Published or Unpublished.</p>

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

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

Table 119. 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 119. User Details - Details tab (continued)

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

Table 120. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement information 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 121. User Details - Accounts tab

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

Table 122. 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 123. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

The lower part of the frame shows more request attributes.

Table 124. Request attributes

Attribute	Description
Application	Type of application.
Name	Name of the entitlement.
Description	Brief description of the entitlement.
Owner	Owner of the entitlements that are 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.
Details	For a selected entitlement, click: <ul style="list-style-type: none"> • Information icon for getting the Entitlement Details. • Notes icon for reading a possible note that is specified in the previous step.


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 125. 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 finished processing a request, click the request and click **Execute** to mark the request as completed.

Account management: authorizing a request

You can authorize different types of request for the account management.

- Create Account
- Update Account
- Detailed Request

Account management: executing a request

You can execute different types of request for the account management.

- Create Account
- Update Account
- Detailed Request

Selecting users in a new request to assign entitlements and roles

Use this type of requests to assign entitlements and roles to users.


The **Users** tab is the first step of the wizard. You can search and select users with the following filters. Click the **Filter**, enter one or more values, and then click **Search**.

Table 126. User filters

Filter	Description
User Type	The type of user. For example, Administrative, Business, Employee, Training, External.
First Name/Last Name/Master UID	The name or surname or the unique identifier of the user.
Enabled	The user is enabled to receive assignments of entitlements.
Activity	The business activity that the user is involved with. After the selection of the activity, you can flag Hierarchy to search also all the activities that are defined from this point down in the hierarchical structure.

Users are listed in a table that shows a number of attributes.

Table 127. Attributes in the Users list

Attribute	Description
User Details	Click  User Details to open the User details window. This window shows several user details like external data, assigned entitlements, assigned accounts, and rights.
First Name	The name of the user
Last Name	The surname of the user
User ID	The Unique identifier of the user
User Type	The type of user. For example, Administrative, Business, Employee, Training, External.
Group [Code]	The Organization Unit [Univocal identifier of the OU] to which the user belongs

To select all the listed users, flag the check box in the attributes row. To select particular users, select the corresponding check boxes in the user rows.


Select  **Info** to display the User details window. This window shows additional information about the user in a number of tabs.

Table 128. 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 129. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement information 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 130. User Details - Accounts tab

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

Table 131. User Details - Rights


Detail	Description
Name	Name of the entitlement.

Table 131. User Details - Rights (continued)

Detail	Description
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

Table 132. 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 information 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 133. 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.

Selecting roles in a new request to assign entitlements and roles

The Catalog tab is the second step of the wizard.

In the **Catalog** page, you can choose the entitlements and roles for the users that you selected in the Users step of the wizard.

The upper part of the page summarizes 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 the following items: <ul style="list-style-type: none"> • The Risk Activities Tree (related to a specific user) in the Risk Info tab • The Activities that are involved in a specific risk, in the Mitigations tab

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

The lower part of the page shows a set of tabs:

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

Depending on the configuration of the Activity, some of these tabs might not be present.

Current Entitlements tab

The **Current Entitlements** tab lists the entitlements that are assigned to the user. You can search (click **Filter/Hide Filter** and click **Search**) a specific entitlement with the filters that are shown next:


Table 134. Current Entitlement filters.

Filter	Description
Name	Name of the Entitlement.
Family	Family of the Entitlement.
Description	Brief description of the Entitlement.

You can run the following actions on the entitlements that are listed:

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

To remove an entitlement, click **Remove**.

To enter or change the validity of an entitlement, select **Validity**. In the Date Selection window, click  **Calendar** to enter the end date, and click **OK** to confirm. The **Validity** pushbutton is highlighted in orange. To remove the end date, click **Validity**.

Next, select **Business Roles** to assign business roles, or **Next** to move to the Shopping Cart tab to process the request.


Business Roles tab

The **Business Roles** tab shows a list of available Business Roles for the selected user. Select **Filter/Hide Filter**, and click **Search**, to find specific business roles with any of the following filters:

Table 135. Business Role filters.

Filter	Description
Name	Name of the Entitlement.
Family	Family of the Entitlement.
Description	Brief description of the Entitlement.

Select **Add** to assign any of the listed business roles to the user. The **Add** pushbutton is highlighted in green.

If the added business roles have dependencies, the  **Dependencies** pushbutton is displayed. Select it to open the Dependencies window, where you can add more dependencies.

To add dependencies, select **To Cart**, which is 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.

Next, select **Application Roles** to assign applications roles, or **Next** to move to the Shopping Cart tab to process the request.

Application Roles tab

You can assign application roles to the user in the Application Roles section. Application roles are also known as IT roles.

In the **Application Roles** tab, the Applications window opens by default. Select an application from the list to display a list of application roles in the **Applications Roles** tab. Close the Applications window to exit from it.

You can also select **Filter/ Hide Filter** and use any of the following filters to search for specific application roles:

Table 136. Application Role filters.

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

Click **Add** next to the application roles that you want to assign to the user. The **Add** pushbutton is 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.

Next, select **Permissions** to assign permissions, or **Next** to move to the Shopping Cart tab to process the request.

Permissions tab

You can assign permissions to the user in the Permissions section.

In the **Permissions** tab, the Applications window opens by default. Select an application from the list to display a list of permissions in the **Permissions** tab. Close the Applications window to exit from it.

You can also select **Filter/ Hide Filter** and use any of the following filters to search for specific permissions:

Table 137. Permission filters.

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

Click **Add** next to the permissions that you want to assign to the user. The **Add** pushbutton is 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.

Select **Next** to move to the Shopping Cart tab to process the request.


Reviewing your new request to assign entitlements and roles

The **Shopping Cart** page displays a summary tree structure of the new request.


Priority declares the priority level that is assigned to this request. If the field is enabled, you can change the priority level. Select the field to display the available priority levels to which you can move the request.

The **Operation** column lists the operations that you specified in the previous page. They can be one of the following operations:

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

If you click  **Clear**, the operation is revoked and is excluded from the request.

The **Name** column lists the entitlements that are impacted by the operations.

If the entitlement is a **Permission**, it can have one or more associated  **Rights**. You can assign a **Value** to each right.

A Right is defined by two attributes: Key and Value.


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 of the following type:


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

With a single-value Right with lookup, you can choose a single value V_x from a set of several values (V_1, V_2, \dots, V_N)

With a multi-value Right with lookup, you can 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** pushbutton is available nearby. Click it to display the **Rights** window, where you can select values.








The **Application** column lists the name of the applications to which the entitlements belong.


The presence of the  **Visibility Violation** icon in the **VV** column, denotes an entitlement in Visibility Violation.

An entitlement is in **VV** when it is not associated to the **OU**, but is assigned to a single user of that **OU**. The entitlement is not available to the other users of the **OU**.

The following pushbuttons might be enabled for each entitlement. They are displayed next to the **VV** column.

Table 138. Pushbuttons and Icons in the Shopping Cart page.

Button/Icon	Description
 Notes	Opens the Notes window, where you can write remarks for the operation.
 Validity	Opens the Date Selection window, where you can enter the Start Date and the End Date of the role assignment.
Pushbuttons and Icons available only for the Admin Access Request	
 Application resources	Opens the Resource Assign window, where you can select one or more Applications for assignment.
 OU resources	Opens the Resource Assign window, where you can select one or more Organization Units for assignment.
 BRole resources	Opens the Resource Assign window, you can select one or more Business Roles for assignment.
 Risk resources	Opens the Resource Assign window, where you can select one or more Risks for assignment.
 Attribute Hierarchy resources	Opens the Resource Assign window, where you can select an Attribute Hierarchy for assignment.

The **New Start Date** and **New End Date** columns list the dates that are defined with  **Validity**.

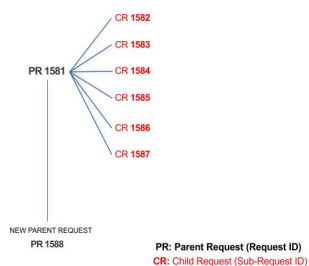
Authorizing a request to assign entitlements and roles

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 example, **Request ID 1581** generates the six **Sub-Request IDs** that range from 1582 to 1587.

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

When you are logged-in as approver, some of the request (and subrequest) listed through the REQUEST REPORT EXE might not be visible because out of the scope of the approver.

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

Table 139. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Authorizable	Request is waiting for authorization.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles.
Expired	Request exceeded the time limit that is specified by its Priority without being processed.
In execution	Request is waiting for the propagation to the target system.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in Approved status.
Partially Authorized	Request with some sub requests in Authorizable status.
Partially Completed	Request with all sub requests at end of lifecycle, some of them in Completed status and some of them in Failed Completion status.
Partially Executed	Request with some sub requests in Executed status.
Partially Terminated	Request with some sub requests in Completed status and some in progress.
Pending	Source request is waiting for formalization by one or more approvers.
Rejected	Request can no longer be processed. It is a final status for the request.
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

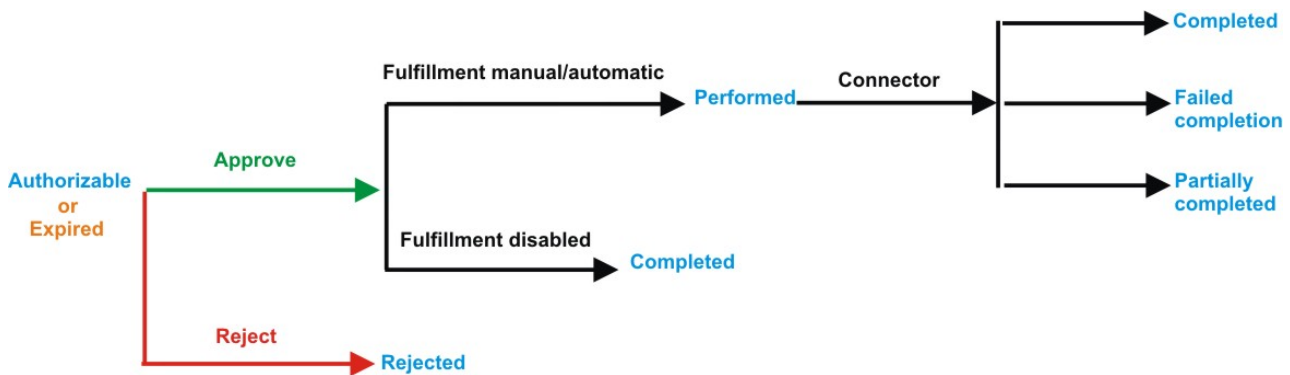


Figure 9. Subrequest status

Table 140. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization.
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Automatic, it means that the connector aligned every permission on the target system. If the fulfillment is on Manual, a human operator aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its Priority without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

You can search specific requests with the following filters. Click **Filter**, enter your data, and click **Search**.

