

IBM Security Identity Governance and Intelligence  
Version 5.2.1

*Administration Topics  
for Administrators*





IBM Security Identity Governance and Intelligence  
Version 5.2.1

*Administration Topics  
for Administrators*







---

# Table of contents

Table list . . . . .	vii	<b>Chapter 6. Data import with Bulk Data Load.</b> . . . . .	<b>61</b>
<b>Part 1. Administrators.</b> . . . . .	<b>1</b>	Creating a bulk load operation . . . . .	61
<b>Chapter 1. Administration Console</b> . . . . .	<b>3</b>	<b>Chapter 7. Entitlement administration</b> . . . . .	<b>63</b>
<b>Chapter 2. Data Model and Main Features: overview</b> . . . . .	<b>5</b>	Adding an entitlement. . . . .	63
IBM Security Identity Governance Core Data Model . . . . .	5	Adding an entitlement to an organizational unit . . . . .	64
Concept of realm . . . . .	6	Adding entitlements to an attribute group . . . . .	64
Organization unit. . . . .	8	<b>Chapter 8. Group administration.</b> . . . . .	<b>67</b>
User, attributes and polyarchies . . . . .	9	Adding an organizational unit . . . . .	67
Hierarchy of Entitlements . . . . .	10	Creating an attribute hierarchy . . . . .	68
Employment and resources . . . . .	14	Configuring the attribute hierarchy . . . . .	68
Rights . . . . .	16	<b>Chapter 9. Password administration</b> . . . . .	<b>71</b>
Applications . . . . .	18	Changing account passwords for users . . . . .	71
Accounts . . . . .	20	Forcing a password change . . . . .	72
IBM Security Identity Governance and Intelligence extended data model . . . . .	21	Configuring password services . . . . .	72
Business activities model and RBAC model. . . . .	22	Configuring the password service in Access Governance Core . . . . .	73
Risk definition and detection in IBM Security Identity Governance and Intelligence . . . . .	23	Configuring the password service in Process Designer . . . . .	75
Segregation of Duties (SoD): a specific type of Risk . . . . .	25	<b>Chapter 10. Target type administration</b> . . . . .	<b>79</b>
External SoD . . . . .	25	Target definition file or adapter profile . . . . .	80
Risk mitigation: classes of mitigation . . . . .	26	Importing target types (adapter profiles). . . . .	80
Mitigation Actions . . . . .	29	Importing the attribute map for a target type . . . . .	81
Domains: conflicting and risk activities . . . . .	30	Account defaults on a target type . . . . .	82
How to read the tree of the risks of a user . . . . .	32	Adding account defaults to a target type . . . . .	83
Introduction to rules engine . . . . .	33	Changing account defaults for a target type . . . . .	84
Drools rules engine. . . . .	34	Removing account defaults from a target type. . . . .	85
IBM Security Identity Governance and Intelligence integration interface . . . . .	36	<b>Chapter 11. Target administration</b> . . . . .	<b>87</b>
Brief introduction to events . . . . .	38	Target status . . . . .	88
Basic Structure of the Interface . . . . .	39	Creating targets . . . . .	88
Examples of Rules . . . . .	41	Changing targets . . . . .	90
The rules engine (RE) in AG Core Architecture: read-from and write-to branches . . . . .	42	Deleting targets . . . . .	91
Synchronization branch . . . . .	43	Account defaults on a target. . . . .	92
Complete Architecture of the IBM Security Identity Governance Integration Interface . . . . .	43	Adding account defaults to a target . . . . .	92
SAP GRC integration scheme . . . . .	45	Changing account defaults for a target . . . . .	94
ReST integration scheme . . . . .	45	Removing account defaults from a target . . . . .	95
Introduction to audit . . . . .	46	Viewing the target connection status . . . . .	96
<b>Chapter 3. Identity Governance and Intelligence modules.</b> . . . . .	<b>51</b>	Testing the target connection . . . . .	96
<b>Chapter 4. Account administration.</b> . . . . .	<b>57</b>	Reconciliation management . . . . .	97
Adding an account . . . . .	57	Reconciliation timeout and failure threshold . . . . .	99
<b>Chapter 5. Application administration</b> . . . . .	<b>59</b>	Reconciling accounts immediately on a target . . . . .	99
Adding an application. . . . .	59	Creating a reconciliation schedule . . . . .	100
		Changing a reconciliation schedule . . . . .	101
		Deleting a reconciliation schedule . . . . .	102
		Viewing reconciliation requests . . . . .	103
		<b>Chapter 12. User administration</b> . . . . .	<b>105</b>
		Adding a user . . . . .	105

Configuring user access to Service Center applications . . . . .	106
Assigning an administrator role to a user . . . . .	107
Adding columns to the UserErc table . . . . .	107

**Chapter 13. Introduction to Access Governance Core. . . . . 109**

AG Core Architecture . . . . .	109
Managing the Administration Realm . . . . .	112
Manage . . . . .	117
Users . . . . .	117
Groups . . . . .	134
Roles . . . . .	140
Application . . . . .	147
Accounts . . . . .	163
Resources . . . . .	170
Configure . . . . .	174
Certification campaigns . . . . .	174
Certification data sets . . . . .	181
Admin roles . . . . .	183
Rules . . . . .	186
Concept of Rule Flow . . . . .	193
Email . . . . .	193
Hierarchy (Polyarchies) . . . . .	195
Rights Lookup . . . . .	199
Monitor . . . . .	199
Report . . . . .	199
Role Compare . . . . .	199
Scheduled tasks . . . . .	201
TARGET inbound - Account events . . . . .	201
TARGET inbound - Access events . . . . .	204
OUT events . . . . .	205
IN - User events . . . . .	208
IN - Org. Unit events . . . . .	210
INTERNAL events . . . . .	211
Tools . . . . .	214
Bulk Data Load . . . . .	214
Settings . . . . .	243
Core configurations . . . . .	243
Configure password service . . . . .	251

**Chapter 14. Introduction to Access Risk Controls . . . . . 255**

Manage . . . . .	256
Business activities . . . . .	256
Business Activity Mapping . . . . .	259
Mitigation controls . . . . .	260
Risk definition . . . . .	263
Domains . . . . .	265
Configure . . . . .	267
Configurations . . . . .	267
Monitor . . . . .	267
Dashboard . . . . .	267
Risk violations . . . . .	269
Scheduled tasks . . . . .	272
Configuration comparison . . . . .	272
Report . . . . .	275
Tools . . . . .	275
Bulk Data Load . . . . .	275
Refresh violation detection . . . . .	287

**Chapter 15. Introduction to Process Designer . . . . . 289**

Authorization process roadmap . . . . .	290
Modeling an activity . . . . .	294
Manage . . . . .	304
Activity . . . . .	304
Process . . . . .	306
Configure . . . . .	313
Menu . . . . .	314
Rules . . . . .	315
Monitor . . . . .	322
Statistics . . . . .	322
Settings . . . . .	323
Language management . . . . .	324
Entity display . . . . .	324

**Chapter 16. Introduction to Enterprise Connectors . . . . . 325**

The Identity Governance and Intelligence ERC model . . . . .	326
Channel mode of the connector . . . . .	327
Building a connector . . . . .	328
Manage connectors . . . . .	329
Driver configuration . . . . .	332
Driver Attributes List . . . . .	334
Channels and Rules . . . . .	335
Monitor . . . . .	341
Connectors status . . . . .	341
Reconciliation status . . . . .	343
Settings . . . . .	346
Introduction to IRA agent . . . . .	348
Prerequisites . . . . .	349
IRA setup and patches . . . . .	350
Installation procedure . . . . .	352
Remote agent for active directory . . . . .	352

**Chapter 17. Introduction to Access Optimizer . . . . . 357**

Architecture and components . . . . .	357
The Access Risk approach . . . . .	359
Defining an Access data set . . . . .	361
Measuring access risk criteria . . . . .	363
Reducing risk distribution . . . . .	367
Monitoring access risk trend over time . . . . .	367
Role mining guidelines . . . . .	368
Optimal Role-Set algorithm . . . . .	369
The Minability index . . . . .	370
Direct or hierarchal assignments: concept of entitlement type . . . . .	370
Spread . . . . .	376
Farness . . . . .	377
Maps . . . . .	379
Role map . . . . .	380
Risk Map . . . . .	396
Map management . . . . .	396
Access Optimizer: Guide to modeling . . . . .	398
Phase 1: Data snapshot . . . . .	399
Phase 2: Data exploration algorithm . . . . .	400
Phase 3: Risk analysis process . . . . .	401
Phase 4: Role mining algorithm . . . . .	401

Phase 5: Role acceptance . . . . .	402
Manage . . . . .	402
Data Exploration analysis and details . . . . .	402
Role mining . . . . .	405
Configure . . . . .	423
Data snapshot . . . . .	423
Access data sets . . . . .	428
Relevance criteria . . . . .	430
Monitor . . . . .	431
Access distribution . . . . .	431
Coverage factors . . . . .	432
Access summary . . . . .	432
Access trend. . . . .	434
Report. . . . .	434
Scheduled tasks . . . . .	435
Tools . . . . .	435
Bulk data load . . . . .	435
Reset flags . . . . .	437
Settings . . . . .	438
Attributes . . . . .	438
Mining Attributes . . . . .	438
Data file template . . . . .	438
Mining Data file template . . . . .	443

## Chapter 18. Introduction to Access

<b>Risk Controls for SAP . . . . .</b>	<b>449</b>
ARCS Data Model. . . . .	449
SAP roles and risk entitlements . . . . .	450
Business Activity Mapping: ARCS to ARC. . . . .	451
Activity Tree: aligning ARC to ARCS . . . . .	452
Introduction to the ARCS-SAP adapter agent. . . . .	453
Distribution . . . . .	453
Installation procedure . . . . .	454
ARCS-SAP adapter agent functions . . . . .	454
ARCS-SAP adapter Agent:User Role. . . . .	458
Manage . . . . .	459
Business activities . . . . .	459
Activities and permissions . . . . .	462
Risk Definitions . . . . .	464
Domains . . . . .	465
Configure . . . . .	467
Configurations . . . . .	467
SAP System . . . . .	468
Rules . . . . .	468
Monitor . . . . .	475
User Violations . . . . .	475
SAP Role Violations . . . . .	476
SAP authorization violations . . . . .	478
Role warnings . . . . .	479
Report. . . . .	479
Tools . . . . .	480
Data refresh . . . . .	480
Bulk Data Load . . . . .	481
Configuration Set Comparison. . . . .	484

## Chapter 19. Introduction to Report Designer . . . . . 487

Report modeling for the Identity Governance and Intelligence platform . . . . .	487
Report classification: product reports and new reports . . . . .	495
Report status and report category . . . . .	508
Available reports . . . . .	508
Available dashboard items . . . . .	514
Building a new report: A brief roadmap . . . . .	515
Manage . . . . .	515
Query . . . . .	515
Report. . . . .	520
Dashboard . . . . .	522
Configure . . . . .	528
Report assignment. . . . .	528
Menu . . . . .	533
Settings . . . . .	536
Edit labels tab . . . . .	537
System entities . . . . .	538
Scope . . . . .	539
Custom filters . . . . .	541
Monitor . . . . .	542
Report queue . . . . .	542

## Chapter 20. Introduction to Task Planner . . . . . 545

Architecture and components . . . . .	545
Guide to task modeling . . . . .	546
How to implement a new job . . . . .	548
Manage . . . . .	552
Jobs . . . . .	552
Tasks . . . . .	554
Monitor . . . . .	559
Settings . . . . .	560
Scheduler. . . . .	560
Context . . . . .	562

## Chapter 21. Request . . . . . 563

## Chapter 22. Download. . . . . 569

---

## Part 2. Appendixes . . . . . 573

### Appendix. Accessibility features for IBM Security Identity Governance and Intelligence . . . . . 575

### Index . . . . . 577



---

## Table list

1. Administration Console modules . . . . .	3	51. Permission Details . . . . .	155
2. Audit events table . . . . .	46	52. Entitlements . . . . .	158
3. Common buttons and icons . . . . .	54	53. User details . . . . .	158
4. Account administration tasks . . . . .	57	54. Entitlements . . . . .	158
5. Application administration tasks . . . . .	59	55. Organization Unit . . . . .	159
6. Data import tasks . . . . .	61	56. User filter details . . . . .	160
7. Entitlement administration tasks . . . . .	63	57. User Details . . . . .	160
8. Group administration tasks . . . . .	67	58. Entitlements . . . . .	161
9. Password administration tasks . . . . .	71	59. Permission . . . . .	162
10. Configuration items for Configure Forgotten Password Service . . . . .	74	60. Entitlements . . . . .	162
11. Activity scope tabs of ManagerPasswordResetGEN . . . . .	76	61. Application . . . . .	162
12. Target type administration tasks . . . . .	79	62. Resource filters . . . . .	171
13. Target administration tasks . . . . .	87	63. Resource note . . . . .	172
14. User administration tasks . . . . .	105	64. Resource Type filters . . . . .	172
15. Assignable functions . . . . .	115	65. Note about the Administration Resource Type	173
16. Available filters to list users. . . . .	117	66. Cert_Campaign_Reviewer_Tab . . . . .	177
17. Available actions on a selected user. . . . .	118	67. Cert_Campaign_Scheduling_Tab . . . . .	178
18. User details . . . . .	120	68. Columns for Entitlement View . . . . .	180
19. Entitlement filters . . . . .	121	69. Entity filters . . . . .	181
20. Entitlement properties . . . . .	122	70. Keys for properties . . . . .	184
21. Resources filters . . . . .	124	71. Entitlements filters. . . . .	185
22. Account details . . . . .	125	72. Symbols of the Rules editor. . . . .	188
23. Functions . . . . .	126	73. Email settings attributes . . . . .	194
24. IN events filters. . . . .	128	74. Cautionary note. . . . .	194
25. IN Event structure . . . . .	129	75. Email template attributes . . . . .	195
26. OUT Events filters . . . . .	130	76. Details of roles listed for comparison.	200
27. OUT Event structure . . . . .	131	77. Filters you can specify to list Target inbound - account events. . . . .	202
28. Group details . . . . .	135	78. Target inbound - account event details.	202
29. Entitlement filters and details . . . . .	137	79. Filters you can specify to list Target inbound - Access events. . . . .	204
30. Organizational unit resource filters . . . . .	139	80. Target inbound - access event details.	204
31. User filters . . . . .	140	81. OUT queue filters . . . . .	206
32. Role filters . . . . .	140	82. Attributes of OUT events. . . . .	206
33. Role details . . . . .	142	83. Filters you can specify to list user events in input from external target systems. . . . .	208
34. Keys for properties . . . . .	143	84. Details of User events in input from external target systems. . . . .	208
35. Filters to search for the entitlements that make up a role. . . . .	143	85. Filters you can specify to list Organization Unit events in input from external systems. . . . .	210
36. Filters to search for the users assigned with the entitlement. . . . .	144	86. Details of User events in input. . . . .	210
37. Filters to search for the OUs associated with the entitlement. . . . .	145	87. Filters you can specify to list internal events.	211
38. Filters to search for the permissions that are in a role. . . . .	145	88. Details of internal events. . . . .	212
39. Manager filters . . . . .	146	89. Insert Entitlements record track . . . . .	216
40. Right properties. . . . .	146	90. Insert Organization Units Track . . . . .	218
41. Application details. . . . .	147	91. Insert Users record track. . . . .	220
42. Note about multi-value properties . . . . .	148	92. Remove Entitlements from OU Track	222
43. Permission filters . . . . .	149	93. Remove Entitlements Track . . . . .	223
44. Permission filters . . . . .	150	94. Note about terms . . . . .	224
45. Rights attributes . . . . .	152	95. Remove User-OU-Entitlement Assignments Track . . . . .	226
46. History attributes . . . . .	152	96. User-OU-Entitlement Assignments Track	229
47. User filters . . . . .	153	97. Add Internal Resources to User/Entitlement Track . . . . .	232
48. Application note . . . . .	153	98. Note about resources . . . . .	233
49. Dashboard set . . . . .	154		
50. Permission filter details . . . . .	155		

99. Combinations of parameters available for adding Internal Resources . . . . .	234	153. IRA setups. . . . .	350
100. Insert Organization Units Track . . . . .	236	154. IRA patches. . . . .	350
101. Insert Property Record Track. . . . .	237	155. Administrator actions. . . . .	352
102. Entity Logic Keys combinations. . . . .	238	156. <b>Add Service</b> window fields. . . . .	353
103. Add Internal Resources to User/Entitlement Track . . . . .	238	157. <b>Add service</b> fields . . . . .	354
104. Note about resources . . . . .	239	158. Remove services . . . . .	354
105. Combinations of parameters available for adding Internal Resources . . . . .	240	159. Predefined access risk criteria. . . . .	364
106. Insert External Roles record track . . . . .	241	160. Relevance filters . . . . .	364
107. Remove External Roles record track . . . . .	242	161. The Relevance Reduction Approach. . . . .	366
108. General configuration attributes. . . . .	244	162. Optimal Role-Set parameters . . . . .	369
109. User virtual attributes - repository details. . . . .	247	163. Candidate Role . . . . .	393
110. Options for the creation of internal events associated to local operations. . . . .	251	164. Analysis filters. . . . .	402
111. Activity attributes . . . . .	294	165. Analysis details. . . . .	403
112. Type attribute values . . . . .	295	166. Partition attributes. . . . .	404
113. Mode attribute values. . . . .	295	167. Entitlements/Users Statistics filters. . . . .	405
114. Context attribute values . . . . .	296	168. Role mining search filters. . . . .	406
115. Functionality attribute values . . . . .	296	169. Role mining analysis attributes. . . . .	406
116. Visibility levels by Beneficiary . . . . .	299	170. Optimal role-set parameters. . . . .	407
117. Visibility levels by application . . . . .	299	171. Data exploration details. . . . .	408
118. Visibility levels . . . . .	300	172. Dashboard set. . . . .	409
119. Activity identifiable attributes: required data . . . . .	300	173. Role statistics filters. . . . .	410
120. Required data items . . . . .	301	174. Entitlement details. . . . .	412
121. Repository attributes . . . . .	303	175. Entitlement filters . . . . .	413
122. Symbols of the Rules editor. . . . .	317	176. Entitlement details . . . . .	414
123. Available filters to search connectors . . . . .	329	177. Candidate Role attributes . . . . .	415
124. Connector details . . . . .	330	178. User attributes . . . . .	416
125. Global configuration properties for connectors. . . . .	331	179. Candidate Role attributes . . . . .	417
126. Driver properties . . . . .	333	180. OU attributes. . . . .	418
127. Adding targets . . . . .	333	181. User filters. . . . .	418
128. New Object Class node attributes. . . . .	334	182. User details. . . . .	419
129. Object Class Field node attributes. . . . .	334	183. Candidate Role attributes . . . . .	420
130. Event fields . . . . .	336	184. Application attributes. . . . .	421
131. Rule Package Actions . . . . .	337	185. Entitlement details. . . . .	421
132. Rules Package pane Actions. . . . .	337	186. User details. . . . .	422
133. Mapping pane columns when Operation = Source.. . . . .	338	187. Data snapshot details . . . . .	424
134. Mapping pane columns when Operation = Destination. . . . .	339	188. File import details . . . . .	425
135. Target Cache filters . . . . .	340	189. History filters . . . . .	426
136. Main Target Cache attributes . . . . .	341	190. Filters for entitlements . . . . .	427
137. Connector filters . . . . .	341	191. Filters for Entitlement hierarchies . . . . .	427
138. Connector attributes . . . . .	342	192. filters for assignments. . . . .	428
139. Details box attributes. . . . .	342	193. Data sets details/attributes. . . . .	429
140. Scheduling box attributes . . . . .	342	194. Relevance Criteria details. . . . .	430
141. Connector History filters. . . . .	343	195. History filters . . . . .	431
142. Connector History attributes . . . . .	343	196. Access distribution filters. . . . .	431
143. Connector filters . . . . .	344	197. Analysis filters . . . . .	433
144. Connector attributes . . . . .	344	198. Analysis attributes. . . . .	433
145. Details box attributes. . . . .	344	199. Access distribution filters. . . . .	434
146. Scheduling box attributes . . . . .	345	200. Bulk data load details. . . . .	435
147. Advanced Settings box attributes . . . . .	345	201. File import details . . . . .	436
148. Connector History filters. . . . .	346	202. Reset details.. . . . .	437
149. Connector History attributes . . . . .	346	203. Column details . . . . .	439
150. <b>Settings</b> > <b>IDEAS driver</b> panel layout. . . . .	347	204. Column details . . . . .	443
151. New Object Class node attributes. . . . .	347	205. z_start_sync - INPUT parameters.. . . . .	455
152. Object Class Field node attributes. . . . .	347	206. z_start_sync - OUTPUT parameters. . . . .	455
		207. z_get_job_status - OUTPUT parameters. . . . .	456
		208. z_get_sync_data - INPUT parameters. . . . .	456
		209. z_get_sync_data - OUTPUT parameters. . . . .	457
		210. ROLE_DATA. . . . .	457
		211. OTHER_DATA. . . . .	457
		212. z_get_single_role - INPUT parameters. . . . .	458
		213. z_get_single_role - OUTPUT parameters. . . . .	458

214. z_get_tcode - INPUT parameters. . . . .	458	262. Query Attributes. . . . .	516
215. z_get_tcode - OUTPUT parameters. . . . .	458	263. Report filters. . . . .	520
216. Structure of TCODE_DATA. . . . .	458	264. Report attributes. . . . .	520
217. Business activity filters. . . . .	459	265. Dashboard item fields. . . . .	523
218. Activity details. . . . .	460	266. Dashboard item filters . . . . .	524
219. Permission filters. . . . .	461	267. Details tab fields . . . . .	525
220. Permission filters. . . . .	463	268. Organization Unit visibility tab fields	526
221. Permission attributes. . . . .	463	269. Application visibility tab fields. . . . .	526
222. Permission details. . . . .	463	270. Layout tab fields . . . . .	526
223. Activity filters. . . . .	464	271. Filter tab fields . . . . .	527
224. Available filters to find a Risk definition.	464	272. Localization tab fields. . . . .	527
225. Details of a Risk definition. . . . .	465	273. Report filters. . . . .	528
226. Domain details. . . . .	466	274. Report attributes. . . . .	528
227. Permissions filters. . . . .	466	275. Assignable entitlement filters. . . . .	529
228. Activities filters. . . . .	467	276. Entitlement filters. . . . .	529
229. Symbols of the Rules editor. . . . .	470	277. Assignable Reports filters. . . . .	530
230. Filters to find conflicting users . . . . .	475	278. Report filters. . . . .	530
231. Filters helpful for searching a domain or an		279. Report attributes. . . . .	531
activity for conflicting users. . . . .	476	280. Assignable Entitlement filters. . . . .	531
232. Filters you can use to find SAP roles.	477	281. Entitlement filters. . . . .	532
233. Filters you an use to find SAP authorizations.	478	282. Assignable reports filters. . . . .	533
234. Filters you an use to find role warnings.	479	283. Report filters. . . . .	534
235. Add Risk Entitlement to Activity Track (sheet		284. Report attribute. . . . .	534
1). . . . .	481	285. Localization Code filters.. . . . .	537
236. Add Risk Entitlement to Activity Track (sheet		286. Entity Key Filters. . . . .	538
2). . . . .	482	287. Entity Key Details. . . . .	538
237. Insert Risk Entitlement Track. . . . .	482	288. Scope search attributes. . . . .	539
238. Remove Risk Entitlement Track. . . . .	484	289. Scope Details . . . . .	540
239. Filters available to search for conflicting users		290. Custom Filter Attributes.. . . . .	541
in a configuration set comparison. . . . .	485	291. Filter details. . . . .	542
240. Filters available to search for conflicting		292. Report execution statuses. . . . .	542
entitlements in a configuration set		293. Report properties. . . . .	543
comparison. . . . .	486	294. Job filters.. . . . .	552
241. Product queries . . . . .	488	295. Job attributes. . . . .	552
242. Schema specification . . . . .	490	296. Job details. . . . .	552
243. Product scopes . . . . .	492	297. Job Class parameters. . . . .	553
244. Available entities. . . . .	498	298. Task filters. . . . .	553
245. Visibility options for each entity. . . . .	499	299. History filters. . . . .	554
246. Report columns configuration. . . . .	500	300. Task filters. . . . .	554
247. Product custom filters. . . . .	501	301. Task attributes. . . . .	555
248. Filter type. . . . .	502	302. Task details. . . . .	555
249. Send email pane details. . . . .	503	303. Job attributes. . . . .	556
250. Additional data pane details. . . . .	503	304. Job Class parameters. . . . .	557
251. Analysis reports available . . . . .	509	305. Simple execution attributes.. . . . .	557
252. ARCS reports available . . . . .	509	306. Advanced execution attributes.. . . . .	558
253. Audit reports available . . . . .	510	307. History filters. . . . .	558
254. Campaigns reports available . . . . .	510	308. Task attributes. . . . .	559
255. Export reports available . . . . .	511	309. History filters. . . . .	559
256. Optimizer reports available . . . . .	511	310. Scheduler Set. . . . .	561
257. Policies reports available. . . . .	512	311. Scheduler attributes. . . . .	561
258. Status reports available . . . . .	512	312. History filters. . . . .	561
259. Sync reports available. . . . .	513	313. Configuration steps. . . . .	563
260. Violations reports available . . . . .	514	314. Report execution Status. . . . .	569
261. Dashboard items available . . . . .	514		





---

## **Part 1. Administrators**

An administrator can access the Administration Console and define administrator users for a single module or all the Identity Governance and Intelligence modules. Administrators are authorized to perform a selected set of tasks on specific modules.

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



---

## Chapter 1. Administration Console

Administration Console is an administration dashboard that provides control over the various management features of Identity Governance and Intelligence.

### Logging in to the Administration Console

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

### General options

The console includes the following general options:

**Act as** Grants user access to the system if the user is delegated as an administrator.

**Logout** Exits the user from the console.

**Change Password** Enables the user to change the current password.

**Help** Displays the help information.

**License** Displays information about Identity Governance and Intelligence licenses and upgrades.

### Modules

The console includes a list of Identity Governance and Intelligence modules. Every module contains a set of common characteristics, which are outlined in Chapter 3, “Identity Governance and Intelligence modules,” on page 51.

For more information about the different Administration Console modules, see the corresponding references.

Table 1. Administration Console modules










Image	Description
 Chapter 13, “Introduction to Access Governance Core,” on page 109	 Chapter 17, “Introduction to Access Optimizer,” on page 357

Table 1. Administration Console modules (continued)

Image	Description
 <p>Chapter 14, "Introduction to Access Risk Controls," on page 255</p>	 <p>Chapter 18, "Introduction to Access Risk Controls for SAP," on page 449</p>
 <p>Chapter 15, "Introduction to Process Designer," on page 289</p>	 <p>Chapter 19, "Introduction to Report Designer," on page 487</p>
 <p>Chapter 16, "Introduction to Enterprise Connectors," on page 325</p>	 <p>Chapter 20, "Introduction to Task Planner," on page 545</p>
 <p>Chapter 11, "Target administration," on page 87</p>	

## Realms

After you log in, select an operating realm. You do not need to log in again if you want to change realms.

### Demo

A predefined realm with a large amount of coherent data that can be used for learning various about aspects of Identity Governance and Intelligence.

### Sandbox

An empty realm with one basic data set that is used to start the operation.

### Admin

The administration realm.

After you select a realm, click the module that you want. For every module, a specific tab opens by default.

---

## Chapter 2. Data Model and Main Features: overview

All the features available in IBM® Security Identity Governance and Intelligence are based on different specialized integrated modules and on several architectural elements.

IBM Security Identity Governance and Intelligence uses these main architectural elements:

- A solid data model, for matching all the main characteristics of any organization.
- A flexible rules engine, for customizing the business policies for every organization.
- An integration interface, for integrating IBM Security Identity Governance and Intelligence platform with the pre-existing organization's architecture and the related repositories that contain users' information and authorizations.
- Several features of advanced customization for fitting the special needs of any organization.

You need a solid knowledge of these basic aspects before you start the administration activities of the platform:

- Core Data Model
- Extended Data Model
- Rules Engine
- Integration Interface
- Audit

---

### IBM Security Identity Governance Core Data Model

AG Core provides a modeler capable of systematically outlining an organization's current situation as it relates to its different parts through a procedure that defines organizational and technical components.

This description of a realm is implemented by a database that literally photographs how the company is structured in terms of its

- Organization units
- Users
- Resources
- Applications
- Other elements of the IBM Security Identity Governance and Intelligence data model.

Based on this description, an authorization profile is built for each user within the organization. The authorization profile determines what a user can do within the realm and what resources are available.

An authorization profile intrinsically introduces rules about the visibility of objects that are described in the realm. Only those applications and resources that are outlined in the user's profile are made accessible to the user.

The main elements of the IBM Security Identity Governance and Intelligence data model are shown in the following Figure.

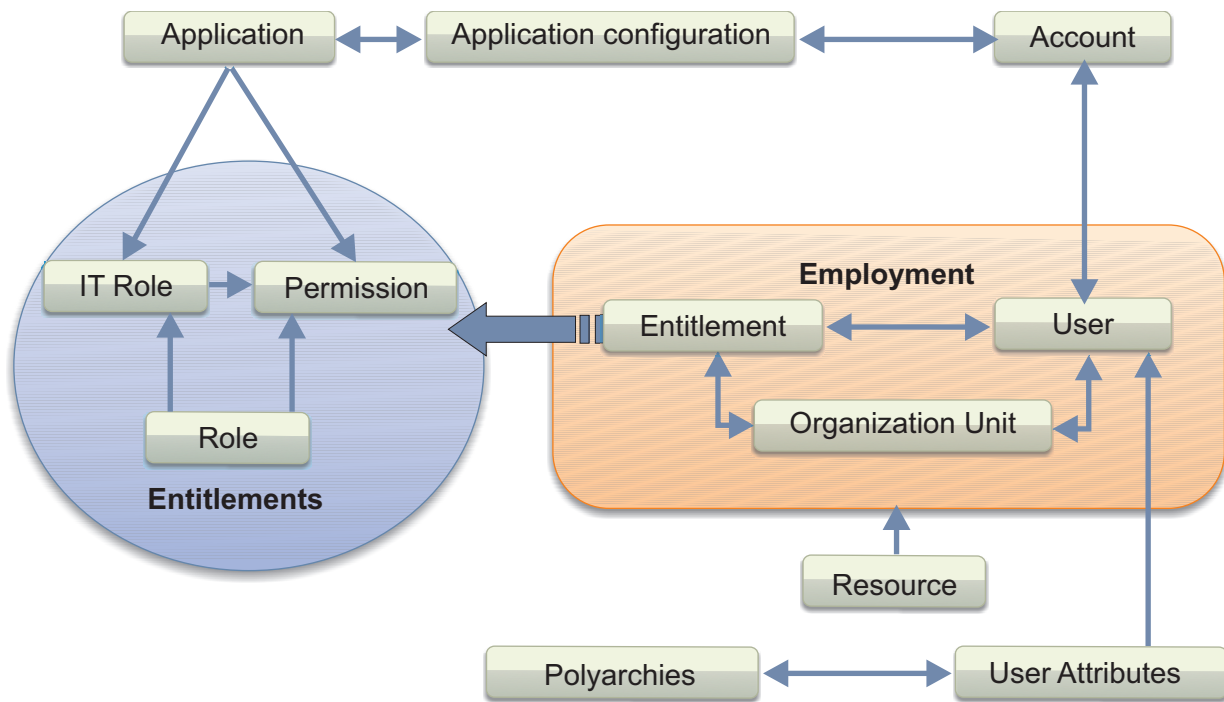


Figure 1. IBM Security Identity Governance and Intelligence data model

IBM Security Identity Governance and Intelligence data model has these main elements:

- Realm
- User
- “Organization unit” on page 8
- Entitlement
- Resource
- “Rights” on page 16
- “Applications” on page 18
- “Accounts” on page 20

## Concept of realm

IBM Security Identity Governance and Intelligence Platform can manage multiple realms. It enables the modeling of multiple organizations to define the management of each of these organizations and keeps the contexts separate in relation to the different realms.

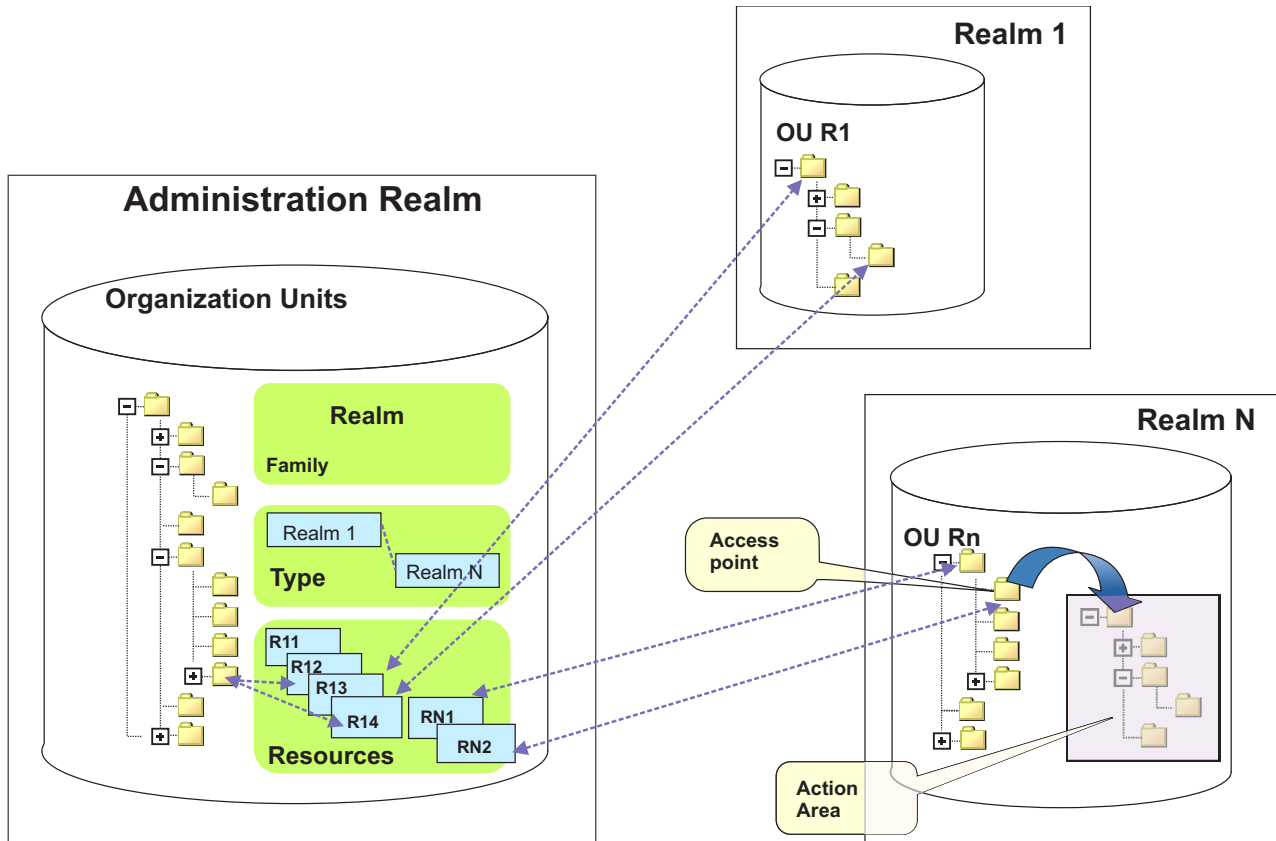


Figure 2. IBM Security Identity Governance and Intelligence realms

Each realm is separated from other realms. Data separation is assured and different set of policies can be applied for each realm. This feature can be useful for service providers, where each realm can contain a single customer.

IBM Security Identity Governance and Intelligence is provided with two standard realms:

#### Administration Realm

In this realm, IBM Security Identity Governance and Intelligence administrators, product administrators who can access product configuration and monitoring, are managed.

#### Production Realm

This default realm is not empty. It provides some basic configurations such as product rules, reports, and other basic settings.

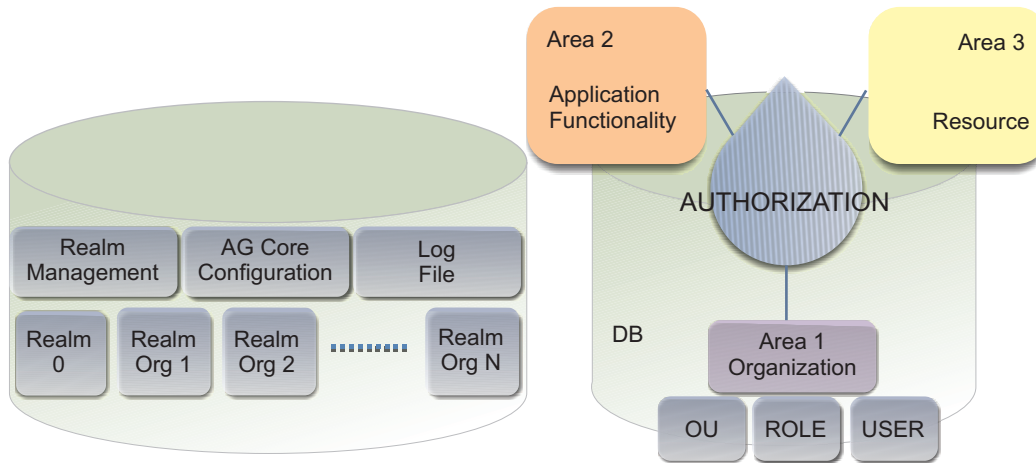


Figure 3. Logic architecture of the IBM Security Identity Governance and Intelligence Core DB

From a logical viewpoint, the IBM Security Identity Governance and Intelligence Core DB can be laid out in two main sections:

- The first section contains information for managing the realms and data for the AG Core configuration.
- The second section of the database contains as many copies as the number of realms or different organizations that are managed. Realm 0 is used to define administrators and authorizations that are related to them.

## Organization unit

An organization unit is a basic element of an organization. An organization can be hierarchically structured in different ways according to different classifications.

For example, some organizations are organized by a geographical classification.

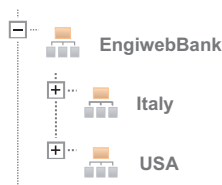


Figure 4. Geographical organization

Others must be organized through a hierarchy of functional units.





Figure 5. Hierarchical organization

Others might use a combination of both approaches.



Figure 6. Mixed organization

Other possible classifications can be built as well.

In the IBM Security Identity Governance and Intelligence Core Model, every type of organization can be described as a hierarchy of organization units (OUs). Every OU in the hierarchy is displayed as an expandable directory tree if associated child elements exist with a free number of distinct levels in the hierarchy. A single OU is aggregated to a set of users and to a set of entitlements that can be assigned to every user.

## User, attributes and polyarchies

In IBM Security Identity Governance and Intelligence, identities are called users.

A user represents a set of information that is connected to an individual or virtual identity (service users).

IBM Security Identity Governance and Intelligence supports the concept of primary and secondary users as well as user multiple entries (UME).

A UME can have more than one account on the same target system.

If users are separated for organizational reasons, IBM Security Identity Governance and Intelligence tightly connects the primary user with secondary users, UME, or both by automatically synchronizing any changes.

Different roles and permissions can be granted to primary and secondary users. IBM Security Identity Governance and Intelligence automatically incorporates authorizations for analysis (like SOD and risks).

In IBM Security Identity Governance and Intelligence a user:

- belongs to a specific group of a hierarchy
- is characterized by a set of permissions

- is aggregated to an account (at least one)
- can dispose of a set of resources
- is characterized by a set of user attributes.

User attributes can be expanded at any time.

## Attributes and Polyarchies

In addition to the traditional representation of an organization as a hierarchy of Organization Units (OUs), other hierarchical views, commonly indicated as polyarchies, can be built based on user attributes.

A Polyarchy can be created at anytime by grouping users based on attribute values.

If the attribute contains hierarchy path, it is translated in a hierarchy notation; otherwise, the attribute is represented as a flat hierarchy.

For example, a multinational enterprise can build a polyarchy by using the attribute LOCALITY for grouping users based on their current workplace. You can then apply specific rules that are related to local regulatory laws, to certify a compliance criteria for any group of users.

## Attribute-based Access Roles

Use the Access Governance Core module to build hierarchies based on different User attributes.

These attributes are made available through the Attribute Mapping of the USER\_ERC table.

A user who belongs to a certain hierarchy can be linked to a specific Role related to that hierarchy.

For example, when you begin a complex project, you can set up a hierarchy of projects, structured in N sub-areas (Project 1, Project 2, ... Project N).

User Mark Brown, who belongs to an OU named Manager, holds all the roles needed for running managerial tasks in the Manager OU.

But Mark Brown is also the Project Manager of Project 3 in the Projects hierarchy. He is therefore assigned also all the necessary Access Attributes Roles (ABA Roles) for Project 3.

From this point of view, the traditional Role assignment policy, which is based mainly on OU hierarchy, is a specific instance of the ABA Roles approach.

## Hierarchy of Entitlements

In the IBM Security Identity Governance and Intelligence data model, an entitlement identifies a structured set of permissions. These permissions are assigned to a generic user to access the resources of an organization.

The following list describes the various types of entitlements:

### Permission

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

### IT Role

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

- IT Roles
- Permissions

### External Role

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

- External Roles
- Permissions

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

### Business Role

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

- Business Roles
- IT Roles
- External Roles
- Permissions

The following icons represent these entitlements:



Business Role (BRole)



IT Role



Permission



External Role

A business role (BRole) can be hierarchically formed by business roles, IT roles, external roles, and permissions. An IT role can be formed by IT roles and permissions. An external role can include other external roles and permissions.

The generic hierarchical structure of an entitlement is shown in the following figure.

## Entitlement: Hierarchical Structure

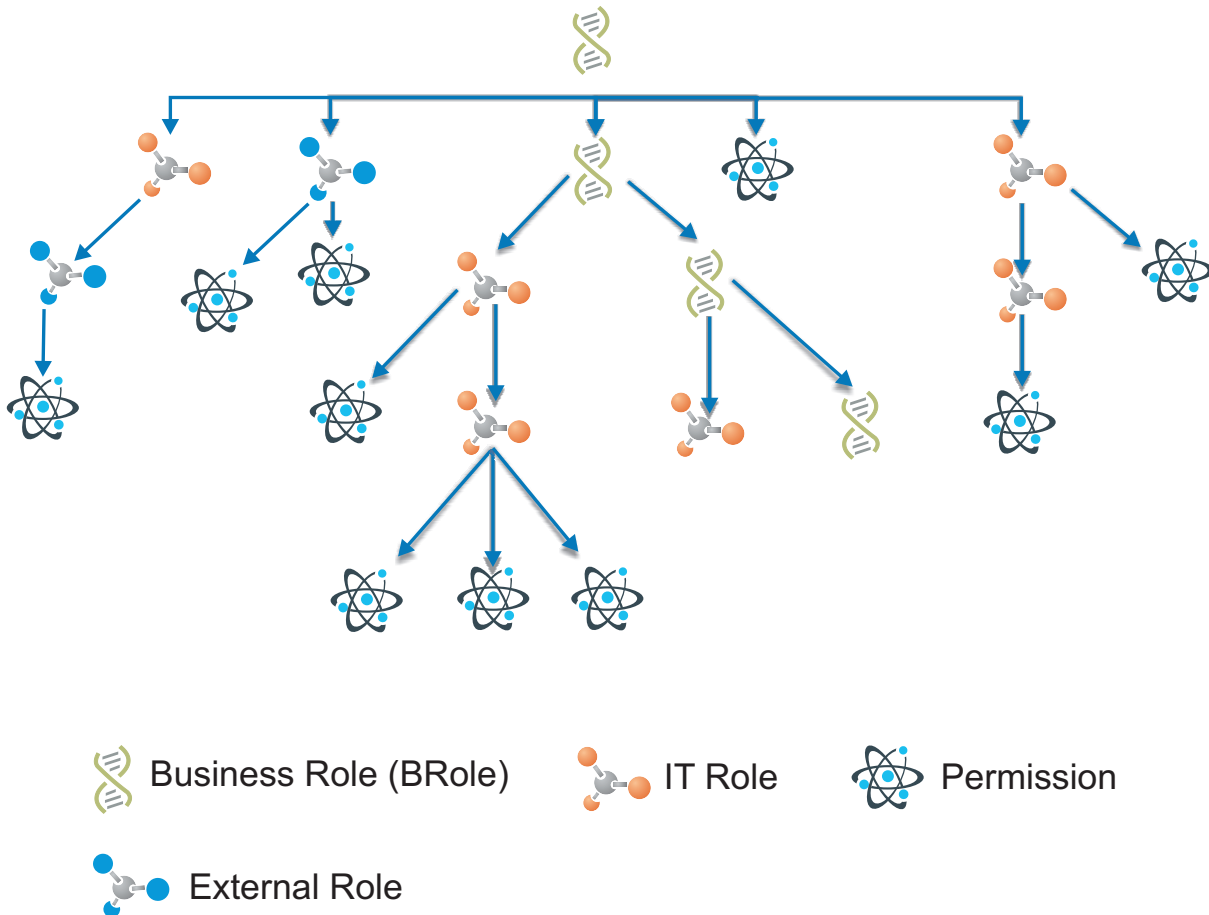


Figure 7. Structure of a generic entitlement

The IBM Security Identity Governance and Intelligence entitlements model does not limit the number of hierarchy levels.

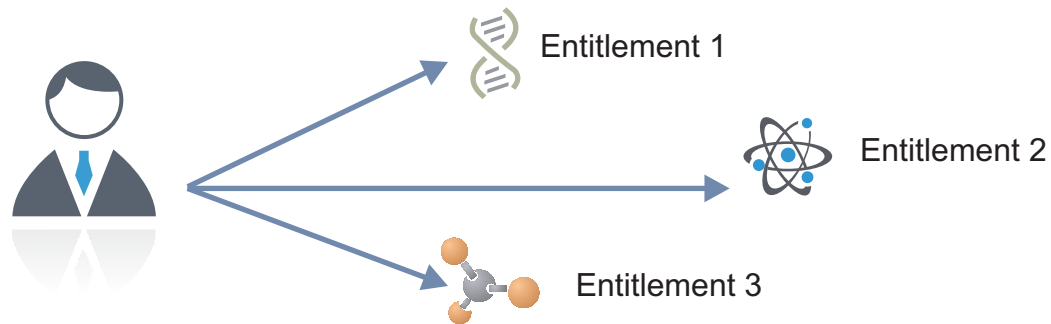
Permissions represent the basic elements on which authorizations are built. The permissions of an application are mapped with target system authorizations that are directly assigned to the users.

In IBM Security Identity Governance and Intelligence you can select  $N$  permissions that are filtered by an application in several sections. The IT Role object collects a set of permissions that are related to the same application.

You can have two types of scenarios.

- an entitlement that is assigned in a direct mode (direct assignment)
- an entitlement that is in a hierarchical structure (hierarchical assignment) is assigned in a hierarchical mode.

## Direct Assignment



## Hierarchical Assignment

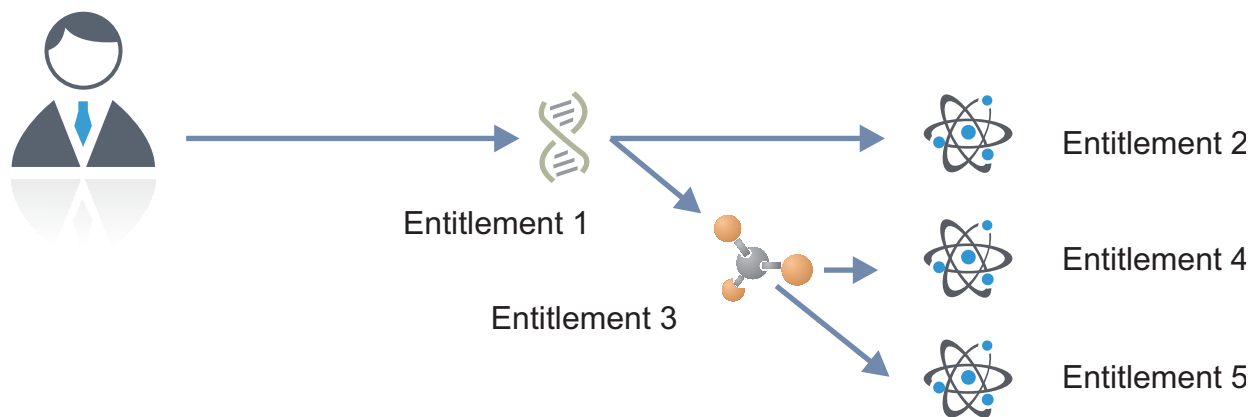


Figure 8. Direct and hierarchical assignment

If you assign the Entitlement 2 (Permission 2) to a user, you directly assign the Entitlement 2 only.

If you assign the Entitlement 1 (Business Role 1) to a user, you directly assign the Entitlement 1. Hierarchically, the user is assigned the Entitlements 2 - 5.

The permissions grouped in an external role are by definition handled by hierarchical assignment, since they cannot be granted individually.

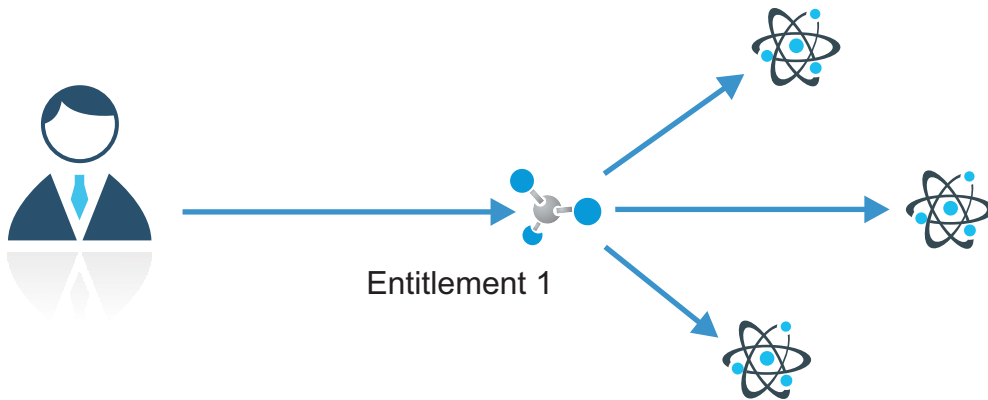


Figure 9. Hierarchical assignment for external roles

Before an entitlement is assigned, it must be published. An entitlement can be in the system, but is not available for assignment unless it is published.

## Employment and resources

When an entitlement is assigned to a user that belongs to a specific OU, it also defines the user's employment. By extension, if a user is assigned two or more entitlements, two or more employments are defined for the user.

Resources are entities that are needed for a user to perform business activities. The resources are assigned to employment definitions.

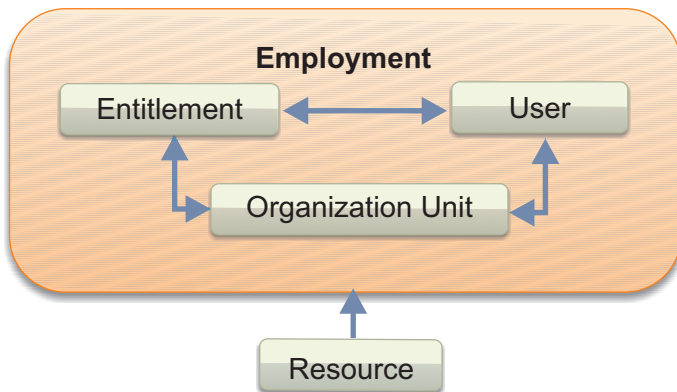


Figure 10. Employment and resources

Each employment can have any number or type of resources. The same resources can be assigned to different employments.

The use of resources considerably increases the flexibility and granularity for the definition of the IBM Security Identity Governance and Intelligence authorization profiles.

### Aggregation user - entitlement can be considered as the "first-level" of authorization

Two different Users (U1, U2) who are assigned the same Business Role (BR1), possess the same first level of authorization.

### Aggregation employment - resource can be considered as the "second-level" of authorization

Two different Users (U1, U2), are assigned the same business role (BR1)

and belong to the same OU. They are characterized by the same employment, although their operations can be differentiated by their resource.

As an example, consider a banking scenario where two employees are in two different branches, one in Rome and the other in Milan.

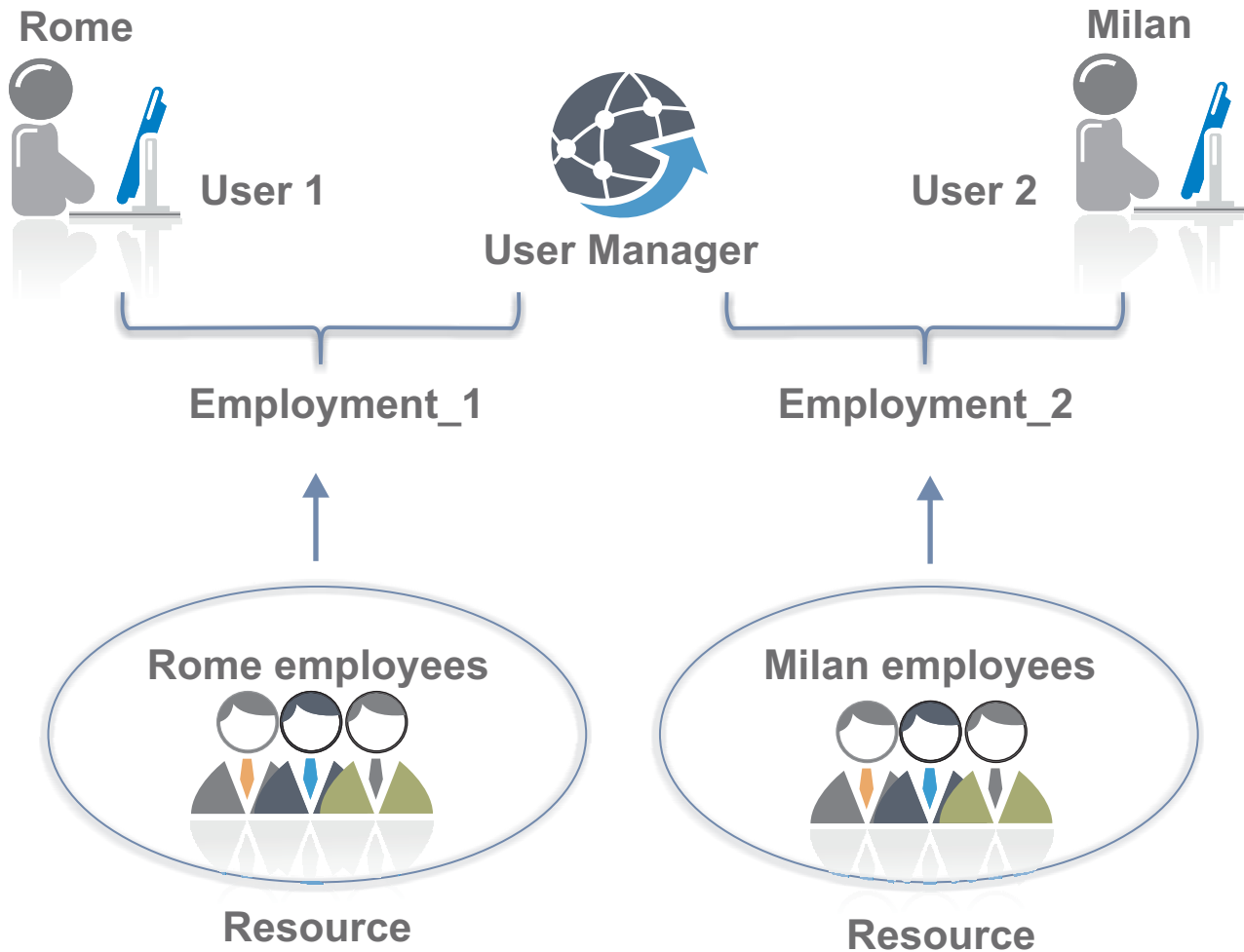


Figure 11. Second level of authorization

Holding the same role, they can access the same set of functions, but must obviously relate to the customers of their own respective branches. A customer resource that defines every customer through a current account number, differentiates the two users' operating environments, even if they hold the same role.

A resource can be connected to a user directly or by inheritance from the OU that it belongs to. Resources (objects in the RBAC model) are important for Authorization Server operations where unstructured data is the main part of the authorization process. Unstructured data can be network folders, files, or documents.

All the main entities of IBM Security Identity Governance and Intelligence model such as hierarchies, applications, roles, and risks are modeled as internal resources.

They are used to restrict administrator access rights to a subset of administered entities. The intersection of different subsets of resources defines the scope.

Two IBM Security Identity Governance and Intelligence administrators with the same basic authorizations with different scopes have different operational impacts inside the organization. For example, two user managers or two security officers can have different sets of assigned resources.

## Rights

Rights are extra attributes that are related to permissions.

A Right is defined by two qualifiers: **Key** and **Value**.

**Key** is an identifying name, while **Value** can be defined every time the right is defined.

**Value** can have a default value that can later be modified.

Rights can be either single-value or multi-value.

The following figure shows an example for a single-value right.

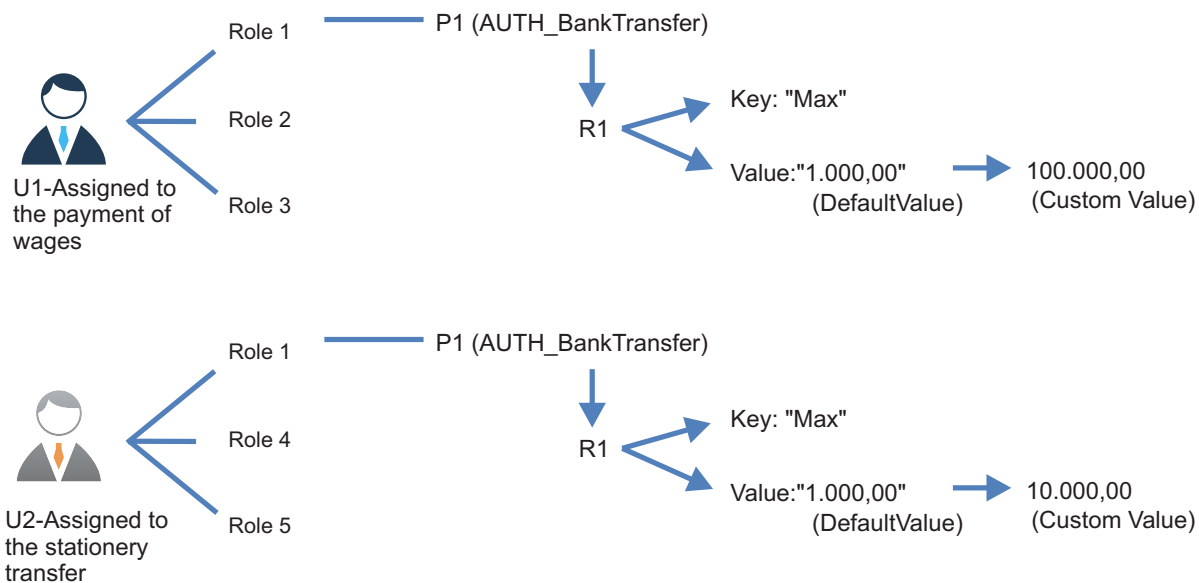


Figure 12. Single-value right

In this example, users U1 and U2 run different assignments. Both can make transactions (P1), as defined by the the Role1 business role assigned to them.

Assigning a right, R1, to permission, P1, you can define the range of values available for transactions of each user.

Both U1 and U2 have the same default value of \$1,000.00 as the lower boundary, but they have different upper boundaries.

U1 up to \$100,000.00



U2 up to \$10,000.00

The upper customized boundary value of R1 is defined when the permission is assigned to the user.

The following figure shows an example of a multi-value right.

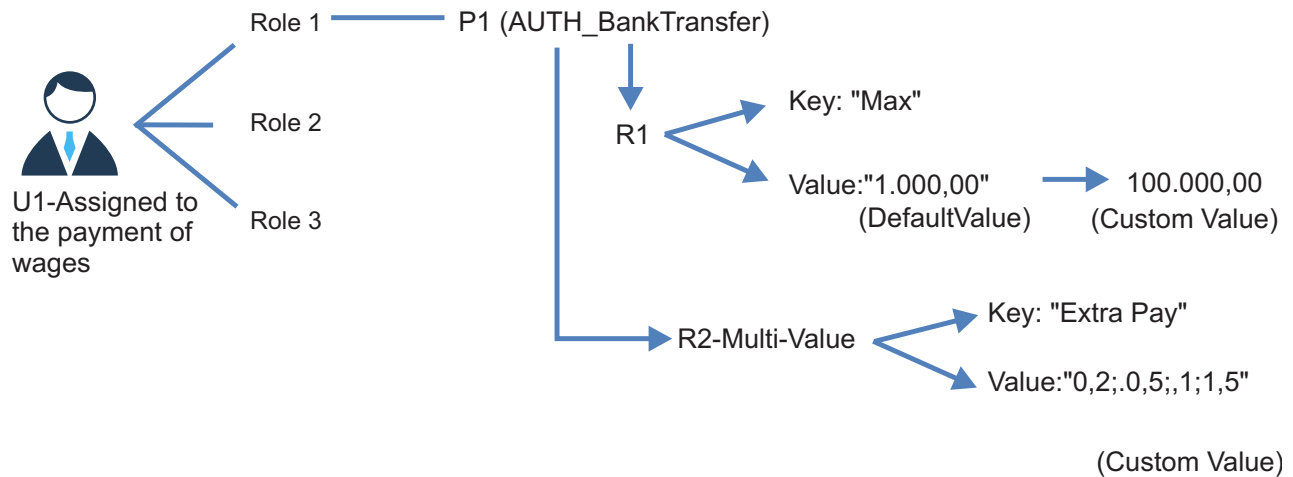


Figure 13. Multi-value right

User U1 is assigned to the payment of wages by rights R1 and R2. User U1 can modify the amount of wages for a worker according to a business policy named Extra Pay, the key of R2. The extra pay is a variable amount that is added according to the value of a multiplier, the R2 value. In the example, R2 has four possible values.

0,2 ; 0,5 ; 1 ; 1,5.

As the example shows, you can assign more than one single-value or multi-value right to the same permission.

You can choose from a predefined set of values by using **lookup**. These predefined values are assigned when a right is defined and added to a permission.

#### Lookup for a single-value right

You can choose only one value from the list of values.

#### Lookup for a multi-value right

You can choose one or more values from the list of values.

For more information about rights, see the following topics.

- Life-Cycle of a Right
- Rights and Resources

### The lifecycle of a right

The lifecycle of a right is based on three steps:

1. Define a right and add it to a permission:
  - a. Define a lookup table of values (optional): you can define multiple lookup tables, to represent different set of values. See **Access Governance Core > Configure > Rights Lookup**.

- b. Define a right joined to a permission (see **Access Governance Core > Manage > Application Access > Rights**).
2. Assign a right to a user.
3. After you assign a right to a user, the value of a right can be updated. See **Access Governance Core > Manage > Users > Rights**.

You can assign rights to a user in different modules of IBM Security Identity Governance and Intelligence:

Assignment	Modules
Assign a permission aggregated to a right.	Access Governance Core, Business Activity Mapping
Assign an entitlement that hosts a permission aggregated to a right.	Access Governance Core
Assign a one or more permissions to an activity.	Access Risk Controls
Assign a permission or entitlement through an authorization workflow.	Access Request
Assign a permission or entitlement through the rule engine.	Access Governance Core or any other business process triggered by a rule

## Rights and resources

It is important to understand the difference between rights and resources.

- A resource determines a second level of authorization for a specific entitlement.
- A right determines the set of values for a generic transaction that is enabled by a permission.

Returning to the example shown for resources, consider a banking scenario where two employees are in two different branches, one in Rome and the other in Milan. They have the same role and they can access the same set of functions but have different customer resources that are specific to the branches.

Add a permission, **Check Validation**. It has a single-value right, **Amount**, in which the value joined to the key can vary. The bank can provide a policy that uses a specific procedure to validate any check that exceeds a specified value.

Two employees with the same role who work on different customer resources with a specific permission that enables them to validate checks. Use the right added to the permission to enable different validation policies.

## Applications

In IBM Security Identity Governance and Intelligence, an application is a set of permissions that are related to a certain target. IBM Security Identity Governance and Intelligence visualizes and extends the concept of target as a "pure technical view" of an IT application and is only suitable for provisioning.

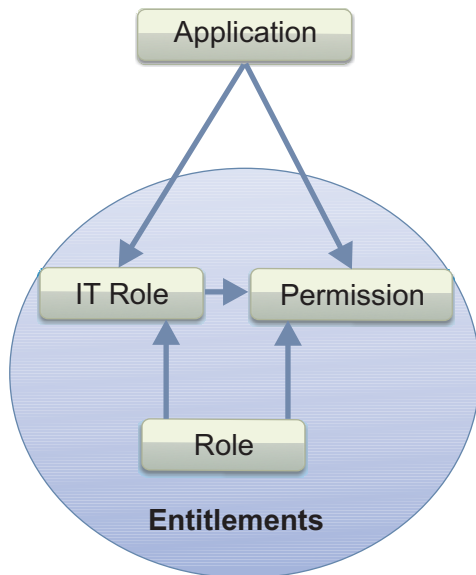


Figure 14. Application entitlements

Every target can host several applications. A target can be often used as an authentication or authorization server, for example Active Directory (AD), where different applications share different permissions with a single account.

Many applications that are connected to the same target can share account configuration policies and can be subject to several:

- Provisioning policies
- Logical configurations
- Risks

Applications, targets, and account policies, for example password policies or UID rules, are tied together. There can be one or more targets to an application, or one or more accounts to a target, or one or more accounts to an application. The IBM Security Identity Governance and Intelligence model manages the policies that are implied in these relations. For example, password synchronization between different targets that share an account policy.

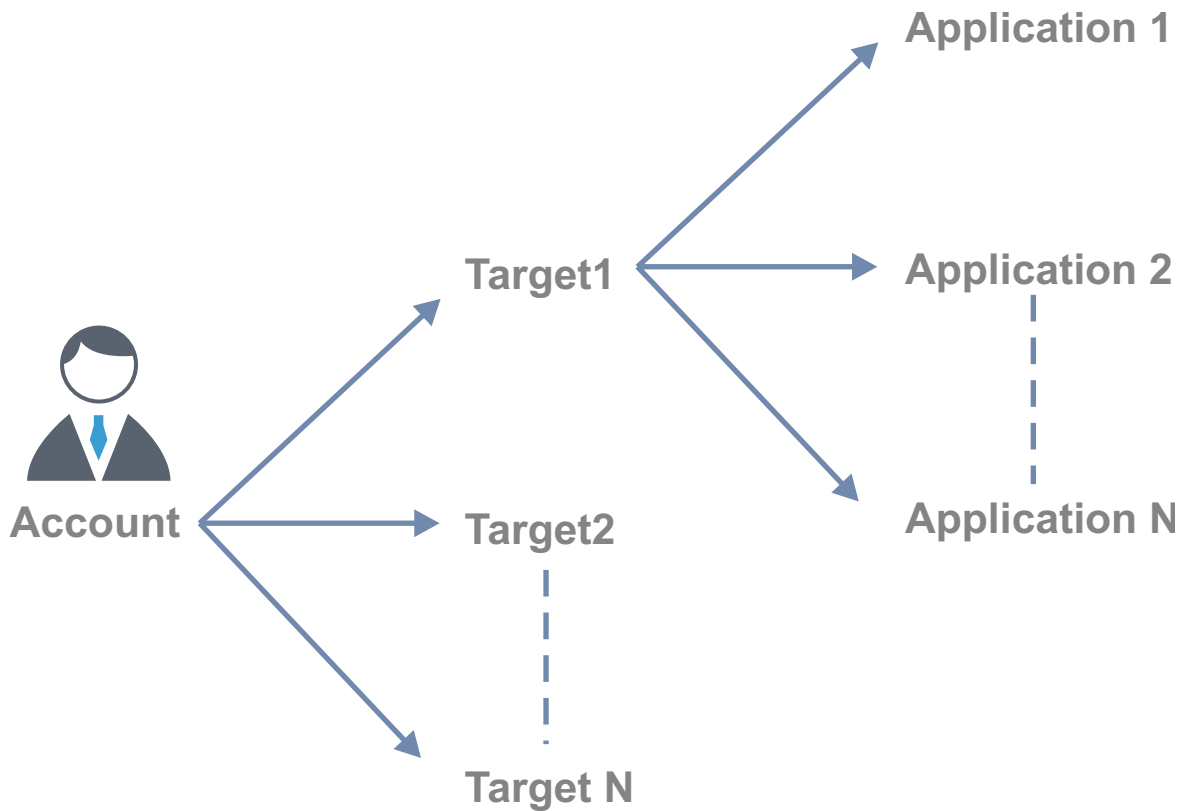


Figure 15. Accounts, targets, and applications

Applications can be either:

**Custom**

These applications use Java API or the web services of IBM Security Identity Governance and Intelligence platform, the IBM Security Identity Governance and Intelligence SDK, for authentication or authorization activities. For this type, the AG Core module operates as the authorization server.

**External**

These applications use external authorization systems that are connected to the AG Core module.

For example, Active Directory (AD) is an external authorization system or target system.

IBM Security Identity Governance and Intelligence can be also configured to send events, such as add or remove permissions, to targets or applications. These events are sent through the IBM Security Identity Governance and Intelligence Integration Interface and Enterprise Connectors module.

**Accounts**

In the IBM Security Identity Governance and Intelligence data model, a user can be added to a specific account.

An account is the IT representation of an identity, expressed through an account configuration, made-up by a set of user information such as UID, email, password, and status. An account configuration is used by an application that requires authentication of the user.

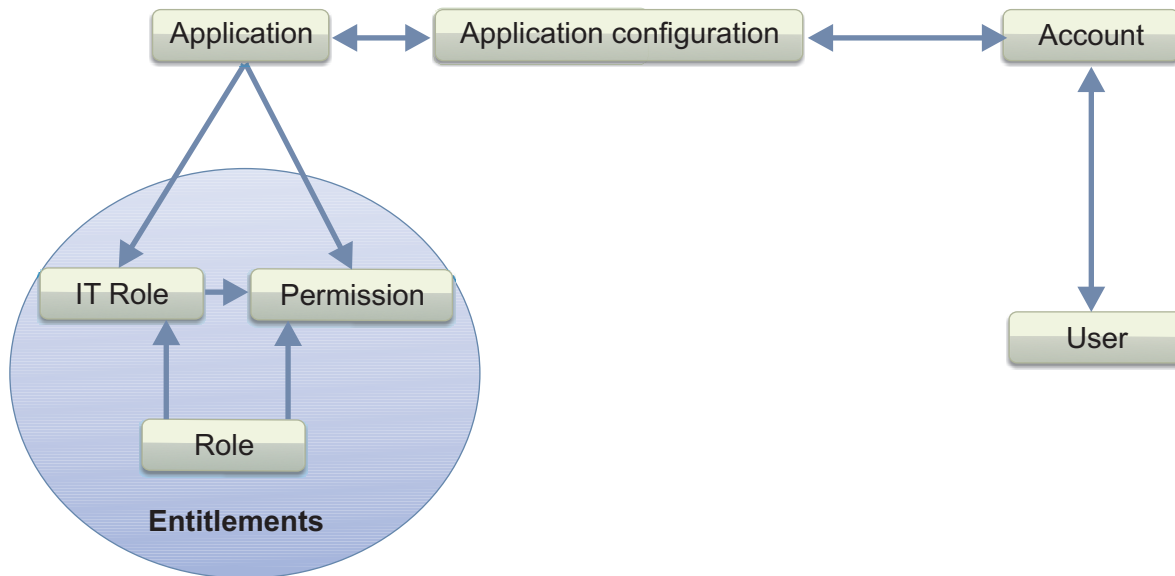


Figure 16. Application and account relationship

Several users can be associated with the same account configuration and use the same authentication rules for the same application.

Account configurations are used to define account properties; in particular, password settings.

In IBM Security Identity Governance and Intelligence, multiple accounts can be assigned to a single user. The user can manage different passwords and lock status for each application.

Every user that is registered in the IBM Security Identity Governance and Intelligence platform is automatically added to the IBM Security Identity Governance and Intelligence account configuration.

**Note:** In IBM Security Identity Governance and Intelligence, entitlements are tied to users rather than to accounts. A role is assigned to a user and cannot be assigned to an account because a role can contain permissions for different applications that are related to different accounts.

---

## IBM Security Identity Governance and Intelligence extended data model

The IBM Security Identity Governance and Intelligence extended data model supports the risk definition and detection layer of IBM Security Identity Governance and Intelligence.

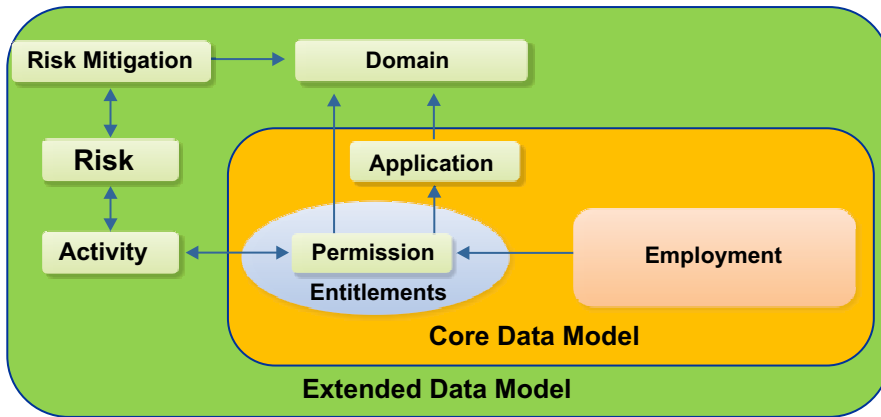


Figure 17. IBM Security Identity Governance and Intelligence extended data model

The Access Risk Controls (ARC) module manages this layer based on two relationships.

- The relation between the business activities model and the RBAC model.
- The relation between risks and business activities.



Figure 18. IBM Security Identity Governance and Intelligence extended data model - subsystem risk, activity, and permission

IBM Security Identity Governance and Intelligence extended data model has these main model elements:

- Business Activities Layer and RBAC Model
- Risk Definition and Detection
- Segregation of Duties
- Risk Mitigation
- Mitigation Actions
- Domains
- The Risk's Hierarchy

## Business activities model and RBAC model

IBM Security Identity Governance and Intelligence integrates and correlates the business activities model of an organization and the RBAC model that IBM Security Identity Governance and Intelligence is based on.

Business activity is an innovative key concept for modeling a specific task or set of tasks by defining a specific part of a generic business process. A process can be structured as a set of activities.

An activity identifies an operation or a uniform set of operations that the user can perform.

A generic business process is structured through a set of activities. Each activity can be subdivided into subactivities. Multiple activities can be grouped to form a macro-activity. An activity hierarchy is defined and organized as a tree structure, an activity tree.

Each activity requires one or more entitlements. An entitlement is the permission that a user needs to perform the activity.

In the RBAC model, a role is a particular type of entitlement that can be assigned to a user. The role and can have multiple permissions that are arranged in a hierarchy.

By linking the business model to the RBAC model, each activity can be aggregated to the necessary entitlements or permissions.

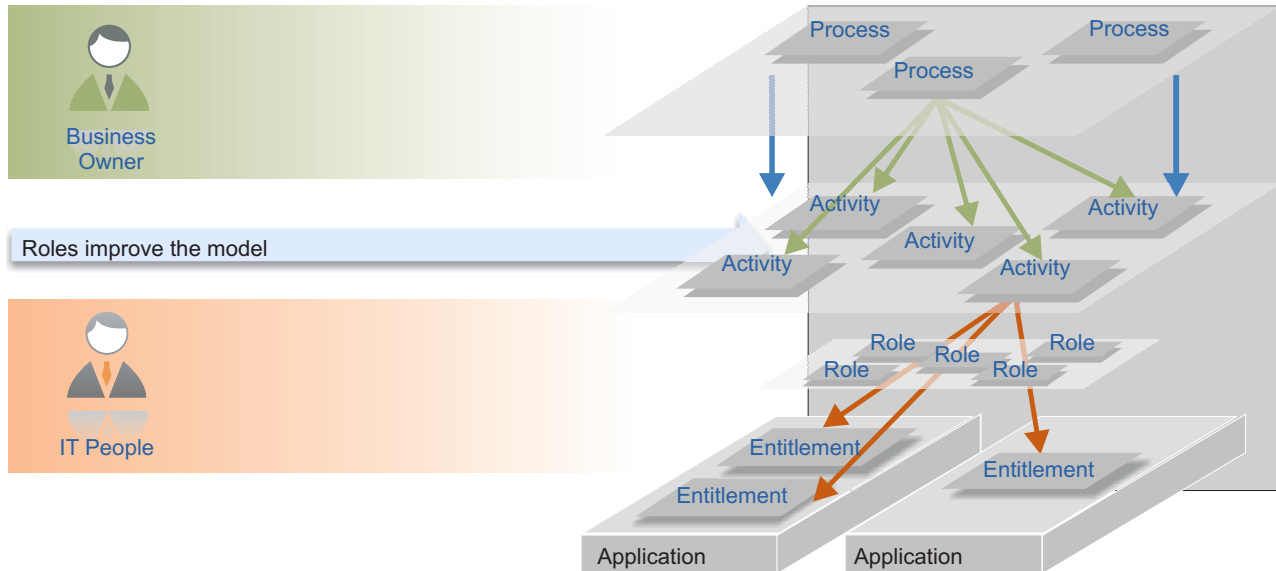


Figure 19. Business model linked to the RBAC model

## Risk definition and detection in IBM Security Identity Governance and Intelligence

Risk is a wide range of possible critical situations that can be associated with a generic business activity.

In the IBM Security Identity Governance and Intelligence data model, a specific business activity can be associated with a risk.

This information is used to evaluate the "aggregated risk" of the set of activities that are assigned to a user.

Consider a financial management activity and an ICT technical activity. Typically, these types of activities require specialized and extensive knowledge.

Is it reasonable to entrust these activities to the same user?

From an organizational standpoint, depending on the user's prevalent competency, either financial or technical, there is a valid risk in assigning these two unrelated activities to a single user. An activity such as financial management can be considered sensitive even if it is not part of a set of activities. It makes sense to associate a risk evaluation to a single activity.

Generally, possible aggregations are of the following type:

- A risk to a single activity
- A risk to a single set of at-risk or conflicting activities
- Multiple risk to a single activity
- Multiple risk to a single set of at-risk or conflicting activities

According to this information, it is possible to evaluate the aggregated risk of the set of activities that are assigned to a user.

The ARC module extends features of the RBAC model by introducing the concept of at-risk activities and provides the tools necessary to link activities to entitlements or permissions.

The assessment of the risk level of activities can be translated into the risk level of entitlements or permissions that are assigned to users involved in those activities.

The following figure shows all the IBM Security Identity Governance and Intelligence extended data model elements that are involved in the risk definition and detection layer.

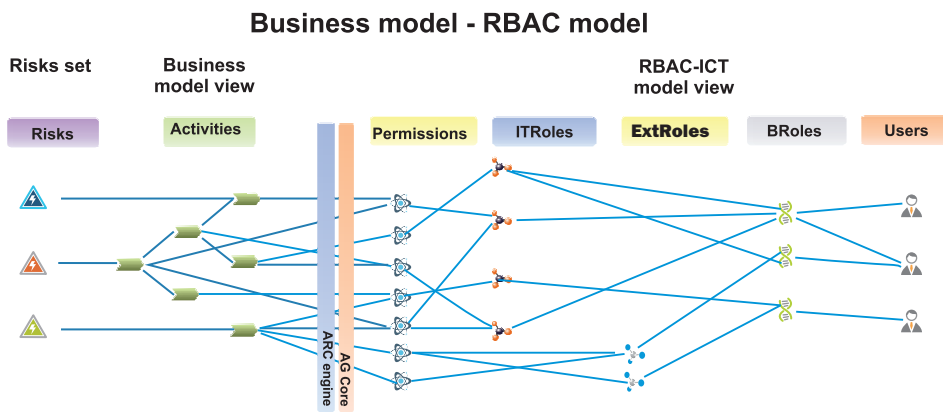


Figure 20. ARC engine and AG Core: Business Model - RBAC Model

The figure shows an example with few elements.

In a generic large organization, you might find:

- Permissions (>200,000)
- IT roles (>100,000)
- External roles (>15000)
- Business roles (>1000 and <5000)
- Business activities (<500).

In a large organization, the number of business activities is drastically lower than roles and permissions.

The advantage of defining risks as activity-driven is clear. By using the assessment of risk that is associated with activities, conflicts among permissions or entitlements can be traced. Conflicts among roles are easier to trace. They are less complex because the number of activities is lower than the number of permissions or BRoles.



## Segregation of Duties (SoD): a specific type of Risk

It is important to prevent members of an organization from gaining operational privileges that might cause conflicts of interest that can be detrimental to the organization.

You must establish constraints when you assign entitlements to users.

Segregation of duty (SoD) mechanisms are designed to manage conflicting relationships between certain model entities. Entities that are characterized by reciprocal conflict, cannot be aggregated to the same user.

IBM Security Identity Governance and Intelligence data model identifies a SoD risk as a specific type of risk. Most of the existing models for SoD show that conflicts are defined based on permissions and roles.

Defining conflicting roles can lead to inconsistent results.

For example, an organization has three roles, R1, R2, and R3. Two of these roles, R1 and R2, are defined as conflicting.

If R2 and R3 are built with the same permissions, then both pairs (R1, R2) and (R1, R3) would give the user access to conflicting permissions. Basically R2 is equivalent to R3, even though, by definition, only the pair (R1, R2) can be considered as conflicting roles.

According to the RBAC model, roles are containers of groups of permissions; the user's actual operating capacity depends on the permissions that define the operational characteristics of a role.

In the previous example, one method is to redefine the conflicting permissions. The conflict between roles is caused by the conflicting permissions.

In large organizations, IT systems can register hundreds of thousands of permissions. Redefining permissions is impractical.

The ARC module offers a different approach that reduces the complexity of the problem. An SoD is defined by activities. An SoD risk arises when a specific set of activities is performed.

There is also the option of managing External SoD, based on risk information provided directly by an external system.

## External SoD

In some situations, it is possible to read risk information raised on a given user from an external target system.

This action proceed through a **ReST** web service or a specific **Java class** that transforms the data from the target system in a consistent IGI format.

The risk detected, related to users registered into IGI database, is shown in the same way as the "internal SoD" information.

However, internal/external SoD are two options mutually exclusive and you can set it from **Access Governance Core > Settings > General** panel of **Access Governance Core** module.

When you use External SoD, some functions are not effective because External SoD is not associated with some elements of IGI data model.

Generally, any type of function that involves the management of risk mitigation is not relevant when External SoD is set.

The following functions might be available through the User Interface, but they do not provide relevant results when you set the External SoD:

- Associate mitigation to SoD Risks. See **Access Risk Controls > Manage > Mitigation Controls > Applicable Risks > Actions > Add** or any functions in **Access Risk Controls**.
- Configure a campaign of type **Risk Violation Mitigation**. See **Access Governance Core > Configure > Certification Campaigns > Actions > Add**.
- Run certification campaigns of type **Risk Violation Mitigation**. See **Access Certifier**.
- Run a specific subset of reports. See the official list of available reports.

## Risk mitigation: classes of mitigation

You can reduce risks by preventing users from performing activities that conflict with each other.

Sometimes in a business situation, users must be able to work despite the presence of an SoD conflict or other types of risk.

For example, a user that is covering for another employee, who is on holiday, needs to gain access to a particular repository of the company. A risk violation review detects a conflict and denies the user access to the repository.

If the SoD requirements are strictly observed, the data in this repository is inaccessible, and the user cannot perform the functions of the absent employee. The company loses productivity and in some cases, more than an SoD violation can be generated.

You can use a mitigation control policy to resolve this situation.

Mitigation control is a policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

The user can access the restricted repository, if a mitigation control that provides a complete and in-depth trace of the user's activity on the repository, is activated.

This solution:

- Does not nullify the SoD or other type of risk constraints that arise from the conflict analysis.
- Enables the user to perform work activities.

Mitigation Control is not a workaround to evade the SoD or other types of risk requirements. Rather, it is an added control that enables the user to perform some needed tasks during a transitory but critical time period. You can aggregate a mitigation control to a user for an indefinite time period. A user can have *N* aggregated mitigation controls.

The same user can be involved in a set of risks or conflicting activities.

You can aggregate mitigation controls in a number of ways:

- A single mitigation control with a single set of risks or conflicting activities
- A single mitigation control with a subset of a set of risks or conflicting activities
- More than one mitigation control that is aggregated to a single set of risks or conflicting activities - over mitigation
- Sets of conflicting activities that are not aggregated to any mitigation control - under mitigation
- A mitigation control that is not aggregated to any activity.

It is common to have different sets of risk activities, where every set can be characterized by a specific risk. A user that is involved in a specific set of activities, is exposed to the related risks.

For every specific risk, several mitigation controls are available and every set of risk activities can be aggregated to more than one risk.

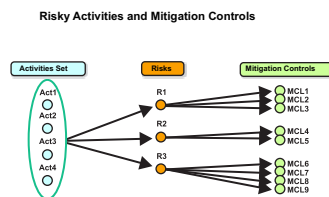


Figure 21. Risk activities and mitigation controls

The following figure displays a simple case, where every set of risk or conflicting activities is composed of two activities only.

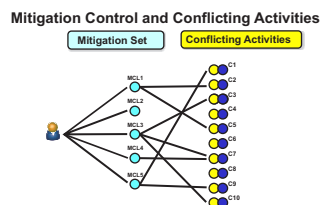


Figure 22. Mitigation model

MCL4 is aggregated to C7 only.

Mitigation control MCL1 is aggregated to C2 and C5; MCL3 to C3, C7, and C10; and MCL5 to C1 and C9.

C7 is aggregated to MCL3 and MCL4.

C4, C6, and C8 are not aggregated to any mitigation control.