Table 141. Filters

Filter	Description
Request ID	The 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	The identifier of the IAG actor who generated the request.
Beneficiary Identity	The identifier of the beneficiary of the request.

Table 141. Filters (continued)

Filter	Description
Type	The action that is requested.
Status	The status of the sub request.
Created between	<p>Start Date The start of a time interval when the request was submitted.</p> <p>End Date The end of a time interval when the request was submitted.</p>

Requests are displayed with the following details:

Table 142. Request details.

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 view the following information:


Table 143. 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 page shows the following information about the **Actors of the Request**:

Table 144. Details of a request - upper section

Box	Details
Request	<p>ID The unique identifier of the request.</p> <p>Type The type of the request.</p> <p>Status The status of the request.</p> <p>Priority The priority that is assigned by the applicant to the request.</p> <p>Created on The date (dd/mm/yyyy) and time (hh/mm) that the request was created.</p>
Applicant/ Beneficiary/ Delegator/	<p>Group The group of the Applicant/Beneficiary/Delegator.</p> <p>First Name The given name of the Applicant/Beneficiary/Delegator.</p> <p>Last Name The surname of the Applicant/Beneficiary/Delegator.</p> <p>User ID The unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.</p>
Modified Entitlement	<p>Application The application with which the entitlement is associated.</p> <p>Name The name of the entitlement.</p> <p>Description A description of the entitlement.</p> <p>Publishing Status The Publishing Status of the entitlement. Can be Published or Unpublished.</p>

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


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

Table 145. 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

Table 145. User Details - Details tab (continued)

Detail	Description
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 146. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement information 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 147. User Details - Accounts tab

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

Table 148. 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 149. User Details - Rights


Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.


Table 149. User Details - Rights (continued)

Detail	Description
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

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

Table 150. Request attributes

Attribute	Description
Application	Type of application.
Name	Name of the entitlement.
Description	Brief description of the entitlement.
Owner	Owner of the entitlements that are 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.
Details	For a selected entitlement, click: <ul style="list-style-type: none"> • Information icon for getting the Entitlement Details. • Notes icon for reading a possible note that is specified in the previous step.

Click the  **Info** icon to open the Entitlement information window and view the 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 in the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 151. 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 (Application 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 (Application Roles)
- External Roles
- Permissions

The following icons represent these entitlements:



If an entitlement has request notes, the  **Note** icon is available. Click it to open the Notes window and show the contents of the note.

In the center of the page, you find:

- Elements that are related with the request that needs to be authorized.
- Elements that are related to the approver of the request.

Select an option at the bottom to process the request.

Back Returns you to the list of requests without acting.

Approve

Approves the request.

Reject Rejects the request.

Redirect

Redirects the request to another approver. The Request Redirection window displays a list of candidate users. Select the user to whom you want to redirect the request for approval or rejection.

This option does not change the status of the request.

Send Back

This option is displayed only if the request was redirected to you by the original approver. You can return the request to the original approver, if you determine that you cannot approve or reject it. Write comments in the **Additional Notes** box.

This option does not change the status of the request.

Note:

A request arrives to an approver A with a certain set S of fields; the approver (according to the design of the authorization activity) might add another set S1 of information fields.

Clicking **Approve**, the request sent to the next step of the flow is made up by the fields $S \cup S1$.

Clicking **Redirect**, for sending the request to another approver AR, this last one can see only the set of fields S.

If A edit the information before the redirection, all edited information is lost.

AR might add a set of fields S2; if AR click on **Approve**, the request sent to the next step of the flow, is made up by the fields $S \cup S2$.

If the approver AR click on **Send Back**, the information that are edited by AR is lost.

The **Redirect** and **Send Back** actions are used only to switch requests among approvers, without any update to the request information.

Executing a request to assign entitlements and roles

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.

The requests that were submitted in the system are listed in one of the following statuses:

Table 152. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Authorizable	Request is waiting for authorization.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles.
Expired	Request exceeded the time limit that is specified by its Priority without being processed.
In execution	Request is waiting for the propagation to the target system.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in Approved status.
Partially Authorized	Request with some sub requests in Authorizable status.
Partially Completed	Request with all sub requests at end of lifecycle, some of them in Completed status and some of them in Failed Completion status.
Partially Executed	Request with some sub requests in Executed status.
Partially Terminated	Request with some sub requests in Completed status and some in progress.
Pending	Source request is waiting for formalization by one or more approvers.
Rejected	Request can no longer be processed. It is a final status for the request.
Terminated With Reservation	This status includes 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**, enter your data, and click **Search**.

Table 153. Filters

Filter	Description
Request ID	The 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	The identifier of the IAG actor who generated the request.
Beneficiary Identity	The identifier of the beneficiary of the request.
Type	The action that is requested.
Status	The status of the sub request.

Table 153. Filters (continued)

Filter	Description
Created between	<p>Start Date The start of a time interval when the request was submitted.</p> <p>End Date The end of a time interval when the request was submitted.</p>

Requests are displayed with the following details:

Table 154. 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 view the following information:


Table 155. 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 page shows the following information about the **Actors of the Request**:

Table 156. Details of a request - upper section

Box	Details
Request	<p>ID The unique identifier of the request.</p> <p>Type The type of the request.</p> <p>Status The status of the request.</p> <p>Priority The priority that is assigned by the applicant to the request.</p> <p>Created on The date (dd/mm/yyyy) and time (hh/mm) that the request was created.</p>
Applicant/ Beneficiary/ Delegator/	<p>Group The group of the Applicant/Beneficiary/Delegator.</p> <p>First Name The given name of the Applicant/Beneficiary/Delegator.</p> <p>Last Name The surname of the Applicant/Beneficiary/Delegator.</p> <p>User ID The unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.</p>
Modified Entitlement	<p>Application The application with which the entitlement is associated.</p> <p>Name The name of the entitlement.</p> <p>Description A description of the entitlement.</p> <p>Publishing Status The Publishing Status of the entitlement. Can be Published or Unpublished.</p>

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


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

Table 157. 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

Table 157. User Details - Details tab (continued)

Detail	Description
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 158. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement information 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 159. User Details - Accounts tab

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

Table 160. 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 161. User Details - Rights


Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.


Table 161. User Details - Rights (continued)

Detail	Description
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

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

Table 162. Request attributes

Attribute	Description
Application	Type of application.
Name	Name of the entitlement.
Description	Brief description of the entitlement.
Owner	Owner of the entitlements that are 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.
Details	For a selected entitlement, click: <ul style="list-style-type: none"> • Information icon for getting the Entitlement Details. • Notes icon for reading a possible note that is specified in the previous step.

Click the  **Info** icon to open the Entitlement information window and view 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 163. 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 (Application 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 (Application Roles)
- External Roles
- Permissions

The following icons represent these entitlements:



If an entitlement has request notes, the  **Note** icon is available. Click it to open the Notes window and show the contents of the note.

Generating a request to delegate administrative roles

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

The scope of this activity is limited to Administrative Roles. The procedure that you follow is similar to the one that you follow for delegating common roles.

The activity follows three steps:

- Select the user who delegates (Delegator)

- Select the users who are delegated (New Delegation)
- Select the administrative role to delegate (Catalog)

Authorizing a request to delegate administrative roles

You can view a summary of the requests to delegate an administrative role that were submitted. From this list, you can act on the ones that await your approval.

The scope of this activity is limited to Administrative Roles. The procedure that you follow is similar to the one that you follow for delegating common roles. See Authorizing a Delegation request.

Executing a request to delegate administrative roles

You can view a summary of the requests to delegate an administrative role that were submitted. From this list, you can operate on the ones that await your action.

The scope of this activity is limited to Administrative Roles. The procedure that you follow is similar to the one that you follow for delegating common roles. See Executing a Delegation request.

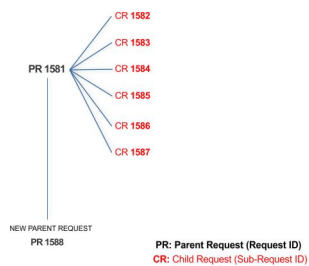
Viewing requests in your Daily Work scope

You can view a summary of generated requests that are 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 example, **Request ID 1581** generates the six **Sub-Request IDs** that range from 1582 to 1587.

You can view all the requests that are registered by the Request Report activity. When you are logged-in as approver, some of the requests and subrequests might not be visible because they are out of the scope that was defined for an approver.

The requests that were submitted are listed in their status. A request can be in one of the statuses that are described in the following table:

Table 164. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.