The following references describe the four classes of mitigation:

- Under Mitigation
- Over Mitigation
- Under/Over Mitigation
- Complete Mitigation

## Under mitigation

Under mitigation occurs if an MCL is not aggregated to the conflicting activities, as shown for C3 in the following figure:

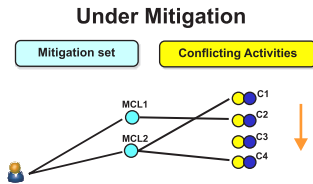


Figure 23. Under mitigation model

## Over mitigation

Over mitigation occurs if the mitigation control MCL3 is aggregated to C5 only, as shown in the following figure:

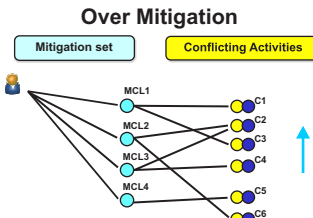


Figure 24. Over mitigation model

MCL2 and MCL3 are aggregated to the same pairs of risking/conflicting activities. So, in this case the aggregation arrow MCL3-C2 can be deleted.

## Under-over mitigation

Under-over mitigation occurs if an MCL is not aggregated to some of the conflicting activities and one or more MCLs are aggregated to the same activities, as shown in the following figure:

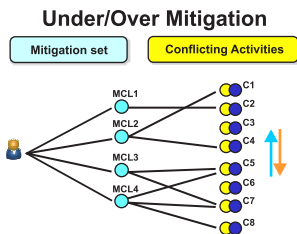


Figure 25. Under-over mitigation model

C3 and C6 do not have any MCL aggregated, while MCL3 and MCL4 are aggregated to the C5 and C7.

## Complete mitigation

Complete mitigation occurs if every set of risk or conflicting activities is covered by at least one mitigation, as shown in the following figure:

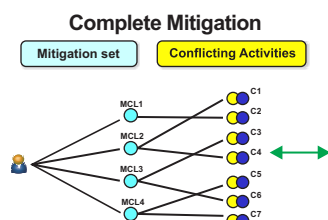


Figure 26. Complete mitigation model

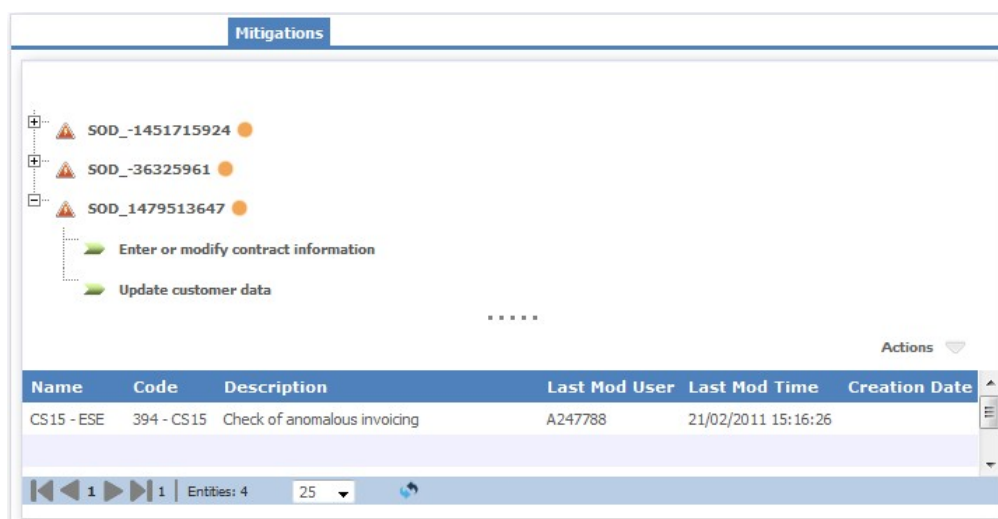
## Mitigation Actions

Segregation of Duties (SoD) a particular type of Risk

In IBM Security Identity Governance it is possible to define Mitigation actions, according to the Risk management needs related to a User.

The first step is to deploy a Mitigation and join it a specific Risk (see ARC module, **Manage > Mitigation Controls > Actions menu > Add**).

Thus, through two modules of IBM Security Identity Governance, ARC and AGC, will be possible to join a Mitigation to a User, through the **Mitigations** tab, shown below:



### Mitigation GUI

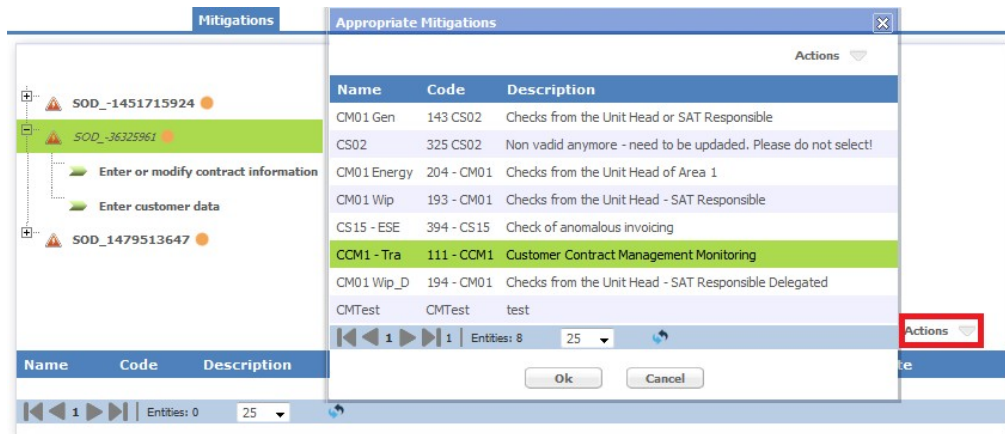
In the upper part of the GUI are listed the Risk joined to a User.

In the lower part are listed the Mitigations already assigned to the User.

In this sample, the Mitigation **CS15 - ESE**, is already assigned to the User but not is joined to any of the Risks shown in the GUI; so, we say the the User is in a situation of Over Mitigation. Remove a useless action of mitigation is not mandatory, but can be considered a "best practice".

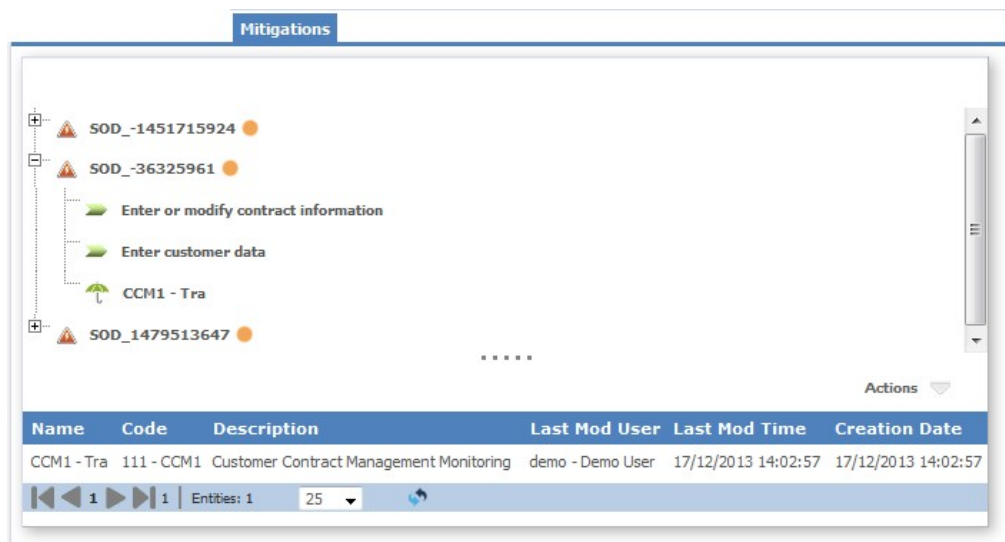
A generic Risk it is characterized by any set of risky Activities; in the sample, a Risk defined by only two Activities.

After the selection of a Risk, from the **Actions** menu , will be possible to add/remove a Mitigation (**Add/Remove** button):



Mitigation GUI: add a Mitigation to a selected Risk

The Mitigation just added, useful to mitigate the Risk **SOD\_-36325961**, is shown in the Risk tree with a green umbrella icon and is listed in the lower side of the GUI:



Mitigation GUI: added Risk

## Domains: conflicting and risk activities

A domain is a set of data that is subject to conflict analysis.

Domains are used to separate an enterprise into logically separate business areas.

It can coincide with the entire set of model data or with a single subset.

The data domain is used by the ARC module to implement a "correlation" between the activities a conflict analysis is required for.

Consider for example, the case of the two activities A1 and A2:

- A1: Payment of suppliers
- A2: Quality control of goods that are purchased by suppliers

To avoid a potential conflict of interest, these activities must not be completed by the same user.

Assume that activity A1 is performed by a user in relation to stationary goods in a certain OU within the company. The same user is authorized to complete activity A2 relating to raw materials used for the production processes of the OU. For example, PVC sheets that are used to produce molded plastic utensils.

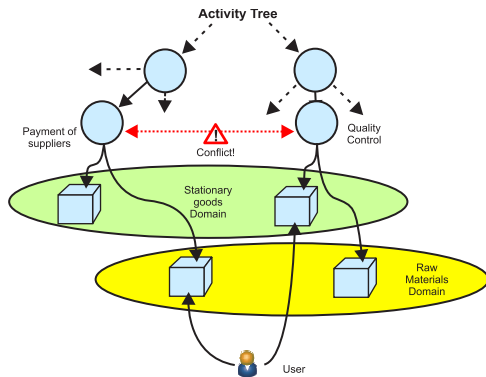


Figure 27. Data domains

The analysis of conflicts is performed where it is logical to perform it, where the two activities can occur on the same data domain.

You must contextualize the meaning of activities A1 and A2 by introducing two different domains, stationary goods and raw materials. Using two domains neutralizes the conflict between activities A1 and A2 for the user.

In the ARC model, a data domain is identified as a set of data on which various applications can operate. A domain can be identified by a set of applications. However, an application can be contained in various domains. Suppose that each application has only one corresponding permission. By using the ARC module, it is possible to aggregate applications with domains by using the link between applications and permissions. Permissions are in turn related to the domains.

The following figure shows a qualitative example of the description:

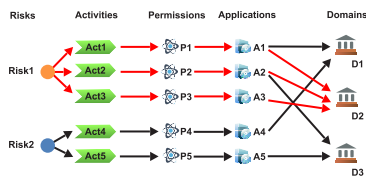


Figure 28. Activities, permissions, and domains

Assume that two risks exist: Risk1 and Risk2.

Risk1 arises if a generic user runs all of the three activities: Act 1, Act 2, and Act 3.

The same occurs for Risk 2 joined to activities: Act 4 and Act 5.

In this example, the five activities are linked to the five permissions P1, P2, P3, P4, and P5. These five permissions are linked 1:1 to five applications A1, A2, A3, A4, and A5.

The red arrows indicate that activities Act 1, Act 2, and Act 3 need permissions P1, P2, and P3 that link to application A1, A2, and A3. These three applications are hosted on Domain D2.

Risk1 falls into D2 and any user that performs Act1, Act2 and Act3 is considered as a risk user in that domain.

A user who performs activities Act 4 and Act 5 is not considered a risk user because those permissions and applications are linked to different domains D1 and D3. Risk 2 is neutralized.

## How to read the tree of the risks of a user

The **Risk Info** graphical user interface (GUI) hosts an expandable tree structure.

At the root level, **Level 0**, you find one or more domains at the same level. 🏠

Expanding the **Domain** node, you can find one or more risks at **Level 1**.

Risks are divided into two categories:

- 🔥 **SOD risk**
- 🏢 **Generic risk**

Every risk is characterized by a specific risk level:

- 🔴 High
- 🟠 Medium
- 🔵 Low

For every risk at **Level 2**, you find at least one set of risky activities. ➡

For every activity at **Level 3**, all of the entitlements that are associated with that activity are listed.

For any generic couple, **Activity 1 - Activity 2** for example, that consists of conflicting, or risky, activities, every **Activity 1** entitlement conflicts with every **Activity 2** entitlement.

A mitigating action, indicated by the presence of the following icon, is provided for a risky activity or for a couple of conflicting activities: 🌂

One or more mitigations can be provided for each risk.



---

## Introduction to rules engine

IBM Security Identity Governance and Intelligence platform implements a complete model of a generic organization, containing:

- All entities that are registered in the organization such as users, applications, and roles
- Links and relationships between these entities
- Sets of application policies and processes that the organization uses to manage these entities such as automatic creation of a company email account for a new user or employee.

To cater to different organizations, the IBM Security Identity Governance and Intelligence platform needs to be structured in the following manner.

- With a robust data model, to manage common and standard authorization paradigms
- With a flexible engine to construct business policies that cover different situations in various organizations, ones that vary throughout the lifecycle of an organization.

IBM Security Identity Governance and Intelligence adopts a solution that delegates business policy definition to a specific module, the rules engine (RE).

Rules can be used in different situations, which in IBM Security Identity Governance, represents a layer of intelligence that enhances the expressive nature of the data model. The RE guarantees the flexibility and expressive strength that is required to model the customization of all company processes, especially those processes that are subject to frequent change.

The RE applies rules to available data to manage customized mechanisms for the various organizations.

In the current version, rules are available in these modules:

- The AG Core module
- The Process Designer module
- The Enterprise Connectors module
- The Access Risk Controls for SAP module

To access the Rules section in the modules Access Governance Core, Process Designer and Access Risk Control for SAP, from the tabs bar of any UI module, select **Configure > Rules**.

To access the Rules sections in the Enterprise Connectors module, from the tabs bar select **Manage > Connectors > Channels**.

The rules are managed in the following sections.

- Pre mapping rules
- Post mapping rules
- Response rules

## Drools rules engine

A rules engine (RE) is a module that automates the management of certain highly variable processes. The fundamental concept consists of separating the objects that are involved in processes from the logic that implements those processes.

The logic is defined by writing rules. For each process, the RE recognizes which rules to apply and on which objects to operate. If there is a variation in the logic, the rules can be changed without having to intervene in the system architecture. The IBM Security Identity Governance and Intelligence framework uses the open source Drools Rules Engine ([www.jboss.org/drools](http://www.jboss.org/drools)), which enables the properties and advantages mentioned.

### Introduction to Drools

You must understand the fundamental characteristics of Drools to understand the rest of the manual. Drools has its own syntax for writing rules in a declarative, concise, and unambiguous format. A rule has the following structure:

```
when
conditions
then
actions
```

The *conditions* are edited according to certain rules of Drools syntax. According to this syntax, setting up a condition means verifying a deed.

The context in which the rules are applied is characterized by a group of deeds. All these deeds, which describe the present situation in which the RE operates, are asserted in a working memory.

To understand whether to apply a rule, the RE verifies whether a deed was effectively asserted in the working memory. If it has, then the rule is applied.

The *actions* area is edited in normal Java code and contains the actions to perform if the conditions are verified. The rules that are to be applied are contained in a production memory. The RE compares the actions that are hypothesized in the rules in the Production Memory with those deeds that are asserted in the working memory. If there is a compatibility, the RE executes one or more rules.

**Note:** The *conditions* wording that is normally adopted in the Drools documentation can be misleading.

This area is only declared when the rule is applied. The rule is applied only if the presupposed actions are effectively asserted in the working memory.

Conditions that determine the context-based effect of rules are normally set up in the *actions* area. These conditions can hypothesize on deeds present in the working memory.

The deeds asserted in the working memory represent the situation under examination. Architecturally, a deed can be the presence of an event, a user or both, in the working memory.

## Elements of Drools syntax

You must understand the essential syntax notions. Setting up a condition according to Drools is equivalent to presupposing a deed. A deed is represented as an object in the working memory. If the object is found, the deed is asserted, and an action can be performed.

To presuppose the presence of an object, you must state it in the *conditions* area of the rule. If a user wants to verify the presence of a UserBean:

```
UserBean()
```

A variable that supports the potential object that is found can be declared as follows:

```
user : UserBean()
```

Thus, if a user bean is found, it is supported by the user variable. The variables that are declared as such, are local, that is, they have limited visibility to the Rule. Object searches can be filtered according to their attributes.

To verify the UserBean Name=James, write:

```
UserBean ( name == James )
```

This syntax is admitted only if a method exists to read the attribute **getName()**.

Starting from the attribute name, Drools can go back to the corresponding method and use it to extract the value of the object that is found. If the extracted value coincides with the presupposed value, Drools proceeds with the action. Attributes of the object that is found can be supported in local variables, which are stated in brackets:

```
UserBean ( username : name )
```

The name of the user that is found is supported in the local variable *username*. Lastly, the Drools function **eval**, which considers a Boolean expression that is written in Java language, is often used:

```
user : UserBean()  
eval ( user.getName() == James )
```

Conditions can be written by using normal Java, if necessary.

**Note:** In the *conditions* area of the standard rules that is provided by the AG Core, only a group of beans are declared without using conditions on the bean attributes or the **eval** function.

All other types of conditions are set in the *actions* area with a normal Java IF construct. Each loaded rule, in the presence of the requested bean, is always applied. Programmers, however, are free to use their preferred strategy to set the conditions of the written rules.

The *actions* area is written in Java code. Programming in Java requires knowledge of all the classes necessary for implementing the actions.

In particular, the following two types of classes are used to write rules for IBM Security Identity Governance and Intelligence.

**Beans** Beans represent the objects that are managed by the AG Core.

**Actions**

Actions represent the actions that can be executed on these objects through the AG Core administration module.

For example, an instance of the UserBean class can represent a user.

This instance has attributes that contain data of the user that it represents. The possible actions on the users are represented in the methods of the UserAction class.

If a corresponding action class is not defined for an object, no actions are expected on that object. The get and set method types are responsible for reading and modifying attributes of the corresponding bean.

Each rule has objects that are available in the working memory only. The Action methods can be applied on these objects only.

---

## IBM Security Identity Governance and Intelligence integration interface

As a centralized RBAC repository for IBM Security Identity Governance and Intelligence platform authorizations, the AG Core must be integrated with an organization's previous architecture. Typically, in such pre-existing architectures, the available repositories that contain users' personal information and authorizations are not well-formed RBAC repositories.

The AG Core thus interacts with the surrounding environment in various ways:

**AG Core Administration Module**

Through the administration module, all main aspects of an organization can be described and translated to the IBM Security Identity Governance and Intelligence data model.

**Provisioning**

The AG Core can interface with a provisioning module that integrates a component for authorization workflow management.

**Batch** A batch is group of procedures for bulk data loading and realignment.

**External Repository**

An external repository is a generic repository for data that must be kept aligned with data in the AG Core. By maintaining data alignment, the AG Core can propagate authorizations to other systems.

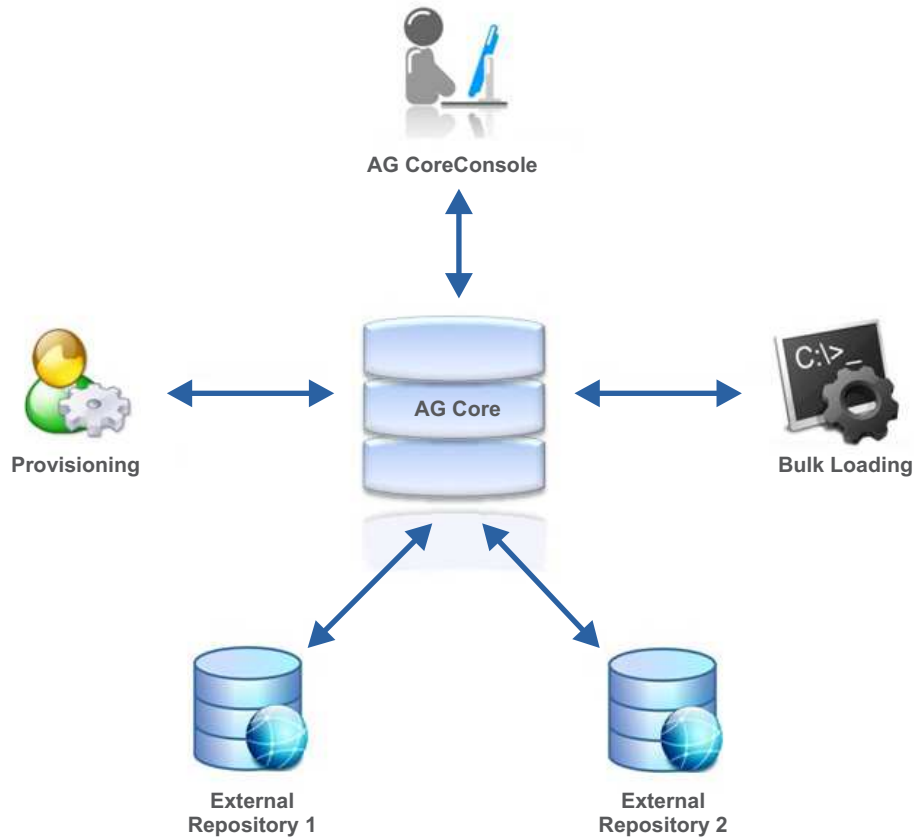


Figure 29. AG Core integration

The external repositories connect to the AG Core through a dedicated integration interface (II). Any number of external repositories can connect through this interface.

A flexible interface synchronizes and aligns the AG Core with the external repositories.

AG Core interacts with two types of repositories:

- Personal data repository
- Authorization repository

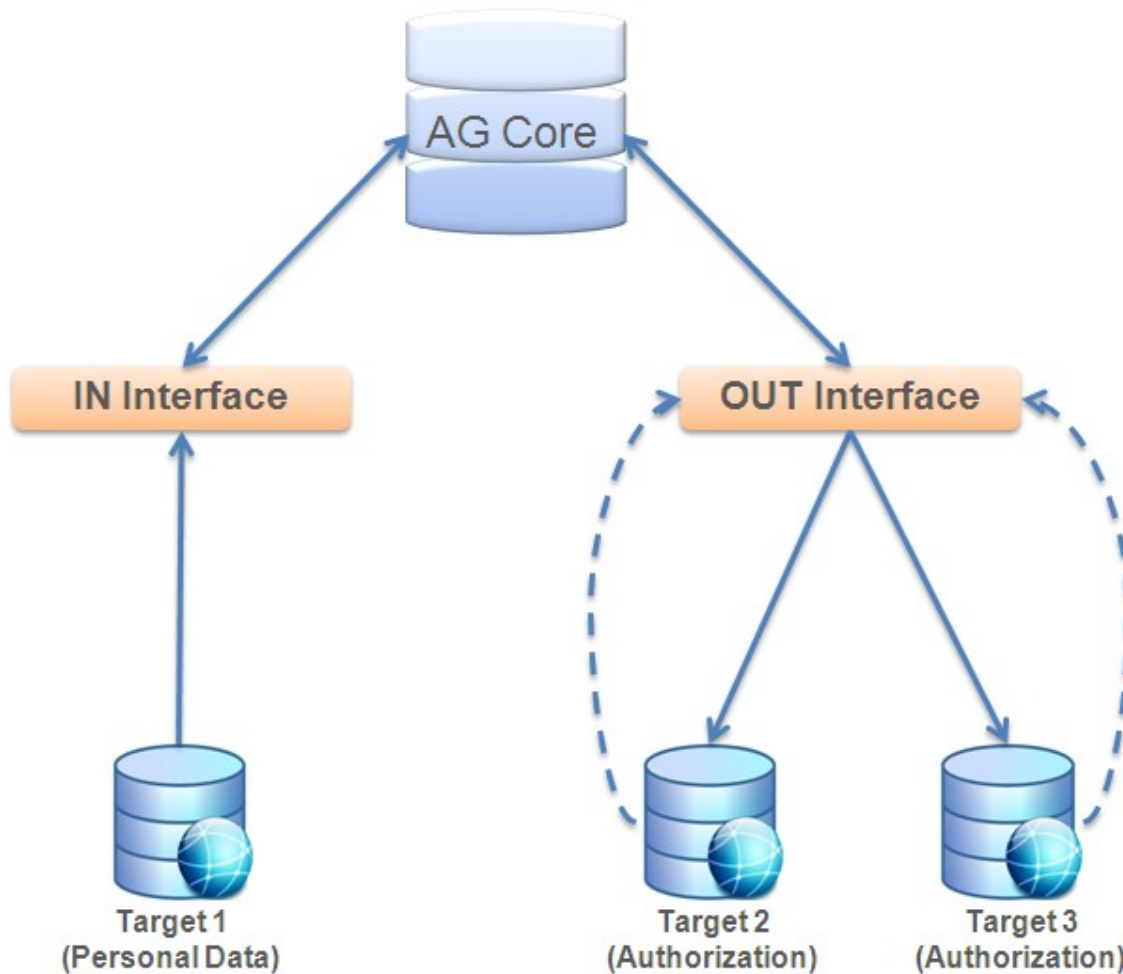


Figure 30. Types of external repositories

The basic framework has an input interface that passes information from personal data systems to the AG Core. Through the output interface, the AG Core transmits authorization information to the target systems. Any number of target systems can be connected to both the input and the output. The interface distinctly manages communication with each of them.

## Brief introduction to events

The integration interface (II) synchronizes and aligns the data in the AG Core database with the data in the target systems.

Events play a key role in synchronization management. An event is a brief yet complete description of interaction between any of the architecture's parts and any one of its elements.

Usually, the AG Core itself or the target systems generate events. Each time a system acts on the data, the executed changes are copied into appropriate packages, events, which are then sent to inform the other "listening" systems about the action.

Events are contained in appropriate event tables that are integral parts of the interface that is used to communicate with the target systems. The AG Core always communicates with the interface through events.

The target system that is connected through the input interface communicates each change that is made to its data. The interface then works to create an event with the required alignment information and transmits it to the AG Core.

The AG Core itself changes the data, creates the corresponding events, and transmits them to the output interface that is connected to the respective target systems.

For each event, a state attribute is always set and indicates the event's state within the connection flow.

An event can have one of the following states:

**Unprocessed**

The event is generated but data alignment is not yet executed.

**Success**

The data alignment was successful. An event in this state can automatically be eliminated or kept as a reminder of the modification.

**Error** The event was generated correctly but a data alignment error was detected.

## Basic Structure of the Interface

The following topic provides more information about the structure of the IBM Security Identity Governance and Intelligence integration interface (II).

The following figure provides a more detailed illustration of the basic structure of the IBM Security Identity Governance II.

*Figure 31. Layered structure of the integration interface*

The II communicates with external systems through the USER\_ERC and USER\_EVENT\_ERC tables.

The USER\_ERC table contains a copy of user data from the external system.

The IBM Security Identity Governance enterprise connector module (ECONN) is the principle way of loading data into the USER\_ERC table.

The USER\_EVENT\_ERC table contains information that is related to authorization changes registered in the AG Core, in the form of events. This table contains events that are ready for transmission to the target systems.

EVENT\_IN and EVENT\_OUT are event tables that are required for communication between the interface and the AG Core.

OU\_ERC contains information that is related to OU changes.

AG Core and USER\_ERC are involved in both directions for the following reasons:

- The AG Core calculates some attributes and writes them back to the table, making them available for targets;

- Some attributes are linked with the AG Core database PERSON table and are automatically synchronized in both directions. See flow 4.

The structure of the USER\_ERC table can be highly customized to fit the needs of each client. Different targets use different fields, which are then carried back to the USER\_ERC table.

It is fundamental to establish which attributes in the USER\_ERC table are mapped to the AG Core table/attributes. See the following diagram.

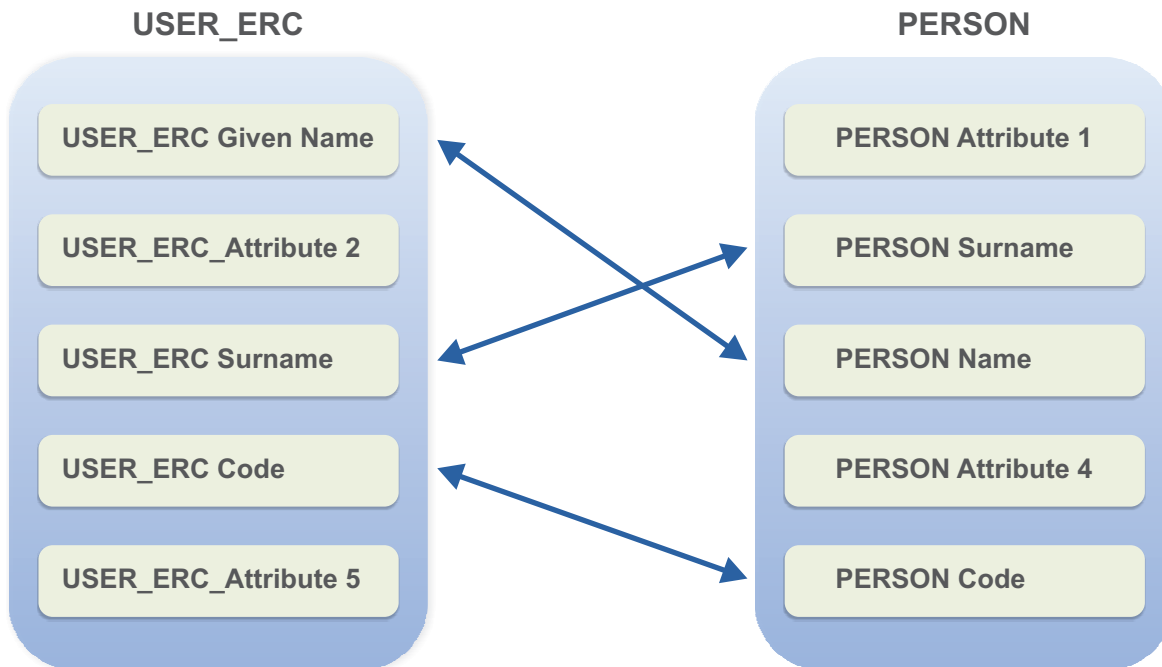


Figure 32. Virtualization of attributes in the PERSON table

In the diagram, attribute 1 **USER\_ERC Given Name** of the USER\_ERC is mapped to attribute 3 **PERSON Name** of the PERSON table that contains the user's personal data in the AG Core module.

When USER\_ERC is modified by the external personal data system, the data that is contained in attribute 1 of USER\_ERC is copied in attribute 3 of PERSON. The contrary is also true: changing **PERSON Name** automatically changes **USER\_ERC Given Name**. See bidirectional flow 4.

However, it is possible to map other attributes of USER\_ERC, outside of PERSON table, and visualize them as external data in the Data frame of the User Management GUI of AG Core.

For example, you can consider the **USER\_ERC** table as repository involved into the virtual mapping.

Each attribute can be set in two different modes:

#### Mode 1

The **USER\_ERC** attribute (listed under the column **Name**), is mapped with an attribute of **PERSON**. Changing the value of an attribute in one table causes



the same change in the other table. To customize an attribute with Mode 1, insert the name of the **PERSON** attribute to be associated, preceded by an underscore ("\_"), into the **Label** column.

#### Mode 2

The attribute in **USER\_ERC** is only displayed among the users' external data, on the User Management page of the AG Core Console. To customize an attribute by using Mode 2, insert the attribute and assign it a name in the **Label** text-box. In this case, the change in **USER\_ERC** is also reflected in the external table.

## Examples of Rules

In the IBM Security Identity Governance and Intelligence platform, the rules engine provides the flexibility and expressive strength that is required to model the customization of company processes.

Rules can be used in different situations, which in IBM Security Identity Governance and Intelligence, represents a layer of intelligence that enhances the expressive nature of the data model. Rules are used to implement specific and dynamic behaviors.

The following example situations demonstrate how the AG Core is linked to the external repository by integrating specific rules with simple **USER\_ERC** attribute mapping.

#### Example 1

In an external system that contains personal data, the **User Type** attribute is set for each user. It is defined by a grouping of codes that have a specific meaning in the system, for example 46=External Consultant. Assume that there is one attribute with the same meaning, but that the types have different names, External Consultant=Consultant.

In this case, the simple mapping that is described in the previous paragraph does not work.

The problem can be resolved with a rule that implements the following simple logic:

```
if type=46 AG Type=Consultant
```

This rule must be applied automatically each time a mapping is executed.

#### Example 2

Assume that based on the value of each **USER\_ERC** attribute, the value of the **PERSON** attribute can be calculated from either of the following methods:

```
NAME and SURNAME à MAIL=<NAME>.<SURNAME>@<companyname>.com
```

```
ID NUMBER à USERID=<constant><ID NUMBER>
```

Again, a rule can automatically implement the same logic. The use of a rule is not limited to mappings between **USER\_ERC** and **PERSON**. It can also be applied in many general cases of communication between the AG Core and an external repository. See the following examples.

#### Example 3

A rule can be used to automatically create an account on the target system when a new user is inserted.

#### Example 4

Certain codes in the external system can indicate whether a user is on sick-leave, on holiday, or temporarily transferred. Based on these codes, a rule can be used to temporarily disable the user's account.

#### Example 5

As a function of **User Type**, **OU Type**, or **Reason for Transfer**, a rule can regulate which roles the user maintains when the user is transferred from one OU to another.

#### Example 6

By using a rule, you can ensure that a user has an account on the target system before you assign an entitlement to that user. If the user has no account, one can be created.

## The rules engine (RE) in AG Core Architecture: read-from and write-to branches

Each time there is a new event to manage, the RE is activated and applies rules based on the type of event.

For more information about events, see “Brief introduction to events” on page 38.

The RE directly interfaces with the event tables. It periodically polls them and applies rules when it finds new events.

The RE filters event propagation and takes responsibility for any newly generated event. It analyzes the event changes and applies the appropriate rules according to company policies.

The following diagram illustrates the flow structure that enables communication between the target system that contains personal data and the AG Core:

Figure 33. Read-from communication: flow 1

Each time the target system changes the **USER\_ERC** table, an event that describes what occurred is automatically generated in the **EVENT\_IN** table. The rules engine notices the presence of a new event in the **EVENT\_IN** table and applies the rules necessary for proper AG Core data alignment.

The following diagram illustrates the flow structure that enables communication between the AG Core and the generic target system:



Figure 34. Write-to communication: flow 2

The AG Core changes the data and generates the necessary events to describe the change. The RE takes charge of the events and processes them. After the RE successfully processes the events, it passes them to the output interface, which then communicates the updates to the appropriate target systems.

Only correctly processed events are propagated to the output interface. If any errors are detected during event processing, propagation is blocked until the operator takes further action.

When an error is detected, an operator intervenes to remove the cause of the error and restarts event processing by using functions that are provided by the AG Core module.

## Synchronization branch

The usual approach with target systems is to establish a master-subordinate mechanism between the target systems and the AG Core. The user authorizations are not set by single target system consoles. The AG Core communicates the user authorizations to the target system consoles.

When you migrate to an RBAC system managed by IBM Security Identity Governance and Intelligence, a transitional period in which operators continue to directly set and use the target systems is important.

However, synchronizing changes that are executed directly on the target systems is complicated because authorizations are managed through roles that use the RBAC standard.

In non-RBAC-based target systems, entitlements are directly assigned to users and are not mediated by RBAC standards.

The IBM Security Identity Governance and Intelligence framework contains a synchronization branch with an interface. The interface informs the AG Core about what occurred in the target systems, which avoids misalignment or inconsistencies.

Because of the rules that are implemented for this branch, the RE can automatically repair an error condition or send the event, which provokes an inconsistency.

After an error occurs, the administrator runs an analysis from a dedicated section of the AG Core module. In this case, from the AG Core, rules can be used to set a resolution strategy that assigns the functions to the users.

The following diagram illustrates the structure of the synchronization branch:



Figure 35. Synchronization branch

## Complete Architecture of the IBM Security Identity Governance Integration Interface

The IBM Security Identity Governance and Intelligence architecture includes all branches that allow the AG Core module to interface with all types of external systems.

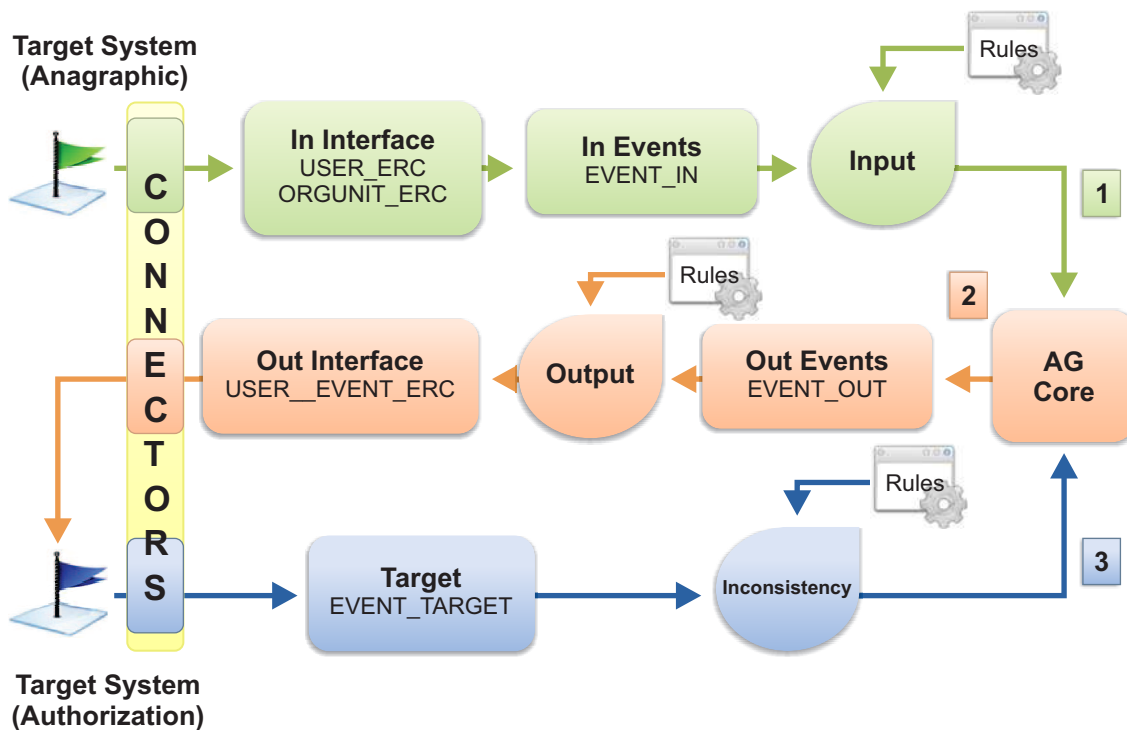


Figure 36. IBM Security Identity Governance and Intelligence II overview

The diagram displays the interface tables and three distinct flows:

- Read-from (flow 1)
- Write-to (flow 2)
- Synchronization (flow 3)

Events that are generated during propagation of information to the three branches are classified in the input events (EVENT\_IN), output events (EVENT\_OUT), and synchronization events (EVENT\_TARGET). The table ORGUNIT\_ERC contains a copy of the organization unit data that is registered in the personal data system. The function of this table is identical to that of USER\_ERC.

Another important element that is shown in the figure is the ECONN module layer. Through all the previously outlined branches, this module is involved in communications and alignment between the AG Core centralized DB and the peripheral target systems.

However, the logical behavior of the II is not dependent on the presence of an ECONN layer.

The following list is a brief summary of the three branches:

#### Read-from

Each change that is made to data in the personal data target systems is copied to the USER\_ERC for a user or ORGUNIT\_ERC for an OU in the input interface. This action generates a new event in the input events table. The event contains the minimum information that is required to reconstruct what was modified. The input RE takes responsibility for the event. It applies the input rules and, if no processing problems occur, communicates the information to the AG Core, which can then be aligned.

### Write-to

Each change that is made to data in the AG Core generates a new event in the output events table. The event contains the minimum information that is required to reconstruct what was modified. The output RE takes responsibility of the event. It applies the output rules. It communicates the information to the output interface if no processing problems occur. The output interface propagates the information to the target system, which can then be aligned.

### Synchronization

Each change to the data in any of the authoritative target systems generates a new event in the EVENT\_TARGET table. The event contains the minimum information that is required to reconstruct what was modified. The inconsistency RE takes responsibility for the event. It applies the inconsistency rules. If no processing problems occurs, it aligns the AG Core.

## SAP GRC integration scheme

Identity Governance and Intelligence can interface a SAP GRC system, with a particular focus on External SoD features. The interaction can be managed through a ReST or a Java interface.

The basic common scheme of integration is shown below:

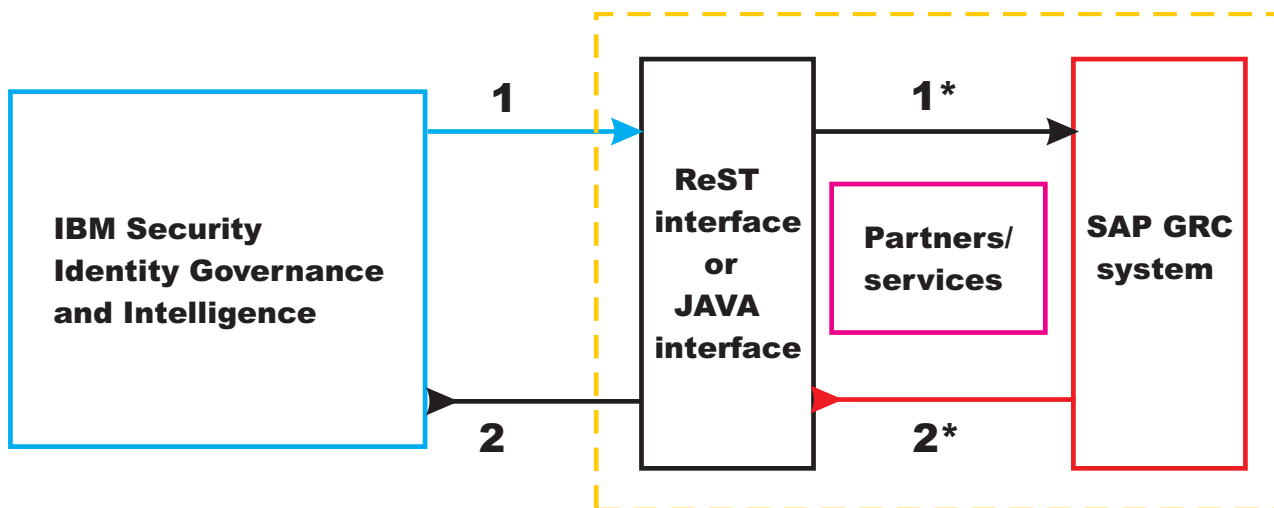


Figure 37. SAP GRC integration

- 1 - Start a request to the ReST/Java interface.
- 1\* - The ReST/Java interface transforms the request in a consistent SAP GRC format.
- 2\* - The SAP GRC system returns the requested data.
- 2 - The ReST/Java interface converts the data provided in step 2\* to a consistent Identity Governance and Intelligence format.

## ReST integration scheme

Identity Governance and Intelligence includes a ReST (Representational State Transfer) web service layer that can use HTTP to exchange data with an external target system.

The basic common scheme of integration is shown below:

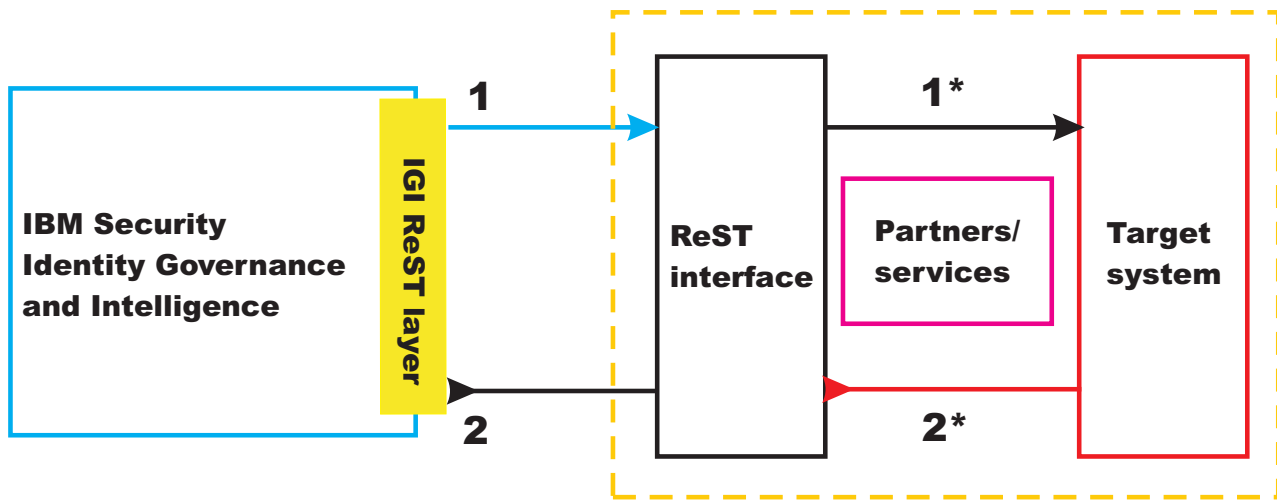


Figure 38. ReST integration

- 1 - A request is sent from the ReST layer of Identity Governance and Intelligence to the ReST interface of the target system.
- 1\* - The ReST interface of the target system converts the request to a consistent target system format.
- 2\* - The target system returns the requested data to the ReST interface.
- 2 - The ReST interface converts the data provided in step 2\* to a consistent Identity Governance and Intelligence format.

## Introduction to audit

IBM Security Identity Governance and Intelligence Audit is a centralized module. By default, it is always active.

All the IBM Security Identity Governance and Intelligence modules are required to send notifications to the Audit module for large sets of operations.

The following table shows a sample of an audit events table.

Table 2. Audit events table

Event ID	Description	Module
1	LOGIN	AG Core
2	LOGIN WARNING	AG Core
3	LOGIN ERROR	AG Core
4	Sub module access	AG Core
5	Password change	AG Core
6	Delegation start	AG Core
7	Delegation end	AG Core
8	Disabled	AG Core
11	Resource to user added	AG Core
12	Resource to user removed	AG Core

Table 2. Audit events table (continued)

Event ID	Description	Module
13	Org unit to user - internal resource added	AG Core
14	Org unit to user - internal resource removed	AG Core
15	Application to user - internal resource added	AG Core
16	Application to user - internal resource added	AG Core
17	Entitlement to user - internal resources added	AG Core
18	Entitlement to user - internal resources removed	AG Core
19	Activity to user - internal resources added	AG Core
20	Assigned role to user	AG Core
21	Removed role from User	AG Core
23	User assigned to OU	AG Core
23	Move user to OU	AG Core
24	Profile assigned to role	AG Core
26	Role assigned to OU-single	AG Core
27	Role removed from OU-single	AG Core
28	Role assigned to OU-hierarchy	AG Core
29	Role removed from OU-hierarchy	AG Core
30	IT role assigned to role	AG Core
31	IT role removed from role	AG Core
32	Profile assigned to role	AG Core
33	Removed profile from role	AG Core
40	New role	AG Core
41	Role removed	AG Core
42	Add user	AG Core
43	User removed	AG Core
44	User modified	AG Core
45	Add Org.Unit	AG Core
46	Org.Unit removed	AG Core
47	Add delegation to user	AG Core
48	Delegation removed	AG Core
49	Add account	AG Core
50	Account removed	AG Core
60	Add remediation to user	AG Core

Table 2. Audit events table (continued)

Event ID	Description	Module
61	Remove Remediation from user	AG Core
62	Risk added to user	AG Core
63	Risk removed from user	AG Core
64	Add remediation state to user	AG Core
65	Remove remediation status from user	AG Core
71	Core engine error	AG Core
72	Core engine alert	AG Core
80	Organization unit entitlement attestation approved	AG Core
81	Organization unit entitlement attestation revoked	AG Core
82	Organization unit entitlement attestation required	AG Core
85	User entitlement attestation approved	AG Core
86	User entitlement attestation revoked	AG Core
87	User entitlement attestation required	AG Core
90	User remediation attestation approved	AG Core
91	User remediation attestation revoked	AG Core
92	User remediation attestation required	AG Core
40000	Release to AGC	Access Optimizer (AO)
40001	Risk Based Campaign	Access Optimizer (AO)
50000	Insert activity	Process designer (PD)
50001	Update activity	Process designer (PD)
50002	Delete activity	Process designer (PD)
50003	Insert workflow	Process designer (PD)
50004	Update workflow	Process designer (PD)
50005	Delete workflow	Process designer (PD)
60000	Download report	Report designer (RD)
60001	Insert query	Report designer (RD)
60002	Update query	Report designer (RD)
60003	Delete query	Report designer (RD)
60004	Insert report	Report designer (RD)



Table 2. Audit events table (continued)

Event ID	Description	Module
60005	Update report	Report designer (RD)
60006	Delete report	Report designer (RD)
60007	Submit report	Report designer (RD)
70000	Adding permission to user	Enterprise connectors (ERC)
70001	Removing permission from user	Enterprise connectors (ERC)
70002	Suspending user	Enterprise connectors (ERC)
70003	Activating user	Enterprise connectors (ERC)
70004	Creating user account	Enterprise connectors (ERC)
70005	Deleting user account	Enterprise connectors (ERC)
70006	Renaming user	Enterprise connectors (ERC)
70007	Modifying user account	Enterprise connectors (ERC)
70008	Start reconciliation	Enterprise connectors (ERC)
70009	End reconciliation	Enterprise connectors (ERC)
80000	Start task	Task planner (TSKP)
80001	Stop task	Task planner (TSKP)
80002	Synchronize	Task planner (TSKP)
90000	Generate request	Access requests (AR)
90001	Authorize request	Access requests (AR)
90002	Execute request	Access requests (AR)
90003	Execute request by rule	Access requests (AR)
100000	Save configurations	Email service
100001	Insert template	Email service
100002	Update template	Email service
100003	Delete template	Email service
100004	Submit email	Email service



---

## Chapter 3. Identity Governance and Intelligence modules

Every Identity Governance and Intelligence module has a set of common features.

### General features

- For every module, a specific tab opens by default.
- There are **Help** and **Logout** options in the module frame.
- There is an IBM logo that you can mouse over to activate the Icons bar where you can directly access the other modules.

### Tabs

In every module, you can always find two levels of tabs that are indicated in the red rectangle.

The action area tabs are in the first level of tabs. They indicate general actions you can perform on entities in the second level of tabs. The second level displays a set of specific working areas.

There might be a third level tab, which is known in a blue rectangle. It has one or more specific operations that belong to one of the second level tabs.

The following figure shows an example of the 3-levels tabs module:

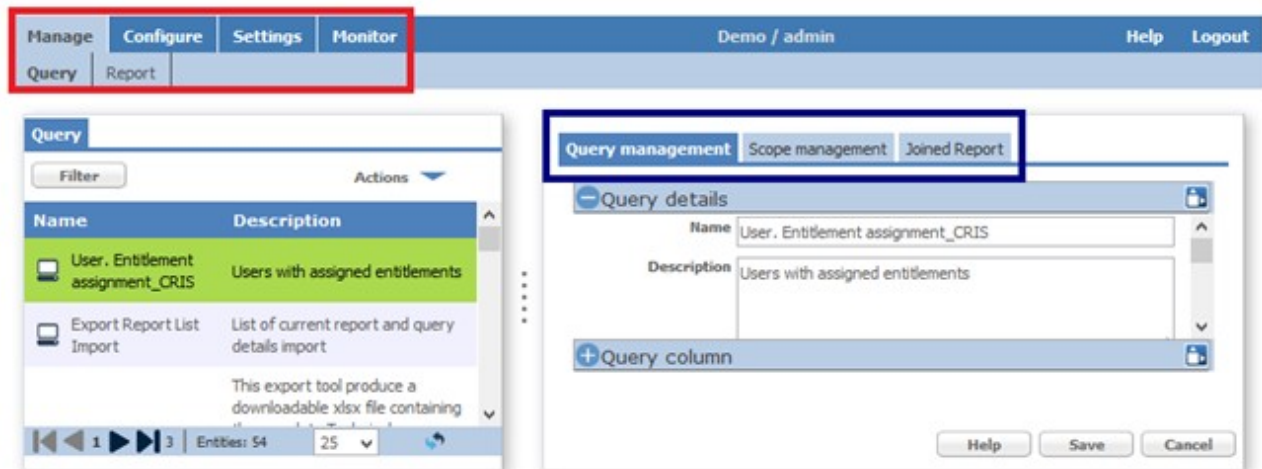


Figure 39. Example of a generic Identity Governance and Intelligence module GUI with three levels of tabs

### Frames

The standard GUI is organized in two frames.

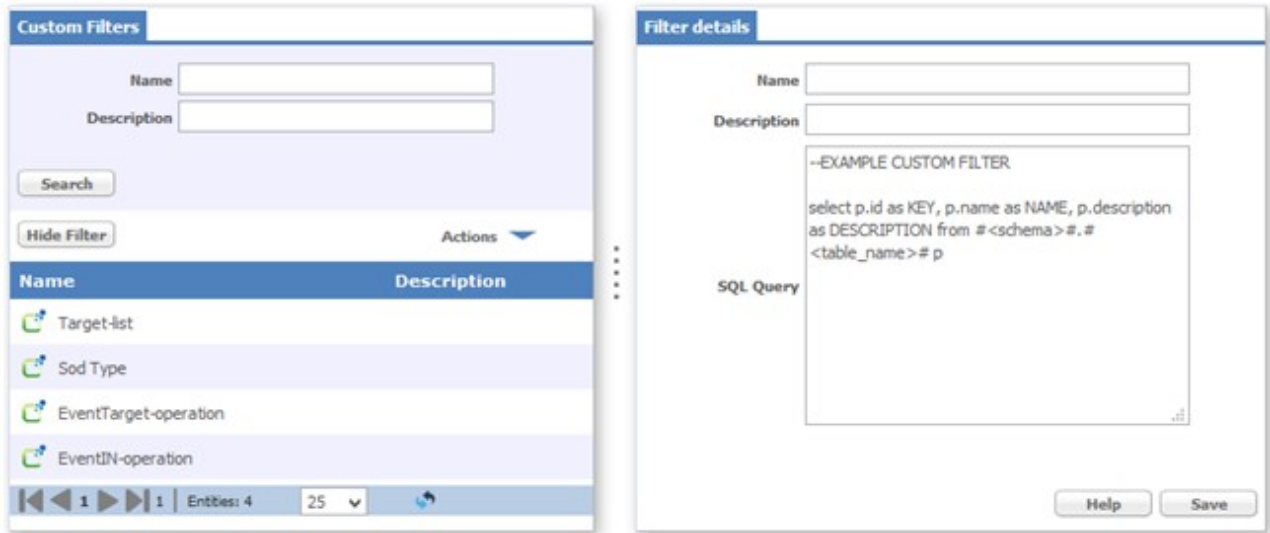


Figure 40. Example of a typical section of a generic Identity Governance and Intelligence module

On the left frame, you can find the following common elements.

**Filter/Hide Filter**

Show or hides the filters option.

In most cases, search filters correspond to a subset of the attributes of an item. The following wildcard characters modify the search criteria:

- % Searches for any sequence of characters.
- \_ (underscore) Indicates a single character.

**Search**

Gets results according to the filters setting.

**Go to** 

Navigates through the pages.

**Pagination**

Selects the number of items that are paged after the search operation, such as 10, 25, 50, 100, or 200.

**Refresh** 

Refreshes the contents.

**Actions**

Contains functional buttons that perform operations such as **Add**, **Remove**, **Import**, **Export**, **Build**.

**Note:** Every Identity Governance and Intelligence module can have a different set of functional buttons in the actions menu.

In the lists of items that are subdivided into one or more information columns, you can click any column heading to reorder the list items for that specific column. In these frames, you can also find one or more buttons to perform specific operations.

The right frame consists of dedicated sections to perform different kinds of operations. In these frames, it is common to find command buttons and accordion panes. Typical command buttons are of the following type:

**Save** Saves the performed operations.

**Cancel**

Deletes all the data that is entered in the different fields.

Different operative sections can be hosted into accordion panes. In the following example, you see the **Query management** section of the **Report Designer** module with two accordion panes.

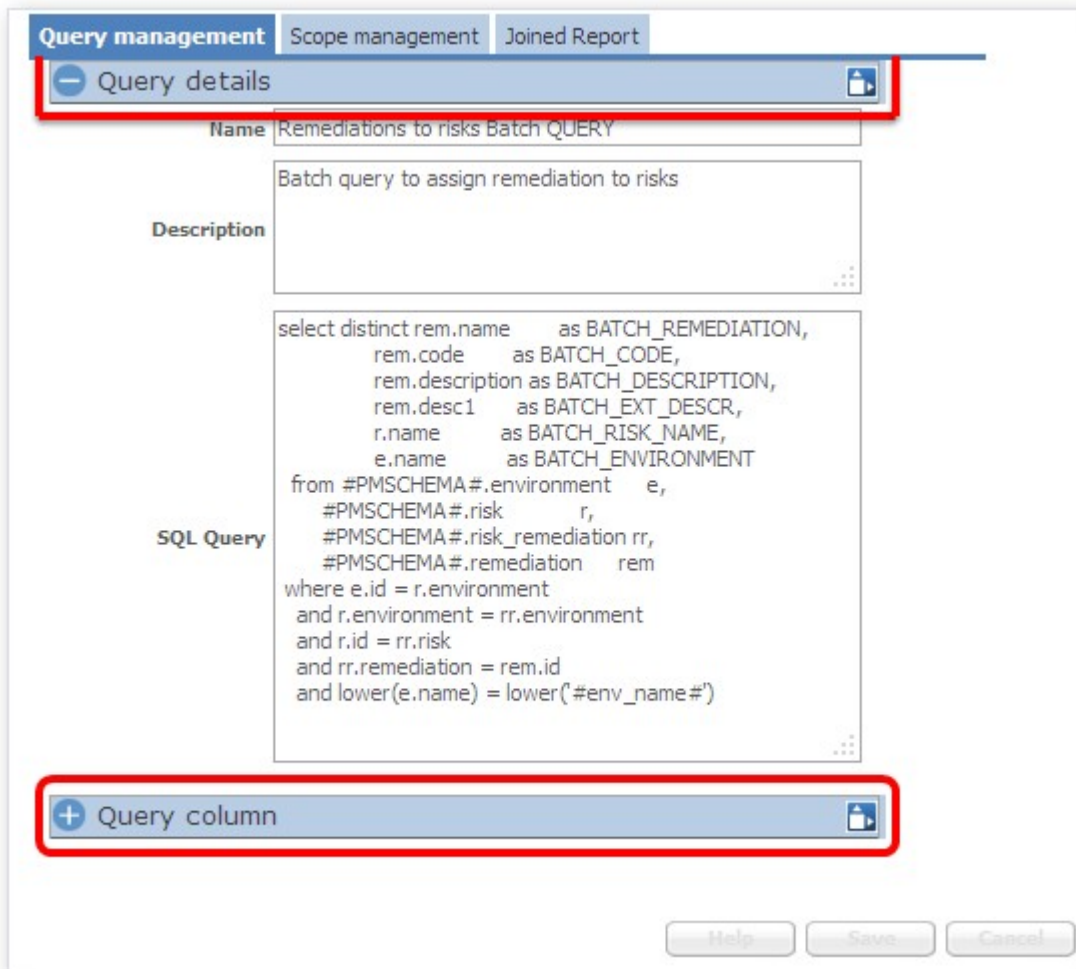






Figure 41. Example of accordion panes

To open or close the panes, click anywhere on the pane bar title. Click the **Maximize**  / **Minimize**  buttons to maximize or minimize the pane.

## Buttons & Icons

The following table lists the most common icons and buttons in Identity Governance and Intelligence modules.

Table 3. Common buttons and icons

Button / Icon	Description
	Represents a product type of item in the Report Designer module.
	Represents a custom type of item in the Report Designer module.
	Clears the contents that are inserted in a text box.
	Searches for specific entity or item.
	Moves an item up or down.
	Refreshes the page.
	Opens or closes accordion panes.
	Displays the details of an item.
	Indicates an item in a hierarchy.
	Indicates the error status of an item.
	Indicates the completed status of an item.
	Represents the status of a request <ul style="list-style-type: none"> <li>• Complete</li> <li>• Error</li> <li>• Warning</li> </ul>
	Maximizes or minimizes the frame.
	Represents the Permission type of entitlement.
	Represents the IT Role type of entitlement.
	Represents the Business Role type of entitlement.
	Represents the organization unit.
	Represents the UME entity.
	Represents the user entity.
	Represents a generic risk.
	Represents a Segregation of Duties risk
	Represents the Segregation of Duties level. <ul style="list-style-type: none"> <li>• High</li> <li>• Low</li> <li>• Medium</li> </ul>

Any Identity Governance and Intelligence module can be customized to use a subset of specific icons.





---

## Chapter 4. Account administration

Identity Governance and Intelligence administrators use the Administration Console to do account administration tasks, such as adding accounts.

### Account administration tasks

Use the Administration Console to do these tasks:

*Table 4. Account administration tasks*

Task	Refer to
Add an account to the system	"Adding an account"

#### Related information:

Accounts

Describes how to customize an account configuration for an application.

---

## Adding an account

Complete this task to register a new account into the Identity Governance and Intelligence data model.

### About this task

An account in the Identity Governance and Intelligence data model is a grouping of applications. All policies that are associated with the account are applied to the related applications.

### Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage > Accounts**.
4. In the **Account Configuration** tab, click **Actions > Add**.
5. In the **Details** tab, define a basic Account profile. See the related help topic for the options and their descriptions.

**Name** Specify a name for the Account.

#### Fulfillment

Set the value to **Automatic**.

6. Click **Save**. The created account is automatically listed and selected in the **Account Configuration** tab.
7. Access the **Password Creation** tab and select the **Enable Password Construction** check box.
8. Click **Save**.
9. In the Information window, click **Ok**.

#### Related information:

Accounts

Describes how to customize an account configuration for an application.



---

## Chapter 5. Application administration

Identity Governance and Intelligence administrators use the Administration Console to do application administration tasks, such as adding applications.

### Application administration tasks

Use the Administration Console to do these tasks:

*Table 5. Application administration tasks*

Task	Refer to
Add an application to the system	"Adding an application"

#### Related information:

"Accounts" on page 163

Describes how to customize an account configuration for an application.

---

## Adding an application

Complete this task to register a new application. By default, a new application is joined to the default *System Account IDEAS* and the related *Events Marker IDEAS*.

### Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage > Applications**.
4. In the **Applications** tab, click **Actions > Add**.
5. In the **Details** tab, define a basic Application profile. See the related help topic for the options and their descriptions.
6. Optional: If you want to create a new event marker with the same name of the application, select **<NEW>** from the **Events Marker** combination box. Otherwise, select the event marker that you want to use.
7. Click **Save**.

#### Related information:

"Application" on page 147

Documents the functions required for the management of Applications.



---

## Chapter 6. Data import with Bulk Data Load

Identity Governance and Intelligence administrators use the Administration Console to do data import tasks, such as importing users and entitlements into your security model.

### Data import tasks

Use the Administration Console to do these tasks:

Table 6. Data import tasks

Task	Refer to
Populate the data model	"Creating a bulk load operation"

Bulk Data Load in the Access Governance Core module  
You can load bulk data in the AG Core database.

Bulk Data Load in the Access Risk Controls module  
You can load large amounts of data.

Bulk Data Load in the Access Risk Controls for SAP module

---

## Creating a bulk load operation

Complete this task to populate the data model.

### Procedure

1. Log in to the Administration Console.
2. Select any of these modules:
  - **Access Governance Core**
  - **Access Risk Controls**
  - **Access Risk Controls for SAP**
3. Select **Tools > Bulk Data Load**.
4. In the **Action** tab, select one of the supported operations.
5. In the **File Batch** tab, upload the Excel XLS file corresponding to the selected operation. See the related help topic for the options and their descriptions.

**Note:** The status of the operation, *Pending* to *Completed* is displayed at the bottom of the tab.

6. In the Information window, click **Ok**.

Bulk Data Load in the Access Governance Core module  
You can load bulk data in the AG Core database.

Bulk Data Load in the Access Risk Controls module  
You can load large amounts of data.

Bulk Data Load in the Access Risk Controls for SAP module



---

## Chapter 7. Entitlement administration

Identity Governance and Intelligence administrators use the Administration Console to do entitlement administration tasks, such as adding roles and adding entitlements to organizational units.

### Entitlement administration tasks

Use the Administration Console to do these tasks:

*Table 7. Entitlement administration tasks*

Task	Refer to
Add an entitlement	"Adding an entitlement"
Add an entitlement to an organizational unit	"Adding an entitlement to an organizational unit" on page 64
Add entitlements to an attribute group	"Adding entitlements to an attribute group" on page 64

#### Roles

A role identifies the set of permissions and resources to which the person has access. Use this set of panels to define and manage entitlements in your organization.

#### Entitlements

You can view all the entitlements that are already associated to a group of a selected hierarchy.

---

## Adding an entitlement

Complete this task to register a new entitlement into the Identity Governance and Intelligence data model.

### Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage > Roles**.
4. Select the **FlatView** tab and click **Actions > Add**.
5. In the **Details** tab, define a basic entitlement profile. Specify information in the following fields and in the other fields, if applicable. See the related help topic for the options and their descriptions.
  - Name
  - Code
  - Type
  - Application
6. Click **Save**.
7. In the Information window, click **Ok**.

### Related information:

## Roles

A role identifies the set of permissions and resources to which the person has access. Use this set of panels to define and manage entitlements in your organization.

---

## Adding an entitlement to an organizational unit

You must assign the entitlement to the organizational unit before you can assign the entitlement to a user that belongs to the same hierarchy of the organizational unit.

### Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage > Groups**.
4. In the **Hierarchy** field, select **ORGANIZATIONAL\_UNIT**.
5. In the **View** tab, select the organizational unit from which to add the entitlement.
6. Access the **Entitlements** tab and click **Actions > Add**.
7. In the Add window, select the entitlement and click **OK**.
8. In the Insert Group Entitlements window, select the values for the following options. See the related help topic for the options and their descriptions.

### Default

Select any of these options:

- **No** for a basic configuration.
- **Yes** to automatically assign this entitlement to all users that are added to the group.
- **Yes, and align users** to automatically assign this entitlement to all users of the group. In this case, the administrator must assign the appropriate set of resources to each user.

### Visibility Violation

Select **No** for a basic configuration.

### Enabled

Select **Yes** for a basic configuration.

### Hierarchy

Select the check box to assign the organizational unit to the hierarchy.

9. Click **OK**.

### Related information:

#### Entitlements

You can view all the entitlements that are already associated to a group of a selected hierarchy.

---

## Adding entitlements to an attribute group

Complete this task to join a set of entitlements to a group of an attribute hierarchy. For example, you can assign the entitlements to the users of the organizational unit.



## About this task

The following procedure is an example way of completing this task. To create a different behavior, you can select other configuration settings based on your requirements or preferences.

### Procedure

1. Complete “Creating an attribute hierarchy” on page 68.
2. Select **Manage > Groups**.
3. In the **Hierarchy** field, select the hierarchy.
4. In the **View** tab, select the group to which the entitlement is to be added.
5. Access the **Entitlements** tab.
6. Click **Actions > Add**.
7. In the Add window, select the entitlement to be added and click **OK**.
8. In the Insert Group Entitlements window, select the values for the following options. See the related help topic for the options and their descriptions.

#### Default

Select any of these options:

- **No** for a basic configuration.
- **Yes** to automatically assign this entitlement to all users that are added to the group.
- **Yes, and align users** to automatically assign this entitlement to all users of the group. In this case, the administrator must assign the appropriate set of resources to each user.

#### Visibility Violation

Select **No** for a basic configuration.

#### Enabled

Select **Yes** for a basic configuration.

#### Hierarchy

Select the check box to assign the Entitlement to the hierarchy.

9. Click **OK**.

#### Related information:

##### Entitlements

You can view all the entitlements that are already associated to a group of a selected hierarchy.



---

## Chapter 8. Group administration

Identity Governance and Intelligence administrators use the Administration Console to do group administration tasks, such as adding organizational units.

### Group administration tasks

Use the Administration Console to do these tasks:

*Table 8. Group administration tasks*

Task	Refer to
Add an organizational unit to the system	"Adding an organizational unit"
Create an attribute hierarchy	"Creating an attribute hierarchy" on page 68
Configure a hierarchy to structure the organizational unit	"Configuring the attribute hierarchy" on page 68

#### Groups

You can use the following functions to manage a hierarchy. The main hierarchy available is the ORGANIZATIONAL\_UNITS hierarchy.

#### Hierarchy (Polyarchies)

In the IBM Security Identity Governance model, polyarchies provide different organizational views in a hierarchical notation.

---

## Adding an organizational unit

Complete this task to register a new organizational unit.

### About this task

The hierarchies of an organizational unit are a specific case of "Configuring the attribute hierarchy" on page 68.

### Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage > Groups**.
4. In the **Hierarchy** field, select **ORGANIZATIONAL\_UNIT**.
5. In the **View** tab, select which organization unit to add the new one and click **Actions > Add**.
6. In the **Details** tab, define a basic Organization Unit profile. See the related help topic for the options and their descriptions.
7. Click **Save**.
8. In the Inheritance window, specify whether to inherit the Entitlements and Resources that are deployed in the parent Organization Unit by selecting the corresponding check box.
9. Click **OK**.
10. In the Information window, click **Ok**.

**Related information:**

“Groups” on page 134

You can use the following functions to manage a hierarchy. The main hierarchy available is the ORGANIZATIONAL\_UNITS hierarchy.

---

## Creating an attribute hierarchy

Complete this task every time you need to build a hierarchy.

### Procedure

1. Complete “Configuring the attribute hierarchy.”
2. Select **Configure > Hierarchy**.
3. In the **Hierarchy** tab, click **Actions > Build**.
4. Select **Monitor > Scheduled Task** to check the build status. If the status is Completed, the build completed successfully.
5. To check the result, select **Configure > Attribute Groups** and select the attribute hierarchy that just built.

### Related information:

Hierarchy (Polyarchies)

In the IBM Security Identity Governance model, polyarchies provide different organizational views in a hierarchical notation.

---

## Configuring the attribute hierarchy

Complete this task to create a hierarchy to structure the organizational unit.

### About this task

Identity Governance and Intelligence provides a mechanism to build an infinite number of hierarchies. The most common and traditional is the hierarchy of the organizational unit.

You can build a hierarchy based on:

#### User attributes

Every administrator can map their own and specific user attributes.

**Rules** Administrator can have an unlimited number of rules. Every rule can be configured with a different behavior.

The **Field** list contains the attributes of the **User Data** list. It refers to the **UserErc** table. To view these attributes, follow these steps:

1. From the Access Governance Core, select **Settings > Core Configurations > User Virtual Attributes**.
2. In the **Repository** tab, select the **UserErc** table.
3. Access the **Attribute Mapping** tab.

### Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Configure > Hierarchy**.
4. In the **Hierarchy** tab, click **Actions > Add**.
5. In the **Details** tab, define a basic hierarchy profile. See the related help topic for the options and their descriptions.

**Name** Specify the hierarchy name.

**Configuration Type**

Select the configuration type.

**Manual**

Only the hierarchy is created. You must add the groups and users manually.

**Simple**

The group is created by using the value selected from **Fieldlist**.

**Advanced**

The group is created by using an existing rule. You can opt to build the hierarchy automatically through a scheduled job or once.

**Value** Select from the following values.

**Single Value**

A node is added for each value of the attribute. Each user with that attribute is added in that node.

**Multi Value**

A node is added for each value of the attribute. If the attribute has multiple values, each value must be separated by a separator char. Specify the character in the **Separator Char** field. A user is added in each node with the specified value.

**Hierarchy**

The path that is specified in the selected **Field** of each user is used to create the hierarchical tree structure. Each user is added in the last node specified in the selected **Field**.

**UserID Attribute (Automatic Scope Assignment)**

Select this check box to assign the administrator role and its relative scope to the hierarchy.

**UserID Assigned Role**

If you selected **UserID Attribute (Automatic Scope Assignment)**, select an administrative role.

**Note:** The selected role must have the **Attribute Hierarchy** already selected from **Access Governance Core > Configure > Admin Roles > Scope**.

**User ID Hierarchy**

If you selected **Single Value**, select this check box to get a hierarchical tree structure, in which each node is set as a child of a node that has the same name as one of the users in that group.

6. Click **Save**.

**Related information:**

Hierarchy (Polyarchies)

In the IBM Security Identity Governance model, polyarchies provide different organizational views in a hierarchical notation.



---

## Chapter 9. Password administration

Identity Governance and Intelligence administrators use the Administration Console to do password administration tasks, such as configuring the password service and changing account passwords for users.

### Password administration tasks

Account passwords are used to access the accounts that a user is entitled to use. Accounts correspond to applications.

Service Center passwords are used to log in to the Service Center.

Use the Administration Console to do these tasks:

*Table 9. Password administration tasks*

Task	Refer to
Change a user's password for one or more accounts.	"Changing account passwords for users"
Force a password change for a Service Center user.	"Forcing a password change" on page 72
Configure the password service to enable password changes from the Service Center.	"Configuring password services" on page 72

For information about password-related tasks that managers and help desk personnel can do in the Service Center, see Password management.

#### Related information:

"Accounts" on page 124

You can create and manage user accounts and set user passwords.

---

## Changing account passwords for users

You can change the password for one or more accounts of a specific user.

### Before you begin

The Identity Governance and Intelligence administrator, also known as the *Super Admin*, or other administrators must complete this task to change the password of a user.

### About this task

Account passwords are used to access the accounts that a user is entitled to use. Accounts correspond to applications. For example, the Service Center application is associated with an account named Ideas. If you change the password of a Service Center user, you select Ideas from the list of accounts.

## Procedure

1. Log in to the Administration Console.
2. Select **Access Governance Core**.
3. Select **Manage > Users**.
4. Select the user that you want to change the password for.
5. In the **Accounts** tab, select the account for that user.
6. Select **Actions > Change Pwd**.
7. In the **Change Password** window, specify the new password in the **Password** and **Confirm Password** fields, and click **OK**.

## Results

The user password is changed. Click **OK** when you see the message that indicates a successful operation.

### Related information:

“Accounts” on page 124

You can create and manage user accounts and set user passwords.

---

## Forcing a password change

You can force users to change their password the next time that they log in to the Service Center.

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

## Procedure

1. Log in to the **Administration Console**.
2. From the Administration Console, select **Access Governance Core**.
3. Select a user, and then select the **Accounts** tab for that user.
4. Select the account that you want to force the password change for, and then click **Actions > Force Pwd**.

## Results

A green check mark is displayed in the **Force Change Pwd** column. The user is prompted to change the password during the next login to the Service Center.

### Related information:

“Accounts” on page 124

You can create and manage user accounts and set user passwords.

---

## Configuring password services

You must configure the password service in Access Governance Core to enable the features that are related to password management for Service Center users.

### About this task

You must configure the password service to enable the following features:



**Forgot password**

Enables users to reset their Service Center password if they forget it. Users are first authenticated with their predefined security questions. Then, they can enter a new password or receive a system-generated password at their registered email address. Depending on the configuration setup, users might have the option to edit their email address.

**Self Care**

An application in the Service Center where users can change their own passwords.

**Password reset**

An account change process of the Access Requests application where a manager or entitled person can reset the password of a requesting user. This requires further configuration in the Process Designer. Two predefined workflows, one for the user manager and one for the application manager administrative roles, are provided ready-for-use.

To learn how to configure the password service in the Access Governance Core, see “Configuring the password service in Access Governance Core.”

To learn how to configure the account change process for changing passwords in the Process Designer, see “Configuring the password service in Process Designer” on page 75.

## **Configuring the password service in Access Governance Core**

Configure the Password service in Access Governance Core to enable the Forget password, Self Care, and Password reset features and to set up and manage the security questions.

**About this task**

This is a required action to set up the user authentication process - based on security questions - that verifies the identity of users who must use the Forget your password feature or ask their manager or other entitled personnel (for example, a Help Desk operator) to reset their Service Center password.

**Procedure**

1. Log in to the Administration Console.
2. Select **Access Governance Core**.
3. Select **Settings > Configure Password Service > Configure Forgotten Password Service**.
4. Complete the items described in the following table:

Table 10. Configuration items for Configure Forgotten Password Service

Section	Item	Description
Admin configuration	Enable password service	<p>Flag this check box to enable the following services:</p> <p><b>Forgot password</b> Enables users to reset their password to enter Service Center if they forget it. Users are first authenticated with security questions. Then, they can enter a new password or receive a one-time password at their registered email address. Depending on the configuration setup, users might have the option to change their email address.</p> <p><b>Self Care</b> Service Center module where users can change their passwords</p> <p><b>Password reset</b> An Account Change process of the Access Requests module where a manager or entitled person can reset the password of a requesting user.</p>
Security questions configuration	Number of security questions asked at first login	Number of security questions to ask a new user. The answers provided at this time are saved and used as benchmarks for verification when the user forgets the login password.
	Number of security questions asked for reset	Number of questions to ask a user who has forgotten a password. This number must be smaller or equal to the number of questions asked at first login.
	Number of failed attempts allowed	<p>If the user is unable to correctly answer all the questions asked for reset in the number of attempts specified here, the password is not provided. The user must follow a different process to ask for help. For example, the user might call the Help-desk, an administrator, or a manager.</p> <p><b>Note:</b> This option applies to the Forgot password and Self Care features. It does not affect Password reset.</p>
	Minimum length of the answer	The minimum number of characters required for every answer.

Table 10. Configuration items for Configure Forgotten Password Service (continued)

Section	Item	Description
Mode configuration	Allow user to change password immediately	After a user successfully answered the security questions, the user is prompted to enter a new password and can login immediately.
	Send one-time password to known user address	After a user successfully answered the security questions, a new password is emailed to the user. The password is valid for only one login where the user is prompted to enter a new password.
	Allow user to edit email address	Select this check box to let the user edit the address where the password is sent.

5. Select the **Security Questions** tab.
6. Select **Actions > Add** and add security questions. Add new questions in English before you add them in other languages. New questions are saved with the **Active for user** check box not selected. This means that they are not visible to users. To make a question available for use, select the check box. Clear the check box before you edit a question or add a locale. This is not necessary when you remove a question. When a question is removed or thoroughly modified, users who have that question in their Forgot password list are asked to answer a new question at their next login.

## Results

The Password service is configured. To configure the **Password reset** service for the Access Requests module, see “Configuring the password service in Process Designer.”

## Configuring the password service in Process Designer

You must configure an account change workflow in the Process Designer to create a workflow for password reset requests in the Access Requests application of the Service Center.

### Before you begin

You must also configure the password service in the Access Governance Core to enable the password reset workflows.

### About this task

A password reset workflow is the process that a manager or entitled user runs through to reset the Service Center password of another user. The workflow runs in the Access Requests application.

Two preconfigured workflows of this kind are provided:

#### ManagerPasswordReset

This workflow is configured for a user that is entitled with the User Manager administrative role. It empowers the User Manager (the applicant) to enter a new password for a user who belongs to the same organization unit (the beneficiary). The applicant does not use security questions to verify the identity of the beneficiary, types a new password for the beneficiary, and edits the email address of the beneficiary, if

necessary. As the applicant submits the request, an email with the new password is forwarded to the beneficiary.

### HelpDeskPasswordReset

This workflow is configured for a user that is entitled with the Application Manager administrative role. It empowers the Application Manager (the applicant) to enter a new password for any user, regardless of which organization unit the user belongs to (the beneficiary). The applicant uses security questions to verify the identity of the beneficiary, has the system generate a password, but cannot edit the email address of the beneficiary. As the applicant submits the request, an email with the new password is sent to the beneficiary.

Both workflows include a request generation and a request execution activity. From a practical point of view, the password is created and emailed to the beneficiary after the applicant clicks **Submit** at the end of the request generation flow.

You can use these workflows as they are, modify them, or configure new workflows starting from an Account Change process. As an example, the following procedure shows how to view or modify the details of the ManagerPasswordReset workflow.

### Procedure

1. Log in to the Administration Console.
2. Select **Process Designer**.
3. Select **Manage > Process**.
4. Select ManagerPasswordReset in the list of processes. The right part of the window displays the workflow details. If you plan to modify the details, set the **Status** to **Off line**. A workflow in off line or in maintenance status is not available to users in the Access Requests application.
5. Click **Next** to proceed to the Configuration window where you can view the two activities that make up this workflow. The activities are:

#### ManagerPasswordResetGEN

Is the part of the flow where:

- The user (beneficiary) whose password must be reset and the accounts for which the password grants access are selected.
- The new password is entered and emailed to the beneficiary.

#### ManagerPasswordResetEXE

Is the part of the flow where the request is displayed in a list of requests to an entitled operator. There is no action for the operator except to acknowledge whether the request was completed.

6. Click **ManagerPasswordResetGEN** to display the details of this activity. Under **Activity scope**, you find the following tabs:

Table 11. Activity scope tabs of ManagerPasswordResetGEN

Tab	Content
Beneficiary	Provides a selection of the type of users for whom the applicant (the User Manager in this case) can reset a password. This affects the list of users displayed in the Users page of the request in Access Requests.

Table 11. Activity scope tabs of ManagerPasswordResetGEN (continued)

Tab	Content
Application	Provides a selection of the type of applications (accounts) accessible to the user for which the applicant can reset a password. This affects the list of accounts displayed in the Accounts page of the request in Access Requests.
Required Data	Provides configuration options for the request, where the account operation is Change Password. This affects the contents of the remaining pages of the request, such as: <ul style="list-style-type: none"> <li>• Whether there are security questions to verify the identity of the beneficiary</li> <li>• If the applicant is requested to enter his/her own password</li> <li>• If the applicant types the new password or has it generated automatically</li> <li>• If the new password is emailed to the beneficiary or communicated by other means</li> <li>• If the beneficiary's email address can be updated on the moment</li> </ul>
Email data	Provides the template for the text of the email sent to the beneficiary with the new password. Templates are managed in <b>Access Governance Core &gt; Configure &gt; Email</b> .

You can edit the choices selected in these tabs to better meet your requirements.

7. Click **Ok** or **Cancel** to close the Activity window.
8. Click **ManagerPasswordResetEXE** to display the details of this activity. Remember that the Execution activity of this work flow is nominal. **Activity scope** includes the following tabs:
  - Beneficiary
  - Application
9. Click **Ok** or **Cancel** to close the Activity window.
10. Click **Next** to proceed to the Assign window where the activities are assigned to one or more roles. The window displays the role to which ManagerPasswordResetGEN is assigned. In this case the role is User Manager. You can add other roles or replace the existing one with the **Actions > Add/Remove** buttons. When you add a role, you can choose from the roles that are defined in the Access Governance Core.
11. Click the **ManagerPasswordResetEXE** tab to view the role that this activity is assigned to. In this case, the activity is assigned to the Operator role.
12. If you have changed the configuration options, click **Save** and put the workflow back on line. Otherwise, proceed to another process, tab, or close the window.

## Results

The User Manager finds the **ManagerPasswordResetGEN** tab in the Access Requests application of Service Center. The User Manager selects this tab to use a wizard that helps create and email a password for another user. Similarly, an Operator can use the **ManagerPasswordResetEXE** tab to view a list of the latest ManagerPasswordResetGEN requests that are submitted and their status.

### Related information:

“Accounts” on page 124

You can create and manage user accounts and set user passwords.

---

## Chapter 10. Target type administration

Target integration automates data collection from distributed target systems and reflects changes that are initiated from Identity Governance and Intelligence. Target systems are repositories for user account information.

### Overview

A *target type*, also called a *target profile*, is a category of related targets that share schemas. It defines the schema attributes that are common across a set of similar managed resources.

Target types are templates that are used to create targets for specific instances of managed resources. For example, if you have several Lotus® Domino® servers that users need access to, you might create one target for each server by using the Lotus Domino target type.

A target type is defined in the target definition file of an adapter, which is a Java™ Archive (JAR) file that contains the profile. The target type for an adapter is created when the adapter profile is imported. For example, a target type is defined in the `PosixLinuxProfile.jar` file.

Some target types are installed by default when you install IBM Security Identity Governance and Intelligence. You can install other target types when you import the target definition files for adapters for managed resources. The IBM Security Identity Governance and Intelligence adapter provides a target type definition for a managed resource. There is a target type for each type of supported managed resource, such as UNIX or Linux.

For information about supported adapters, see Identity Brokerage Adapters.

### Target type administration tasks

You can do the following tasks from the Target Administration Console:

Table 12. Target type administration tasks

Task	Refer to
Import target definition files, also called adapter profiles.	“Importing target types (adapter profiles)” on page 80
Map target type account attributes to Identity Governance and Intelligence user attributes.	“Importing the attribute map for a target type” on page 81
Define account defaults for a target type by mapping to a user attribute directly or by using JavaScript.	“Adding account defaults to a target type” on page 83
Change account defaults for a target type.	“Changing account defaults for a target type” on page 84
Remove account defaults from a target type.	“Removing account defaults from a target type” on page 85

---

## Target definition file or adapter profile

A *target definition file*, also called an *adapter profile*, defines the type of managed resource that IBM Security Identity Governance and Intelligence can manage.

The target definition file creates the target types for IBM Security Identity Governance and Intelligence.

The target definition file is a Java archive (JAR) file that contains the following information:

- Target information, including definitions of the account provisioning operations, such as add, delete, suspend, or restore.
- Target provider information, which defines how IBM Security Identity Governance and Intelligence communicates with the managed resource.
- Schema information, including the LDAP classes and attributes.
- Account and target forms and the label for the attributes for creating targets and requesting accounts on those targets. They are displayed in the user interface.

---

## Importing target types (adapter profiles)

As an administrator, you can import a target definition file, which creates a target type. Target definition files are also called adapter profile files, which are provided with the various Identity Brokerage Adapters. The adapter profile is required because it defines the types of resources that the Identity Governance and Intelligence server can manage.

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

The file to be imported must be a Java archive .JAR file. You can create a target type for an adapter that provides a .JAR file.

### About this task

The adapter profile is used to create an adapter service on the Identity Governance and Intelligence server and to establish communication with the adapter. If the adapter profile is not installed, you cannot manage the targets. Import the adapter profiles to create target definitions for the targets.

This task can be completed from the Target Administration Console. To import a target type, complete these steps:

### Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget. The Administration Console is displayed.
2. From the Administration Console, select **Target Administration**. The Target Administration Console is displayed.
3. From the navigation tree, select **Manage Target Types**. The Manage Target Types page is displayed.



4. On the Manage Target Types page, click **Import**. The Import Target Type page is displayed.
5. On the Import Target Type page, complete these steps:
  - a. In the **Target Definition File** field, type the directory location of the file or click **Browse** to locate the file. For example, if you are installing the IBM Security Identity Governance and Intelligence adapter for a Windows server that runs Active Directory, locate and import the ADProfileJAR file  
.  
The adapter profiles are in the target cache.
  - b. Click **OK**.