Table 164. Request Status (continued)

Status	Description
Authorizable	Request is waiting for authorization.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles.
Expired	Request exceeded the time limit that is specified by its Priority without being processed.
In execution	Request is waiting for the propagation to the target system.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in Approved status.
Partially Authorized	Request with some sub requests in Authorizable status.
Partially Completed	Request with all sub requests at end of lifecycle, some of them in Completed status and some of theme in Failed Completion status.
Partially Executed	Request with some sub requests in Executed status.
Partially Terminated	Request with some sub requests in Completed status and some in progress.
Pending	Source request is waiting for formalization by one or more approvers.
Rejected	Request can no longer be processed. It is a final status for the request.
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

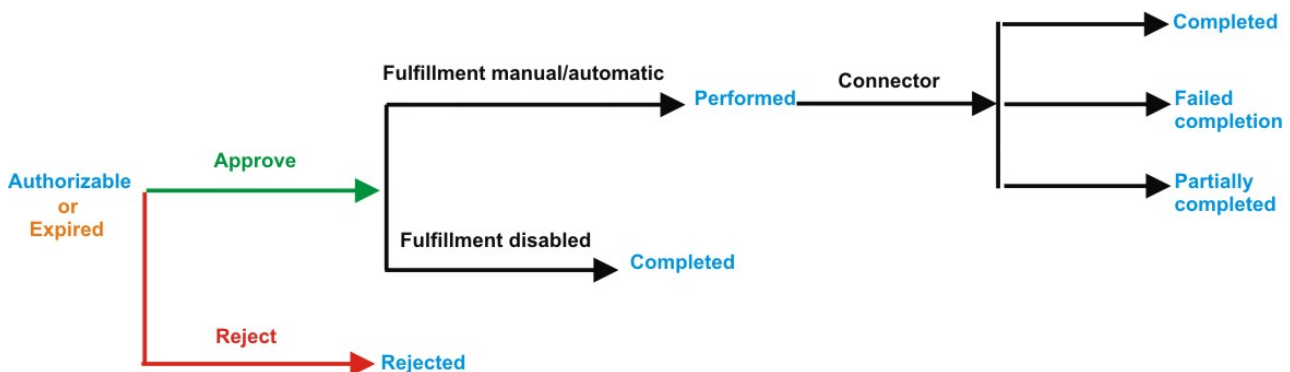


Figure 10. Subrequest status

Table 165. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization.

Table 165. Subrequest status (continued)

Status	Description
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Automatic, it means that the connector aligned every permission on the target system. If the fulfillment is on Manual, a human operator aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its Priority without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

You can search specific requests with the following filters. Click **Filter**, enter your data, and click **Search**.

Table 166. Filters

Filter	Description
Request ID	The 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	The identifier of the IAG actor who generated the request.
Beneficiary Identity	The identifier of the beneficiary of the request.
Type	The action that is requested.
Status	The status of the sub request.
Created between	<p>Start Date The start of a time interval when the request was submitted.</p> <p>End Date The end of a time interval when the request was submitted.</p>

Requests are displayed in the same page and include the following attributes:

Table 167. 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.

Table 167. Request attributes. (continued)

Attribute	Description
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 view the following information:

Table 168. 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 page shows the following information about the **Actors of the Request**:

Table 169. Details of a request - upper section

Box	Details
Request	<p>ID The unique identifier of the request.</p> <p>Type The type of the request.</p> <p>Status The status of the request.</p> <p>Priority The priority that is assigned by the applicant to the request.</p> <p>Created on The date (dd/mm/yyyy) and time (hh/mm) that the request was created.</p>

Table 169. Details of a request - upper section (continued)

Box	Details
Applicant/ Beneficiary/ Delegator/	<p>Group The group of the Applicant/Beneficiary/Delegator.</p> <p>First Name The given name of the Applicant/Beneficiary/Delegator.</p> <p>Last Name The surname of the Applicant/Beneficiary/Delegator.</p> <p>User ID The unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.</p>
Modified Entitlement	<p>Application The application with which the entitlement is associated.</p> <p>Name The name of the entitlement.</p> <p>Description A description of the entitlement.</p> <p>Publishing Status The Publishing Status of the entitlement. Can be Published or Unpublished.</p>

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


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

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	

Table 171. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement information 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 172. User Details - Accounts tab

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

Table 173. 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 174. User Details - Rights


Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.


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

Table 175. Request attributes

Attribute	Description
Application	Type of application.
Name	Name of the entitlement.
Description	Brief description of the entitlement.
Owner	Owner of the entitlements that are 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.

Table 175. Request attributes (continued)

Attribute	Description
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.
Details	For a selected entitlement, click: <ul style="list-style-type: none"> • Information icon for getting the Entitlement Details. • Notes icon for reading a possible note that is specified in the previous step.

Click the  **Info** icon to open the Entitlement information window and view the 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 in the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 176. 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 (Application 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 (Application Roles)
- External Roles
- Permissions

The following icons represent these entitlements:



If an entitlement has request notes, the  **Note** icon is available. Click it to open the Notes window and show the contents of the note.

Generating a request to delegate entitlements

You can generate a request to delegate an entitlement to a user. Then, you submit the request to the user who authorizes it.

The **Delegator** tab is the first step of the wizard, where you select the user whose entitlements must be temporarily delegated to someone else.

Note: Use the **Delegator** tab only for the complete activity of delegation (delegation of entitlements of a User A to a User B). The "personal delegation" activity, consisting in the action of delegating one's entitlements to another user, starts from the Delegate tab.

You can search and select users by clicking **Filter/Hide Filter** and then **Search**. The following filters are available:

Table 177. User filters


Filter	Description
User Type	The type of user. For example, Administrative, Business, Employee, Training, External.
First Name/Last Name/Master UID	The name or surname or the unique identifier of the user.
Enabled	The user is enabled to receive assignments of entitlements.

Table 177. User filters (continued)

Filter	Description
Activity	The business activity that the user is involved with. After the selection of the activity, you can flag Hierarchy to search also all the activities that are defined from this point down in the hierarchical structure.

The delegators are displayed with the following attributes:

Table 178. Attributes in the Users list

Attribute	Description
User Details	Click  User Details to open the User details window. This window shows several user details like external data, assigned entitlements, assigned accounts, and rights.
First Name	The name of the user
Last Name	The surname of the user
User ID	The Unique identifier of the user
User Type	The type of user. For example, Administrative, Business, Employee, Training, External.
Group [Code]	The Organization Unit [Univocal identifier of the OU] to which the user belongs

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  **Info** to display a user's Details window, which displays the following information in a set of tabs:

Table 179. 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 180. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement information 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 181. User Details - Accounts tab

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

Table 182. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

Table 183. 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  **Info** in the **Entitlement** tab to display the Entitlement information window, which displays the information summarized in the **Structure** tab:

Table 184. 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 (Application 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 (Application Roles)
- External Roles
- Permissions

The following icons represent these entitlements:



Click **Next** to display the Delegate pane.

This tab is the second step of the wizard, where you select the users for the delegator's entitlements.

Selecting delegates for a delegator's entitlements

The **Delegate** tab is the second step of the Delegation wizard.

Use the Delegate pane to select the users to whom the delegator's entitlements are to be temporarily assigned.

The upper part of the pane displays information about the delegator user or about the user who is logged in for personal delegation.

The lower part of the pane displays a list of the users from which you can select the delegates. Select **Filter** to narrow the search to specific users.

To select the entire list of users, select the check box on the attributes row, otherwise check the one in the row of a particular user.

Click **Next** to move to the Catalog pane.

This tab is the third step of the wizard, where you select the entitlements to delegate and submit the request to a user who has the authority to accept it.

Selecting entitlements in the Catalog tab

The **Catalog** tab is the third step of the wizard.

In the Catalog page, you choose the entitlements of the Delegator user that you want to delegate to the users that you selected in the Delegate step.

The upper part of the page summarizes the information about the delegator and the delegates. The section that provides the delegate information shows also the level of incompatibility that is involved in selecting the users that are listed:



The user is free of risk.



The level of risk that is attributed to the user is low.



The level of risk that is attributed to the user is medium.



The level of risk that is attributed to the user is high.

The lower part of the page includes the following tabs:

Select Roles for Delegation

A list where you select the Delegator's entitlements that you want to assign to the delegates. Click **Filter** to search for specific entitlements.

Delegated Roles

A list that includes any entitlements that the Delegator and the Delegates already share.

The page includes also:

- The **Priority** field, where you can set a priority level for the request. This field might not be enabled, based on the setup of this type of requests.
- A **Request Notes** field for optional remarks.

When you are ready to generate the request, click **Submit**. Then, click **Ok** on the confirmation window that follows. The new request is displayed in the Service Center session of the assignee of the administrative role that authorizes Delegation requests.

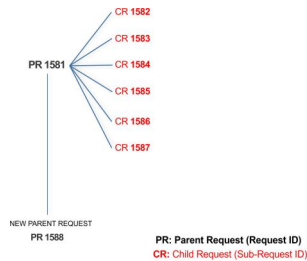
Authorizing a Delegation request

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 example, **Request ID 1581** generates the six **Sub-Request IDs** that range from 1582 to 1587.

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

When you are logged-in as approver, some of the request (and subrequest) listed through the REQUEST REPORT EXE might not be visible because out of the scope of the approver.

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

Table 185. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Authorizable	Request is waiting for authorization.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles.
Expired	Request exceeded the time limit that is specified by its Priority without being processed.
In execution	Request is waiting for the propagation to the target system.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in Approved status.
Partially Authorized	Request with some sub requests in Authorizable status.
Partially Completed	Request with all sub requests at end of lifecycle, some of them in Completed status and some of them in Failed Completion status.
Partially Executed	Request with some sub requests in Executed status.
Partially Terminated	Request with some sub requests in Completed status and some in progress.

Table 185. Request Status (continued)

Status	Description
Pending	Source request is waiting for formalization by one or more approvers.
Rejected	Request can no longer be processed. It is a final status for the request.
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

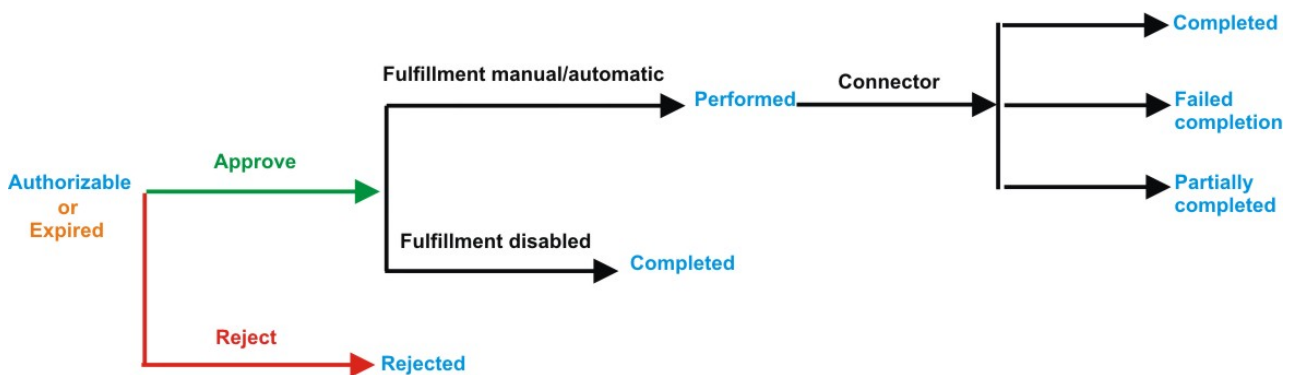


Figure 11. Subrequest status

Table 186. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization.
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Automatic, it means that the connector aligned every permission on the target system. If the fulfillment is on Manual, a human operator aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its Priority without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

You can search specific requests with the following filters. Click **Filter**, enter your data, and click **Search**.