## Results

A message indicates that you successfully imported a target type.

## What to do next

The import occurs asynchronously, which means it might take some time for the target type to load into IBM Security Identity Governance and Intelligence from the properties files and to be available in other pages. On the Manage Target Types page, click **Refresh** to see the new target type. If the target type is not displayed in a reasonable amount of time, check the log files to determine why the import failed.

If the adapter profile is successfully imported, create a target that uses the adapter profile. See “Creating targets” on page 88. For more information, see *Creating a Service* in the relevant Adapter product documentation.

If you cannot create a target with the adapter profile or open an account on an existing target, the adapter profile was not installed correctly during the import. You must import the adapter profile again.

---

## Importing the attribute map for a target type

You can map the Identity Brokerage Adapters account attributes with the Identity Governance and Intelligence system attributes.

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

If the adapter package contains a mapping definition file and is specified as a requirement in the guide, complete this task after Importing target types (adapter profiles). The imported file must be a DEF file.

### About this task

The attribute mappings for all supported adapters are configured and require no further action.

This task is required for new and custom adapters. See the *Development and Customization Guide* at <http://www-01.ibm.com/support/docview.wss?uid=swg21687732> for instructions.

## Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, select **Manage Target Types**.
4. In the **Target Type** table, click the icon ( ▶ ) next to the target type to show the available tasks. The tasks that you can do depend on the type of target.
5. Click **Attribute Mapping**.
6. On the Import Attribute Mapping page, click **Browse** to locate the file. For example, if you are installing the IBM Security Identity Governance and Intelligence adapter for a Windows server that runs Active Directory, locate and import the `ADprofileMapping.def` file.
7. Click **OK** to import the file. The import occurs asynchronously. It might take some time for the target type to load from the properties files and to be available in other pages.

---

## Account defaults on a target type

You can define default values for account attributes either on a target or target type. This step is required only for required attributes, which are indicated in the user interface with an asterisk (\*).

### Types of account defaults

#### Target type account defaults

When account defaults are defined at the *target type level*, they apply to all targets of that type. However, you can override a target type default by defining an account default at the *target level*.

#### Target account defaults

These defaults are initially inherited from the target type account defaults, but they become local to the target as soon as it is changed. When they become local account defaults, you can change or remove them. Changes and removals do not affect the target type account defaults.

You must specify the account defaults for the required attributes of the target. The required attributes are indicated by an asterisk (\*). Provisioning fails if the required attributes are not defined. For example, the attributes *Full name* and *Last name* are required for LDAP. For more information, see “Account defaults on a target” on page 92.

### Options for defining default values for account attributes

**Basic** You can hardcode default values for an account attribute.

#### Advanced

You can code JavaScript to retrieve data from Identity Governance and Intelligence objects and set the value for an account attribute. As a starting point, you can create a basic account default and then use the advanced option to edit the generated JavaScript.

For account defaults, you can use the JavaScript objects *subject* and *service*, where

*subject* is a **DirectoryObject** that represents a person.

*service* is a **DirectoryObject** that represents a target.

The following example shows the JavaScript for the **Gecos** (comments) attribute.

```
return "Account for "+ subject.name+" on "+service.name;
```

## Adding account defaults to a target type

You can add account defaults to a target type. This task is required only for the attributes in the user interface that are marked with an asterisk (\*).

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

The target type must exist. If it does not exist, you must import the profile for the target type. See Importing target types (adapter profiles).

### About this task

You can add default values for attributes. When you create a target instance from this target type, the account defaults for the target type are copied to the target.

You must specify the account defaults for the required attributes of the target. The required attributes are indicated by an asterisk (\*). Provisioning fails if the required attributes are not defined. For example, the attributes *Full name* and *Last name* are required for LDAP. For more information, see “Account defaults on a target” on page 92.

### Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Target Types**.
4. In the **Target Types** table, click the icon ( ▶ ) next to the target type and then click **Account Defaults**.
5. On the Select an Account Attribute page, click **Add**.
6. On the Select an Attribute page, select an account attribute. Take one of the following actions:
  - Add a default value.
    - a. Click **Add**.
    - b. Complete the appropriate fields, which vary depending on the type of target.
    - c. Click **OK**. The attribute default is added.
  - Add a script that specifies a default value.
    - a. Click **Add (Advanced)**.
    - b. Type the JavaScript code in the **Script** field. For account defaults, you can use the JavaScript objects *subject* and *service*.

Where

*subject* is a **DirectoryObject** that represents a person.

*service* is a **DirectoryObject** that represents a target.

The following example shows the JavaScript for the **Gecos** (comments) attribute.

```
return "Account for "+ subject.name+" on "+service.name;
```

- c. Click **OK**.
7. On the Select an Account Attribute page, finish adding attribute defaults to the target type.
8. Click **OK** to save the changes and to close the page.
9. Add more account defaults or click **Close**.

## Results

A message indicates that you successfully saved the account defaults on the target type.

## Changing account defaults for a target type

You can change the account defaults for a target type.

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

### Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Target Types**.
4. In the **Target Types** table, click the icon ( ▶ ) next to the target type and then click **Account Defaults**.
5. On the Select an Account Attribute page, select the check box next to the attribute that you want to modify and take one of the following actions:

**Note:** The template value for the attribute is updated in the list on the Select an Attribute page.

- Changes the default value for the selected attribute.

**Note:** If you select this option when an attribute currently has a scripted default value, the existing script is overwritten with the template value that you specify.

- a. Select **Change**.
- b. Complete the appropriate fields, which vary depending on the target type.
- c. Click **OK**.
- Add or change the script that specifies a default value for the selected attribute.
  - a. Select **Change (Advanced)**.
  - b. Type the JavaScript code in the **Script** field.
  - c. Click **OK**.
6. On the Select an Account Attribute page, finish changing attribute defaults for the target type.
7. Click **OK**.
8. Change more account defaults or click **Close**

## Results

A message indicates that you successfully saved the account defaults on the target type.


## Removing account defaults from a target type

You can remove account defaults from a target type.

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

### Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Target Types**.
4. In the **Target Types** table, click the icon (  ) next to the target type and then click **Account Defaults**.
5. On the Select an Account Attribute page, select the check box next to the attribute that you want to remove and click **Remove**. Selecting the check box at the top of this column selects all attributes. The attribute default is removed from the list on the Select an Attribute page.
6. On the Select an Account Attribute page, finish removing attributes from the target type.
7. Click **OK**.
8. Remove more account defaults or click **Close**.

## Results

A message indicates that you successfully removed the account defaults from the target type.



---

## Chapter 11. Target administration

A *target* represents a user repository for a resource, such as an operating system, a database application, or another application that IBM Security Identity Governance and Intelligence manages. For example, a managed resource might be a Lotus Notes® application, and a service can be defined for a Lotus Notes User Repository.

### Overview

Targets are created from target types, which represent a set of managed resources that share similar attributes. For example, a default target type that represents Linux systems is one of the target types that is installed by default when you install IBM Security Identity Governance and Intelligence. Target types are also installed when you import the target definition files for the adapters for those managed resources.

Most targets provide an interface for provisioning accounts to users, which usually involves some workflow processes that must be completed successfully. Users access these targets by using an account on the target.

A *target owner* identifies the person who owns and maintains a particular target.

A user's profile is represented as an *account*.

### Target administration tasks

Use the Target Administration Console to do these tasks:

Table 13. Target administration tasks

Task	Refer to
Create targets.	"Creating targets" on page 88
Modify targets.	"Changing targets" on page 90
Delete targets.	"Deleting targets" on page 91
Schedule an account reconciliation.	"Creating a reconciliation schedule" on page 100
Initiate an immediate account reconciliation.	"Reconciling accounts immediately on a target" on page 99
View reconciliation status.	"Viewing reconciliation requests" on page 103
Define account defaults for a target by mapping to a user attribute directly or by using JavaScript.	"Adding account defaults to a target" on page 92
Change account defaults for a target.	"Changing account defaults for a target" on page 94
Remove account defaults from a target.	"Removing account defaults from a target" on page 95
View the connection status of a target.	"Viewing the target connection status" on page 96
Test the target connection.	"Testing the target connection" on page 96
Import target definition files, also called adapter profiles.	"Importing target types (adapter profiles)" on page 80

Table 13. Target administration tasks (continued)

Task	Refer to
Define account defaults for a target type (adapter profile) by mapping to a user attribute directly or by using JavaScript.	“Adding account defaults to a target type” on page 83
Change account defaults for a target type.	“Changing account defaults for a target type” on page 84
Remove account defaults from a target type.	“Removing account defaults from a target type” on page 85

## Target prerequisite

A target might have another target that is defined as a target prerequisite. Users can receive a new account only if they have an existing account on the target prerequisite. For example, Target B has a target prerequisite of Target A. If a user requests an account on Target B, the user must first have an account on Target A to receive an account on Target B.

---

## Target status

The IBM Security Identity Governance and Intelligence server tracks its ability to make remote connections and send provisioning requests to adapters on a per target basis. This ability is reflected in the Status for each target on the Manage Targets panel. On this panel, you can also search for targets with a specific status.

The value options in the **Status** list contain status values for each target:

**Active** Targets that function with no known issues.

**Failed** Targets that encountered a problem. For example, a connection test might fail or a request was not completed on an endpoint because of a problem with making a remote connection.

**Unknown**

Targets that never attempted a connection test or never received and processed a request.

---

## Creating targets

Create an instance of a target from a target type, such as the Linux profile or another adapter profile that you installed.

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can create a target in IBM Security Identity Governance and Intelligence, you must create a target type. Alternatively, use one of the target types that were automatically created when you installed Identity Governance and Intelligence. You can create a target type by importing the adapter profile. Alternatively, you can add new schema classes and attributes for the target to your LDAP directory. Before you can create a target for an adapter, the adapter must be



installed, and the adapter profile must be created.

## About this task

The target name and description that you provide for each target are displayed on the console. Therefore, it is important to provide values that make sense to your users and administrators.

To create a target instance, complete these steps:

## Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget. The Administration Console is displayed.
2. From the Administration Console, select **Target Administration**. The Target Administration Console is displayed.
3. From the navigation tree, click **Manage Targets**. The Select a Target page is displayed.
4. On the Select a Target page, click **Create**. The Create a Target wizard is displayed.
5. On the Select the Type of Target page, select a target type and click **Next**.  
If the table contains multiple pages, you can do the following tasks:
  - Click the arrow to go to the next page.
  - Type the number of the page that you want to view and click **Go**.
6. On General Information page, specify the values for the target instance. The content of the General Information page depends on the type of target that you are creating. The creation of some targets might require more steps. It is specific to the profile (adapter). See the adapter's *Installation and Configuration Guide* for the more information.
7. On the Users and Groups page, which is displayed only for LDAP targets, complete the required fields.
8. On the Authentication page, which does not display for every target type, complete the required fields.
9. On the Dispatcher Attributes page, specify information about the dispatcher attributes and click **Next** or **OK**. The Dispatcher Attributes page is displayed only for IBM Security Directory Integrator based targets.
10. On the Status and Information page, view information about the adapter and managed resource and click **Next** or **Finish**. The adapter must be running to obtain the information.
11. Optional: On the Application Information page, type a name and description for the application, and then click **Finish**.
12. Optional: Click **Test Connection** to validate that the data in the fields is correct, and then click **Next** or **Finish**. If the connection fails, contact the analyst who is responsible for the computer on which the managed resource runs.

## Results

A message is displayed, indicating that you successfully created the target instance for a specific target type.

## What to do next

Specify the account defaults for the target attributes. The required attributes are indicated by an asterisk (\*). Provisioning fails for required attributes that are not defined. For example, LDAP requires the attributes **Full name** and **Last name**. For more information, see “Account defaults on a target” on page 92.

Select another target task, or click **Close**. When the Select a Target page is displayed, click **Refresh** to refresh the **Targets** table and display the new target instance.

---

## Changing targets

You can change the information for a target instance.

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can change a target in IBM Security Identity Governance and Intelligence, you must create a target instance.

### About this task

You must specify the password when you test the target connection.

### Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:
  - a. Option. Click **Refresh** to update the **Targets** table
  - b. Type information about the target in the **Search information** field.
  - c. Select a target type from the **Target type** list.
  - d. Select a status from the **Status** list and click **Search**. A list of targets that matches the search criteria is displayed.

If the table contains multiple pages, you can do the following tasks:

    - Click the arrow to go to the next page.
    - Type the number of the page that you want to view and click **Go**.
5. In the **Targets** table, select the check box next to the target that you want to change and then click **Change**.
6. Change the values for the target instance and click **OK**. The changes that you can make to the target depends on the type of target. It is specific to the profile (adapter). See the adapter's *Installation and Configuration Guide*.
7. Select another targets task or click **Close**.

## Results

A message is displayed, indicating that you successfully changed the target instance.

---

## Deleting targets

Delete target instances when necessary. For example, you might delete a target instance for an obsolete application.

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can delete a target in IBM Security Identity Governance and Intelligence, a target instance must exist.

### Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:
  - a. Option. Click **Refresh** to refresh the **targets** table.
  - b. Type information about the target in the **Search information** field.
  - c. Select a target type from the **Target type** list.
  - d. Select a status from the **Status** list.
  - e. Click **Search**. A list of targets that matches the search criteria is displayed.  
If the table contains multiple pages, you can do the following tasks:
    - Click the arrow to go to the next page.
    - Type the number of the page that you want to view and click **Go**.
5. In the **Targets** table, select the check box next to the target that you want to remove and click **Delete**. Selecting the check box at the top of this column selects all target instances.
6. On the Confirm page, click **Delete** to remove the selected target instance or click **Cancel**. The targets are removed automatically from all policies that currently reference them. If all targets referenced by a policy are deleted by this operation, the entire policy is also deleted. All accounts that are related to that target are also deleted. However, they are not de-provisioned from the managed resource.
7. Select another targets task, or click **Close**.

## Results

A message indicates that you successfully deleted the target instance.

---

## Account defaults on a target

You can define default values for account attributes either on a target or a target type. This step is required only for the attributes in the user interface that are marked with an asterisk (\*).

### Types of account defaults

#### Target type account defaults

When account defaults are defined at the *target type level*, they apply to all targets of that type. However, you can override a target type default by defining an account default at the *target level*.

#### Target account defaults

These defaults are inherited from the target type account defaults, but they become local to the target as soon as it is changed. Local account defaults can be changed or removed. Changes and removals do not affect the target type account defaults.

You must specify the account defaults for the required attributes of the target. The required attributes are indicated by an asterisk (\*). Provisioning fails if the required attributes are not defined. For example, the attributes *Full name* and *Last name* are required for LDAP. For more information, see “Account defaults on a target.”

### Options for defining default values for account attributes

**Basic** You can hardcode default values for an account attribute.

#### Advanced

You can code JavaScript to retrieve data from Identity Governance and Intelligence objects and set the value for an account attribute. As a starting point, you can create a basic account default and then use the advanced option to edit the generated JavaScript.

For account defaults, you can use the JavaScript objects *subject* and *service*, where *subject* is a *DirectoryObject* that represents a person, and *service* is a *DirectoryObject* that represents a target. For example, the JavaScript for the **Gecos** (comments) attribute is:

```
return "Account for "+ subject.name+" on "+service.name;
```

## Adding account defaults to a target

You can add default values for attributes. When you create an account for a target, the default values are provided. This task is required only for the attributes that are marked with an asterisk (\*) in the user interface.

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You must create a target instance before you begin this task.

## About this task

Defaults are inherited from the target type account defaults, but they become local to the target as soon as they are changed. Local account defaults can be changed or removed. Changes and removals do not affect the target type account defaults.

A message indicates whether account defaults are already defined on the target type. If you click **OK**, the account defaults for the target type are copied to the target. You can either change the account defaults or remove them from the target. Changes and removals do not affect the account defaults on the target type.

You must specify the account defaults for the required attributes of the target. The required attributes are indicated by an asterisk (\*). Provisioning fails if the required attributes are not defined. For example, the attributes *Full name* and *Last name* are required for LDAP. For more information, see “Account defaults on a target” on page 92.

## Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:
  - a. Type information about the target in the **Search information** field.
  - b. Select a target type from the **Target type** list.
  - c. Select a status from the **Status** list and click **Search**. A list of targets that matches the search criteria is displayed.

If the table contains multiple pages, you can do the following tasks:

    - Click the arrow to go to the next page.
    - Type the number of the page that you want to view and click **Go**.
5. In the **Targets** table, click the icon ( ▶ ) next to the target to show the tasks that can be done. The tasks depend on the type of target.
6. Click **Account Defaults**.
7. On the Select an Account Attribute page, click **Add**.
8. On the Select an Attribute page, select an account attribute.
9. Choose one of the following options to add the attribute default to the list on the Select an Attribute page:
  - Add a default value.
    - a. Click **Add**.
    - b. Complete the appropriate fields, which vary depending on the type of target.
    - c. Click **OK**.
  - Add a script that specifies a default value.
    - a. Click **Add (Advanced)**.
    - b. Type the JavaScript code in the **Script** field. For account defaults, you can use the JavaScript objects *subject* and *service*.

Where

*subject* is a **DirectoryObject** that represents a person.

*service* is a **DirectoryObject** that represents a target.

The following example shows the JavaScript for the **Gecos** (comments) attribute.

```
return "Account for "+ subject.name+" on "+service.name;
```

- c. Click **OK**.
10. On the Select an Account Attribute page, click **OK** when you finish adding attribute defaults to the target instance.
11. Add another account default or click **Close**.

## Results

A message indicates that you successfully saved the account defaults on the target.

## Changing account defaults for a target

You can change the account defaults for a target instance.

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You must create account defaults for the target or target type before you begin this task.

### About this task

You can change the default values for attributes. The changed default values do not affect existing accounts; they are used for new accounts that are created on the target.

### Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:
  - a. Type information about the target in the **Search information** field.
  - b. Select a target type from the **Target type** list.
  - c. Select a status from the **Status** list and click **Search**. A list of targets that matches the search criteria is displayed.

If the table contains multiple pages, you can do the following tasks:

    - Click the arrow to go to the next page.
    - Type the number of the page that you want to view and click **Go**.
5. In the **Targets** table, click the icon (▶) next to the target to see the tasks that can be done on the target. The tasks that you can do depend on the type of target.
6. Click **Account Defaults**.
7. On the Select an Account Attribute page, select the check box next to the attribute that you want to modify.
8. Choose one of the following options to update the template value on the Select an Attribute page:

- Change the default value.

**Note:** If you select this option when an attribute currently has a scripted default value, the existing script is overwritten with the template value that you specify.

- Click **Change**.
  - Complete the appropriate fields, which vary depending on the type of target.
  - Click **OK**
- Adds or change a script that specifies a default value for the selected attribute.
    - Click **Change (Advanced)**.
    - Type the JavaScript code in the **Script** field.
    - Click **OK**
9. On the Select an Account Attribute page, click **OK** when you finish changing attribute defaults.
  10. Select another account default task or click **Close**.

## Results

A message indicates that you successfully saved the account defaults on the target.

## Removing account defaults from a target

You can remove account defaults from a target instance.

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You must create account defaults for the target before you begin this task.

### Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:
  - a. Type information about the target in the **Search information** field.
  - b. Select a target type from the **Target type** list.
  - c. Select a status from the **Status** list and then click **Search**. A list of targets that matches the search criteria is displayed.
 

If the table contains multiple pages, you can do the following tasks:

    - Click the arrow to go to the next page.
    - Type the number of the page that you want to view and click **Go**.
5. In the **Targets** table, click the icon ( ▶ ) next to the target to show the tasks that can be done on the target, and then click **Account Defaults**. The tasks that you can do depend on the type of target.

6. On the Select an Account Attribute page, select the check box next to the attribute that you want to remove. Selecting the check box at the top of this column selects all attributes.
7. Click **Remove**. The attribute default is removed from the list on the Select an Attribute page.
8. On the Select an Account Attribute page, finish removing attributes from the target instance and click **OK**.
9. Select another account default task or click **Close**.

## Results

A message indicates that you successfully removed the account defaults from the target.

---

## Viewing the target connection status

You can view the connection status for the targets that you own on Target Administration Console.

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can view a target's connection status, a target instance must exist.

### Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. To view the details for each target connection, expand **Target Connection Status** ( ▶ ).
4. Optional: Change the target configuration and test the connection.
  - a. Click the target name.
  - b. On the Change Target page, change the settings.
  - c. Click **Test Connection**.

---

## Testing the target connection

You can test the connection for the targets that you own.

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can test a target's connection, a target instance must exist.



## About this task

**Note:** You also can test the target connection when you create or change a target with **Manage Targets** task.

If you modify a target, you must specify the password when you test the connection.

The Target Administration Console shows the connection status for all the targets that you own.

## Procedure

To test the target connection, complete these steps:

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. On the Welcome page, expand the **Target Connection Status** twistie (▸) to view the details for each target connection.
4. Click the target name.
5. Click **Test Connection**. A message indicates whether the connection is successful.
6. If necessary, change the target's configuration and test the connection again.

---

## Reconciliation management

Reconciliation synchronizes the accounts and supporting data to the IBM Security Identity Governance and Intelligence central data repository from a managed resource. Reconciliation is required so that Identity Governance and Intelligence data is consistent and up-to-date with the remote resource.

### Reconciliation overview

Reconciliation ensures the accuracy of permissions and accounts data for the managed targets. Reconciliation can be scheduled to run routinely (for example, daily) or initiated by the administrator. The reconciliation schedule is stored in the Identity Governance and Intelligence database.

When the reconciliation schedule is triggered, Identity Brokerage runs a reconciliation through an Identity Brokerage Adapter. It compares the search results of the recent reconciliation with the data stored in the target cache. Identity Brokerage stores the delta data, change events, in the Recon Change Event database. Changes are saved in the target cache. These changed events are retrieved and posted back to the Target Administration Console.

During reconciliation, new accounts on the managed resource are created in the Identity Governance and Intelligence repository and assigned to the user based on the adoption policy for the target. If there is no user match for the account, the account is displayed as an orphan account that an Identity Governance and Intelligence administrator can manually assign to a user. Modified accounts on the managed resource are updated to the Identity Governance and Intelligence repository. Accounts that are removed from the managed resource are also removed from Identity Governance and Intelligence.

You can manage schedules for reconciliation or initiate a reconciliation activity immediately. To determine an ownership relationship, reconciliation compares account information with existing user data stored on Identity Governance and Intelligence. It first looks for the existing ownership in Identity Governance and Intelligence. It then applies adoption rules that are configured for the reconciliation.

If there is a match of a user login ID to an account, the software creates the ownership relationship between the account and the person. It also verifies that the accounts fit in the constraints of a defined policy. If there is no match, it lists the unmatched accounts as orphaned accounts.

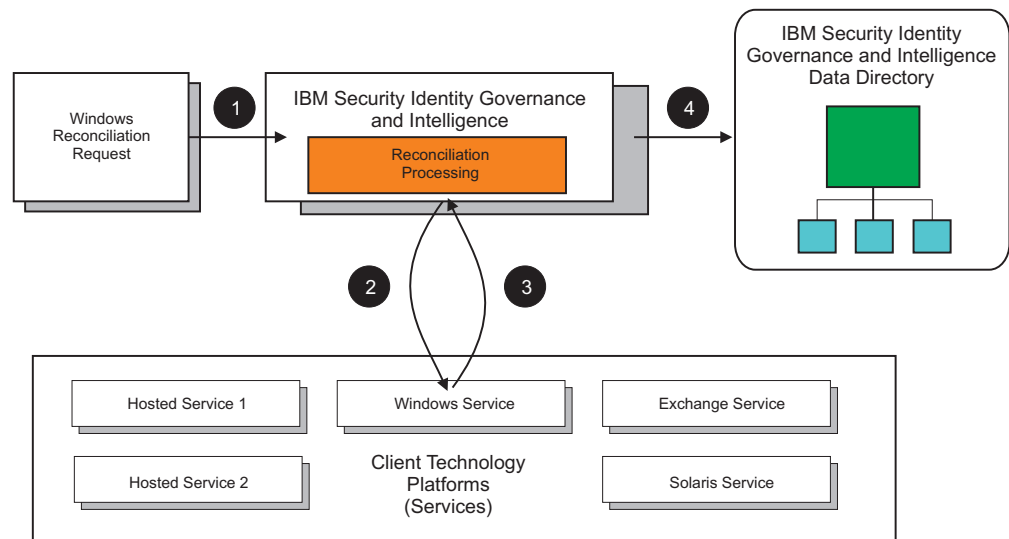
You run reconciliation to load accounts and supporting account information, which includes groups, into Identity Governance and Intelligence. Reconciliation inserts accounts from the managed resources into the Identity Governance and Intelligence directory.

Managed target accounts can be excluded from reconciliation on the Identity Governance and Intelligence and on the managed target itself for some adapters.

Set up reconciliation schedules based on the frequency of data changes. Leave enough time between two reconciliations. Avoid unnecessary reconciliations.

## Reconciliation process

The following illustration is an overview of the reconciliation process. In this example, the software reconciles Windows Server data.



The numbered steps in the following table correspond to the illustration.

Step	Description
1	An administrator submits a reconciliation request to a system with security that is managed by Identity Governance and Intelligence.
2	The software sends the reconciliation request to the selected target.
3	The target collects information from the system and sends the information to Identity Governance and Intelligence.

Step	Description
4	The software reads the information and reconciles the Identity Governance and Intelligence directory with account information from the target.
5	Identity Governance and Intelligence attempts to find the account owner.

## Reconciliation timeout and failure threshold

During reconciliation, you must consider the timeout and failure thresholds.

### Timeout

Reconciliation timeout is the duration of the reconciliation. Reconciliation can be scheduled, or it can be triggered on demand from the Target Administration Console. You can set the timeout value only for a scheduled reconciliation. There is no option to modify the default timeout value for reconciliation on demand.

The default maximum timeout value for reconciliation on demand is 600 minutes.

### Failure threshold

Reconciliation failure threshold (**enrole.reconciliation.failurethreshold**) is the maximum number of local accounts to delete at the end of a reconciliation.

You can configure this property. Keep the following points in mind:

- If the system exceeds the value you specified, then no local account or supporting data entries are deleted.
- If the value is followed by %, it specifies the maximum as a percentage. Otherwise, the value is the total number of local accounts before reconciliation starts plus the new accounts that are returned after the reconciliation.
- The default value is 15%. There is no limit.

#### Related tasks:

“Creating a reconciliation schedule” on page 100

You can schedule a reconciliation for account and attribute data or only for supporting data from the managed target.

#### Related information:

Getting and setting the reconciliation failure threshold

## Reconciling accounts immediately on a target

You can initiate a reconciliation activity immediately on a target, rather than scheduling the reconciliation.

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you begin this task, you must create a target instance.

### Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.

2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:
  - a. Type information about the target in the **Search information** field.
  - b. Select a target type from the **Target type** list.
  - c. Select a status from the **Status** list, and then click **Search**. A list of targets that matches the search criteria is displayed.  
If the table contains multiple pages, you can do the following tasks:
    - Click the arrow to go to the next page.
    - Type the number of the page that you want to view and click **Go**.
5. In the **Targets** table, click the icon ( ▶ ) next to the target to show the tasks what can be done. The tasks depend on the type of target.
6. Click **Reconcile Now**.
7. Click **Submit** to request an immediate reconciliation activity.
8. Optional: To view the results, click **View the status of the reconciliation request**.
9. To prevent the reconciliation from running at the scheduled time, change or delete the scheduled reconciliation.
10. Click **Close**.

## Results

A message indicates that you successfully submitted a reconciliation request to run immediately.

## Creating a reconciliation schedule

You can schedule a reconciliation for account and attribute data or only for supporting data from the managed target.

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you begin this task, you must create a target instance.

### Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:
  - a. Type information about the target in the **Search information** field.
  - b. Select a target type from the **Target type** list.
  - c. Select a status from the **Status** list.
5. Click **Search** . A list of targets that matches the search criteria is displayed.  
If the table contains multiple pages, you can do the following tasks:
  - Click the arrow to go to the next page.

- Type the number of the page that you want to view and click **Go**.
6. In the **Targets** table, click the icon ( ▶ ) next to the target to show the tasks. The tasks that you can do depend on the type of target.
  7. Click **Set Up Reconciliation**.
  8. On the Manage Schedules page, click **Create**. The Set Up Account Reconciliation notebook is displayed.
  9. On the General page, type information about the reconciliation schedule.
  10. On the Schedule page, select a schedule interval for the reconciliation. The fields that are displayed depend on the scheduling option that you select.
  11. Click **OK**.
  12. Take one of the following actions:
    - Select another target task and click **Refresh** to refresh the **Targets** table.
    - Click **Close**.

## Results

A message indicates that you successfully created a reconciliation schedule.

## Changing a reconciliation schedule

After you create a reconciliation schedule, you can change it if necessary.

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

A reconciliation schedule must exist.

### Procedure

To change a reconciliation schedule, complete these steps:

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:
  - a. Type information about the target in the **Search information** field.
  - b. Select a target type from the **Target type** list.
  - c. Select a status from the **Status** list and click **Search**. A list of targets that matches the search criteria is displayed.
 

If the table contains multiple pages, you can do the following tasks:

    - Click the arrow to go to the next page.
    - Type the number of the page that you want to view and click **Go**.
5. In the **Targets** table, click the icon ( ▶ ) next to the target to show the tasks. The tasks that you can do depend on the type of target.
6. Click **Set Up Reconciliation**.
7. On the Manage Schedules page, select the check box next to the reconciliation schedule that you want to modify and click **Change**. The Set Up Account Reconciliation notebook is displayed.

8. Change the information on the General and Schedule pages and click **OK**.
9. Take one of the following actions:
  - Select another target task and click **Refresh** to refresh the **Targets** table.
  - Click **Close**.

## Results

A message indicates that you successfully updated an existing reconciliation schedule.

## Deleting a reconciliation schedule

After you create a reconciliation schedule, you can delete it if necessary.

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

A reconciliation schedule must exist.

### Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:
  - a. Type information about the target in the **Search information** field.
  - b. Select a target type from the **Target type** list.
  - c. Select a status from the **Status** list, and then click **Search**. A list of targets that matches the search criteria is displayed.

If the table contains multiple pages, you can do the following tasks:

    - Click the arrow to go to the next page.
    - Type the number of the page that you want to view and click **Go**.
5. In the **Targets** table, click the icon ( ▶ ) next to the target to show the tasks. The tasks that you can do depend on the type of target.
6. Click **Set Up Reconciliation**.
7. On the Manage Schedules page, select the check box next to the reconciliation schedule that you want to delete. Selecting the check box at the top of this column selects all reconciliation schedules.
8. Click **Delete**.
9. On the Confirm page, click **Delete** to delete the selected reconciliation schedule or click **Cancel**.
10. Take one of the following actions:
  - Select another target task and click **Refresh** to refresh the **Targets** table.
  - Click **Close**.

## Results

A message indicates that you successfully removed the reconciliation schedule.

## Viewing reconciliation requests

You can view the reconciliation requests and their status.

### Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you begin this task, you must create a target instance and schedule reconciliations.

### Procedure

To view the status of reconciliation requests, complete these steps:

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:
  - a. Type information about the target in **Search information**.
  - b. Select a target type from the **Target type** list.
  - c. Select a status from the **Status** list and click **Search**. A list of targets that matches the search criteria is displayed.

If the table contains multiple pages, you can do the following tasks:

    - Click the arrow to go to the next page.
    - Type the number of the page that you want to view and click **Go**.
5. In the **Targets** table, click the icon ( ▶ ) next to the target to show the tasks. The tasks depend on the type of target.
6. Click **View Reconciliation Requests**.
7. On the View Reconciliation Requests page, specify the search criteria and click **Search**. A list of reconciliation requests is displayed.
8. Optional: Cancel one or more reconciliation requests by selecting the check box next to a request and clicking **Cancel Request**.





---

## Chapter 12. User administration

Identity Governance and Intelligence administrators use the Administration Console to do user administration tasks, such as adding users to the system.

### User administration tasks

Use the Administration Console to do these tasks:

Table 14. User administration tasks

Task	Refer to
Add a user to the system	"Adding a user"
Configure user access	"Configuring user access to Service Center applications" on page 106
Assign an administrator role to a user	"Assigning an administrator role to a user" on page 107
Extend the UserErc table with extra columns to import more user data from another system	"Adding columns to the UserErc table" on page 107
Populate the data model	"Creating a bulk load operation" on page 61

#### Related information:

"Users" on page 117

Select this tab to define and manage users and items associated to them, such as entitlements, resources, accounts, rights and more.

---

## Adding a user

Complete this task to register a new user into the Identity Governance and Intelligence data model.

### Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage > Users**.
4. In the **Users** tab, click **> Actions > Add**.
5. In the **Details** tab, define a basic User profile. Specify information in the following fields and in the other fields, if applicable. See the related help topic for the options and their descriptions.
  - First Name
  - Last Name
  - Master UID
  - OU Master
6. Click **Save**.
7. In the Password window, create the password for the User.
8. Click **Ok**.

#### Related information:

“Users” on page 117

Select this tab to define and manage users and items associated to them, such as entitlements, resources, accounts, rights and more.

---

## Configuring user access to Service Center applications

Complete this task to enable Users to access the Application in Service Center. These Applications must be properly configured. Users must have the right Roles to access one or more Application.

### About this task

Being authorized to access an Application does not imply that you can run every task available within that Application. For example, you can have the Entitlement to work with Access Certifier. However, if no configured campaigns exist, then you cannot run any campaign review in this module.

### Procedure

1. Create a User. See “Adding a user” on page 105.
2. Log in to the Service Center. Use the credential of the User that you created. No applications are displayed in the Service Center landing page.
3. Assign a Role to the User. See “Assigning an administrator role to a user” on page 107.

Option	Description
<b>User Manager</b>	The user can view and access the following applications: <ul style="list-style-type: none"><li>• Reports</li><li>• Access Certifier</li><li>• Access Requests</li></ul> <b>Note:</b> A diagnostic message is displayed when the Access Requests application is not correctly configured.
<b>Application Manager</b>	The user can view and access the following applications: <ul style="list-style-type: none"><li>• Business Activity Mapping</li><li>• User-account matching</li></ul> <b>Note:</b> In particular, because the applications are hooked to an account, the accounts manageable in User-account matching depends by the scope application.
<b>Risk Manager</b>	This role is required to manage several activities in the Access Requests workflows.
<b>Employee</b>	This role is required to manage several activities in the Access Requests workflows.
<b>Reviewer Supervisor</b>	This role is required in Access Certifier.

4. Log in to the Service Center. Use the credential of the User you created. All applications are displayed in the Service Center landing page.

### Related information:

“Admin roles” on page 183

Admin roles are used to manage IBM Security Identity Governance and

## Assigning an administrator role to a user

Complete this task to assign an administrator role to a User.

### About this task

A set of default administrative roles are provided at installation to help ease the configuration of the other Identity Governance and Intelligence features. New roles can be added and the role structure can be modified. However, the modification of administrative roles must be done by an expert administrator.

### Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Configure > Admin Roles**.
4. In the **Flat View** tab, select one of the administrator roles.
5. Access the **Users** tab, click **Actions > Add**.
6. In the Add Users window, select one of the registered users and click **OK**.
7. Optional: In the Date Selection window, set the validity period of the assignment and click **OK**.
8. In the Resources window, define the scope specified for the selected administrator role by selecting entries from the table and selecting the **Add** and **Remove** icons.
9. Click **OK**.

#### Related information:

“Resources” on page 170

Describes how to manage resources and resource types.

---

## Adding columns to the UserErc table

You can extend the UserErc table with extra columns to import additional user data from another system.

### Before you begin

This task consists of two steps:

1. Adding the columns in the USER\_ERC table in the Identity Governance and Intelligence database.
2. Mapping the new attributes in the UserErc repository in Access Governance Core.

To complete this task, you must be an Identity Governance and Intelligence administrator.

### About this task

The UserErc repository contains user data that is imported from an external system through an Identity Governance and Intelligence enterprise connector. The columns of the repository are mapped in the users table of the Access Governance Core database. The columns follow the specifics that are defined through user virtualization in Access Governance Core.

The attributes of the UserErc repository correspond to the columns of the USER\_ERC table in the database. If you need extra columns to take in external data, follow this procedure.

## Procedure

1. Add the new column to the USER\_ERC table in the database.

On Oracle:

- a. Use sqlplus to connect to user IGA\_CORE.
- b. Run the following command:

```
alter table USER_ERC add new_column_name VARCHAR2(512 CHAR);
```

where *new\_column\_name* is the name of the column you are adding. For example, to add column HIRED\_ON, run:

```
alter table USER_ERC add HIRED_ON VARCHAR2(512 CHAR);
```

On DB2:

- a. Use clppplus to connect to user igacore.
- b. Run the following command:

```
alter table USER_ERC add new_column_name VARCHAR(512);
```

where *new\_column\_name* is the name of the column you are adding. For example, to add column HIRED\_ON, run:

```
alter table USER_ERC add HIRED_ON VARCHAR(512);
```

2. Log in to the Administration Console.
3. Select **Access Governance Core**.
4. Select **Settings > User Virtual Attributes**
5. Select the **UserErc** repository in the left pane, and click **Attribute Mapping** in the right pane.
6. Click **Actions > Add**. The Select attribute to add window is displayed.
7. Scroll down, select the attribute name that corresponds to the column you added in the USER\_ERC table, and click **Ok**. The new attribute is added on top of the **Name** column in the Attribute Mapping pane.
8. Proceed to add a label and to complete the mapping for the new attribute.

## Results

The new attribute is displayed with the user external data in the **Manage > Users** window of Access Governance Core.

---

## Chapter 13. Introduction to Access Governance Core

Access Governance Core (AG Core) is the central IBM Security Identity Governance and Intelligence module, dedicated to the implementation of the authorization processes.

It creates a centralized authorization system based on the role-based access control (RBAC) model, as defined by the Standard ANSI/INCITS 359-2004.

The key consideration is a user's role within an organization. Based on that role, the user is assigned the authorization to use specific organization resources and functions.

The Access Governance Core assigns to users, specific authorization profiles and oversees the management their lifecycles.

Access Governance Core provides a modeler that systematically outlines the current structure of an organization's organizational and technical components. The outline or organizational description is called a realm. It is implemented by a database that literally photographs how the company is structured, in terms of its organization units, users, resources, and applications.

Based on this description, an authorization profile is built for each user within the organization. The profile determines what a user can do within the realm, what resources can be accessed, and what operations can be performed on these resources.

The definition of an authorization profile intrinsically introduces rules that control the visibility of objects that are described in the realm. It makes only those applications, functions, and resources that are outlined in the user's profile accessible to the user.

A special feature in the Access Governance Core allows for multi-Realm management. You can define the management of multiple organizations and maintain their separate contexts that relate to different realms.

The Access Governance Core flexible architecture can integrate easily within existing IT architectures. Its scalable functions allow it to manage its progressive introduction within the host system.

---

### AG Core Architecture

To understand the AG Core architecture, study the following outline. It specifies the essential highlights of each component module.

The AG Core comprises the following elements:

- Administration Module
- Security API
- WSDL Interface
- EJB Layer
- DAO Layer

- DB (Identity Repository)

## **Administration Module**

The Administration module allows the complete management and configuration of AG Core. It is used to outline the Realm. It populates the organizational model under examination and defines entitlements for users who are a part of it.

The Administration realm, REALM 0, is always present. It contains the list of all administrators and their relative authorizations.

One or more administrators can be defined inside each realm. Each administrator can have a different degree of visibility to the entire realm or just one part of it, and a different set of functions to manage. The interface is multilingual.

## **Security API**

Security APIs provide tools for implementing a set of security services that cut across the entire AG Core architecture. They can be employed within any application client, serving to access the AG Core and its prerogatives.

Specifically, security APIs allow for the implementation of authentication policies that present varying degrees of resistance, based on different outlines that define the required security level.

Traditional authentication outlines are available that are based on a user name and password or advanced ones that are based on compliant smart cards PKCS11 and digital certificates X.509.

Available Java classes enable the management of the following security items:

- The authentication phase
- The security contexts that are related to entities that are logging on AG Core
- The security tokens that are involved in AG Core transactions
- The SAML communication standard.

## **WSDL Interface**

This part of the architecture allows for a set of web services to be exposed externally, which implements the same methods made available by the Security APIs.

Due to the nature of this technology, based on standards such as SOAP and XML, these services are available from any client web service consumer, without any platform limitations.

The APIs are available in both JAVA and .NET versions.

## **EJB Layer**

AG Core is entirely developed by using J2EE-EJB technology. To optimize performance, EJB-stateless sessions were employed. However, it is impossible to trace users who are calling an EJB method or to know whether they are authorized to do so. Management of these sessions is not possible.

The solution to the problem is the use of an XML token. It is signed and even encoded in some of its parts that contain a definition of the permission user. The token is created during the login phase, by using security APIs, and is populated with data from the user who requested access. After it is signed and eventually encoded, the token is given back to the caller application.

Every EJB method that differs from the login requires a token as a parameter.

The EJB reads from the token all the information that is related to the user caller. It returns the value of the method only after it ascertains that the user is authorized for the specified operation, and that the token was not modified. This security service on the EJB layer is requested when the product is installed on devices that are inadequately protected by network systems, and are exposed to external attacks.

When Access Governance Core is set up in an area that is highly protected and deemed secure, this application security mechanism can be disabled. Disabling this mechanism maximizes performance.

## DAO Layer

The DAO layer allows for the uncoupling of the business logic application (EJB) and the physical structure of the database. The interrogation logic of the database is rendered independent from the underlying database management system (DBMS), for example Access, ISAM, or SQL-DB.

## Database

From a logic viewpoint, the IBM Security Identity Governance and Intelligence Core database can be laid out in two main sections:

- The first section contains information for managing the realms and data for the AG Core configuration;
- The second section contains as many copies as the number of realms, the different organizations that are being managed. REALM 0 is used to define the administrators, and the authorizations that are related to them.

Each realm in the second section can be outlined and logically split into three main areas:

- A description of the organization of the company
- The set of applications and functions that can be provided
- The resources to be accessed.

Each of these three areas can be represented by an Entities-Relations diagram that describes the tables physically present on the database, and the relationships between them.



Figure 42. Logic architecture of the AG Core database

The DB is populated:

- According to indications of the realm administrator, through the administration console

- For a database with pre-existing data, the data can be transferred directly to the AG Core database, by using a set of batch procedures.

---

## Managing the Administration Realm

The AG Core distinguishes between an administration realm and other operating realms, which can conceptually be seen as complementary components of the general model.

These realms are identified by a name that is assigned to them by the administrator. For instance, the administration realm for a regional name healthcare unit might be named REALM\_RNHCU. An operating realm is sometimes referred to as just a realm.

The administration realm structure is identical to that of a generic realm. It comprises an application area, organizational area, and a resources area. However, it is managed differently than a generic realm since the administration realm allows for the complete management of administrators that belong to other realms.

All administrator users from other realms must be profiled in the administration realm and assigned the necessary functions to access and use the Access Governance Core. This phase represents the main point of the definition of the administration realm application area. The administrators can be assigned only a subset of the management functions that are expressed by the console, or accessible resources, or both. This subset can be customized at a single administrator level dependent upon on the privileges that are granted in a realm or subtree of the realm. The functions can be assigned either when the Access Governance Core is installed and configured, or afterward, during natural management and fine-tuning phases during the lifecycle of an organization.

The organizational area lists groups of administrators that are authorized to manage their related realms. Groups of administrators must be defined for the realms, and each of these groups is then defined within its relative OU.

Realms to be administered are represented as resource types in the administration realm. The different realms are created during the installation phase through SQL scripts.

### Product Administration

During the AGCore installation procedure, an administration realm is created, along with its related super administrator, who is responsible for defining the initial customizations. In addition, the first operating realm is also created.

The super administrator can create other realms and administrator groups.

**Note:** All operations that are supplied by the AGC for the generic profiling of users are also used for the profiling of administrators.

Accessing the administration realm, you can manage:

- Administrators
- Realms
- Visibility or scope
- Administration roles



## Administrator

An Administrator is a user that is registered as a member of an administration realm. The AG Core super administrator is created during the installation phase, whereas the other administrators must be created later. Administrators have administration privileges on their related realms.

A special category of users exists that can access privileges are assigned to the administrative realm to support the tasks of the super administrator, even in delegated mode.

## Realms

Realms are configured as resource types of a particular resource family, the realms family.

In general, the administration realm includes the following content:

- A resource family called Realms.
- The number of types that belong to the realms family is the same as the number of realms that are installed. The name of the type, **TypeName** *k*, coincides with the name assigned to the realm.
- For each type, a resource that coincides with the root OU for the realm that is defined by the type. The link is implemented through the field scope, in which the root name of the realm must be entered.
- After the root OU is defined, as many other resources can be added as there are organizational units in the realm. These resources can target any OU that differs from the root, to implement the concept of limited scope.

The following figure illustrates the presence of *N* types that belong to the realms family.

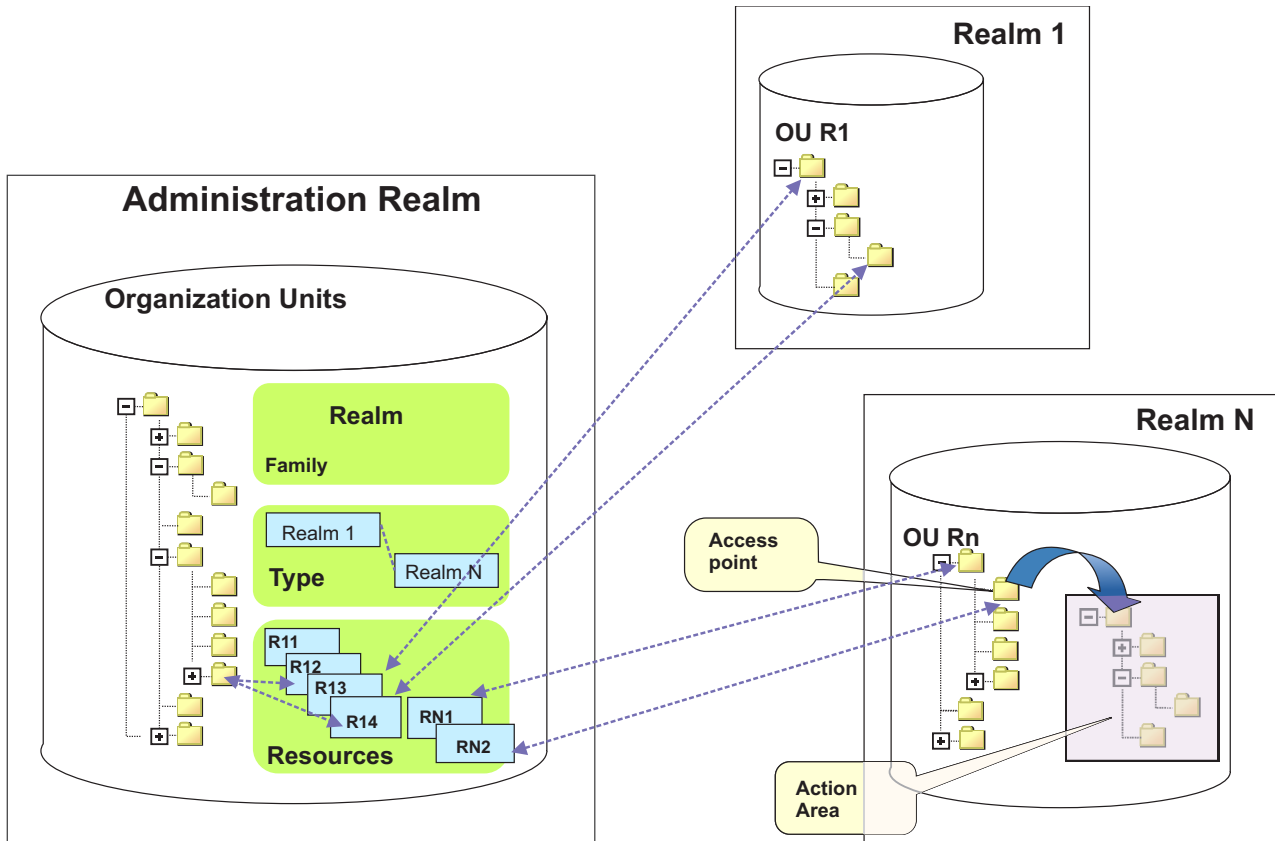


Figure 43. Operating realms as resources of the administration realm

Resources are specified for each type. Four resources are defined for realm type 1.

- R11
- R12
- R13
- R14

Two resources are defined for realm type N

- RN1
- RN2

Realm types 2 - N-1 are not visualized. The resource RN2 is an access point to the OU linked by the arrow. The subtree is visualized in the frame labels as **Action Area**.

### Visibility

A generic OU in the realms tree defines a level of visibility. This visibility can be implemented by constructing an access point, scope, to the organizational structure of the realm.

Each administrator can access the organizational subtree of the realm, whose root coincides with the access point.

There can be more than one access point for every realm. Each administrator can access only one access point.

## Functions that can be assigned in administration realm

The following table provides a list of all available functions on the Access Governance Core in the Administration Realm.

These functions cannot be modified, and can be assigned to roles only:

*Table 15. Assignable functions*

Functions	Description
CHANGE_USER_PWD	Change the user's password.
MODIFY_REALM_SETTINGS	Create, delete, and edit realm settings.
FIND_REALM_SETTINGS	Find realm settings.
MODIFY_USER	Create, delete, and edit user information.
FIND_USER	Find user information.
MODIFY_ORGUNIT	Create, delete, and edit organization units.
FIND_ORGUNIT	Find organization units.
MODIFY_ENTITLEMENT	Create, delete, and edit entitlements.
FIND_ENTITLEMENT	Find entitlements.
MODIFY_USER_ENTITLEMENT	Create, delete, and edit positions or employment of a user.
FIND_USER_ENTITLEMENT	Find positions or employment of a use.
MODIFY_ORGUNIT_ENTITLEMENT	Create, delete, and edit entitlements of an OU.
FIND_ORGUNIT_ENTITLEMENT	Find entitlements of an OU.
MODIFY_RESOURCE	Create, delete, and edit resources.
FIND_RESOURCE	Find resources.
MODIFY_ORGUNIT_RESOURCE	Create, delete, and edit resources of an OU.
FIND_ORGUNIT_RESOURCE	Find resources of an OU.
MODIFY_REALM_SETTINGS	Edit a realm configuration.
MODIFY_USER_ACCOUNT	Edit a user's account, for example, disable user, force change password, reset the last login, or reset login errors.
FIND_USER_ACCOUNT	Find data relative a user's account.
MODIFY_DELEGATED	Create, delete, and edit delegated users.
FIND_DELEGATED	Find delegated users.
MODIFY_ROLE_POLICY	Create, delete, and edit role policies.
FIND_ROLE_POLICY	Find role policies.
MODIFY_SERVICES	Create, delete, and edit services.
FIND_SERVICES	Find services.
MODIFY_USER_RESOURCES	Create, delete, and edit user resources.
FIND_USER_RESOURCES	Find user resources.
MODIFY_USER_SERVICES	Create, delete, and edit user services.
FIND_USER_SERVICES	Find user services.
MODIFY_ENTITLEMENT_SERVICES	
FIND ENTITLEMENT_SERVICES	

Table 15. Assignable functions (continued)

Functions	Description
MODIFY_APPLICATION	Create, delete, and edit applications.
FIND_APPLICATION	Find applications.

A default role, product administrator, in the administration realm is assigned all the functions previously described. Other administrative roles with limited functions can be created for administrators to whom only a subset of functions must be assigned.

Administration realm resources coincide with the access points for the realms to be administered. The realms coincide with resource types.

The resources that are access points for the roots of their realms are created automatically during the Access Governance Core installation. They are created by the SQL scripts that create the realms. The same process occurs for all the resource types that define the realms.

More Resources can be added manually, through the web console, where you might want to delegate the management of special subtrees in the realm to specific administrators. The resources represent organizational units that are roots of the subtree, whose management must be delegated.

The name of each resource type coincides with the name of the realm it represents.

The name of each resource identifies an access point, but doesn't need to coincide with the name of the OU whose subtree is being accessed. The specific selection of the OU is made by entering the OU name in the scope field in the resources data.

To be assigned to an administrator, a resource must first be assigned to the administrator's OU.

Two options are available for assigning resources to OUs:

#### **Inheritability**

If a resource represents the access point to a realm, is assigned to an OU, all administrators with a role in OU inherit the access privileges of the realm.

#### **Hierarchy**

Every resource that is assigned to the OU selected is automatically assigned to all child OUs of the OU.

The two options are not mutually exclusive.

If you decide not to use the inheritability option, the resources must then be assigned manually to users in the OU. However, different resources can be assigned to different users. This type of assignment is known as prompt.

Two administrators on Realm N represent two users who can potentially operate in the entire Realm N. By using prompt, you can assign them two different resources that provide them with two different access points. They act in different operating areas or subtrees in Realm N.

All resources for the administration OU are assigned through inheritability. Each resource that corresponds to each realm root is assigned to the administration OU with the restriction that each user in the administration OU has visibility to all the realms.

It is possible to define groups of administrators in the administration realm.

By creating an OU for each group and then by assigning resources to the defined OUs by inheritability, each user in the group acquires properties specific to the group. Every user that joins the OU inherits the resources of the OU, and has the same access privileges as all the other users in the OU.

Two resources that represent different scopes must not be assigned to the same user on the same realm. Creating two different access points on the same realm for the same administrator creates a conflict.

Two resources that represent different scopes must not be assigned through inheritability to the same OU on the same realm. The only way to create two different access points on the same Realm is to use prompt to assign the resources. One resource is assigned to one administrator and the other resource is assigned to the other administrators.

---

## Manage

The available functions for managing the main entities of this module are contained in the following list.

- Users
- Org Units (OU)
- Attribute Hierarchy
- Roles
- Applications
- Accounts
- Resources

## Users


Select this tab to define and manage users and items associated to them, such as entitlements, resources, accounts, rights and more.

The pane on the left lists the defined users and a number of attributes. You can use the **Filter** button to have only specific users listed. The following fields are available to narrow your search:

*Table 16. Available filters to list users.*

Filter	Description
User Type	Click the arrow and select one of the user types listed. The user type is defined in your security model.
UME	Flag this check box if the users you are searching have more than one account on the same target system.
Search Identity	Enter the name, the surname, or the master UID of the user.

Table 16. Available filters to list users. (continued)

Filter	Description
Associated	<p>If checked, the search result shows only users that are associated with a Group.</p> <p>If not checked, the search result shows only users that are not associated with any Group (for example, when a user is entered in the database but has not yet been associated with any Group).</p> <p><b>Note:</b> A user search run before the user is associated to an OU identifies the user only if the <b>Associated</b> check box is not checked.</p>
Groups	<p>Click the  <b>Browse</b> button to choose the Group of the user.</p>
Hierarchy	<p>If this check box is flagged, the search starts from the root Organization Unit selected in the <b>Groups</b> field and is run on all the hierarchy.</p>

Users are displayed in the Users list with the following symbols:

**User enabled/disabled**



**UME User enabled/disabled**



AG Core can manage various active access keys to applications that are assigned to the same user on a target system. User name and password are typical examples. Such credentials are typically the registration and administration keys that are managed as multiple keys assigned to the same user. A user who is associated to two or more access keys is called a User Multiple Entry (UME) User.

In the left frame, click **Actions** to run the following tasks on a selected user (excepting **Add**):

Table 17. Available actions on a selected user.

Action	Description
New UME	<p>Defines an additional access key for a selected user. As you select this action, the Details pane for the user is displayed in edit mode, where you can enter a new Master UID (the current MASTER UID is displayed as the Parent UID).</p>

Table 17. Available actions on a selected user. (continued)

Action	Description
Show UME	<p>Lists the selected user in multiple rows (one row per access key defined) in the Users list on the left. The Details views corresponding to the rows that follow the first row, list the first Master UID of the user as the Parent UID.</p> <p>Click <b>Search</b> to refresh the Users list when you are done.</p>
Fulfillment	<p>Displays an Entitlements Details window with a list of External roles defined for a selected user.</p> <p>For every permission granted to the user, you can verify the status, the date and the party who granted the permission. This gives you the means to ensure that the user did receive permissions for operating in a specific environment.</p>
Add	<p>Adds a user to the AG Core repository.</p> <p>When you add a user, the <b>Master Account</b>, is automatically created. See Accounts for more information.</p>
Remove	<p>Removes a user from the AG Core repository.</p>

This is the procedure for adding a user.

The content of the right frame changes depending on the tab that is selected in the upper side of the frame. When you click **Manage > Users**, the **Details** tab is shown by default. Under this tab are two distinct accordion panes (click the title bar to expand each pane):


**Details**

As you select a user, shows the user's data defined in the AG Core database.

**Data** Displays data (about the selected user) that is contained in external repositories.

You can view or modify the following details for a selected user in the Details pane:

Table 18. User details

Detail	Description
User Type	Indicates the type of the User. Click the  <b>Browse</b> button to view the choices provided in the User Types window. This data can be used to indicate the level of the user, such as user manager or security officer. For external users, it indicates the type of relationship with the organization, for example, business partner, customer, or supplier.
OU Master	The Organization Unit to which the user belongs.
Master UID	The Univocal identifier of the user.
System UID	<i>To be defined.</i>
Identity UID	<i>To be defined.</i>
Account Expiration	Indicates the expiration date of the User account. It is entered automatically based on the settings defined in the Accounts section. It can be modified by the Administrator.

**Note:** The **User details** pane contains other user information such as: First and last names, email, phone number, the Distinguished Name, SSN/Fiscal Code, gender, date and place of birth, address, city, state, country, and ZIP/Postal Code.

To edit the details of a selected user, select **Edit** at the bottom and click **Save** to validate the changes.

When the **Edit** tab is active, you can transfer a user from one OU to another, or assign a newly registered user to an OU. The entitlements that are aggregated to the user during the transfer process are automatically managed. Click the ellipsis (...) to display the User Transfer window where, in **View**, you can select an OU and then click **Actions > ToggleMngr > OK** to assign the user to the selected OU. After clicking OK on a confirmation window, you are presented with the following choices:

**Assign only default entitlements**

The user loses all previously assigned permissions and receives only the default entitlements in the new OU.

**Assign all compatible entitlements**

The user loses all permissions that are not associated with the new OU. However, the user maintains the entitlements that are common to the two OUs. At least, the user is assigned the default entitlements of the new OU.

The other tabs you can click on a selected user are:

- Entitlements
- User Resources
- Accounts
- Rights
- Mitigation
- Events



**Related tasks:**

“Adding a user” on page 105

Complete this task to register a new user into the Identity Governance and Intelligence data model.

**Entitlements**

Use the **Entitlements** tab to assign or delegate entitlements.

In the **Entitlement** tab you can select two accordion panes:

- **Assigned**
- **Delegated**

The **Assigned** pane shows the entitlements that are permanently assigned to the user in two modes:

- A tree view where the entitlements are listed hierarchically by application (displayed by selecting **View**).
- A plain list of the entitlements ordered by name (displayed by selecting **Search**).

You can filter entitlements, according to filters indicated in the following table.

*Table 19. Entitlement filters*

Filter	Description
<b>Group</b>	The name of a specific group belonging to the hierarchy
<b>Application</b>	The application name.
<b>Type</b>	The entitlement type. It can be one of the following <ul style="list-style-type: none"> <li>• Permission</li> <li>• IT Role</li> <li>• Business Role</li> <li>• External Role</li> </ul>
<b>Name or Code</b>	Entitlement name/code.

Click the **Actions** button to display the following items:

**Add Delegated**

Adds the entitlements of a selected user in the left frame to another user that acts as the delegate of the selected user.

**View Delegated**

Shows all the delegated users of the user that was selected in the left frame.

**Hierarchy**

Shows information about the hierarchical structure of the selected entitlement.

**Details**

Shows the information that is related to all permissions of the selected entitlement.

**Add** Adds an entitlement to the selected user.

## Remove

Removes an entitlement from the selected user. You can use the [Ctrl] or [Shift] keys for multiple selections.

The entitlements assigned to the selected user are listed according to the entitlement properties described in the following table.

Table 20. Entitlement properties

Property	Description
<b>VV</b>	An Entitlement is in VV when you want to assign an entitlement to a specific user of that OU. The entitlement is not available to the other users of the OU.
<b>Name</b>	Entitlement name.
<b>ID Code</b>	Entitlement code.
<b>Application</b>	Application name that is related to the selected entitlement.
<b>Group Name</b>	Name of a specific group belonging to the hierarchy indicated in the column <b>Hierarchy</b>
<b>Group Code</b>	Code of a specific group belonging to the hierarchy indicated in the column <b>Hierarchy</b>
<b>Hierarchy</b>	Name of the Attribute Group Hierarchy which involving the Entitlement
<b>Start/End Date</b>	The start or end date of the entitlement validity period.
<b>Creation Date</b>	The date that the entitlement was assigned to the selected user.
<b>Originator</b>	The code that indicates who assigned the entitlement to the selected user.
<b>Represented Code</b>	The code of the represented user.

The assignment of an entitlement to a user can have an optional validity period. If a validity period is set, there is start date after which the Entitlement assignment is valid and an end date when the assignment expires. These dates can be set during the assignment. The start date is typically the same as or after the creation date. The effective assignment of the entitlement to the user is realized by a scheduled task.

For an Add operation, you can add only the entitlements that are assigned to the Group Name entity of the selected user.

The **Delegated** pane shows the entitlements that were temporarily assigned (delegated) by another user. It displays two panels: the left one shows the identity of the delegator, while the right one shows the properties of the entitlement.

## User Resources

You can add resources to users.

A Resource is assigned to the employment of the user, through the user's entitlements.

Resources can be aggregated to a selected user in two ways:

#### **Inherited**

When a user is aggregated to an OU, the user inherits all the resources that are assigned to the OU.

#### **Assigned**

When a set of resources is assigned to an employment of a user, the user is assigned all of the resources that were assigned to the employment.

When a user is selected in the left frame, the right frame displays the following options:

- To view the resource that is already assigned to the user
- To add new resources
- To remove resources
- To check conflicts on a set of entitlements that is aggregated to a user
- To view the entitlement hierarchy.

A set of *Resource* accordion panes is displayed that directly refers to the entities of the IBM Security Identity Governance and Intelligence Data Model:

- **External**
- **OU**
- **Entitlement**
- **Application**
- **Resource Type**
- **Resource Family**
- **Risk**
- **Attribute Hierarchy**

### **Resources Accordion panes**

Every accordion pane has two frames.

In the left frame, you can view the user's entitlements. You can filter and search by clicking the **Filter/Hide Filter** button. You can search for entitlements by **Type**, the entitlement type, and by **Name**, the entitlement name, filters.

The **Actions** menu of the left frame, has two buttons, **Parents** and **Conflicts**.

Click **Parents** to open the Entitlement Hierarchy window that shows the hierarchy of the selected entitlement.

Click **Conflicts** to open the Conflict info window that shows the Risk tree in the **Risk info** tab. You can define Mitigation actions from the **Mitigation** tab.

To view the resources, click the **Inherited Resources** tag or on **Assigned Resources** tag in the entitlements list. The results are listed in the right frame.

**Note:** The inherited resources cannot be removed.

From the right frame, click the **Filter/Hide Filter** button, to filter and search resources according to the filters in the following table.

Table 21. Resources filters

Filter	Description
Family	Family of the resource.
Type	Type of resource.
Name	Name of the resource.

The **Actions** menu of the right frame, has two buttons, **Add** and **Remove**.

Click **Add** to open the Entity Resources window that shows the list of available resources. Select the resources that you want to add. You can use the [Ctrl] or [Shift] keys for a multiple selection. Click **Ok** in the window to complete the operation.

To remove an assigned resource, select the resource. Click **Remove** in the Remove Resources window. Click **Ok** to complete the operation.

## Accounts

You can create and manage user accounts and set user passwords.

When a new user is entered, an account named **Ideas** is automatically created for this user in AG Core.

Select **Manage > Account** to get information on accounts.

The Accounts pane displays the list of accounts that are available to the selected user.

Every account is identified by **Configuration Name – ID Code**.

After selecting an account, you can click **Actions** to perform one of the following actions:

### Details

Provides information on the selected account

### Change Date

Displays a calendar where you can change the expiration date of the account

### Force Pwd

Forces a password change

### Suspend/Restore

Displays the Account Suspending Code window where you can suspend or restore an account

### Change Pwd

Enables the Password change action for the selected user

### Reset Login

Resets the login to the selected account

**Add** Creates a User - Account association

### Remove

Removes an account associated with the selected user

Accounts have expiration dates. The administrator can also suspend accounts before they expire.

The **Account Suspension Code** shows fields that describe the reasons for suspending and account:

- **Technical**
- **Security**
- **Terminated**
- **Authoritative**
- **Expire**
- **Maintenance**

Every reason has a severity that ranges from 1 to 9. The severity degree can be customized based on the policies of the organization.

Accounts can be suspended for more than one reason. They are restored when all fields are reset to zero.

**CAUTION:**

**The suspension of the Ideas master account automatically affects all of the other accounts of a user.**

Click **Actions > Details** to see the following data:

*Table 22. Account details*

<b>Detail</b>	<b>Description</b>
<b>Applications</b>	Applications associated with the account configuration
<b>Master UID</b>	Identifies the user on the AG Core module
<b>Last Login</b>	Date of the last login
<b>Last Login Error</b>	Date of the last login error
<b>Number of Login Errors</b>	Number of consecutive login errors. This value is reset to zero when a correct login is performed.
<b>Last Password Change</b>	Date of the last password change
<b>First Name</b>	Name of the User
<b>Last Name</b>	Surname of the User
<b>Email</b>	Email address of the User
<b>DN</b>	Distinguished Name of the User

## **Rights**

Rights are extra attributes that are related to the permissions.

In the **Rights** tab, you can modify the value of the rights already assigned to a user selected in the **Users** tab.

“Rights” on page 16 are defined by the **Key** and **Value** attributes.

**Key** is an identifying name. You can define **Value** each time. **Value** might have a default value that you can modify.

Rights can be either of the following types:

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

**Access Governance Core > Configure > Rights Lookup** makes the setting of the lookup.

Rights are assigned to a user through the assignment of an entitlement that holds permissions joined to rights.

The assignment can be made mainly:

- During an authorization workflow (Access Request module)
- Through the run of rules (Rule Engine)
- When a permission is assigned to an entitlement. It is assigned to all users that hold the entitlement.

The value of the right is set during the assignment phase.

Moreover, the values of a right can be also **fixed** or **restricted**. This last one only in case of multi-value with lookup. These properties can determine dynamically the value of a right when you have the same right (R1) joined to two distinct entitlements (E1 and E2) that are assigned to the same user.


The following table shows the setting of a single right R1, joined to two entitlements E1 and E2, when these two entitlements are contextually assigned to a user.

*Table 23. Functions*

Right class	E1 (R1)	E2 (R1)	FIXED	RESTRICTED
<b>Single value (SV)</b>	V1	V2	VI XOR V2	Not applicable
<b>Multiple value (MV)</b>	V1, V2	V2, V3, V4	Union = (V1, V2, V3, V4)	Not applicable
<b>SV with Lookup</b>	V1, V2, V3, V4, V5, V6	V1, V2, V3, V4, V5, V6	VI XOR V2	Not applicable
<b>MV with Lookup</b>	V1, V2, V3, V4, V5, V6	V1, V2, V3, V4, V5, V6	Union = (V1, V2, V3, V6)	Any possible subset of Union. See the left column.

The values in the table are an example of possible values for R1. R1 can assume different values when associated to different entitlements.

From the example, it is evident that the most flexible pattern is **MV with Lookup**.

Near the field **Value**, click on  button.

In the pop-up window, select in left list the available values to set.

Click on right blue arrow, thus click **Ok**.

If the right is defined as **Multi Value** multiple values are displayed in the field **Value**.

## Mitigations

If a selected user is assigned a risk level, you can set a mitigation action for one or more of the at risk activities.

See Mitigation actions.

The risk information tree is displayed in the right frame. The first level displays a set of risks. The second level displays the user's at risk activities and any aggregated mitigation actions.

In the following example, an SoD risk results from a pair of activities.

The screenshot shows a web interface with a navigation bar at the top containing tabs: Details, Entitlements, User Resources, Accounts, Rights, Mitigation (selected), Events, and Managers. The main content area is divided into two sections. The upper section displays a tree view under the heading 'new My Risk 1' (marked with a red circle). The tree contains three items: 'My activity 2', 'My activity 1', and 'CM01 Wip\_D'. Below the tree are 'Add' and 'Remove' buttons. The lower section is a table with the following data:

Control Name	Control Code	Description	Last Modified By (User)	Date/Time Last Modified	Creation Date
CM01 Wip_D	194 - CM01	Checks from the Unit Head - SAT Responsible Delegated	demo - Demo User	17/12/2013 12:11:27	17/12/2013 12:11:27

At the bottom of the table, there is a pagination control showing 'Entities: 1' and a dropdown menu set to '25'.

Figure 44. Mitigation: general view

In the lower half of the right frame, the mitigations that are already assigned to the user are listed. In this example, **CM01 Wip\_Dis** is listed.

You can add another mitigation, if any are available, by selecting the risk and clicking **Add**.

In the Appropriate Mitigations window, you can choose the mitigation and click **Ok**.

You can have a user with  $N$  aggregated mitigations. The number  $N$  is the sum of  $K_1+K_2+\dots+K_n$  mitigations that are related to different sets of at risk activities. You can remove the mitigation by selecting it and clicking **Remove**.

## Events

IBM Security Identity Governance uses an integration interface to align and synchronize the data that is contained in the AG Core database with the data that is contained in the target systems.

A central role in the management of the synchronization is assigned to events.

An event is a brief yet complete description of what occurred an element in any part of the architecture. Usually the events can be generated by the AG Core itself or indirectly, by the target systems. Every time a system acts on the data, the changes are copied in appropriate packages, or events. These events are then sent to inform the other systems about that are listening.

Events are contained in appropriate tables of events, which are integral parts of the integration interface for the communication with the target systems. The AG Core communicates with the interface through events.

In the input flow, the target system that is connected to the input interface, communicates each change that is made to its data. The interface creates an event with information that is needed for the alignment, and then transmits it to the AG Core.

In the output flow, the AG Core changes the data and creates the corresponding events. It then transmits the events to the output interface, to which the related Target systems are connected. For each event, a state attribute is set to indicate the status of the event in the connection flow

An event can have one of the following states:

**Unprocessed**

The event was generated, but the alignment of the data is not yet performed.

**Success**

The alignment of the data was run successfully. An event in this state can automatically be eliminated or maintained as memory of the modification.

**Error** The Event was correctly generated, but an error was detected in the alignment of the data.

You can view all the events that belong to a selected user.

The input events are shown in the IN Events accordion pane and the output events are shown in the OUT Events accordion pane.

In the IN Events accordion pane, click Filter/Hide Filter to view the set of filters that are shown in the following table:

*Table 24. IN events filters*

Filter	Description
<b>Status</b>	Event status can assume one of the following three values: <ul style="list-style-type: none"> <li>• Unprocessed</li> <li>• Success</li> <li>• Error</li> </ul>
<b>Operation</b>	Indicates the type of operation that is run on the external table. <p>The following values are allowed:</p> <ul style="list-style-type: none"> <li>• Create user (directly or scheduled)</li> <li>• Modify user (directly or scheduled)</li> <li>• Delete user (directly or scheduled)</li> <li>• Move employee. Moves a user from one OU to another (directly or scheduled)</li> <li>• Custom</li> </ul>



Table 24. IN events filters (continued)

Filter	Description
Account ID	Univocal identifier of the account.
Trace	Brief description of the error cause.
Event Start/End Date	Filters defining the time period for the search.

The set of events that are filtered is shown in a list where every event is characterized by a set of attributes. The attributes are listed in the following table.

Table 25. IN Event structure

Field	Description
ID	Event identifier.
User ERC	User identifier in the USER ERC table.
Operation	The following values are allowed: <ul style="list-style-type: none"> <li>• Create User (directly or scheduled)</li> <li>• Modify User (directly or scheduled)</li> <li>• Delete User (directly or scheduled)</li> <li>• Move Employee (moves a user from one OU to another (directly or scheduled))</li> <li>• Custom</li> </ul>
Status	Event state can assume only three values: <ul style="list-style-type: none"> <li>• Unprocessed</li> <li>• Success</li> <li>• Error</li> </ul>
Trace	Contains the description of an error that occurred during event processing (ordinarily appears as Status = Error).
Identification Number	Contains unique information that is related to the user. For example, in the US with this parameter might be mapped the social security number (SSN).
OU Code	Indicates the unique identifier of an OU.
Action Type	This parameter usually is not used in IBM Security Identity Governance, but might be useful to interface some HR systems. For example, a SAP-HR, that provides this information after some particular actions on users. This parameter can be used even by custom business rules to define or manage some specific behaviors of the system.
Action Reason	This parameter usually is not used in IBM Security Identity Governance, but might be useful to interface some HR systems (es. SAP-HR) that provides this information after some particular actions on Users. This parameter can be used even by custom business rules to define/manage some specific behaviors of the system.
Event Date	Indicates the date of generation of the event.

Table 25. IN Event structure (continued)

Field	Description
Process Date	Indicates the date by which the event must be processed by the RE. Typically this date coincides with the event date but can be later if the events processing is postponed.
Ownership	Indicates the user database that caused the event on the external table.

**Note:** The fields that are indicated from free attribute 1 to *N*, depend on the target system, typically an HR system. These fields can vary widely.

In the OUT Events accordion pane, the set of filters that are shown in the following table is available.

Table 26. OUT Events filters

Filter	Description
Status	Event state can assume only three values: <ul style="list-style-type: none"> <li>• Unprocessed</li> <li>• Success</li> <li>• Error</li> </ul>
Operation	Indicates the type of operation that is run on the external table.  The following values are allowed: <ul style="list-style-type: none"> <li>• Add or remove functions</li> <li>• Add or remove delegation</li> <li>• Disable or enable user</li> <li>• Create, remove, or modify account</li> <li>• Change password</li> <li>• Add or remove service</li> <li>• Add or remove resource</li> </ul>
Operation Code	Label identifying the operation.
Marker	Identifier of the Target system (toward the event is transmitted).
Trace	Brief description of the cause of the error.
Priority	Indicates a priority level for the event: <ul style="list-style-type: none"> <li>• Running: the event was created during the normal operating procedures and has a higher priority.</li> <li>• Batch: the event was created with a lower priority.</li> </ul> Events with the same priority level are processed in the normal order.
Event Start/End Date	Filters defining the time period for the search.

The set of events that are filtered is shown in a list where every event is characterized by a set of attributes. The attributes are listed in the following table.

*Table 27. OUT Event structure*

Field	Description
ID	Event identifier.
User ERC	User identifier in USER ERC table.
Operation	The following values are allowed: <ul style="list-style-type: none"> <li>• Add or remove functions</li> <li>• Add or remove delegation</li> <li>• Disable or enable user</li> <li>• Create, remove, or modify account</li> <li>• Change password</li> <li>• Add or remove service</li> <li>• Add or remove resource</li> </ul>
Status	Event state can assume only three values: <ul style="list-style-type: none"> <li>• Unprocessed</li> <li>• Success</li> <li>• Error</li> </ul>
Priority	Indicates a priority level for the event: <ul style="list-style-type: none"> <li>• Running: the event was created during the normal operating procedures and has a higher priority.</li> <li>• Batch: the event was created with a lower priority.</li> </ul> <p>Events with the same priority level are processed in the normal order.</p>
Trace	Contains the description of an error that occurred during event processing (ordinarily appears as Status = Error).
Target	Identifier of the target system to which the event is transmitted.
Free Attribute 1	Value 1.
Free Attribute 2	Value 2.
Free Attribute 3	Value 3.
...	
Free Attribute N	Value N.
Application	Application that is the object of the action relative to the event.
Operation Code	Label identifying the operation.
Event Date	Indicates the date that the event was generated.
Process Date	Indicates the date by which the event must be processed by the RE. Typically this date coincides with the event date but can be later if the events processing is postponed.

**Note:** The fields that are indicated from Free Attribute 1 to N, depend on the event.

You can perform two functions from the **Actions** menu on a selected event in the IN or an OUT accordion pane.

**Re-Execute**

Reprocess the event.

**Remove**

Deletes the event.

## **Error handling**

Several types of errors can occur during the generation and processing of events.

The following list contains the main causes of errors that are associated with IN or OUT events.

- Temporary interruption of system operation.
- Errors in the structure of a rule.
- Errors that are caused by a lack of necessary data for the correct application of a rule.
- Errors due to data format incompatibilities in the data from the target system.
- Errors in the reprocessing order of events that are already in error.

A brief description of the reason for an error is contained in the **Trace** field.

General policy is to remediate an error on IN or OUT events.

Remedying an event in error means to determine the reason for the error, correct it, and finally reprocess the event through the rule engine (RE). If the cause of an error is not removed, reprocessing the event fails or new error events are generated.

The following list provides a set qualitative strategy to eliminate the causes of errors, for more commons situations:

- If the error is due to a temporary interruption in the system operation, reprocess the events in the correct order.
- If the error is due to a badly written rule, either default or custom, the rule must be corrected before you reprocess the event.
- If the error is due to the incompatibility of data to be entered with data already into AG Core, locate the error. Determine whether the error is in the AG Core data or the data from the target system. You might need to contact the target system and AG Core administrators for assistance.
- If the error is linked to sensitive data that is to be modified, also correct it in the USER ERC table. This operation is not mandatory, but keeps the data in alignment between II and AG Core.
- If the error is caused by AG Core data, it is possible to correct it directly from the AG Core Administration module. The event can be reprocessed only after the cause of the error is corrected.
- If the error is due to other error events, the previous events in error must be identified and corrected.
- If the reprocessing of an event generates of new error events, these events must be corrected before the original event is reprocessed.

Follow this general procedure to manage errors on IN or OUT events.

1. Given an error event, define the filters to identify all events relative to the same user.
2. Select the oldest event in error list.
3. Reconstruct the cause of the error based on available data, according to the indications provided in the preceding sections.
4. Remedy the event based on step 3.
5. Restart the rule engine (RE) to reprocess the event that you corrected
6. If the event is still in error, return to point 3.
7. If the reprocessing is successful, individually select all chronologically consecutive events and restart the RE to reprocess them one at a time.
8. If the generic event produces an error again, go back to point 1.
9. If all errors produced after point 1 are remedied and reprocessed successfully, the problem is resolved.

This procedure is valid for most error situations that can occur. In simpler cases, steps 1, 2 and 3 can be skipped.

## Operation Code

This code specifies the operation that originated the event.

An operation can cause more than one event. For example, the operation for deleting a user implies events for the removal of entitlements from the user before the user is deleted. All of these events are specified by the same operation code.

The Operation Code is a string of characters that are generated based on standard mechanisms.

The standard structure of the Operation Code is

`<prefix>_<code>`

The `<prefix>` can be one of the following types, depending on the architectural module that is generating the event:

### **MR\_SYNC**

The event is generated by the Synchronization flow.

### **MR\_IN**

The event is generated by the read from or input flow.

### **MR\_OUT**

The event is generated by the write to or output flow.

### **PM**

The event is generated by the AG Core module, or is transferred to the AG Core without any code and AG Core transmits the event as though it generated it.

#### **Note:**

The string **PM** is used for AG Core because of legacy reasons.

The `<code>` can be one of the following forms:

#### **Generated by the rule engine**

`<event Id>_<User Id on the Person>`

## Generated by the AG Core

A random number.

Structures differing from the standard structure can also be found.

Applications that are integrated with the AG Core communicate without using the standard Integration Interface. They can send and receive request to and from the AG Core. They can transmit their own operation code for the events that result from the requested operation. The operation code changes depending on the integrated application.

**Note:** If an event is delivered to AG Core by any module without the operation code, it is automatically considered as if the event originated by AG Core. The operation code uses the format:

PM\_<random number>

## Groups

You can use the following functions to manage a hierarchy. The main hierarchy available is the ORGANIZATIONAL\_UNITS hierarchy.

For more information about organizational units, see Organization Units.

The **Groups** combo-box is located above the **View** and **Search** tabs. Use it for filtering the hierarchies that are displayed in the left frame.

The left frame includes also the following tabs:

**View** Select this tab to browse the hierarchy and select a Group.

### Search

Select this tab to search for a Group by name or ID Code (click **Filter** button).

The **Actions** menu in the left frame lists the following actions:

### ToggleMngr

Shows or hides the Group manager. This action is shown only when you select the **View** tab.

**Move** Moves a Group to another position in the tree.

**Add** Adds a Group.

### Remove

Deletes a Group.

### Tree View

After the selection of a Group, switches from the **Search** tab to the **View** tab and provides the position of the selected Group in the hierarchy.

This action is shown only when you select the **Search** tab.

Use the **Add** action to create a new Group.

Here the procedure for adding an organization unit.

You can then specify the following options to the new Group:

### **Inherit Parent Entitlements**

All the entitlements that are assigned to the parent Group are automatically assigned to the new Group.

### **Inherit Parent Resources**

All the resources that are assigned to the parent Group are automatically assigned to the new Group.

Use the **Remove** action to delete:

#### **A single Group**

A single node.

#### **A Group and its entire subtree**

A single node and all its children.

**Note:** When you run **Remove** on the root of a Group subtree, the children of the Group are automatically moved to the same level of the root Group subtree. In other words, all the Groups that are originally at the L level for the selected subtree, are redistributed to the L-1 level.

Use the **Move** action to choose a new position for a selected Group.

**Note:** The Inherit Parent Entitlements and Inherit Parent Resources options are not supported in a Move action. The Group that was moved maintains the entitlements and resources it had in its previous position.

Use **ToggleMgr** to show or hide the managers of the OUs. Double-click the root node of the organization to refresh the data.

The right frame displays different panes depending on the tab you select in the upper side of the frame. The **Details** tab is selected by default. It includes the following accordion panes:

- **Details**
- **Group Properties**



For editing information in these panes, click **Edit** tab and after the modify of the information, click on **Save** button.

The **Details** pane is automatically displayed when you select a Group in the left frame. It shows the Group data extracting it from the AG Core database. The Group details are:

*Table 28. Group details*

<b>Detail</b>	<b>Description</b>
Parent Group	The name of the parent Group (automatically set after the Group selection in the left frame).
Type	The type of Group.
Name	The name that is used in the Organization to identify the Group.
ID Code	The univocal identifier of the Group.
Exclude from SoD Validation	Indicates whether the Segregation of Duties (SoD) control is enforced or bypassed.

Table 28. Group details (continued)

Detail	Description
Owner	The user who has responsibility over the selected Group. Use the  User and  Clear buttons to enter a user or to clear the field.
Description	A short description of the Group.

The **Group Properties** pane displays properties that provide additional information on a selected Group. They are custom properties and are defined by the Administrator. For example, the value of a property can be an external link to the set of implementation and compliance rules that must be followed by the Group. You can also add the values of these properties in the structure of a Rule.

Properties are made up by the <Name,Value> attributes.

Use the **Actions** menu in this pane to add or delete properties for a selected Group.

**Add** Adds a property.

**Remove**  
Deletes a property.

**Save** Saves a property.

**Note:** You can define multi-value properties. In the **Group Properties** pane, click **Add** and specify a property named PROP\_1 with a VALUE\_1 value. Click **Add** again and enter the same PROP\_1 property name with a different value VALUE\_2.

The other Group-related operational tabs available in the right pane are:

- Entitlements
- Group Resources
- Users
- Analysis

**Related tasks:**

“Adding an organizational unit” on page 67  
Complete this task to register a new organizational unit.

**Entitlements**

You can view all the entitlements that are already associated to a group of a selected hierarchy.

The **Entitlements** tab lists all the entitlements that are already aggregated to a group.

Entitlements can be assigned to a user only if they are already assigned to the group to which the user belongs. The following table lists the available filters.



Table 29. Entitlement filters and details

Filter	Description
<b>Type</b>	The type of entitlement: <ul style="list-style-type: none"> <li>• Permission</li> <li>• IT role</li> <li>• Business role</li> <li>• External role</li> </ul>
<b>Application</b>	The name of the application that includes the entitlement.
<b>Name or Code</b>	Name or operational code that is used within the organization to identify the entitlement.
<b>Enabled</b>	This attribute is a binary attribute: <b>Yes</b> The entitlement can be assigned to users. <b>No</b> The entitlement exists in the system but cannot be assigned to other users.
<b>Administrative</b>	If this check box is selected, only administrative entitlements are listed in the resulting list.

An entitlement can be characterized by a set of main attributes

#### **Role Alignment Violation**

An entitlement is in Role Alignment Violation (VV column) when an entitlement is assigned to a user of n group and not available for all other users in the group.

#### **Default**

An entitlement is automatically assigned to each user in a group. It is useful for modeling a basic entitlement with common functions that are assignable to all users that belong to a group.

#### **Enabled**

An entitlement is available for the users in the group.

#### **Note:**

1. Setting an entitlement as a default, automatically assigns it to every new user of the group. It is not automatically assigned to the users already present in the group.
2. For a Role Alignment Violation, you can change the initial Yes value to the final No value. However, you cannot do the opposite because the Role Alignment Violation can detect only when an entitlement is assigned for the first time to a specific group.

The **Actions** menu of this tab, lists the available functions.

#### **Conflicts**

Provides information about risks that are related to the selected entitlement.

#### **Hierarchy**

Shows the entitlement hierarchy.

**Details**

Provides specific information about all the permissions that are joined to a selected entitlement.

**Status** Shows the status of the permissions. The status of the permissions can be TBD, Ignored, Missing Activity, or Linked.

**Add** Adds an entitlement.

**Remove**

Deletes an entitlement. Ticking the **Hierarchy** check-box, it is possible to remove the entitlement through the entire group hierarchy.

Here the procedure for adding an entitlement to an organization unit.

The **Conflicts** operation shows information about risks that are related to the entitlements of the group. Use the [Ctrl] or [Shift] keys to make multiple selections.

If all entitlements must be tested, no selection is needed.

You can use the **Status** operation to set or managed some attributes of an entitlement that is already aggregated to the OU.

Use the Role Status Management window to manage or set the following options.