Table 187. Filters

Filter	Description
Request ID	The 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	The identifier of the IAG actor who generated the request.
Beneficiary Identity	The identifier of the beneficiary of the request.
Type	The action that is requested.
Status	The status of the sub request.
Created between	<p>Start Date The start of a time interval when the request was submitted.</p> <p>End Date The end of a time interval when the request was submitted.</p>

Requests are displayed in the same page and include the following attributes:

Table 188. 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 hour (hh:mm) the request was created.
Status	Request Status.
Priority	The priority that is assigned to the request.

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

Table 189. 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 189. 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 page shows the following information about the **Actors of the Request**:

Table 190. Details of a request - upper section

Box	Details
Request	<p>ID The unique identifier of the request.</p> <p>Type The type of the request.</p> <p>Status The status of the request.</p> <p>Priority The priority that is assigned by the applicant to the request.</p> <p>Created on The date (dd/mm/yyyy) and time (hh/mm) that the request was created.</p>
Applicant/ Beneficiary/ Delegator/	<p>Group The group of the Applicant/Beneficiary/Delegator.</p> <p>First Name The given name of the Applicant/Beneficiary/Delegator.</p> <p>Last Name The surname of the Applicant/Beneficiary/Delegator.</p> <p>User ID The unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.</p>
Modified Entitlement	<p>Application The application with which the entitlement is associated.</p> <p>Name The name of the entitlement.</p> <p>Description A description of the entitlement.</p> <p>Publishing Status The Publishing Status of the entitlement. Can be Published or Unpublished.</p>

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


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

Table 191. 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 192. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement information 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 193. User Details - Accounts tab

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

Table 194. User Details - Activities tab

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

Table 194. User Details - Activities tab (continued)


Detail	Description
Description	Brief description of the activity

Table 195. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

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

Table 196. Request attributes

Attribute	Description
Application	Type of application.
Name	Name of the entitlement.
Description	Brief description of the entitlement.
Owner	Owner of the entitlements that are 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.
Details	For a selected entitlement, click: <ul style="list-style-type: none"> • Information icon for getting the Entitlement Details. • Notes icon for reading a possible note that is specified in the previous step.

Click the  **Info** icon to open the Entitlement information window and view the 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 in the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 197. 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 (Application 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 (Application Roles)
- External Roles
- Permissions

The following icons represent these entitlements:



If an entitlement has request notes, the  **Note** icon is available. Click it to open the Notes window and show the contents of the note.

In the center of the page, you find:

- Elements that are related with the request that needs to be authorized.
- Elements that are related to the approver of the request.

Select an option at the bottom to process the request.

Back Returns you to the list of requests without acting.

Approve
Approves the request.

Reject Rejects the request.

Redirect
Redirects the request to another approver. The Request Redirection window displays a list of candidate users. Select the user to whom you want to redirect the request for approval or rejection.

This option does not change the status of the request.

Send Back
This option is displayed only if the request was redirected to you by the original approver. You can return the request to the original approver, if you determine that you cannot approve or reject it. Write comments in the **Additional Notes** box.

This option does not change the status of the request.

Note:

A request arrives to an approver A with a certain set S of fields; the approver (according to the design of the authorization activity) might add another set S1 of information fields.

Clicking **Approve**, the request sent to the next step of the flow is made up by the fields $S \cup S1$.

Clicking **Redirect**, for sending the request to another approver AR, this last one can see only the set of fields S.

If A edit the information before the redirection, all edited information is lost.

AR might add a set of fields S2; if AR click on **Approve**, the request sent to the next step of the flow, is made up by the fields $S \cup S2$.

If the approver AR click on **Send Back**, the information that are edited by AR is lost.

The **Redirect** and **Send Back** actions are used only to switch requests among approvers, without any update to the request information.

Executing a Delegation 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 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.

The requests that were submitted are listed in their status. A request can be in one of the statuses that are described in the following table:

Table 198. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Authorizable	Request is waiting for authorization.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles.
Expired	Request exceeded the time limit that is specified by its Priority without being processed.
In execution	Request is waiting for the propagation to the target system.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in Approved status.
Partially Authorized	Request with some sub requests in Authorizable status.
Partially Completed	Request with all sub requests at end of lifecycle, some of them in Completed status and some of them in Failed Completion status.
Partially Executed	Request with some sub requests in Executed status.
Partially Terminated	Request with some sub requests in Completed status and some in progress.
Pending	Source request is waiting for formalization by one or more approvers.
Rejected	Request can no longer be processed. It is a final status for the request.
Terminated With Reservation	This status includes 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**, enter your data, and click **Search**.

Table 199. Filters

Filter	Description
Request ID	The 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	The identifier of the IAG actor who generated the request.

Table 199. Filters (continued)

Filter	Description
Beneficiary Identity	The identifier of the beneficiary of the request.
Type	The action that is requested.
Status	The status of the sub request.
Created between	<p>Start Date The start of a time interval when the request was submitted.</p> <p>End Date The end of a time interval when the request was submitted.</p>

Requests are displayed in the same page and include the following attributes:

Table 200. 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 hour (hh:mm) the request was created.
Status	Request Status.
Priority	The priority that is assigned to the request

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

Table 201. 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 201. 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 page shows the following information about the **Actors of the Request**:

Table 202. Details of a request - upper section

Box	Details
Request	<p>ID The unique identifier of the request.</p> <p>Type The type of the request.</p> <p>Status The status of the request.</p> <p>Priority The priority that is assigned by the applicant to the request.</p> <p>Created on The date (dd/mm/yyyy) and time (hh/mm) that the request was created.</p>
Applicant/ Beneficiary/ Delegator/	<p>Group The group of the Applicant/Beneficiary/Delegator.</p> <p>First Name The given name of the Applicant/Beneficiary/Delegator.</p> <p>Last Name The surname of the Applicant/Beneficiary/Delegator.</p> <p>User ID The unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.</p>
Modified Entitlement	<p>Application The application with which the entitlement is associated.</p> <p>Name The name of the entitlement.</p> <p>Description A description of the entitlement.</p> <p>Publishing Status The Publishing Status of the entitlement. Can be Published or Unpublished.</p>

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


Click the  **Info** icon to open the User details window and show the information in a set of 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 information 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 205. User Details - Accounts tab

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

Table 206. User Details - Activities tab

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

Table 206. User Details - Activities tab (continued)


Detail	Description
Description	Brief description of the activity


Table 207. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

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

Table 208. Request attributes

Attribute	Description
Application	Type of application.
Name	Name of the entitlement.
Description	Brief description of the entitlement.
Owner	Owner of the entitlements that are 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.
Details	For a selected entitlement, click: <ul style="list-style-type: none"> • Information icon for getting the Entitlement Details. • Notes icon for reading a possible note that is specified in the previous step.

Click the  **Info** icon to open the Entitlement information window and view the 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 in the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 209. 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 (Application 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 (Application Roles)
- External Roles
- Permissions

The following icons represent these entitlements:



If an entitlement has request notes, the  icon is available. Click it to open the Notes window and show the contents of the note.

Authorize escalation

When a request exceeds a defined risk acceptance level, it is escalated to a Risk Manager or similar administrative role. The Risk Manager has several options to address requests that present user risks.

The **Authorize Escalation** tab lists requests that were escalated to you because they include incompatibilities. When the system detects a risk in a generated request, the request is automatically routed from the appointed approver to the Risk Manager or similar role.

Requests that are escalated because of their inherent risk, are shown with the **Incompatibility** status in a Request Report list. A request to add roles to a beneficiary who is associated with a high level of risk is an example of a request with incompatibilities. The request must be handled by a Risk Manager.

You can search specific requests with the following filters. Click **Filter**, enter your search data in the filter fields, and click **Search**.

Table 210. Filters for requests in Incompatibility status

Filter	Description
Request ID	The Unique identifier of the request. In this list, cumulative requests are not partitioned into subrequests.
Applicant Identity	An identifier of the user who generated the request.
Beneficiary Identity	An identifier of the beneficiary of the request.
Created	<p>Start Date The start of a time interval when the request was submitted.</p> <p>End Date The end of a time interval when the request was submitted.</p>

The requests are listed with the following details:

Table 211. Request details

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
Type	Request type. One example is User Access Change.
Created on	Day (dd/mm/yyyy) and time (hh:mm) when the request was submitted
Priority	Priority that is assigned to the request

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

Table 212. 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 request details. The upper part of the page displays information about the request and its actors. The information boxes that are displayed are based on the type of request.

Table 213. Request and request actor details






Actor	Detail	Description
Request	Request ID	Univocal identifier of the Request
	Status	The request status is displayed as Escalation
	Priority	The priority that is assigned to the request. It can be High, Medium, Low, or Unassigned.
	Created on	Date (dd/mm/yyyy) and time (hh:mm) when the request was submitted
	Type	Type of request. For example, User Access Change.
	Risk Status	<p>The risk status of the request. The level of risk is indicated by one of the following colored dots:</p> <p> Low</p> <p> Medium</p> <p> High</p> <p>Click the colored dot to open a window that displays the following items:</p> <ul style="list-style-type: none"> • The Risk Activities Tree (related to a specific user) in the Risk Info tab • The Activities that are involved in a specific risk, in the Mitigations tab <p>For information on the Service Center mitigation configuration user interface, see How to read the tree of the risks of a user.</p>

Table 213. Request and request actor details (continued)

Actor	Detail	Description
Applicant/ Beneficiary/ Delegator	Group	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  Info to view user details and the entitlements, accounts, business activities, and rights that are assigned to the user.
Inserted Entitlement/ Modified Entitlement	Application	The name of the application to which the entitlement belongs
	Name	The name of the inserted or modified entitlement. Click  Info to open a window with complete information about the entitlement.
	Description	A short description of the entitlement
	Publishing Status	Indicates whether the entitlement is published or not. If the entitlement is published, it can be assigned to users.