Role Status options	
Option	Description
<b>Default</b>	Four values are available: <i>(empty)</i> No actions. <b>No</b> The entitlement is not a default entitlement. <b>Yes</b> The entitlement is a default entitlement. <b>Yes and align Users</b> The entitlement is a default entitlement and is assigned to all users in the OU.
<b>Enabled</b>	Three values are available: <i>(empty)</i> No actions. <b>Yes</b> The entitlement is ready to be assigned to users. <b>No</b> The entitlement exists in the system but cannot be assigned to other users.
<b>Span hierarchy</b>	If this check box is checked, the entitlement status is propagated down the hierarchy.

The **Add** operation adds an entitlement to the selected group and to determines all the parameters that are related to the status of the entitlement.

The **Remove Entitlement** operation deletes the selected entitlement. Use the [Ctrl] or [Shift] keys for a multiple selection.

**Note:** A default entitlement can be removed from a user just like any other entitlement.

**Related tasks:**

Adding an entitlement to an organizational unit

You must assign the entitlement to the organizational unit before you can assign the entitlement to a user that belongs to the same hierarchy of the organizational unit.

## Group Resources

Resources can be assigned to a user only if they are already assigned to the Group to which the user belongs.

The following table lists the available filters.

*Table 30. Organizational unit resource filters*

Filter	Description
Name	The name of the resource family.
Resource Type	The resource type name.
Resource Family	The resource family name.
Inheritable	In this column is indicated if the resource is or not inheritable. An inheritable resource is characterized by a green icon.

The **Actions** menu lists the available functions.

**Add** Assign a resource to a selected Group.

**Remove**

Deletes a resource from the selected Group.

A Resource can be assigned with either of two options.

**Hierarchy**

When a resource is assigned to an Group, the same resource is also assigned to the entire sub-tree under the Group. If a resource is removed, it is removed from the entire sub-tree as well.

**Inheritance**

The resource is automatically assigned to all users added in the Group.

**Note:** A resource that is assigned to an Group by inheritance is assigned to every new user in the Group. The resource is not assigned to the users that exist in the Group when the inheritance option is set.

## Users

In this tab are shown users aggregated to the Organization Unit selected in the left frame.

The table below list the available filters (click the **Filter/Hide Filter** button):

Table 31. User filters

Filter	Description
User Type	This information allows to define different categories of users. See also User>Details.
Surname/Name/Code	This field can host the Surname or the Name or the Master UID of the user.
OU	Automatically set on OU selected in the left frame.
Hierarchy	If this check-box is ticked, the search is extended to users of OUs belonging to the sub-tree whose root coincides with OU field.

## Roles

A role identifies the set of permissions and resources to which the person has access. Use this set of panels to define and manage entitlements in your organization.

Roles can be published or unpublished. A published role is shown in bold italics.

A published role (the role name is shown in bold/italic) can be assigned to the following categories:

- One or more organizational units (OUs)
- One or more users

An unpublished role cannot be assigned to OUs or users.

In the hierarchical organization of a generic role, any component of the hierarchy can be published or unpublished, without any regard to the position of the specific component.

A role can be also object of:

- Consolidation (one shot): on demand, a group of entitlements can be organized into a Role (Business Role or IT Role)
- Persistent Consolidation: the role is periodically consolidated (by running a job with the Task Planner module)

A consolidated role is shown in bold/orange.



A role under persistent consolidation is shown in bold/italic/blue.

You can use filters to search for specific roles. The following table lists the available search filters for roles:

Table 32. Role filters

Filter	Description
Type	Indicates one of the following entitlement types: <ul style="list-style-type: none"> <li>• Permission</li> <li>• IT Role</li> <li>• Business Role</li> <li>• External Role</li> </ul>

Table 32. Role filters (continued)

Filter	Description
<b>Application</b>	Indicates the name of the application to which the entitlement is related. Use  <b>Application</b> and  <b>Clear</b> to set an Application or clear the field.
<b>Name or Code</b>	Indicates the entitlement name, or the code that identifies it.
<b>Published</b>	The published attribute can have these values: <b>Yes</b> The role is published. <b>No</b> The role is unpublished. <b>All</b> Do not distinguish between published and unpublished roles.

The roles are listed by:

- Name
- Application
- Description

and are sorted by role type.

**Important:** Unfulfilled permissions and external roles are not displayed in the list.

Select a role and click **Actions** to display the following list of actions:

**Role Version**

Assigns a version to a role. The base version is 0.

**Rollback**

Returns the role to the previous version of the Role; from version *N* to version *N-1*.

**Consolidate**

Consolidating a role, built on a set of entitlements, implies replacing this set of entitlements, assigned to a user, with the consolidated Role (for all the users who match this condition).

**Dismiss**

Reverses the consolidation operation.

**Enable persistent consolidation**

Enables the persistent consolidation of a Role.

**Disable persistent consolidation**

Disables the operation of persistent consolidation

**Publish**

Publishes a role to assign it to an OU.

**Unpublish**

Reverses the operation of publishing a role.

**Add**    Creates a role. No role needs to be selected to start this action.

**Remove**

Deletes a role.







Here the procedure for adding an entitlement.

**Note:** You can import a role also with Access Optimizer (for releasing a role after a role mining analysis), or through connectors or using a dedicated bulk load procedure.

You can use also import :Access Optimizer (for releasing a role after a role mining analysis) or import through connectors.

You can publish an entitlement immediately after it is added. The **Details** tab shows data about a selected entitlement. The following table describes the details of an entitlement:

Table 33. Role details

Area	Detail	Description
Info	Version	Number from 0 to $N$ that indicates the version of the role.
	Owner	User who is responsible for the selected role. Use  <b>User</b> and  <b>Clear</b> to set a user or clear the field.
	Name	Name that is used in the organization to identify the role.
	Code	A code that is used in the organization to identify the role.
	Description	A brief description of the role.
	Type	Indicates one of the following entitlement types: <ul style="list-style-type: none"> <li>• Business Role</li> <li>• External Role</li> <li>• IT Role</li> <li>• Permission</li> </ul>
	Application	The name of the application that is related to the selected role. Use  <b>Application</b> and  <b>Clear</b> to set an application or clear the field.
	Permission Type	This attribute tags and categorizes a set of permissions into a specific <b>Type</b> .
	Entitlement Families	The family of which the selected role is part.
	Expiration	The expiration date of the role. When an entitlement expires, some automatic controls might be run. Use  <b>Calendar</b> and  <b>Clear</b> to set a date or clear the field.
Last Review Date	Date of the last authorized modification on the entitlement.	
Business info	Business Name	Field for future use.
	Business Policy	Field for future use.

An entitlement can be associated to a set of properties that characterize it.

The **Entitlement Properties** pane displays properties for an entitlement. Properties influence the behavior of entitlements. For example, a property can have a value that is used by a rule to manage a business process in the organization.

A property consists of a <Name, Value> pair. Use **Actions** on the upper right to **Add** or **Remove** properties.

Every property is characterized by a set of properties, as shown in the following table.

*Table 34. Keys for properties*

Property	Description
<b>Name</b>	Name of the property.
<b>Description</b>	Description of the property.
<b>Searchable</b>	For future use.
<b>Multivalue</b>	Property can have a set of values rather than a single value.

Use the following procedure to create a new property.

1. Click **Add**. An empty line appears.
2. Click **Add Key**.
3. Choose a key from **Key Properties**.
4. Click **Add Value** and enter a value.
5. If the property is multi-valued, use **Actions > Add** to add multiple values.
6. Click **Save**

The operational tabs for entitlements are:

- Management
- Users
- Org Units
- Permissions
- Rights
- Analysis
- History

**Related tasks:**

“Adding an entitlement” on page 63

Complete this task to register a new entitlement into the Identity Governance and Intelligence data model.

## Management



Use the **Management** tab to build the hierarchy of a role.

You can use the following filters to search specific entitlements:

*Table 35. Filters to search for the entitlements that make up a role.*

Filter	Description
<b>Type</b>	The entitlement type can be one of the following: <ul style="list-style-type: none"> <li>• Permission</li> <li>• IT Role</li> <li>• Business Role</li> <li>• External Role</li> </ul>
<b>Search Entitlement</b>	The role name.

Table 35. Filters to search for the entitlements that make up a role. (continued)

Filter	Description
Application	The name of the application to which the entitlement is related. Use the  the <b>Application</b> attribute box to set an Application or clear the field.  <b>Clear</b> buttons on the <b>Application</b> attribute box to set an Application or clear the field.

Select an entitlement and click **Actions** to display the following list:

#### Conflicts

Checks conflicts that are related to a set of entitlements.

#### Hierarchy

Shows the tree structure of the selected entitlement.

**Add** Adds an entitlement at the hierarchy level of the entitlement that is selected in the **Hier View** tab.

#### Remove

Deletes an entitlement.

#### Users

Use this tab to view the users who are assigned with the selected role.

You can use the following filters to search specific users:

Table 36. Filters to search for the users assigned with the entitlement.

Filter	Description
User Type	The category to which the user belongs as defined in the organization's structure.
UME	A digital identity for a user that can have more than one account on the same target system.
Search Identity	The first name, last name, or the master UID of the user.
Associated	If checked, the search result lists only users who are assigned to an OU.  If cleared, the search result lists only users that are not associated with any OU; for example, new users who have not yet been assigned to any OU.
Groups	The name of the attributes group from which the user search starts.
Hierarchy	If this box is checked, the search is extended to users of OUs that belong to the subtree whose root coincides with the <b>Groups</b> field.

Use the **Remove** function from the **Actions** menu to delete a user from the list. This operation is similar to removing the role from the set of roles available for the user.



## Org Units

The **Org Units** tab shows the OUs that host the selected role.

You can use the following filters to search OUs:

Table 37. Filters to search for the OUs associated with the entitlement.

Filter	Description
<b>Groups</b>	The name of a specific attribute group. In this case it is the attribute group to which the organizational unit belongs.
<b>Name</b>	The name of a specific group of the hierarchy. In this case it is the name of the OU.
<b>ID Code</b>	The ID of a specific group of the hierarchy.

Click **Actions** and select one of the following:

**Add** Adds an OU to the list of OUs associated with the entitlement.



**Remove**  
Deletes an OU.

## Permissions

The **Permissions** tab shows the permissions that are included in the selected role.

You can use the following filters to search for specific permissions:

Table 38. Filters to search for the permissions that are in a role.

Filter	Description
<b>Application</b>	The application that is related to the permission. Use the  <b>Application</b> and  <b>Clear</b> buttons on the right side of the attribute box to set an application or clear the field.
<b>Type</b>	The type of permission, as defined within the organization.
<b>Name</b>	The name that is used within the organization to identify the permission.
<b>Status</b>	The status of the permission: <ul style="list-style-type: none"> <li><b>Linked</b> The permission is joined to an activity.</li> <li><b>Ignored</b> The permission is not joined to any activity.</li> <li><b>Missing Activity</b> The operator does not know to which activities to join the permission.</li> <li><b>To be Defined (TBD)</b> The permission is not joined to any activity but is not in the status <b>Ignored</b> or <b>Missing Activity</b>.</li> </ul>

## Managers

The **Managers** tab shows the managers that are aggregated to the selected role.

The following table lists the available manger filters.

Table 39. Manager filters

Filter	Description
<b>Admin Role</b>	The administrative role that is selected from a list of administrative roles.
<b>First Name</b>	The given name of the manager.
<b>Last Name</b>	The surname of the manager.
<b>Master UID</b>	The unique identifier of the manager.
<b>Admin Role assignment</b>	The assignment can have either of the following values: <ul style="list-style-type: none"> <li>• <b>Direct</b></li> <li>• <b>By Delegation</b></li> </ul>

After a user is selected from the list, click **Tree View** to display the position of the manager in the OU.

## Rights

This tab shows the Rights aggregated to the Entitlement selected in the left frame.





The right frame displays two panels.

The left panel lists the existing Entitlement - Application associations.

The **Name** (of the Right) is the available filter (click the **Filter/Hide Filter** button).

As you select an Entitlement - Application binomial, the right panel shows the properties of the associated Right:

Table 40. Right properties.

Property	Description
MVal/Lookup	The  green icon indicates that the Right is MultiValue and/or with Lookup.
<b>Name</b>	The name of the Right.
<b>Status</b>	The status of the Right: <ul style="list-style-type: none"> <li>• <b>None:</b> this icon  indicates that no specific policy is defined for assigning a Right to a User.</li> <li>• <b>Restricted:</b> this icon  indicates that when the Right is assigned to a User, it is possible to choose values only from a predefined set.</li> <li>• <b>Fixed:</b> this icon  indicates that it is not possible to choose a specific value (or a set of values) for the Right, because its values are preset.</li> </ul>
<b>Actions</b>	The following operations are available: <b>Edit</b> , <b>Show</b> , and <b>Clear</b> .

Click the **Edit** button to display the Lookup Management window, where you can select one or more values.

- Select the **Value** check box to select all the values that are listed.
- For a **Single Value** Right, the Insert Value window opens, allowing the dedicated value to be inserted.
- From the Lookup Management window, you can click **Fixed** and **Restricted** to change the status of the Right.

Click the **Show** button to open the View Values window that shows the value of the Right.

## Application

Documents the functions required for the management of Applications.

The Applications frame includes the **Name** and **Account** filters that are used to search Applications (click the **Filter/Hide Filter** button to specify them). It includes also command buttons that you can use to run basic operations on applications.

In this same frame, use the **Add/Remove** button to add or remove an application. Adding an application implies linking an Application to a specific Account.

Here the procedure for adding an application.

Generally, several Applications can be linked to a specific Account configuration.

This association allows to consistently manage a set of Applications regarding the operating attributes that define how a User has access to the system. This mechanism increases the degree of security for accessing an Application and implies a series of password controls associated to the User's account.

With the **Modify SoD** button, you can decide whether an Application must be excluded or not from SoD checks (the related checkbox in the **Details** tab and the SoD column in the Applications frame are automatically updated).

The Details pane shows details of the Application selected in the left frame:

Table 41. Application details




Application	Details
Info	<p><b>Owner</b> The user who is responsible for the selected Entitlement. Use the  <b>User</b> and  <b>Clear</b> buttons on the right side of the attribute's box to insert a User or clean the field.</p> <p><b>Name</b> The name that is used by the Organization to identify the Application.</p> <p><b>Description</b> A short description of the Entitlement.</p>

Table 41. Application details (continued)

Application	Details
Policy	<p><b>System Account</b> If this radio button is selected, the Account of the Application is the IDEAS System Account.</p> <p><b>Custom Account</b> If this radio button is selected, the Application Account can be customized.</p> <p><b>Disable out/target events generation</b> If this check box is selected, the generation of the out/target events is disabled.</p> <p><b>Events Marker</b> Name of the Events.</p> <p><b>Exclude from Risk validation</b> If selected, SoD control is enabled. The same data is also reported in the SoD column in the Applications frame (  icon).</p>


An Application can be added to a set of properties that characterize it.

The Application Properties pane displays properties that can add specific information for the selected Application.

For example, a Property can have a value that is used by a Rule to manage a business process of the Organization.

A Property is identified by a pair of attributes, **Name** and **Value**, and can be easily added or removed with the **Add** or **Remove** buttons placed in the upper right side of the pane. The values of a property can be freely edited and saved with the **Save** button.

Table 42. Note about multi-value properties

	<p><b>Note:</b></p> <p>MULTI-VALUE properties are possible.</p> <p>For example, you can specify a PROP_1 property and associate it a VALUE_1 value. You can then add a line in the Application Properties pane and specify the same property name (PROP_1) associated to a different value (VALUE_2).</p>
---	---

The operating tabs for Applications are:

- Application Access
- Users
- “Analysis” on page 153

- “Permission Type” on page 163

**Related tasks:**

“Adding an application” on page 59

Complete this task to register a new application. By default, a new application is joined to the default *System Account IDEAS* and the related *Events Marker IDEAS*.

**Application Access**

Documents how to manage application permissions.

The **Application Access** tab displays the Permissions already defined for the Application selected in the left frame. You can use the following filters to find permission definitions (selecting the **Filter/Hide Filter** button):

*Table 43. Permission filters*

Filter	Description
<b>Name</b>	The name of the Permission.
<b>Permission Type</b>	The permission type. This information can be useful to group Permissions. Generally, Permission types are loaded through a bulk load procedure.
<b>Application</b>	
<b>Status</b>	<p>Status of the Permission:</p> <p><b>Linked</b> The permission is joined to an activity.</p> <p><b>Ignored</b> The permission is not joined to any activity.</p> <p><b>Missing Activity</b> The operator does not know to which activities to join the permission.</p> <p><b>To be Defined (TBD)</b> The permission is not joined to any activity but is not in the status <b>Ignored</b> or <b>Missing Activity</b>.</p>

You can select the following buttons to take the related actions:







- **Set Auth:** sets two types of authentication (not mutually exclusive). They are **Weak Authentication** (UserID-Password) and **Strong Authentication** (Cert.X.509, Smartcard, Bio, ...).
- **Add:** adds a Permission.
- **Remove:** removes a Permission.
- **Fulfill**
- **Unfulfill**
- **Publish:** publishes a Permission and makes it available for association with one or more OUs and one or more Users.
- **Unpublish**

The tabs listed below become available in the right frame after you select a Permission:

## Details

The **Details** tab on the right displays the Permission data, described in the table below:

Table 44. Permission filters

Detail	Description
<b>Name</b>	The name used in the Organization to identify the Permission.
<b>Business Name</b>	Field left for future use.
<b>Description</b>	Short description of the Entitlement.
<b>Permission Type</b>	Type of Permission (used to tag different subset of Permissions of the same Application).
<b>Scope type</b>	Types of Scope: <ul style="list-style-type: none"><li>• <b>Model</b>: the resource is assigned by the Employment (<b>Entitlement &gt; OU &gt; User</b>)</li><li>• <b>Scope</b>: the resource is assigned directly to the Owner (<b>Entitlement &gt; Owner</b>)</li><li>• <b>Both</b>: the resource is assignable in Model and Scope type.</li></ul>
<b>Owner</b>	The user who is responsible for the selected Permission. Use the  <b>User</b> and  <b>Clear</b> buttons on the right side of the attribute's box to insert a User or clean the field.
<b>Expiration</b>	The expiration date of the Permission. Some automatic controls can be made when a Permission expires .
<b>Last Review Date</b>	The date of the last authorized modification on the Permission.
<b>Enable Workflow Checking</b>	Enables the <b>Check Workflow</b> field.
<b>Check Workflow</b>	A Flow Process can be set here to run a number of actions on the Entitlement. Use the  <b>Check Workflow</b> and  <b>Clear</b> buttons on the right side of the attribute's box to insert a Flow Process or clean the field.
<b>Enable Authorization Workflow</b>	Enables the <b>Authorization Workflow</b> field.
<b>Authorization Workflow</b>	A Flow Process can be set here to perform actions on the Entitlement. Use the  <b>Check Workflow</b> and  <b>Clear</b> buttons on the right side of the attribute's box to insert a Flow Process or clean the field.

Click the **Edit** and **Save** tabs to change the values of the Permission details.

## Properties

The **Properties** tab displays properties that can add specific information to the selected Permission.

A Property is identified by the **Name** and **Value** pair of attributes. Properties can be easily added or removed with the **Add** or **Remove** buttons placed in the upper right side of the pane. The values of a property can be freely edited and saved with the **Save** button.

You can add several properties to any Permission. To add one or more Properties to a selected Permission, select the related checkbox on the Property row.

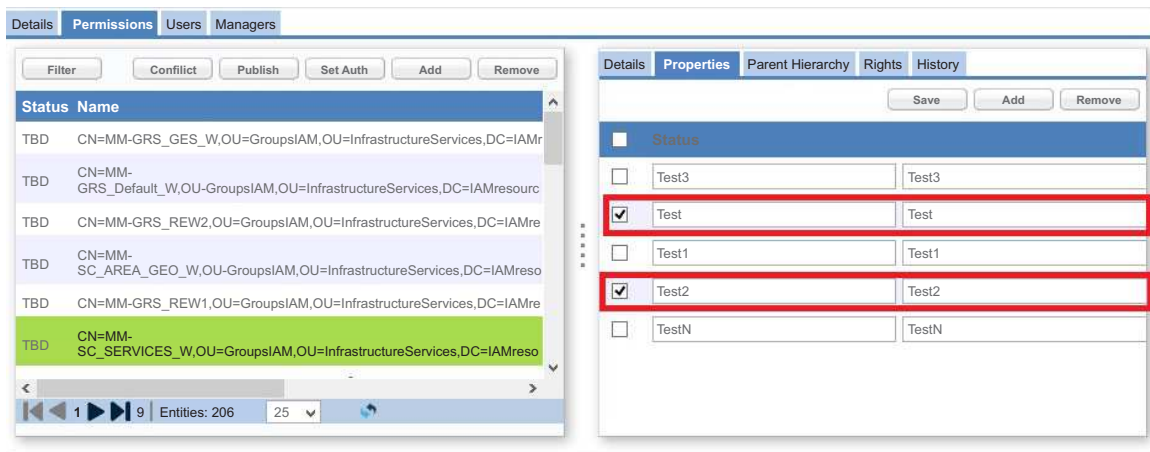


Figure 45. Selecting properties

In the example above only the Test and Test2 Properties are associated to the selected Permission and define when a Permission will be assigned to an Entity (Application, Business Roles, ITRoles, ...).

Other Properties can be associated at a later time. **To select all the Properties**, select the checkbox on the blue attribute-bar.

### Parent hierarchy

In this tab you can view the Entitlement structure that hosts the selected Permission.

### Rights

“Rights” on page 16 are additional attributes and are related to the Permissions. A Right determines the set of values that can characterize the generic transaction enabled by a Permission.

A Right is defined by the **Key** and **Value** attributes.

Each Right attribute can be:

- **Single Value:** only one value can be set.
- **Multi Value:** more than one value can be set for the same attribute.

In both cases (single/multi value) you can choose from a predefined set of values (Lookup attribute).

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

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

If you select the Lookup attribute, you must also specify, in the **List Name** text-area, the key of the Lookup table connected to the set of values that will be proposed to value the Right during the assignment of the Permission.

The **Rights** tab displays Rights that are already defined for a Permission and allows to add/remove Rights (with the **Add/Remove** button).

Table 45. Rights attributes

Attribute	Description
<b>Name</b>	The name of the Right.
<b>Lookup (Y/N)</b>	Tick this checkbox for enabling a Lookup table.
<b>List Name</b>	The key of the Lookup table.
<b>Multi-Value</b>	Select this checkbox to make the Right a multi value one.

You can add multiple rights to a Permission. Use the related check box on the Rights row to add one or more Properties to a selected Permission.

**To select all the Rights**, select the checkbox on the blue attribute-bar.

Click the **Save** button to confirm any update.

### History

The **History** tab lists all the changes made on a selected entitlement or permission. You can search a specific change by clicking **Filter/** and setting the **Revision** and **Date** filters.

The following history attributes shown:

Table 46. History attributes

Attribute	Description
<b>Revision</b>	The ID number of the revision of the selected entitlement or permission.
<b>Operation</b>	The operation involved with the update. The following types of operations are available: <ul style="list-style-type: none"> <li>• Edit</li> <li>• Insert</li> <li>• Delete</li> <li>• Add Entitlement</li> <li>• Remove Entitlement</li> <li>• Permission Type</li> <li>• Owner</li> <li>• Entitlement Family</li> <li>• Workflow Auth</li> <li>• Workflow Check</li> </ul>
<b>Field Label</b>	The technical field (the column of a specific table of the AGC DB) involved with the operation in the <b>Operation</b> attribute.
<b>Old Value</b>	The value of the <b>Field Label</b> attribute before the update operation.
<b>New Value</b>	The value of the <b>Field Label</b> attribute after the update operation.



Table 46. History attributes (continued)

Attribute	Description
Date	The date of the update operation.

Click **Undo** to ignore the update in **in the last operation** and to restore the previous entitlement or permission data.

## Users


Documents how to manage application users.

The **Users** tab displays the Users defined for the Application selected in the left frame. Users can be filtered by click the **Filter/Hide Filter** button and using the following filters:

Table 47. User filters

Filter	Description
Search Identity	This field can have the Name, the Surname or the User ID of a User.
Associated	If selected, the search result will include only Users defined to an OU.  If not selected, the search result will include only Users that are not defined to any OU (for example, when a User has just been entered in the DB but has not yet been defined to any OU).
OU	Automatically set on a selected OU.
Hierarchy	If this checkbox is selected, the search is extended to Users of OUs belonging to the subtree whose root coincides with the OU field.

Table 48. Application note

	<p><b>Note:</b></p> <p>A user might have an Account joined to an Application, but not any entitlement assigned and related to that Application. In this case, the user not will be present in the list.</p>
---	---

## Analysis

An *analysis* is the object that contains all the data required for a data analysis. The **Analysis** tab provides graphical dashboards and detailed information about the Entitlements (Permissions) and Users associated with the selected Application.

This tab displays information in the following categories:

- “Statistics” on page 154
- “Entitlement map” on page 154
- “Permissions” on page 155
- “Users” on page 159

## Statistics:

This tab displays statistics information through charts and diagrams.

The following statistics are available:

### Assignment Statistics

**Assignment Statistics** illustrates the statistics on assigned Entitlements, and Users with and without assignments.

Table 49. Dashboard set

Dashboard	Description
Entitlements	The entitlements (permissions) registered in the organization. The diagram illustrates the number of assigned and unassigned Entitlements - Permissions, and Roles.
Assignments	All user-entitlement assignments. The chart illustrates the number of assigned Permissions, and Roles to Users.
Users	The users who belong to the organization. The diagram illustrates the number of Users with directly assigned Permissions, with just Roles, and without assignments.
Permissions	The entitlements (permissions) registered in the organization. The diagram illustrates the number of Permissions unassigned, directly assigned, and assigned through Roles.

### Entitlement Statistics

**Entitlement Statistics** illustrates the number of Entitlements assigned to the following data elements.

- Users
- Permissions
- Organization Units
- Applications

Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests and then click **Search**.

You can sort the displayed data in ascending or descending order, based on the data elements provided.

### Entitlement map:

This tab displays the Entitlement and User association through a map diagram.

In the map, the vertical axis shows the entitlements whereas the horizontal axis shows the users. The black boxes show when an entitlement is assigned to a user.

You can select from the following actions:

- **Reshuffle**: by clicking **Reshuffle** the map will change. This operation is possible, after selecting the area.

- **Select area:** click **Select Area** to highlight an interested area. With the left mouse button click a block on the map to define the start position of the area. The area selected between the start/end positions will be covered with a yellow mask.
- **Single select:** allows you to return to single select mode. The single selection is possible only when the action is performed on the selected area, after the area involved is highlighted in yellow. The single block that is highlighted is the end position block of the **Select Area** action.
- **Zoom in/Zoom out:** the zoom action modifies the resolution of the map.

### Permissions:

View this tab for an analysis of the Permissions assigned to the selected Application and its relations to other data elements such as Users and Organization Units.

This tab has the following sub categories.

- Permission
- Permission Details
- Users
- Organization Units

### Permission

The **Permission** tab lists all Permissions assigned to the selected Application.

In this tab, you can:

- Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests and then click **Search**.
- Select a Permission to view the details of the Users and Organization Units assigned with it, in the right pane.

Table 50. Permission filter details

Filter	Description
Name	Name of the entitlement.
Application	Name of the application.
User Coverage	Type of user coverage. Directly assigned.

### Permission Details

The **Permission Details** tab lists the Permission details, and the statistics of Users and Organization Units associated with the selected permission.

Table 51. Permission Details

Permission Details tab	Fields and descriptions
Permission	<p><b>Application</b> Name of the application.</p> <p><b>Name</b> Name of the entitlement.</p>

Table 51. Permission Details (continued)

Permission Details tab	Fields and descriptions
Users	<p><b>Users</b> Number of users assigned to the selected entitlement.</p> <p><b>User Support (%)</b> Percentage of users to be assigned to the permission, from the entire set of users involved in the analysis.</p> <p><b>Covered with just Roles</b> Number of users covered with the Role entitlement.</p> <p><b>User Coverage (%)</b> Percentage of users that are assigned to the permission, from the entire set of users involved in the analysis.</p>

Table 51. Permission Details (continued)

Permission Details tab	Fields and descriptions
Organization Units	<p><b>Org Units</b> Number of organization units involved in the selected entitlement.</p> <p><b>Org Unit Support (%)</b> Percentage of organization units to be assigned to the permission, from the entire set of organization units involved in the analysis.</p> <p><b>Covered with just Roles</b> Number of organization units covered with the Role entitlement.</p> <p><b>Org Unit Coverage (%)</b> Percentage of organization units that are assigned with the entitlement, from the entire set of organization units that must be assigned with the entitlement.</p> <hr/> <p><b>OU Spread</b> OU Spread indicates the inclination towards obtaining a very scattered or localized entitlement distribution in the OU hierarchy. See Spread.</p> <p><b>Minimum Farness</b> 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.</p> <p><b>Average Farness</b> Average distance of all OUs from the centroid of distribution. See Farness.</p> <p><b>Average Coverage (%)</b> Average percentage of OUs assigned with the entitlement.</p> <p><b>Maximum Coverage (%)</b> Maximum percentage of OUs assigned with the entitlement.</p>

## Users

The **Users** tab lists the Entitlement and User details.



Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests and then click **Search**.

You can sort the displayed data in ascending or descending order, based on the data elements provided.

Table 52. Entitlements

Entitlements	Description
Name	Name of the entitlement.
Application	Name of the application.
Direct Users	Number of users assigned to the selected entitlement.
Permissions	Number of assigned permissions.
Assignments	Number of assignments.
OUs	Number of organization units involved in the selected entitlement.
OU Spread	OU Spread indicates the inclination towards obtaining a very scattered or localized entitlement distribution in the OU hierarchy. See Spread.
Applications	Number of applications assigned with the entitlement.

Table 53. User details

User	Description
In/Out	The user status can be one of the following: <ul style="list-style-type: none"> <li> In Role (Role aggregated to the User)</li> <li> Out of Role (Role not aggregated to the User)</li> </ul>
Last Name	Surname of the user.
First Name	Name of the user.
Master UID	Unique ID assigned to the user.
Organization Unit	Name of the OU, in which the user is registered.

Select a User and click **Actions > View Tree** to view the Organization Unit structure.

### Organization Units

The **Organization Units** tab lists the Entitlement and Organization Unit details.

Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests and then click **Search**.

You can sort the displayed data in ascending or descending order, based on the data elements provided.



Table 54. Entitlements

Entitlements	Description
Name	Name of the entitlement.
Application	Name of the application.
Direct Users	Number of users assigned to the selected entitlement.
Permissions	Number of assigned permissions.
Assignments	Number of assignments.
OUs	Number of organization units involved in the selected entitlement.

Table 54. Entitlements (continued)

Entitlements	Description
OU Spread	OU Spread indicates the inclination towards obtaining a very scattered or localized entitlement distribution in the OU hierarchy. See Spread.
Applications	Number of applications assigned with the entitlement.

Table 55. Organization Unit

Organization Unit	Description
In/Out	The OU status can be one of the following: <ul style="list-style-type: none"> <li> In Role (Role aggregated to the OU)</li> <li> Out of Role (Role not aggregated to the OU)</li> </ul>
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 organization unit.

Select a User and click **Actions > View Tree** to view the Organization Unit structure.

### Users:

View this tab for an analysis overview of the Users assigned with the selected Application.

This tab has the following sub categories.

- User
- User Details
- Permissions
- Applications

### User

The **User** tab lists all Users assigned to the selected Application.

In this tab, you can:

- Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests and then click **Search**.
- Select a User and click **Actions > View Tree** to view the Organization Unit structure.
- Select a User to view the analysis report in the right pane.

Table 56. User filter details

Filter	Description
Master UID	Unique ID assigned to the user.
Last Name	Surname of the user.
First Name	Name of the user.
Organization Unit	Name of the OU, in which the user is registered. Select <b>Hier</b> to include all the Organization Unit starting from the root <b>OU</b> .
Permission Coverage	Type of coverage. Without assignments or with permissions directly assigned.

### User Details

The **User Details** tab lists the User details, and the statistics of Entitlements associated with the selected User.

Table 57. User Details

User Details tab	Fields and descriptions
User	<p><b>Last Name</b> Surname of the user.</p> <p><b>First Name</b> Name of the user.</p> <p><b>Master UID</b> Unique ID assigned to the user.</p> <p><b>Organization Unit</b> Name of the OU, in which the user is registered.</p>
Permissions	<p><b>Permissions</b> Number of assigned permissions.</p> <p><b>Permission Support (%)</b> Percentage of permissions to be assigned to the user, from the entire set of permissions involved in the analysis.</p> <p><b>Covered through Roles</b> Number of permissions covered with the Role entitlement.</p> <p><b>Permission Coverage (%)</b> Percentage of permissions that are assigned to the user, among the entire set of permissions involved in the analysis.</p>



Table 57. User Details (continued)

User Details tab	Fields and descriptions
Applications	<p><b>Applications</b> Number of applications assigned with the entitlement.</p> <p><b>Application Support (%)</b> Percentage of application to be assigned to the user, from the entire set of entitlements involved in the analysis.</p> <p><b>Covered through Roles</b> Number of applications covered with the Role entitlement.</p> <p><b>Application Coverage (%)</b> Percentage of applications that are assigned to the permission, among the entire set of applications involved in the analysis.</p>

### Permissions

The **Permissions** tab lists the Entitlements and Permissions assigned to the selected User.



Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests and then click **Search**.

You can sort the displayed data in ascending or descending order, based on the data elements provided.

Table 58. Entitlements

Entitlements	Description
Name	Name of the entitlement.
Application	Name of the application.
Direct Users	Number of users assigned to the selected entitlement.
Permissions	Number of assigned permissions.
Assignments	Number of assignments.
OUs	Number of organization units involved in the selected entitlement.
OU Spread	OU Spread indicates the inclination towards obtaining a very scattered or localized entitlement distribution in the OU hierarchy. See Spread.
Applications	Number of applications assigned with the entitlement.

Table 59. Permission

Permission	Description
In/Out	<p>The permission status can be one of the following:</p> <ul style="list-style-type: none"> <li> In Role (Role aggregated to the permission)</li> <li> Out of Role (Role not aggregated to the permission)</li> </ul>
Name	Name of the entitlement.
Application	Name of the application.

### Applications

The **Applications** tab lists the Entitlements and Application assigned to the selected User.



Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests and then click **Search**.

You can sort the displayed data in ascending or descending order, based on the data elements provided.

Table 60. Entitlements

Entitlements	Description
Name	Name of the entitlement.
Application	Name of the application.
Direct Users	Number of users assigned to the selected entitlement.
Permissions	Number of assigned permissions.
Assignments	Number of assignments.
OUs	Number of organization units involved in the selected entitlement.
OU Spread	OU Spread indicates the inclination towards obtaining a very scattered or localized entitlement distribution in the OU hierarchy. See Spread.
Applications	Number of applications assigned with the entitlement.

Table 61. Application

Application	Description
In/Out	<p>The application status can be one of the following:</p> <ul style="list-style-type: none"> <li> In Role (Role aggregated to the application)</li> <li> Out of Role (Role not aggregated to the application)</li> </ul>
Name	Name of the application.

## Permission Type

The **Permission Type** tab displays the permission types that are already defined for the selected Application. You can also add a new type, modify, or remove an existing permission type when necessary.

The following fields are available:

Field	Description
Name	The name of the permission.
Description	Short description of the permission.

## Search

To search for specific permission types, use the **Filter** option. Otherwise, click **Hide Filter**.

1. Click **Filter**.
2. Specify information in the provided fields.
3. Click **Search**. Results matching the specified filter are displayed.

## Add

To add a new permission type:

1. Click **Actions > Add**.
2. Specify information in the provided fields.
3. Click **Actions > Save**.

## Modify

To modify a permission type:

1. Edit the information of the selected permission type.
2. Click **Actions > Save**.

## Remove

To remove the permission type:

1. Select the check box of the permission type.
2. Click **Actions > Remove**.
3. In the Remove Permission Type window, click **Ok** to confirm the request.

## Accounts

Describes how to customize an account configuration for an application.

The account configuration identifies a set of elements that determine the mode in which a user accesses an application.

The name of the default account that is provided for an application is IDEAS.

The left frame, which is titled Account Configuration, includes the **Name** and **Description** filters that are used to search Accounts (click the **Filter/Hide Filter** button to specify them).

In the same frame, you can use the **Actions > >Add/Remove** button to add or remove an Account.

Here the procedure for adding an account.

Use the **Details** tab to display details of the selected Account in the left frame. The details are:

Account Configuration details	
Detail	Description
<b>Name</b>	Name of the selected Account.
<b>Description</b>	Short description of the selected Account.
<b>Fulfillment</b>	You can define the following fulfillment options: <ul style="list-style-type: none"> <li>• <b>Automatic</b></li> <li>• <b>Manual</b></li> <li>• <b>Disabled</b></li> </ul>
<b>Connectors</b>	You can use the following radio-buttons to choose the typology of connectors joined to the selected accounts: <ul style="list-style-type: none"> <li>• <b>IDEAS Connectors</b></li> <li>• <b>Third Party</b></li> </ul>
<b>Linked Applications</b>	In this area, click the <b>Edit</b> tab and use the <b>New/Rename/Remove</b> buttons to specify or remove a set of Markers for the selected Account. You can then select <b>Manage &gt; Applications &gt; Details</b> to join an Application to a Marker specified in this panel.

Click **Save** to enable the selections that are made on the attributes you added or modified.

Further attributes that are enabled for configuration are grouped in the following tabs:

- **Account Configuration Detail** (default tab)
- **Creation Policy**
- **Management**
- **Password Creation**
- **Users**
- **Applications**

**Related tasks:**

“Adding an account” on page 57

Complete this task to register a new account into the Identity Governance and Intelligence data model.

**Creation Policy**

Describes how to customize the Creation Policy tab of an Account Configuration for an Application.

Use this tab to customize the following attributes:

Creation Policy settings		
Attribute	Description	
<b>Account</b>	Disable on creation	If selected, disables by default the new Users aggregated in the selected Account Configuration.
	Expiration time (days)	The value can be: <ul style="list-style-type: none"> <li>• 0, to indicate that the Account has no expiration date.</li> <li>• &gt;0, to indicate the number of days after which the Account expires.</li> </ul>
<b>UserID</b>	Concatenate user attributes	Use this text box to join User attributes concatenated by the plus (+) sign. Specify separators between "".  For example: Name + "." + Surname + "@" + MailProvider + "." + "com"
<b>Password</b>	Disable password first check	If selected, verifies that the passwords created or modified by an Administrator follow the rules set for: Password creation.
	Allow empty password	If selected, allows a login without a password request.
	Force Password Change (only for targets that allow it)	If selected, forces a new user, or a user whose password has been modified by the Administrator, to change the password at the next access.

Click the **Save** button to enable the selections made on these attributes.

## Management

Describes how to customize the **Management** tab of an Account Configuration.

Use this tab to customize the Management attributes. These attributes are organized in four sections.

The editing of contents in the **Management** tab, is enabled after the selection of one of the accounts listed in the **Account Configuration** tab.

Some of inners sections are enabled by ticking **Enable** check-box.

The Management attributes are:

Account Management settings		
Attribute	Description	
<b>Account expiration policy</b>	Action to be taken after the account expires	<p>Specifies which of the following actions is to be taken when the account expires:</p> <ul style="list-style-type: none"> <li>• <b>None:</b> no action is taken.</li> <li>• <b>Suspend:</b> the Account is suspended and a code numbered from 1 to 9 must be set. Any customer can freely join a proper meaning to these codes.</li> <li>• <b>Remove:</b> if the User Account has expired, the User is removed from the selected Account Configuration after a certain number of days, that you can set in <b>Remove after (days)</b>.</li> </ul>
	Expiration lock code	Code value (from 0 to 9) for the expiration blocking code.
<b>Password policy</b>	Validity from the last login (days)	The time period, expressed in days, at the end of which the account is blocked if the User does not access the system.
	Password validity (days)	The number of days between two consecutive password expirations.
	Maximum number of passwords retries	The maximum number of consecutive failing attempts, after which the User account is blocked.
<b>Password propagation</b>	Expiration class	Allows to enable password transmission, coded with an appropriate algorithm.
<b>Password expiration notification</b>	Notification time (days)	<p>The number of days before a password expires, that the user is notified of the coming expiration. Use one of these radio-buttons to choose the policy followed when passwords expire:</p> <ul style="list-style-type: none"> <li>• <b>Lock account after password expiration</b></li> <li>• <b>Force change password after password expiration</b></li> </ul>

Click **Save** to enable the selections made on the attributes.



**CAUTION:**  
 Any algorithm can be used to encrypt passwords. The chosen algorithm must be implemented in a class, whose path is to be specified in the Algorithm text-box.

## Password Creation

Describes how to customize the Password Creation tab of an Account Configuration defined for an Application.

This tab includes two accordion panes:


- Password Creation
- Dictionary

The following attributes are featured in the **Password Creation** accordion pane:

Password Creation attributes																																									
Attribute	Description																																								
<b>Enable Password Construction</b>	When selected, enables all the attributes that follow to build a password policy.																																								
<b>Minimum Length</b>	Determines the minimum length of a password. Use <b>No Check</b> to neutralize this control.																																								
<b>Maximum Length</b>	Determines the maximum length of a password. Use <b>No Check</b> to neutralize this control.																																								
<b>Allow Lowercase</b>	Allows the use of lowercase characters.																																								
<b>Minimum Lowercase Characters</b>	Specifies the minimum number of lowercase characters that must be included in a password. Use <b>No Check</b> to neutralize this control.																																								
<b>Allow Uppercase</b>	Allows the use of uppercase characters.																																								
<b>Minimum Upper-case Characters</b>	Specifies the minimum number of uppercase characters that must be included in a password. Use <b>No Check</b> to neutralize this control.																																								
<b>Allow Special Characters</b>	<p>Allows the use of special characters (that is, characters that are not numbers or letters of the alphabet). If this checkbox is selected, the special characters to be allowed can be chosen in the lower bar:</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <input type="checkbox"/> All           <table border="1" style="display: inline-table; border-collapse: collapse; text-align: center;"> <tr> <td>!</td><td>"</td><td>#</td><td>\$</td><td>%</td><td>&amp;</td><td>'</td><td>(</td><td>)</td><td>*</td><td>+</td><td>,</td><td>-</td><td>.</td><td>/</td><td>:</td><td>;</td><td>&lt;</td><td>=</td><td>:</td> </tr> <tr> <td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td> </tr> </table> </div> <p>Select the <b>All</b> checkbox to allow all available special characters.</p>	!	"	#	\$	%	&	'	(	)	*	+	,	-	.	/	:	;	<	=	:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
!	"	#	\$	%	&	'	(	)	*	+	,	-	.	/	:	;	<	=	:																						
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																						
<b>Minimum Special Characters</b>	Specifies the minimum number of special characters that must be included in a password. Use <b>No Check</b> to neutralize this control.																																								
<b>Allow Numerical Characters</b>	Allows the use of numerical characters in passwords.																																								

Password Creation attributes	
Attribute	Description
<b>Minimum Numerical Characters</b>	Specifies the minimum number of numerical characters that must be included in a password. Use <b>No Check</b> to neutralize this control.
<b>Exclude ASCII Extended Characters</b>	If this checkbox is selected, a password cannot contain extended ASCII characters (e.g. ö, ä, ñ, ...).
<b>Verify with Personal Data</b>	If this checkbox is selected, a password cannot contain the User's personal information (for example, User Mario cannot use a password such as 12Mario1971).
<b>Not equivalent to last Password</b>	Verifies that the new password is not the same as the last password used.  Currently, the latest eight passwords are saved, regardless of the enabling of the control; therefore, the user cannot use any of the last eight passwords saved.  When comparing the most recent eight passwords, the passwords are not case sensitive.
<b>Default Password</b>	A default password is automatically added when a User Account is created. It can be modified by the Administrator who creates the Account.