The **Additional Notes** box at center page might contain applicant notes about the request.

For requests that deal with accessing or delegating entitlements and roles, the lower left part of the page lists the following information for each of the requested items:

Table 214. Request attributes





Attribute	Description
Application	The name of the application that comprises the entitlement. Click  Info to display details.
Name	The name and type of the entitlement
Description	A short description of the entitlement
Owner	The owner of the entitlement
Start Date	The starting date that the entitlement is assigned to the user
End Date	The ending date that the entitlement is assigned to the user

Table 214. Request attributes (continued)

Attribute	Description
VV	The Visibility Violation status of the entitlement. The  icon denotes an entitlement in Role Alignment Violation
	Click this icon to display the Entitlement information window, where the following tabs provide more information: <ul style="list-style-type: none"> • Structure • Dependencies • Activity • Rights Structure is always available. It shows the structure of the entitlement. The other tabs are available only when the entitlement is characterized by Dependencies , Activities , or Rights .
	Displays a box that might contain more applicant notes.

The lower right part of the page shows information about the mitigations that are assigned to the user by you as the Risk Manager. **Control Name** is the name of the mitigation; **Description** is short description of the mitigation.

Select one of the following actions:

Back Returns to the list of risk-generating requests.

Approve
Approves the request.

Reject Rejects the request.

Mitigate
Displays the Risk tree. You can also assign the appropriate mitigation to the risk.

After you assigned the appropriate mitigation to the user risk, you can view it in the lower right part of the frame.

Note: This option is available only in requests that deal with user access to entitlements.

Insert/Update entitlement: generating a request

Use this workflow to create or update roles and entitlements. The process takes the form of a request that must be approved by an authorized user.

- Insert Entitlement
- Update Entitlement

Insert entitlements: generating a request

Use this workflow to create roles and entitlements and to submit the requests for their approval.

Role Mining is the initial page. It contains the following tabs:

Role Mining
Use it to discover roles

Data Exploration







Use it to collect information on the current status of User-Entitlements associations

Select one of the two tabs. If you select **Data Exploration** first, you are then lead to select the **Role Mining** tab.

In the Role Mining page, the rows list role mining analyses from where you can select roles or entitlements in a following step.

Select **Filter** and enter any of the search data that is described in the following table. Then, click **Search** to find specific analyses.

Table 215. 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 rows that are displayed in this page represent completed analyses. Analysis attributes are described in the next table.

Table 216. Role Mining and Data Exploration analyses attributes

Attribute	Description
Code	A progressive code number that is automatically attached to the analysis request.

Table 216. Role Mining and Data Exploration analyses attributes (continued)





Attribute	Description
 (Details)	<p>Available for Data Exploration analyses only.</p> <p>Click to display the Partitions pane that shows the partitions generated during the analysis. The partitions are listed by the following attributes:</p> <p>Name Indicates by which column the data was aggregated to run the analysis.</p> <p>Minability Minability value. The value, ranging from 0 to 100, provides an index of how readily assignments can be aggregated into roles.</p> <p>Subsets Entities of the partition.</p> <p>Status One of the following request statuses:</p> <ul style="list-style-type: none"> •  : Complete •  : Error •  : Warning

Table 216. Role Mining and Data Exploration analyses attributes (continued)











Attribute	Description
 (Info)	<p>Click the icon to view information on the analysis.</p> <p>For Role Mining TheInfo window contains two tabs:</p> <p>Details Information boxes show:</p> <ul style="list-style-type: none"> • Historical data about the analysis • Data filters that were selected for the analysis • The options that were selected to run the analysis • Results and statistics of the analysis <p>Map Maps entitlements and users. The black squares indicate entitlements that are assigned to users. The Exceptions and Missing dynamic filters enable you to arrange the assignments to optimize the mapped roles.</p> <p>The Actions tab enables you to run the following actions:</p> <p>New Role Map Request the computation of a new role map with the changes that you make on the current map and other specifications that you might enter.</p> <p>Reshuffle Select this option to re-position the assignments in the map after you used the Remove or Fill Up options. The map is automatically re-arranged to suggest the best role configurations.</p> <p>Select area Use this option to highlight the area that is included between a cell that you selected before and the cell that you will select next. You can then use the</p>

Table 216. Role Mining and Data Exploration analyses attributes (continued)

Attribute	Description
Name	Corresponds to the value that was entered in the Analysis Description field when the analysis was run.
Status	The status of the request can be: <ul style="list-style-type: none">  : Complete  : In progress  : Error  : Warning  : Deleting
Direct	Indicates that the only direct assignments option was specified for the request.
Organizatou Unit	The name of the organization unit on which the analysis was run.
Application	The name of the application on which the analysis was run.
Entitlement Type	The type of the entitlement that was selected for the analysis. The entitlement can be one of the following: <ul style="list-style-type: none">  : Permission  : IT role  : Business role  : External role

You can select **Actions** to run the following options:

Add To define another role mining analysis

Remove

To delete a selected role mining analysis

Follow these steps to create a role after you select one of the analyses in the list:

1. Click **Next** to access the next wizard step in the **Candidate Roles** pane.

The left frame displays the following tabs:

- Roles
- Entitlements
- Users
- Statistics tab

The selection of one of these tabs displays another set of tabs in the right frame. The tabs display more details about the roles, entitlements, and users involved in the analysis.




You must select a candidate role from the list in Roles before you proceed to the next step.

2. Click **Next** to move 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 move 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.
In this pane, **Priority** declares the priority level that is assigned to this request. If the field is enabled, you can change the priority level. Select the field to display the available priority levels to which you can move the request.

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 217. 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.
Entitlement Coverage	This filter can assume three distinct values: <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 218. User details.

User	
Attribute	Description
Last Name	Indicates the User's last name
Name	Indicates the User's name

Table 218. User details. (continued)

User	
Attribute	Description
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
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.

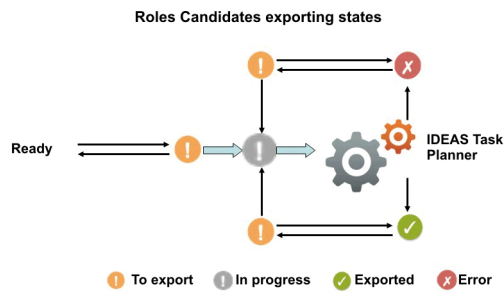


Figure 12. Possible states of candidate roles.

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 219. 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.

Table 219. Entitlement details. (continued)

Detail	Description
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 220. 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.

Table 220. Entitlement filters (continued)

Attribute	Description
User Coverage	<p>This filter can assume three different values:</p> <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 221. 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.
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.

Table 221. Entitlement details (continued)

Attribute	Description
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 **Entitlements** tab.

For each candidate role, the data set in the table below is displayed:

Table 222. 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.
Applications	Indicates the number of applications for the selected candidate role.



Table 222. Candidate Role attributes (continued)

Attribute	Description
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 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 223. 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 224. 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.
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 225. 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:

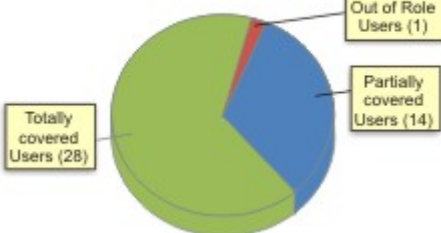
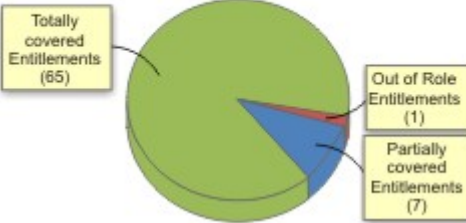
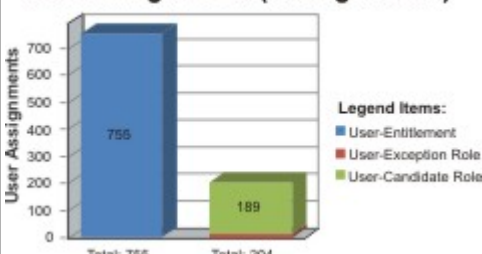
- Analysis Statistics
- Role Statistics

Analysis Statistics

Table 226. Dashboard set.

Dashboard	Description
<p>Total Roles (37)</p> <p>The dashboard displays a pie chart titled 'Total Roles (37)'. The chart is divided into two segments: a large green segment representing 'Candidate Roles (29)' and a smaller red segment representing 'Exception Roles (8)'. Callout boxes with leader lines point to each segment.</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.

Table 226. Dashboard set. (continued)

Dashboard	Description
<p>Analyzed Users (43)</p>  <p>Totally covered Users (28) Partially covered Users (14) Out of Role Users (1)</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>Analyzed Entitlements (73)</p>  <p>Totally covered Entitlements (65) Partially covered Entitlements (7) Out of Role Entitlements (1)</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>User Assignments (Saving 72.98%)</p>  <p>Legend Items: ■ User-Entitlement ■ User-Exception Role ■ User-Candidate Role</p> <p>Total: 755 Total: 204</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 227. 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

Table 227. Role statistics filters. (continued)

Filter	Description
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 13. Example of Statistics with User and Entitlements check boxes selected.


Generating a request to update an entitlement

Create a request to update an entitlement.

As you select the tab that starts the wizard for generating the request, a list of the existing entitlements is displayed.

You can select **Filter** to search for a specific entitlement. Complete one or more of the following fields to narrow your search.

Table 228. Filters that you can use to search for entitlements.

Filter	Description
Application	The name of the parent application. Select  to display a list and select an application
Name or Code	The name or the univocal identifier of the entitlement
Type	Select one of the following entitlement types: <ul style="list-style-type: none"> • Permission • IT Role • Business Role • External Role
Description	A brief description of the entitlement
Group	The name of the organizational unit with which the entitlement is associated

The entitlements that are available are listed with the following attributes under the **Entitlements** tab:

Table 229. Entitlement attributes in an Update Entitlement request generation.









Attribute	Description
Publishing Status	If the entitlement is in Publish status, it can be associated with organizational units. If it is in Not Publish status, it cannot be associated.
Application	The name of the parent application
Entitlement information icon	Select the icon to display the Entitlement information window. This window displays more entitlement information such as: <ul style="list-style-type: none"> • Extra details • Structure • The permissions that make up the entitlement • A list of the entitled users • The organizational units with which the entitlement is associated
Name	The name of the entitlement and the icon that identifies the entitlement type. <ul style="list-style-type: none"> •  Permission •  IT role •  Business role •  External role
Description	A brief description of the entitlement
Owner	The owner of the entitlement

Table 229. Entitlement attributes in an Update Entitlement request generation. (continued)

Attribute	Description
Start Date	The starting date of the entitlement validity period
End Date	The ending date of the entitlement validity period
VV	<p>The  icon denotes an entitlement in Role Alignment Violation.</p> <p>An entitlement is in VV when it is not associated to an OU but to a specific user of that OU. The entitlement is not available to the other users of the OU.</p>
Risk Status	<p>The risk status of the entitlement is indicated graphically.</p> <p> The risk level is low.</p> <p> The risk level is medium.</p> <p> The risk level is high.</p>

Select an entitlement and click **Next** to display the Entitlement Details page. The page includes two accordion panes where you can modify the entitlement. The changes are the object of the request generation process.

Details

You can update the following fields:

- Publishing Status
- Owner
- Name
- Code
- Description
- Expiration

Entitlement Properties

You can change the values of the keys that are listed.

Click **Next** again and you move to the Entitlement Designer page. The page shows the current structure of the entitlement in terms of other entitlements (permissions) that the entitlement comprises. The entitlement details and information show the changes that you made in the previous page. Any permissions that the entitlement comprises are listed under the **Current Structure** tab. Click **Remove** to take a permission off the entitlement structure.

Select **Available Entitlements** to display a list of permissions that you can add to the entitlement. Click **Add** next to the permissions that you choose.

Before you click **Next**, you can click **Analysis** to view the Impact Analysis window. This window shows if conflicts exist in the new structure of the entitlement.

Click **Next** to view a Summary page that displays the following items:

- The entitlement with the updates that you are about to request.
- The **Priority** field, where you can set a priority level for the request. This field might not be enabled, based on the setup of this type of requests.
- A **Request Notes** field for optional remarks.

When you are ready to generate the request, click **Submit**. Then, click **Ok** on the confirmation window that follows. The new request is displayed in the Service Center session of the assignee of the administrative role that authorizes Entitlement Update requests.

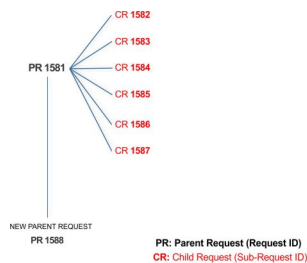
Insert/Update entitlement: processing a request

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 that are registered through the REQUEST REPORT EXE activity.

When you are logged-in as approver, some of the request (and subrequest) listed through the REQUEST REPORT EXE might not be visible because out of the scope of the approver.

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

Table 230. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Authorizable	Request is waiting for authorization.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles.

Table 230. Request Status (continued)

Status	Description
Expired	Request exceeded the time limit that is specified by its Priority without being processed.
In execution	Request is waiting for the propagation to the target system.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in Approved status.
Partially Authorized	Request with some sub requests in Authorizable status.
Partially Completed	Request with all sub requests at end of lifecycle, some of them in Completed status and some of them in Failed Completion status.
Partially Executed	Request with some sub requests in Executed status.
Partially Terminated	Request with some sub requests in Completed status and some in progress.
Pending	Source request is waiting for formalization by one or more approvers.
Rejected	Request can no longer be processed. It is a final status for the request.
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

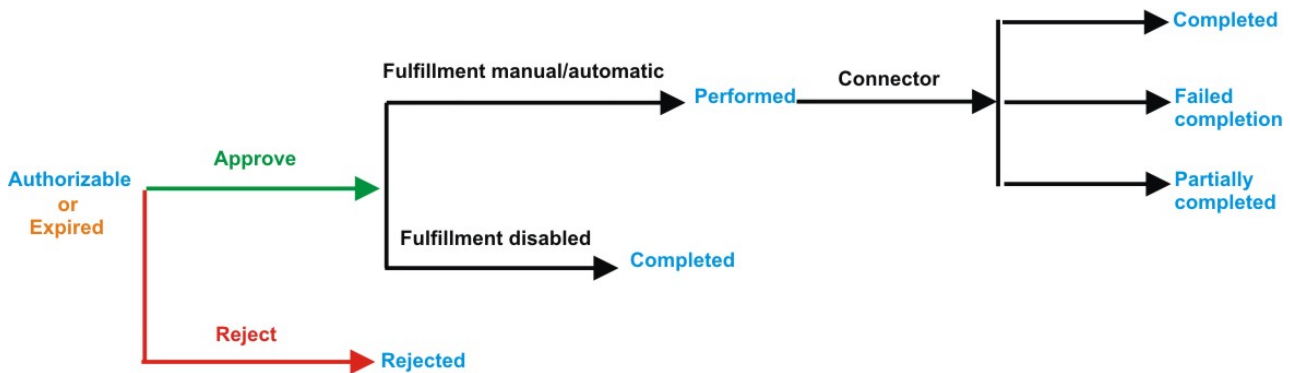


Figure 14. Subrequest status

Table 231. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization.
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Automatic, it means that the connector aligned every permission on the target system. If the fulfillment is on Manual, a human operator aligned every permission on the target system.

Table 231. Subrequest status (continued)

Status	Description
Expired	The request exceeded the time limit that is specified by its Priority without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

You can search specific requests with the following filters.

Click **Filter/Hide Filter** and then click **Search**.

Table 232. Filters

Filter	Description
Request ID	The 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	The identifier of the IAG actor who generated the request.
Beneficiary Identity	The identifier of the beneficiary of the request.
Type	The action that is requested.
Status	The status of the sub request.
Created between	<p>Start Date The start of a time interval when the request was submitted.</p> <p>End Date The end of a time interval when the request was submitted.</p>

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.

Requests attributes	
Attribute	Description
Created on	Date (dd/mm/yyyy) and hour (hh:mm) the request was created.
Status	The status of the subrequests (Sub-Request ID column).
Priority	The priority that is assigned to the request

Click an item under **Applicant** or **Beneficiary** to open the related User details window and show the following information:

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).
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 234. Details of a request - upper section

Box	Details
Request	<p>ID The unique identifier of the request.</p> <p>Type The type of the request.</p> <p>Status The status of the request.</p> <p>Priority The priority that is assigned by the applicant to the request.</p> <p>Created on The date (dd/mm/yyyy) and time (hh/mm) that the request was created.</p>

Table 234. Details of a request - upper section (continued)

Box	Details
Applicant/ Beneficiary/ Delegator/	<p>Group The group of the Applicant/Beneficiary/Delegator.</p> <p>First Name The given name of the Applicant/Beneficiary/Delegator.</p> <p>Last Name The surname of the Applicant/Beneficiary/Delegator.</p> <p>User ID The unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.</p>
Modified Entitlement	<p>Application The application with which the entitlement is associated.</p> <p>Name The name of the entitlement.</p> <p>Description A description of the entitlement.</p> <p>Publishing Status The Publishing Status of the entitlement. Can be Published or Unpublished.</p>

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 subset of fields that are 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 subset of fields that are 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 235. 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

Table 235. User Details - Details tab (continued)

Detail	Description
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 236. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement information 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 237. User Details - Accounts tab

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

Table 238. 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 239. User Details - Rights


Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.


Table 239. User Details - Rights (continued)

Detail	Description
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

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

Table 240. Request attributes

Attribute	Description
Application	Type of application.
Name	Name of the entitlement.
Description	Brief description of the entitlement.
Owner	Owner of the entitlements that are 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.
Details	For a selected entitlement, click: <ul style="list-style-type: none"> • Information icon for getting the Entitlement Details. • Notes icon for reading a possible note that is specified in the previous step.

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 241. 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 (Application 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 (Application 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 that are related to the request to be authorized.
- Elements that are related to the approver of the request.

Select an option at the bottom to process the request.

Back Returns you to the list of requests without acting.

Approve

Approves the request.

Reject Rejects the request.

Redirect

Redirects the request to another approver. The Request Redirection window displays a list of candidate users. Select the user to whom you want to redirect the request for approval or rejection.

This option does not change the status of the request.

Send Back

This option is displayed only if the request was redirected to you by the original approver. You can return the request to the original approver, if you determine that you cannot approve or reject it. Write comments in the **Additional Notes** box.

This option does not change the status of the request.

Note:

A request arrives to an approver A with a certain set S of fields; the approver (according to the design of the authorization activity) might add another set S1 of information fields.

Clicking **Approve**, the request sent to the next step of the flow is made up by the fields $S \cup S1$.

Clicking **Redirect**, for sending the request to another approver AR, this last one can see only the set of fields S.

If A edit the information before the redirection, all edited information is lost.

AR might add a set of fields S2; if AR click on **Approve**, the request sent to the next step of the flow, is made up by the fields $S \cup S2$.

If the approver AR click on **Send Back**, the information that are edited by AR is lost.

The **Redirect** and **Send Back** actions are used only to switch requests among approvers, without any update to the request information.

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 242. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Authorizable	Request is waiting for authorization.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles.
Expired	Request exceeded the time limit that is specified by its Priority without being processed.
In execution	Request is waiting for the propagation to the target system.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in Approved status.
Partially Authorized	Request with some sub requests in Authorizable status.
Partially Completed	Request with all sub requests at end of lifecycle, some of them in Completed status and some of them in Failed Completion status.
Partially Executed	Request with some sub requests in Executed status.
Partially Terminated	Request with some sub requests in Completed status and some in progress.
Pending	Source request is waiting for formalization by one or more approvers.
Rejected	Request can no longer be processed. It is a final status for the request.
Terminated With Reservation	This status includes 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 243. Filters

Filter	Description
Request ID	The 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	The identifier of the IAG actor who generated the request.
Beneficiary Identity	The identifier of the beneficiary of the request.
Type	The action that is requested.
Status	The status of the sub request.

Table 243. Filters (continued)

Filter	Description
Created between	<p>Start Date The start of a time interval when the request was submitted.</p> <p>End Date The end of a time interval when the request was submitted.</p>

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.
Priority	The priority assigned to the request

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


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	

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 245. Details of a request - upper section

Box	Details
Request	<p>ID The unique identifier of the request.</p> <p>Type The type of the request.</p> <p>Status The status of the request.</p> <p>Priority The priority that is assigned by the applicant to the request.</p> <p>Created on The date (dd/mm/yyyy) and time (hh/mm) that the request was created.</p>
Applicant/ Beneficiary/ Delegator/	<p>Group The group of the Applicant/Beneficiary/Delegator.</p> <p>First Name The given name of the Applicant/Beneficiary/Delegator.</p> <p>Last Name The surname of the Applicant/Beneficiary/Delegator.</p> <p>User ID The unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.</p>
Modified Entitlement	<p>Application The application with which the entitlement is associated.</p> <p>Name The name of the entitlement.</p> <p>Description A description of the entitlement.</p> <p>Publishing Status The Publishing Status of the entitlement. Can be Published or Unpublished.</p>

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 246. 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

Table 246. User Details - Details tab (continued)

Detail	Description
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 247. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement information 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 248. User Details - Accounts tab

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

Table 249. 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 250. User Details - Rights


Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.

Table 250. User Details - Rights (continued)

Detail	Description
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

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

Table 251. Request attributes

Attribute	Description
Application	Type of application.
Name	Name of the entitlement.
Description	Brief description of the entitlement.
Owner	Owner of the entitlements that are 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.
Details	For a selected entitlement, click: <ul style="list-style-type: none"> • Information icon for getting the Entitlement Details. • Notes icon for reading a possible note that is specified in the previous step.

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 252. 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 (Application 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 (Application 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.

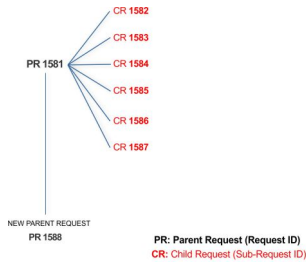
Viewing the requests present in the system

You can view a summary of the generated requests and click a **Request ID** or **Sub-Request ID** to browse the details.

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 IDs**, 1582 - 1587.

You can view all the requests that are registered by the Request Report activity.

Even if you are logged-in as the authorizer, some of the requests and subrequests might not be visible because they are outside the scope that is defined for the authorizer.

The requests that are generated during the authorization process are characterized by a status. The status can be one of the statuses that are summarized in the following table.

Table 253. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Authorizable	Request is waiting for authorization.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles.
Expired	Request exceeded the time limit that is specified by its Priority without being processed.
In execution	Request is waiting for the propagation to the target system.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in Approved status.
Partially Authorized	Request with some sub requests in Authorizable status.
Partially Completed	Request with all sub requests at end of lifecycle, some of them in Completed status and some of them in Failed Completion status.
Partially Executed	Request with some sub requests in Executed status.
Partially Terminated	Request with some sub requests in Completed status and some in progress.
Pending	Source request is waiting for formalization by one or more approvers.
Rejected	Request can no longer be processed. It is a final status for the request.

Table 253. Request Status (continued)

Status	Description
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

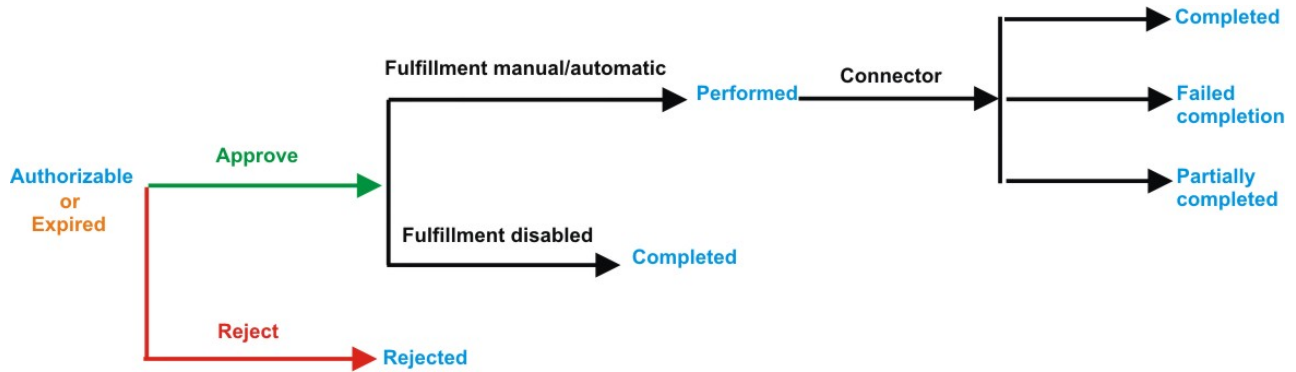


Figure 15. Subrequest status

Table 254. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization.
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Automatic, it means that the connector aligned every permission on the target system. If the fulfillment is on Manual, a human operator aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its Priority without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

You can use filters to search for specific requests. Select **Filter**, enter your search parameters, and click **Search**.

Table 255. Filters

Filter	Description
Request ID	The Unique identifier of the request.

Table 255. Filters (continued)

Filter	Description
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity	The identifier of the IAG actor who generated the request.
Beneficiary Identity	The identifier of the beneficiary of the request.
Type	The action that is requested.
Status	The status of the sub request.
Created between	<p>Start Date The start of a time interval when the request was submitted.</p> <p>End Date The end of a time interval when the request was submitted.</p>

The results are displayed in the same frame. The request attributes shown in each row are listed in the next table.

Table 256. Request attributes

Attribute	Description
Request ID	The univocal identifier of the parent request
Sub-Request ID	The univocal identifier of the child request
Type	The type of the request
Applicant	The name of the applicant of the request
Beneficiary	The name of the beneficiary of the request
Escalation	Specifies whether the request was escalated
Created on	The date (dd/mm/yyyy) and time (hh:mm) that the request was created.
Status	The status of the subrequest
Priority	The priority that is assigned to the request
Notes	Click the icon to display comments that were added by the applicant in the request

In every row, you can select the **Applicant** and **Beneficiary** of a request to open the User details window and view their user information.

Table 257. 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

Table 257. User Details - Details tab (continued)

Detail	Description
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	

You can click **Request ID** and **Sub-Request ID** to view the details of the request and of the subrequest.

The upper part of the frame shows information about the request and about its applicant. Depending on the type of request, other information is displayed.

Table 258. Details of a request - upper section


Box	Details
Request	<p>ID The unique identifier of the request.</p> <p>Type The type of the request.</p> <p>Status The status of the request.</p> <p>Priority The priority that is assigned by the applicant to the request.</p> <p>Created on The date (dd/mm/yyyy) and time (hh/mm) that the request was created.</p>
Applicant/ Beneficiary/ Delegator/	<p>Group The group of the Applicant/Beneficiary/Delegator.</p> <p>First Name The given name of the Applicant/Beneficiary/Delegator.</p> <p>Last Name The surname of the Applicant/Beneficiary/Delegator.</p> <p>User ID The unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.</p>

Table 258. Details of a request - upper section (continued)

Box	Details
Modified Entitlement	<p>Application The application with which the entitlement is associated.</p> <p>Name The name of the entitlement.</p> <p>Description A description of the entitlement.</p> <p>Publishing Status The Publishing Status of the entitlement. Can be Published or Unpublished.</p>

You can click the available  **Info** icons to view further details about an item.

The **Request Notes** occupy the middle section of the frame. 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.

The lower part of the frame shows more information on the request. The contents depend on the request type. If the request concerns a user, an entitlement, or an account, this part of the frame displays details about these items.

When you finished viewing the request details, select **Back** to return to the list of requests.

Viewing expired requests that require to be approved or rejected

You can view a summary of requests that passed their expiration time and that await your approval or rejection. Select a **Request ID** or **Sub-Request ID** to browse the details.

Every request in this list was generated with a priority that defines an expiration time. An Escalation action was also defined if the request was not processed within this time.

The requests that are in this list reached their expiration time without being processed and await your intervention.

You can use filters to search for specific requests. Select **Filter**, enter your search parameters, and click **Search**.

Table 259. Filters that you can use to search for specific requests

Filter	Description
Request ID	The 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	The identifier of the IAG actor who generated the request
Beneficiary Identity	The identifier of the beneficiary of the request

Table 259. Filters that you can use to search for specific requests (continued)

Filter	Description
Created between	<p>Start Date The start of a time interval when the request was submitted.</p> <p>End Date The end of a time interval when the request was submitted.</p>

The expired requests that await your intervention are listed with the attributes that are shown in the following table.

Table 260. Request attributes

Attribute	Description
Request ID	The univocal identifier of the parent request
Sub-Request ID	The univocal identifier of the child request
Type	The type of the request
Applicant	The name of the applicant of the request
Beneficiary	The name of the beneficiary of the request
Created on	The date (dd/mm/yyyy) and time (hh:mm) that the request was created.
Status	The status of the subrequest. In this context, it is always Expired.
Priority	The priority that is assigned to the request

In every row, you can select the **Applicant** and **Beneficiary** of the request to open the User details window and view detailed user information.


You can click **Request ID** and **Sub-Request ID** to view the details of the request and of the subrequest.


The upper part of the frame shows information about the request and about its applicant. Depending on the type of request, other information is displayed.

Table 261. Details of a request - upper section

Box	Details
Request	<p>ID The unique identifier of the request.</p> <p>Type The type of the request.</p> <p>Status The status of the request.</p> <p>Priority The priority that is assigned by the applicant to the request.</p> <p>Created on The date (dd/mm/yyyy) and time (hh/mm) that the request was created.</p>

Table 261. Details of a request - upper section (continued)

Box	Details
Applicant/ Beneficiary/ Delegator/	Group The group of the Applicant/Beneficiary/Delegator. First Name The given name of the Applicant/Beneficiary/Delegator. Last Name The surname of the Applicant/Beneficiary/Delegator. User ID The unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.
Modified Entitlement	Application The application with which the entitlement is associated. Name The name of the entitlement. Description A description of the entitlement. Publishing Status The Publishing Status of the entitlement. Can be Published or Unpublished.

You can click the available  **Info** icons to view further details about an item.

The **Request Notes** and **Additional Notes** boxes occupy the middle section of the frame. These notes can be specified by the author of the request or by a rule. In these fields, you can add free text for any reason during the authorization or execution of the request.

The lower part of the frame shows more information on the request. The contents depend on the request type. If the request concerns a user, an entitlement, or an account, this part of the frame displays details about these items.

Select an option at the bottom to process the request.

Back Returns you to the list of requests without acting.

Approve
Approves the request.

Reject Rejects the request.

Create/Update user: generating a request

You can insert a new user or update information for a registered user.

- Create User
- Update User

Create 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**.

Priority declares the priority level that is assigned to this request. If the field is enabled, you can change the priority level. Select the field to display the available priority levels to which you can move the 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**.

Priority declares the priority level that is assigned to this request. If the field is enabled, you can change the priority level. Select the field to display the available priority levels to which you can move the 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.

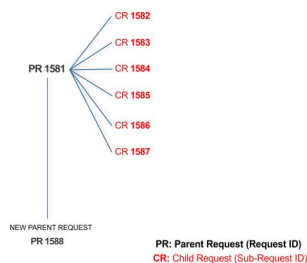
Insert/Update user: processing a request

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 that are registered through the REQUEST REPORT EXE activity.

When you are logged-in as approver, some of the request (and subrequest) listed through the REQUEST REPORT EXE might not be visible because out of the scope of the approver.

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

Table 262. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed.
Authorizable	Request is waiting for authorization.
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles.
Expired	Request exceeded the time limit that is specified by its Priority without being processed.
In execution	Request is waiting for the propagation to the target system.
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in Approved status.
Partially Authorized	Request with some sub requests in Authorizable status.
Partially Completed	Request with all sub requests at end of lifecycle, some of them in Completed status and some of them in Failed Completion status.
Partially Executed	Request with some sub requests in Executed status.
Partially Terminated	Request with some sub requests in Completed status and some in progress.

Table 262. Request Status (continued)

Status	Description
Pending	Source request is waiting for formalization by one or more approvers.
Rejected	Request can no longer be processed. It is a final status for the request.
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

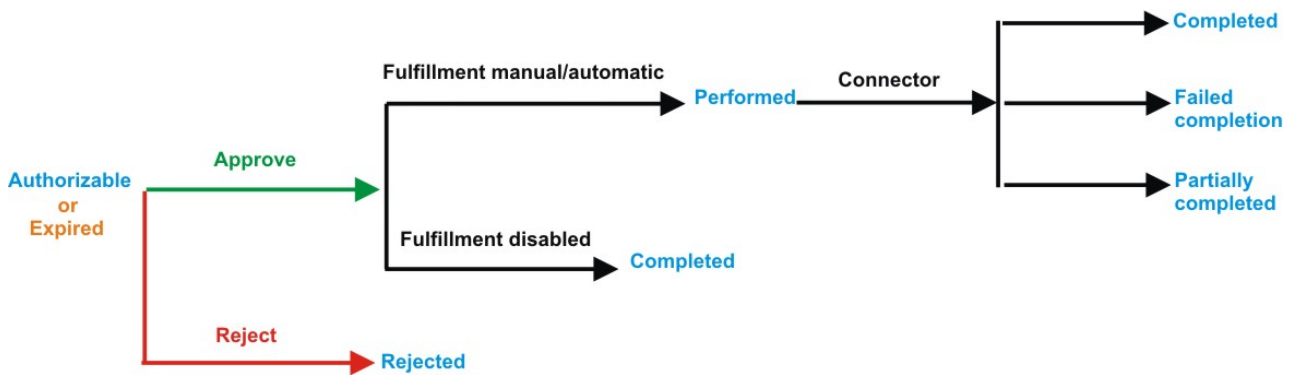


Figure 16. Subrequest status

Table 263. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization.
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Automatic, it means that the connector aligned every permission on the target system. If the fulfillment is on Manual, a human operator aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its Priority without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles.
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

You can search specific requests with the following filters.

Click **Filter/Hide Filter** and then click **Search**.

Table 264. Filters

Filter	Description
Request ID	The 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	The identifier of the IAG actor who generated the request.
Beneficiary Identity	The identifier of the beneficiary of the request.
Type	The action that is requested.
Status	The status of the sub request.
Created between	<p>Start Date The start of a time interval when the request was submitted.</p> <p>End Date The end of a time interval when the request was submitted.</p>

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

Table 265. 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 subrequests (Sub-Request ID column).
Priority	The priority that is assigned to the request

Click an item under **Applicant** or **Beneficiary** to open the related User details window and show the following information:

Table 266. 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

Table 266. User Details - Details tab (continued)

Detail	Description
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 267. Details of a request - upper section


Box	Details
Request	<p>ID The unique identifier of the request.</p> <p>Type The type of the request.</p> <p>Status The status of the request.</p> <p>Priority The priority that is assigned by the applicant to the request.</p> <p>Created on The date (dd/mm/yyyy) and time (hh/mm) that the request was created.</p>
Applicant/ Beneficiary/ Delegator/	<p>Group The group of the Applicant/Beneficiary/Delegator.</p> <p>First Name The given name of the Applicant/Beneficiary/Delegator.</p> <p>Last Name The surname of the Applicant/Beneficiary/Delegator.</p> <p>User ID The unique identifier of the Applicant/Beneficiary/Delegator. Click  Info to view the user details.</p>

Table 267. Details of a request - upper section (continued)

Box	Details
Modified Entitlement	<p>Application The application with which the entitlement is associated.</p> <p>Name The name of the entitlement.</p> <p>Description A description of the entitlement.</p> <p>Publishing Status The Publishing Status of the entitlement. Can be Published or Unpublished.</p>

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 subset of fields that are 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 subset of fields that are 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 268. 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 268. User Details - Details tab (continued)

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

Table 269. User Details - Entitlements tab



Details	Description
	Click Info to open the Entitlement information 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 270. User Details - Accounts tab

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

Table 271. 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 272. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

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

Table 273. Request attributes

Attribute	Description
Application	Type of application.
Name	Name of the entitlement.
Description	Brief description of the entitlement.
Owner	Owner of the entitlements that are 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.
Details	For a selected entitlement, click: <ul style="list-style-type: none"> • Information icon for getting the Entitlement Details. • Notes icon for reading a possible note that is specified in the previous step.

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 274. 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 (Application 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 (Application 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 that are related to the request to be authorized.
- Elements that are related to the approver of the request.

Select an option at the bottom to process the request.

Back Returns you to the list of requests without acting.

Approve

Approves the request.

Reject Rejects the request.

Redirect

Redirects the request to another approver. The Request Redirection window displays a list of candidate users. Select the user to whom you want to redirect the request for approval or rejection.

This option does not change the status of the request.

Send Back

This option is displayed only if the request was redirected to you by the original approver. You can return the request to the original approver, if you determine that you cannot approve or reject it. Write comments in the **Additional Notes** box.

This option does not change the status of the request.

Note:

A request arrives to an approver A with a certain set S of fields; the approver (according to the design of the authorization activity) might add another set S1 of information fields.

Clicking **Approve**, the request sent to the next step of the flow is made up by the fields $S \cup S1$.

Clicking **Redirect**, for sending the request to another approver AR, this last one can see only the set of fields S.

If A edit the information before the redirection, all edited information is lost.

AR might add a set of fields S2; if AR click on **Approve**, the request sent to the next step of the flow, is made up by the fields $S \cup S2$.

If the approver AR click on **Send Back**, the information that are edited by AR is lost.

The **Redirect** and **Send Back** actions are used only to switch requests among approvers, without any update to the request information.

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 17. Summary of permissions statuses



The upper right part of the page contains information about **Last Changed** and about the user who made them.



The icon here indicates that 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**:

Table 275. 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:

Table 276. 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 18. 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.

Business activity Perspective

You can associate activities to one or more permissions or groups.

On the **Business activity tree** tab, you can browse the activity tree for the required activity. On the **Business 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 **Business activity > Actions** menu, **View** switches from the Business activity flat view to the hierarchical view (**Business 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 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:

Table 277. 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:

Table 278. Status labels for reports

Status	Description
Pending	The report is waiting to run.

Table 278. Status labels for reports (continued)

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	Streicher	I	A	primary	staff@34.3 4000:5003 7950
51165	83492	0	s25488	Oi Yan	Fung	I	A	primary	staff@34.3 4000:5003 7837

Figure 19. 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:

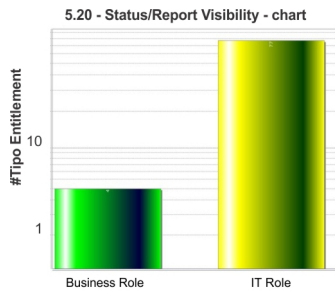


Figure 20. Chart: Bar type

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 7

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 249

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 251

You can view your requests by using the Self Care application in the Service Center.

Chapter 13, “Updating my security questions,” on page 253

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

The administrator must configure the forgotten password service in the Administration Console. Otherwise, the **Forgot your password?** link does not display on the Service Center Login page. For more information, see *Configuring password services*.

Your security questions must already be set up. For more information, see Chapter 13, “Updating my security questions,” on page 253.

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 .

Option	Description
<p>The questions are answered correctly, and your system is configured to generate a new password and prompts you to type an email address.</p>	<p>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.</p>
<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 11

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 251. 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 255
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 257

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 259

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 to refine your search results, 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 279. 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 249

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 to refine your search results, 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 280. 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 251
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 253

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 5.2.3.1 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/about/releasenotes.html>.

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 263
Account 80, 82, 89, 96, 98, 105, 112, 131
Approver 131
Authorization 131

B

Beneficiary 82, 89, 98, 105

D

Dashboard
 home in Service Center 3

E

Execution 131

H

Home
 Service Center 3

R

Request 80, 82, 89, 96, 98, 105, 112, 131

S

Service Center
 home page 3
Sub-Request 82, 89, 98, 105



Printed in USA