Click **Save** to enable the selections made on these attributes.

	<b>CAUTION:</b> When building a password at least one of the four character types (lowercase, uppercase, special, numerical) must be allowed (the related checkbox must be selected).
---	--

A list of terms and the command keys necessary to manage them can be stored in the **Dictionary** accordion pane.

Select the **Enable Vocabulary** checkbox to check that new or modified passwords do not use invalid terms contained in the dictionary.

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

- **Add:** allows to add a new term in the Dictionary.
- **Remove:** allows to remove a term from the Dictionary.
- **Save:** allows to save the latest selections.
- **Cancel:** allows to cancel the latest selections.

The control on invalid terms can be one of the following:

- **Prompt Search:** the system checks that a new or modified password is not exactly the same (**Exact** checkbox selected) as the word defined in the Dictionary.
- Search with **LIKE** filter: the system checks that a new or modified password does not contain a word defined in the Dictionary (**Exact** checkbox not selected).





## Users

Describes how to customize the Users tab of an Account Configuration defined for an Application.

This section includes functions used to manage the Users of the Account **Configuration** selected in the left frame.

The **Users** frame contains filters that can help you search for Users (select the **Filter/Hide Filter** button) and other command buttons that you can use to run basic operations on users.

The attributes of the user filters are:

User filters	
Attribute	Description
Name	User's name.
Last Name	User's last name.
Master UID	User's univocal identifier
User Account Filter	Select the  <b>Account Filter</b> button to choose one or more filters related to the User Account definition.
OU	Select the  <b>OU Search</b> button to choose the OU of a User.
Hierarchy	If this check-box is selected, the search process will be extended to all the hierarchy starting from the root OU specified in the <b>OU</b> field.

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

- **Remove:** allows to remove the selected User-Account.
- **Multiple Account:** allows to make changes to the Account Configuration of any number of Users at the same time. This can be useful when the Administrator has to block a large number of User Accounts.

For example, if you select three users in the Active Directory (AD) account in the left pane, and you click **Actions > Multiple Account**, the Management window displays, where you can make changes on the entire set of users selected.

The Account details of a selected User are shown on the right side of the **Users** tab. They are:

Account Details	
Name	Description
Account Configuration	An Account Configuration is linked to a specific Application and is made-up of a set of values that determine the access policies of a User to an Application (Account).
Applications	Applications linked with the Account Configuration.
Last Login	Date of a User's last Login.
Last Login Error	Date of a User's last Login error.

Account Details	
Name	Description
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 User's last password change.
Master UID	Identifies the User on the AG Core Module.
User ID	Represents the ID of the User on the target; if not explicitly indicated, the AG Core Master UID is assumed valid (see previous row).
Force Password Change	If selected, forces the User to change own password at the next login to the any of the Applications linked to the selected Account.
Account Expiration Date	The Account's expiration date. It can be setup automatically based on settings in Accounts (paragraph 6.6).
Account Blocking Code	Indicates the reason/origin ( <b>Technical, Security, Terminated, Expire, Authoritative, Maintenance</b> ) for blocking an Account. For any reason type, you can use a value from 0 to 9 to further customize the reason for terminating an account.


This panel features the following buttons:

- **Reset Login:** allows to reset a Login.
- **Change Pwd:** allows to change a password.
- **Save:** allows to save changes to an Account.
- **Cancel:** allows to cancel changes made to settings.

## Applications

Describes how to customize the Applications tab of an Account Configuration defined for an Application.

This tab shows the Applications aggregated in the Account selected in the left frame. **Name** and **Account** are the filters available for use (click the **Filter/Hide Filter** button to specify them).

Be aware that you might find the  icon in the SoD column, which indicates that the related Application is out of SoD check (see the check-box **Exclude from SoD validation** in section **Manage > Applications > Details > Policy box**).

## Resources

Describes how to manage resources and resource types.

Resources are entities used by the Organization to run administrative and production procedures. They are organized into Families and Types. A given Family of Resources corresponds to one or more Types, which in turn correspond to one or more Resources. Thus, a Resource cannot be introduced unless at least

one Resource Type (paragraph 6.7.2) is already inventoried; introducing a Resource Type is subordinate to pre-selecting a Family of Resources (paragraph 6.7.3) to which the Resource Type is linked.

The name chosen for the Resource must be univocal within the Type it is associated to.

Each Resource is defined within a specific Family and Type.

Filters available for a Resource are listed in the table below:

*Table 62. Resource filters*

Attribute	Description
Family	Family of the Resource
Type	Resource type
Name	Name used within the Organization to identify the Resource Type
Description	Brief description of the Resource Type

Proceed as follows:

1. In the tab bar select **Settings > Resources**.
2. Click the Resource accordion pane.
3. In the left frame, click the **Filter/Hide Filter** button.
4. Set the data filters needed to search among all types.
5. Click the **Search** button.
6. To add a Resource:
  - a. In the left frame, click the **Add** button.  
In the right frame, the **Edit** tab becomes active.
  - b. Set the attributes for the new resource type.
  - c. Click the **Save** button.
  - d. Click **Ok** in the window that displays the outcome of the operation.
7. To edit a Resource:
  - a. In the left frame, select the resource to be edited.
  - b. In the right frame click the **Edit** tab.
  - c. Modify the attributes of the resource.
  - d. Click the **Save** button.
  - e. Click **Ok** in the window that displays the outcome of the operation.
8. To delete a Resource:
  - a. In the left frame, select the resource to be deleted.
  - b. In the same frame, click the **Delete** button.
  - c. Click **Ok** to confirm the operation.
  - d. Click **Ok** in the window that displays the outcome of the operation.


## Resource Family

A Resource Family is the highest level of abstraction into which Resources can be grouped.

The only available filters are Name and Description. Proceed as follows:

1. In the tab bar select **Settings > Resources**.
2. Click the Resources accordion pane.
3. In the left frame, click the **Filter/Hide Filter** button.
4. Set the data filters (Name, Description) needed to search among all families.
5. Click the **Search** button.
6. To add a new Resource Family:
  - a. In the left frame, click the **Add** button.  
In the right frame, the **Edit** tab becomes active.
  - b. Set the Name and Description attributes for the new family.
  - c. Click **Save**.
  - d. Click **Ok** in the window that displays the outcome of the operation.
7. To edit a Resource Family:
  - a. In the left frame, select the Resource Family to be edited.
  - b. In the right frame click the **Edit** tab.
  - c. Modify the Name and/or Description attributes.
  - d. Click **Save**.
  - e. Click **Ok** in the window that displays the outcome of the operation.
8. To delete a Resource Family:
  - a. In the left frame, select the Resource Family to be deleted.
  - b. In the same frame, click the **Delete** button.
  - c. Click **Ok** to confirm the operation.
  - d. Click **Ok** in the window that displays the outcome of the operation.

Table 63. Resource note

	<p><b>Note:</b></p> <p>The Realms Resource Family is in the Realm Administration created during the installation procedure.</p> <p>This Family of Resources cannot be deleted, since it is required for the operation of the product. If the user attempts to delete it, the system prevents it and displays a warning message.</p>
---	---

## Resource Types

Resource Types are a more specific classification of a set of Resources and is defined within a specific Family. The filters available for a Resource Type are listed in the table below.


Table 64. Resource Type filters

Attribute	Description
Family	Family of Resource Type.
Name	Name used within the Organization to identify the Resource Type.
Description	Brief description of the Resource Type.

Proceed as follows:

1. In the tab bar select **Settings > Resources**.
2. Click the Resource Types accordion pane.
3. In the left frame, click the **Filter/Hide Filter** button.
4. Set the data filters needed to search among all types.
5. Click **Search**.
6. To add a Resource Type:
  - In the left frame, click **Add**.
  - In the right frame, the **Edit** tab becomes active.
  - Set the attributes for the new resource type.
  - Click **Save**.
  - Click **Ok** in the window that displays the outcome of the operation.
7. To edit a Resource Type:
  - In the left frame, select the resource type to be edited.
  - In the right frame click the **Edit** tab.
  - Modify the attributes.
  - Click **Save**.
  - Click **Ok** in the window that displays the outcome of the operation.
8. To delete a Resource Type:
  - In the left frame, select the resource type to be deleted.
  - In the same frame, click the **Delete** button.
  - Click **Ok** to confirm the operation.
  - Click **Ok** in the window that displays the outcome of the operation.

*Table 65. Note about the Administration Resource Type*

	<p><b>Note:</b></p> <p>The Administration Resource Type is in the Realm Administration created during the installation procedure.</p> <p>This Type of Resources cannot be deleted, since it is required for the operation of the product. If the user attempts to delete it, the system prevents it and displays a warning message.</p>
---	---

## Resources into Administration Realm

When you are logged in the Administration Realm, the available operations are the same as the other operations shown in this section. The Administration Realm includes special Resources that cannot be removed, since they are required for the platform operations. If the user attempts to delete them by mistake, the system prevents it and displays a warning message.

---

## Configure

Configuration topics are grouped into sections.

- Certification Campaigns
- “Certification data sets” on page 181
- Rules
- Flow Processes
- Email
- Hierarchy










### Certification campaigns

Certification campaigns can be run on different entities of the data model and on different data sets.

The following features are available for managing a certification campaign.

In the **Certification Search** frame, search certifications for the certification campaign you want. Click **Filter** for **Name**.

The status of a campaign is indicated by the following icons.

-  **active**: Campaign is running and can be managed by reviewers
-  **stopped**: Campaign is complete
-  **stopping**: Campaign is waiting to complete
-  **new**: New campaign that has never run
-  **paused** : Campaign is paused and standing by
-  **preview**: Campaign is available for preview before activation. When it is in preview, only the supervisor can examine the attributes of the campaign. The attributes are set to read-only.
-  **waiting**: Campaign is waiting to start according to the configured schedule
-  **error**: Campaign is in error
-  **launched**: Campaign is queued to be run

You manage a campaign by using the **Actions** menu in the left frame. The following items are available.

- **Add** a new campaign
- **Remove** a selected campaign.
- **Launch** a selected campaign.
- **Active**: the campaign is activated and can be run.
- **Pause** a selected campaign.
- **Close** a selected campaign.
- **Preview** a selected campaign. Use this option to inspect the configuration of a campaign. All configurations are shown read-only. You must be a supervisor to preview a campaign.
- **Clone** a selected campaign. The name of cloned campaign is set to `SourceCampaignName_automaticID`, where *SourceCampaignName* is the name of the selected campaign and *automaticID* is a suffix of 13 digits.

If a campaign is in **Preview** state, the supervisor can inspect the attributes of the Campaign. If the configuration is satisfactory, the supervisor would ask to the AGC Administrator to **Launch** the campaign. If not, the supervisor can ask to **Close** it.

The **Close** action sends a request to a system task, which is scheduled through the Task Planner module.

The **Details** tab shows data relative to the selected Campaign.

The following table describes the details of a Campaign:

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

Use the **Edit** tab to edit the details of a campaign. Click **Save** to save your changes.

The following tabs are shown in the right frame. See the topic for each tab for a description of the functions available.

- **Supervisors**
- **Reviewers**
- **Fulfillment**
- **Scheduling**
- **Notification**
- **View Configuration**



## Supervisors

The **Supervisors** tab displays the supervisors in the campaign that is selected in the left frame.

Supervisors have attributes that are shown in the following table:

Attribute	Description
First Name	Given name of the supervisor
Last Name	Surname of the supervisor
Master UID	Master UID of the supervisor user
Org. Unit	Organizational Unit of the Supervisor

Campaign status is shown by icons.

Icon	Status
	Active
	New

For an active campaign, the supervisors are fixed and the **Actions** menu is not active.

For a new campaign, clicking **Actions** > **Edit** shows the following actions.

- **Add:** Add a supervisor.
- **Remove:** Remove a supervisor.

Click **Save** to enable your selections.

### Note:

- You must configure at least one supervisor.
- If **Escalation Supervisor** is checked in the **Supervisors** tab, the supervisor can receive escalations from reviewers.

## Reviewers

This tab shows all of the reviewers for the selected campaign.

The following table shows reviewer attributes.



Table 66. Cert\_Campaign\_Reviewer\_Tab

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

Click **Save** to enable your settings.

## Fulfillment

This tab shows the fulfillment activities for the selected campaign.

Some of these options are available only for some campaigns.

Fulfillment Detail	Description
<b>Logical deletion</b>	If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are deleted but only logically.
<b>Physical deletion</b>	<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"> <li>• Delete the Account</li> <li>• Lock the Account</li> </ul>
<b>Physical deletion after workflow</b>	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> .
<b>Custom Behaviour</b>	The management of the fulfillment involves a set of rules.

Click **Save** to enable your settings.

## Scheduling

This tab shows the scheduling for the selected campaign.

The following table shows schedule attributes.

Table 67. Cert\_Campaign\_Scheduling\_Tab

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

Click **Save** to enable your settings.

## Notification

This tab shows the notifications for the selected campaign.

Notifications are sent to **Reviewers** and **Supervisors** in the selected campaign.

The following table shows notification attributes.

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

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

Click **Save** to enable your settings.

## View Configuration

This tab shows the view configuration of the selected campaign.

This tab appears if **User Certification Campaign** is selected in the left frame.

In this tab, you configure the columns that are shown in the **User View** and **Entitlement View** for the reviewers and supervisors of the Access Certifier module. Introduction to Access Certifier

You enable the user and entitlement views by setting the following check boxes:


- **User View:** columns available are fixed.
- **Entitlement View:** columns available are determined by the entitlements that are configured.

Click **Edit** to enable and disable columns.

The columns available are shown in the following table.

Table 68. Columns for Entitlement View

Column	Description
<b>Attestation buttons</b>	Makes actions visible. <ul style="list-style-type: none"> <li>• <b>Approve</b></li> <li>• <b>Revoke</b></li> <li>• <b>Sign Off</b></li> <li>• <b>Notes</b></li> <li>• <b>Redirect</b></li> <li>• <b>Redirect to Supervisors</b></li> </ul>
<b>Master UID</b>	UID of the user.
<b>User First Name</b>	Given name of the user.
<b>User Last Name</b>	Surname of the user.
<b>User info buttons</b>	Makes user information visible. <ul style="list-style-type: none"> <li>• <b>Details</b></li> <li>• <b>Entitlements</b></li> <li>• <b>External Data</b></li> <li>• <b>Accounts</b></li> <li>• <b>Activities</b></li> <li>• <b>Rights</b></li> </ul>
<b>OU Name - Code</b>	Name and code of the organizational unit (OU).
<b>OU Owner</b>	Owner of the organizational unit, according to the setting in AGC.
<b>OU Description</b>	Short description of the organizational unit.
<b>Application Name</b>	Name of the application, with the information available about the application.
<b>Application Owner</b>	Owner of the application, according to the setting in AGC.
<b>Application Description</b>	Short description about the application.
<b>Entitlement Name</b>	Name of the entitlement. If the <b>Entitlement Localization</b> option is active, the entitlement is shown as a localized name.
<b>Entitlement ID Code</b>	ID code of the entitlement.
<b>Entitlement Description</b>	Short description of the entitlement.
<b>Entitlement info button</b>	Makes entitlement information visible. <ul style="list-style-type: none"> <li>• <b>Details</b></li> <li>• <b>Structure</b></li> <li>• <b>Activities</b></li> <li>• <b>Rights</b></li> </ul>
<b>VV</b>	Role Alignment Violation property, which is related to an entitlement assigned to a user but not joined to the organizational unit of the user.
<b>User Type Name</b>	Type of user, according to AGC settings.

The position of columns can be changed through the **Up**  and **Down**  arrows.

The first column in this list appears as the leftmost column in the view. The last column appears as the rightmost column in the view.

Click **Save** enable your selections.

## Certification data sets

A Campaign of certification is based on a data set, which is built with elements that are analyzed during the campaign.

The following base entity sets can be used to define a data set.

- **Groups**
- **Users**
- **Applications**
- **Entitlements**
- **Risks**
- **Account**
- **Advanced Settings**

For every entity set (with exception of **Advanced Settings**), you can set a **White List** of elements and a **Black List** of elements.

- **White List:** Consists of elements to be analyzed.
- **Black List:** Consists of elements that are excluded from analysis.

If an element in the white list is also put in the black list, it is not used for the analysis. The final entity set is determined according to the following table.

White List	Black List	Dataset to analyze
$\neq 0$	0	Only WL
$\neq 0$	$\neq 0$	WL - (WL $\cap$ BL)
0	$\neq 0$	ALL - BL
0	0	ALL

The following filters are available for use with the white list and black list.

Table 69. Entity filters

Filter	Description
Group	Name
	ID Code
	Name of the OU
	ID code of the OU

Table 69. Entity filters (continued)

Filter		Description
<b>Users</b>	<b>Name</b>	Given name of the user
	<b>Surname</b>	Surname of the user
	<b>Master UID</b>	Univocal identifier of the User
<b>Applications</b>	<b>Name</b>	Name of the application.
	<b>Marker</b>	Name of a target system.
<b>Entitlements</b>	<b>Type</b>	Entitlement type, one of: <ul style="list-style-type: none"> <li>• Permission</li> <li>• IT Role</li> <li>• Business Role</li> <li>• External Role</li> </ul>
	<b>Application</b>	Name of the application that is related to the entitlement
	<b>Name</b>	Name of the entitlement
<b>Risks</b>	<b>Name</b>	Name of the risk
	<b>Description</b>	Brief description of the risk
	<b>Type</b>	Type of the Risk
<b>Account</b>	<b>Name</b>	Name of the account
	<b>Description</b>	Brief description of the account

Use the **Actions** menu to add an entity (single item or in hierarchy), remove an entity (single item or in hierarchy) or remove all entities.

You can use the **Ctrl** and **Shift** keys to select multiple entities.

For deploying a new data set, proceed as shown below:

1. In the left frame **Datasets**, click on **Actions** > **Add**
2. In the **Details** tab, set the identification attributes of the data set.
3. In the right frame, click the wanted entity tab:
  - **Group**
  - **Users**
  - **Applications**
  - **Entitlements**
  - **Risks**
  - **Account**
4. For the selected entity tab, click **White List** or **Black List** to add it to the wanted list.
5. Select the **Advanced Settings** tab for choosing some advanced filters (selectables according to the data set type indicated at step 2).

Advanced Settings option		
Setting	Description	Type of dataset involved
Visibility Violation	For including assignments in Visibility Violations	Organization Unit Assignments - User Assignment
Disabled	For including disabled users assignment or disabled OU assignments	Organization Unit Assignments - User Assignment
With Violations	For including accounts or user with violations.	Account - User Assignment
Delegated Roles	For including assignment related to delegated roles	User Assignment
Account Disabled	For including the disabled accounts	Account
Account not accessed since xxx Days	For including account not accessed form xxx days.	Account
Assignments	For including the assignments related to a Group and/or to User. It's possible to choose between Default Roles or not.	Organization Unit Assignments - User Assignment

**Note:** The advanced settings work in "logic AND" with other tabs (and alike other tabs) for defining a data set. This means that, for example, if you have a user in **White List** and the option **Disabled** is ticked, the data set is populated only by roles disabled related to that user.

For removing a data set, select it in the left frame **Datasets**, then use **Actions > Remove**.

## Admin roles

Admin roles are used to manage IBM Security Identity Governance and Intelligence applications.

Admin roles are made up of entitlements. You can view both roles and entitlements in **Admin Roles**.

- Choose a view in the left frame. You can choose **Flat View** or **Hierarchy view**. **Flat View** is shown by default.
- Use filters to control the list of roles. Click **Filter**.
- Use the **Actions** menu to manage roles.
  - **Add**
  - **Remove:** Deletes a selected role
  - **Publish:** Publishes a role so you can assign it to an OU
  - **Unpublish:** Unpublishes the role and makes it unavailable to users and OUs.

A role is in one of the following states:

- Published and available to be assigned
- Unpublished and not available to be assigned

A published role can be assigned to the following objects:

- One or more OUs
- One or more users

The following rules govern roles and entitlements.

- Any role or entitlement in the hierarchy can be published and unpublished.
- A newly added entitlement can be published.
- An unpublished role or entitlement is not available for assignment to OUs or users.

The **Details** tab shows data for the selected entitlement. The following table describes the details of an entitlement:

The **Entitlement Properties** pane displays properties for an entitlement. Properties influence the behavior of entitlements. For example, a property can have a value that is used by a rule to manage a business process in the organization.

A property consists of a <Name, Value> pair. Use **Actions** on the upper right to **Add** or **Remove** properties.

Every property is characterized by a set of properties, as shown in the following table.

*Table 70. Keys for properties*

Property	Description
<b>Name</b>	Name of the property.
<b>Description</b>	Description of the property.
<b>Searchable</b>	For future use.
<b>Multivalue</b>	Property can have a set of values rather than a single value.

Use the following procedure to create a new property.

1. Click **Add**. An empty line appears.
2. Click **Add Key**.
3. Choose a key from **Key Properties**.
4. Click **Add Value** and enter a value.
5. If the property is multi-valued, use **Actions > Add** to add multiple values.
6. Click **Save**

Other tabs provide more information on Admin roles:

- “Scope”
- “Management” on page 185
- “Org Units” on page 185
- “Users” on page 186

## Scope

Use the **Scope** tab to choose a scope to join to a role.

When the role is assigned to a user, you are prompted to choose the elements to populate the scope.

Choose from the following scope entities.





- **Org Units**
- **Entitlement**
- **Application**
- **Risk**
- **Attribute Hierarchy**

## Management

Use the **Management** tab to build the hierarchy of Admin Roles.

Click **Filter** to narrow the search. The filters available for the entitlements search are shown in the following table.

Table 71. Entitlements filters

Filter	Description
<b>Type</b>	Type of entitlements: <ul style="list-style-type: none"> <li>• Permission</li> <li>• IT Role</li> <li>• Business Role</li> </ul>
<b>Name</b>	Name of the entitlement.
<b>Application</b>	Application that is related to the entitlement. Use  <b>Application</b> to insert an application. Use  <b>Clear</b> to clear the field.

The following items are available in the **Actions** menu.

- **Conflicts:** Shows conflict information and the risk tree for the selected roles. You can define mitigation actions in the **Mitigation** tab.
- **Parents:** Shows the entitlement hierarchy of the selected entitlement
- **Add:** Adds a selected entitlement
- **Remove:** Removes a selected entitlement

## Org Units

Use the **Org Units** tab to assign organizational units to Admin Roles.

Click **Filter** to narrow the search.

The following filters are available:

OU filters	
Filter	Description
<b>Group</b>	The name of a specific attribute group. In this case it is the attribute group of organizational units.
<b>Name</b>	The name of a specific group of the hierarchy. In this case it is the name of the OU.
<b>ID Code</b>	The ID of a specific group of the hierarchy.

You can select the following in the **Actions** menu:

- **Add** an OU

- **Remove** a selected OU

## Users

Use the **Users** tab to assign users to Admin Roles.

Click **Filter** to narrow the search.

Use **Search Identity** to filter by **Name**, **Surname**, or **Master UID** of the user.

The tab shows all users that have the Admin Role that is selected in the left frame.

In the **Actions** menu, the following actions are available.

- **Edit**: Modify the scope of the user. Change the set of OUs managed by the User according to the selected Admin Role.
- **Add**: Add a user to an Admin Role with the **Add User** window.
- **Remove**: Remove a selected user from an Admin Role.

## Rules

Rules are used to manage different types of events or for the automation of particular policies.

The Rule Classes available are seven:

### Live events

Rules that are triggered by Event Queues (for more information, see Events in Integration Interface). These types of events are processed in real time. Their purpose is to control the input/output data flow.

### Deferred events

Rules that are triggered by the Event Queue IN. These types of events are processed by scheduling (see Task Planner). Their purpose is to aggregate events.

### Authorization Digest

Rules that are triggered by changes in the User data set. These types of events are processed in real time. Their purpose is to validate enforcements.

### Account

Rules for the creation of a user account.

### Advanced

Rules that can be scheduled through Task Planner.

### Attestation

Rules that are automatically applied in campaigns of attestation.

### Hierarchy

Rules for the automatic building of hierarchies based on user attributes.

You can select the class of Rules in the filter section (click **Filter** button).

The filtering approach requires the selection of a **Rule Class** and according to the class, you can select from **Queues** or **Rule Sequence (Flow)** combo boxes.

The **Actions** menu of the tab **Rules** in the left frame lists the following actions:

**Import**

For importing the XML representation of a Rule or of a Rule Sequence (Rule Flow).

**Export** For exporting a Rule or a Rule Sequence (Rule Flow).

**Add** Adds a Group of Rules (function maintained for legacy reason).

**Remove**

Removes a Rule or a Group of rules (for Groups, function maintained for legacy reason).

**Enable/Disable**

Enable or disable a Rule execution into a sequence.

**Move Up/Down**

Move the Rule up/down in the Rule sequence.

In the right frame you can find two main accordion panes:

**Rules Package**

In this accordion pane is available all functions for managing a Rule selected in the left frame.

**Package Imports**

In this accordion pane is present all functions for managing packages of rules.

**Rules Package**

In this accordion pane are available all functions for managing Rules through the Rules editor.

According to the selection on the left tab **Rules**, a set of rule are listed in this pane.

The **Actions** menu hosts the following actions:

**Verify** For checking the formal structure of the code involved in a rule (needs the selection of one of the rule listed).



**Modify**

For modifying the rule, opening the Rules editor pop-up window.

**Delete** For deleting selected rule.

**Create** For creating a new rule.

**Add**

This function add a rule selected by the list to a  **Group** (legacy versions) or  **Rule Sequence** selected in the **Rules** tab, on the left.

**Rules Editor**

The Rules Editor speeds up the writing of code contained in a Rule.

The figure below shows the Rules Editor panel:

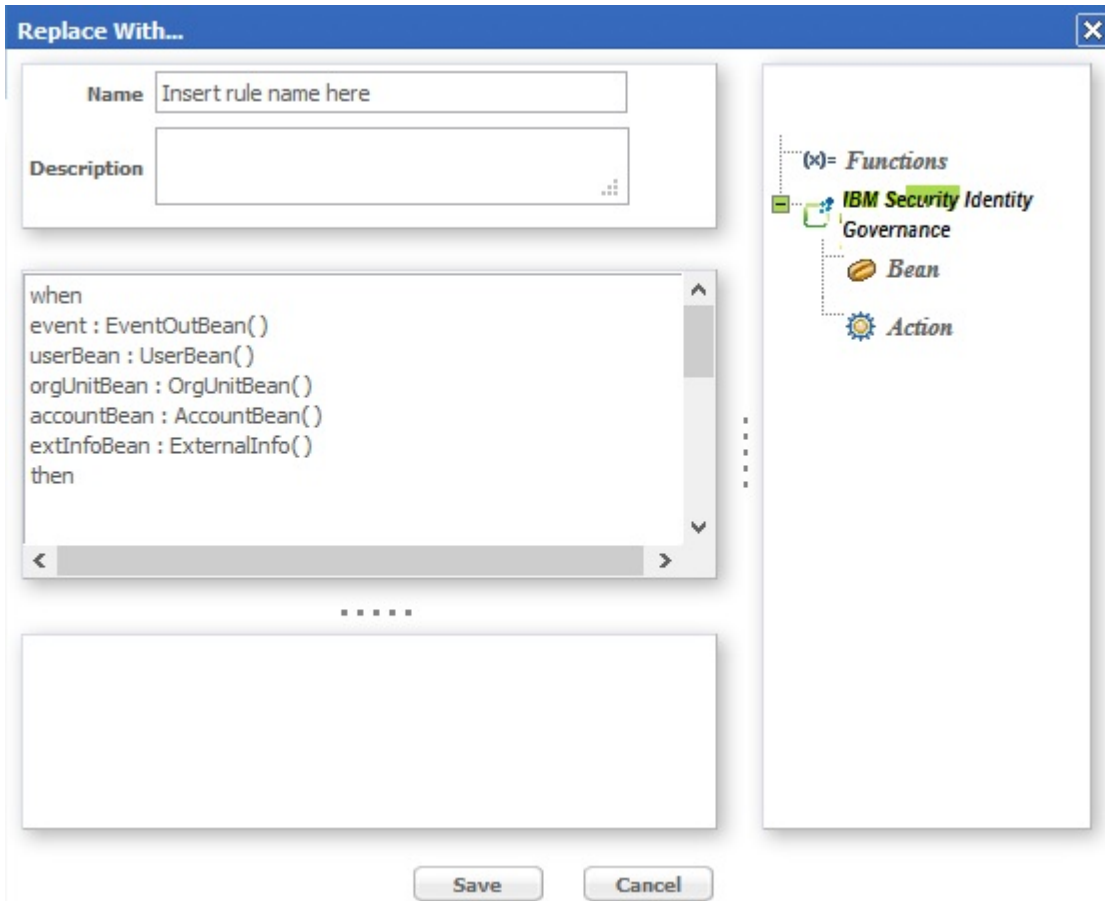


Figure 46. The Rules Editor panel.

The table below shows the symbols of several buttons and icons present in the Rules editor:

Table 72. Symbols of the Rules editor.

Icon	Description
	Import a Java class
	Java class
	New variable
	New function
	Bean
	Action
	Associated rule: rule that is associated to a rules group
	Split: used to construct flow processes in situations that require a branch point.
	Constraints
	Rules group
	Flow process

All the Rules must have the following structure:

- **Condition Area** (between “when” and “then”)
- **Action Area** (immediately after “then”).

The word **when** identifies the beginning of the conditions area.

Any number of conditions can be inserted and the actions will be executed only if all the conditions are verified (logic AND between each condition)

The word **then** identifies the beginning of the actions area.

Actions are written in normal Java code; all classes making up the libraries delivered with the product are available for writing actions.

A complete list and descriptions are available in the **Replace with...**

The conditions are written according to Drools syntax.

Every condition verifies, within the Working Memory, whether or not there are one or more objects identified by the Beans. If such objects are actually found, the actions described above will be executed on them.

The **Replace with...** window contains the code obtained from the Editor.

From the frame on the right side of the window, predefined code blocks can be selected and placed directly into the **Replace with...**

The objects are grouped in a hierarchy and managed through a tree structure.

The **Object** frame contains the nodes corresponding to the higher level object categories. The two initial main categories are:

- Functions
- Ideas

Based on the selection, the objects can be **Functions**, **Bean** or **Action** and their methods are visible below the selected object (fourth level of the tree):

Now, select a leaf object (a method) and insert it into the **Replace With...** frame (left) using the **Actions>Add** button.

This operation can be performed to modify or create a Rule.

**Note:** The name of a Bean can be written without its system path **ONLY** if it has been imported into the Package that contains the Rule.

## Functions

The Functions category contains functions for fundamental Rule-writing constructs; the same frame lists the following four elements:

- if
- ifelse
- ifelseif

- for

Select one of the functions and click **Add** to insert the related parametric code into the **Replace with...** frame, at the end of the already-listed code. The parameters to edit are easily recognized because they are between two '\$' symbols.

For example, in the IF ELSE construct, you have to edit the parameters **CONDITION1**, **ACTION1** and **ACTION2**.

Proceed in one of two ways to edit the parameters:

- Directly write the code instead of the corresponding symbolic string (e.g., **CONDITION1** included between two '\$' characters);
- Use the editor again.

In this last case, click **Field > Bean > AccountBean** and select one of the objects listed, then click **Add**:

Selecting **\$ACTION2\$** places the selected code block in the position that was covered by **\$ACTION2\$**. If none of the parameters in the window are selected, click **Ok** to place the code block at the end of the already-present code. To eliminate a potentially wrong insertion, cancel the corresponding code directly in the **Replace With...** frame.

## Bean and Action Elements

The IBM Security Identity Governance folder contains the following two folders:

- Bean
- Action

These folders contain ALL the Beans and Actions imported into the Rules Package; in particular, the Bean folder contains the Beans imported into the Package that are part of the libraries delivered with the product. Client users of the AG Core can create additional personalized Beans.

This paragraph analyzes how to use a Bean in the Bean folder. By selecting Bean, the content of the Bean folder is presented in the form of a tree, where every Bean is a node and its child nodes represent its methods.

After selecting the Bean, click Add to insert it into the **Replace With...** frame.

Be sure to insert a semicolon (;) at the end of each line and put the code in order.

Be sure to assign the String parameter a string that makes sense.

The Action folders contain ALL Actions imported into the Package of the selected Rule; in particular, the Action folder contains all Actions imported into the Package that are part of the libraries delivered with the product.

The procedure for inserting Actions (even custom Actions) is exactly the same as that for inserting Beans.

## Package Import

From the tabs bar, select **Configure > Rules** then click on the **Package Import** accordion pane on the right.

Configuring a Package consists of declaring certain objects available to all Rules in the Package.

Such a declaration consists of specifying an appropriate Java code in the allotted text box.

To make configuration of the Packages easier, insert blocks of predefined code (on the right side of the frame there is a small vertical toolbar with buttons).

The following actions are available for each Package:

- Import specific classes
- Insert variables
- Insert functions

The Rules programmer can write the Rule's code to directly call the objects that are set up for the Package containing the Rule.

Importing a class into a Package adds a class to a Rule without having to specify the entire path.

For example, after importing the class `UserBean()` into the Package, it is possible to directly write `UserBean()` instead of `com.engiweb.profilemanager.common.bean.UserBean()`.

## Package Editor

An administrator familiar with programming languages can insert any object in the Package by writing the code directly in the text box.

A Package Editor is also available to assist administrators to accomplish this task.

The Editor uses the following buttons, located on the right-hand side of the text box:

-  New Import
-  New Variable
-  New Function

Variables usually support objects that are already instanced with global visibility to all the Rules of the Package; if, for example, there is an object that contains all the parameters required to connect to the DB, the object can be assigned to an "sql" variable (always visible to the Package's Rules) and can be used in the Rule code, as shown in figure above.

Lastly, it is possible to create Functions that always have global visibility to all the rules of a package. For example, if several rules request an operation for the arithmetic average of two numbers, this can be created directly in the Package instead of in each single rule.

## Import a Class


To import a class, click on  **New Import** button in the vertical toolbar on the right-hand side of the Package Imports pane.

The Classes window opens (figure below) with a list of available classes

Choose a class, then click **Ok**.

The Java code corresponding to the selected class is written in the text area on the right-hand side of the Replace With... window.

### Enter a New Variable

To insert a new variable, click on  **New Variable** in the vertical toolbar on the right-hand side of the Package Imports accordion pane.

The text box displays the code corresponding to the declaration of a new variable.

The code is parametric and thus must be edited in the allotted spaces, defined by the characters <>.

Insert the object (specify entire system path) in the space <your class here>.

Insert a variable name in the space <variable name>; this name can then be used in every Rule of the Package.

### Enter a New Function

To insert a new function click on  **New Function** in the vertical toolbar on the right-hand side of the Package Imports accordion pane.

The text box displays the code corresponding to the declaration of a new variable.


The code is parametric and thus must be edited in the allotted spaces, defined by the characters <>.

Edit the parameters as follows:

- Replace <return Type> with the type of objects that result from processing the function (e.g. an integer, a string, a class, etc.).
- Replace <args here> with the list of parameters given to the function at input.
- {} needs to contain the body of the function, i.e., all the code that implements the function.

### How to Schedule a Rules Flow

It is possible to link a Rules Flow to a scheduled Job. The IBM Security Identity Governance Task Planner is the module dedicated to scheduling several types of Jobs that optimize different tasks in the IBM Security Identity Governance Platform. The Flows that can be scheduled belong to the Rule Classes Advanced or/and Deferred Events.

After creating a Flow Process, open the upper toolbar and click on the  button related to the IBM Security Identity Governance Task Planner.

In the Task Planner module, from the tabs bar, select **Manage > Job** Classes to access the Job Classes GUI.



From the list of Job Classes, choose the AdvancedRuleFlow or DeferredEventsRuleFlow (depending on what is needed) then select the Jobs tab and choose a relevant Job from the list produced.

Click on the >Job button in the Jobs frame, then populate the fields with the values of the chosen Job Class.

## Concept of Rule Flow

Understanding the flow process

A Flow Process can manages different Rule Groups.

Each Flow MUST have only one Start point and one End point.

It's a best practice using a Flow when dealing with a large quantity of Rules and objects.

Different types of Flow Processes are available.

Starting from the Rule Classes Authorization Digest and Advanced, it is possible to create a custom Flow Process.

The Flow Process frame (left) lists registered custom Flow Processes.

The following search filters are available (click on **Filter/Hide Filter** button):

Flow Process filters	
Filter	Description
Rules Class	In this field, the type of Rules Class associated with the Flow Process: <ul style="list-style-type: none"><li>• <b>Authorization Digest</b></li><li>• <b>Advanced</b></li></ul>
Name	Process Name

In the **Actions** menu, are hosted all the available buttons for managing Flow Processes, listed below:

- **Add:** to add Flow Processes.
- **Remove:** to remove Flow Processes.

In the **Details** tab, click on the **Edit** tab to edit a Flow Process. This enables the attribute text boxes.

After a Flow is added, it is listed in the **Rules Flow** combo box in the frame **Configure > Rule > Flow Process**.

## Email

This section includes all functions for the email management related to any type of notification needed on the IBM Security Identity Governance platform.

In the **Email Settings** tab some information must be configured, as described in the following table:

Table 73. Email settings attributes

Settings type	Attribute	Description
Basic settings	Sender Email	Email address of the sender of a notification.
Advanced Settings	Debug Mode	If selected, notifications can be sent to the email address specified in the <b>Static Recipient</b> text area.
	Static Recipient	Email address configurable in debug mode to receive notifications.
	Aggregation	You can choose one of the three different options: <ul style="list-style-type: none"> <li>• <b>None:</b> no special policy is applied.</li> <li>• <b>Same Message:</b> with this policy, the body text of several email can be merged into a single message (notification).</li> <li>• <b>Same Recipient:</b> in case of duplicate email, this policy allows a single email to be sent to the recipient.</li> </ul>


In the **Email Template** tab you can find all functions for the management of email templates.

The set of available templates can be filtered (left) using the **Name** and **Description** attributes (by clicking **Filter/Hide Filter**).

In the **Actions** menu, are available the following buttons for managing templates:

- **Add:** to add templates.
- **Remove:** to remove templates.

Table 74. Cautionary note

	<p><b>Note:</b> Every email notification is based on a specific email template.</p> <p>Any business process structured with IBM Security Identity Governance, which requires an email notification, might be inhibited or damaged due to an incorrect <b>Remove</b> operation of the email template involved in the process.</p> <p>Every <b>Remove</b> operation of an email template must be evaluated carefully.</p>
---	---

To add a template implies the definition of the attributes displayed in the right pane and listed in the following table:

Table 75. Email template attributes

Attribute	Description
<b>Name</b>	Name used by the organization to identify the template.
<b>Description</b>	Brief description of the template.
<b>Subject</b>	Subject of the template (expressed in the available languages, selectable using the specific tab).
<b>Body</b>	Body of the template (expressed in the available languages, selectable using the specific tab). The body can be in plain text as well as in HTML format. You can also add a <code>details</code> key that can be replaced with supplementary information (If supported by your system) at send time.

Using the **Preview** button, you can examine the whole structure.

The **Language** button allows you to determine, in the set of the available languages, the languages that can be involved in the template definition (choosing the dedicated tab).

Click **Save** to enable the selections made on the different attributes.

In the **Job Monitor** tab are listed the jobs dedicated to the email notifications that involve the email templates inventoried.

From the **Actions** menu, you can remove the jobs dedicated to the email notifications by clicking **Remove**.

## Hierarchy (Polyarchies)

In the IBM Security Identity Governance model, polyarchies provide different organizational views in a hierarchical notation.

A generic hierarchy is based on a specific user attribute.

An additional hierarchy can be created at any moment by grouping users on attribute values.

If the attribute contains a hierarchy path, this is converted to a hierarchical notation.

Attributes can be classified as:

- **Single Value**
- **Multi Value**
- **Hierarchy**

In the following figure:

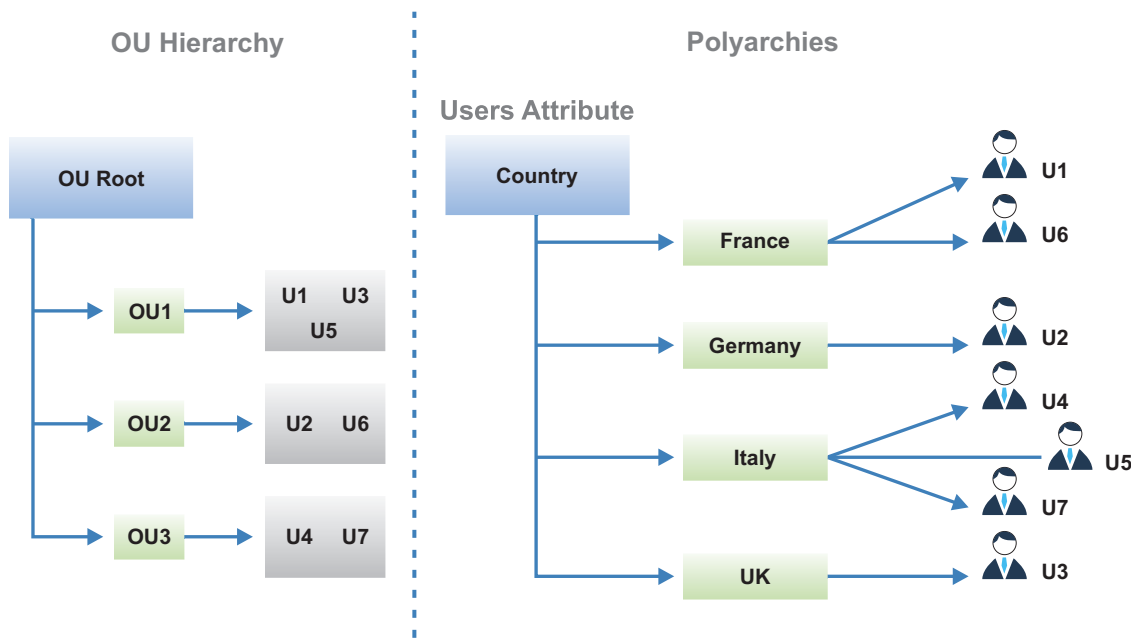


Figure 47. Example: classic OU hierarchy and flat Polyarchy single-value

The polyarchy above shows users grouped on the **Country** attribute.

In the typical organization units hierarchy, we can represent a set of users belonging to the same OU. But a set of users can stay in the same OU and can operate from different geographical locations.

In the example above U1, U3 and U5 are in the same OU1; but if they are grouped by attribute **\_COUNTRY**, U1, U3 and U5 will be displayed on three different countries.

This example shows a flat polyarchy created by setting the single value option.

How is it possible to know in which cities of France the users U1 and U6 are working?

The users U1 and the U6, as described in the previous example, have the same attribute value "France". In this case, to know the city of the users, we can set the option **Hierarchy Value** instead of the **Single Value**.

If the needed data are stored in the database (if the attribute contains a hierarchy path), the result will be as shown in the sample below:

## Polyarchies

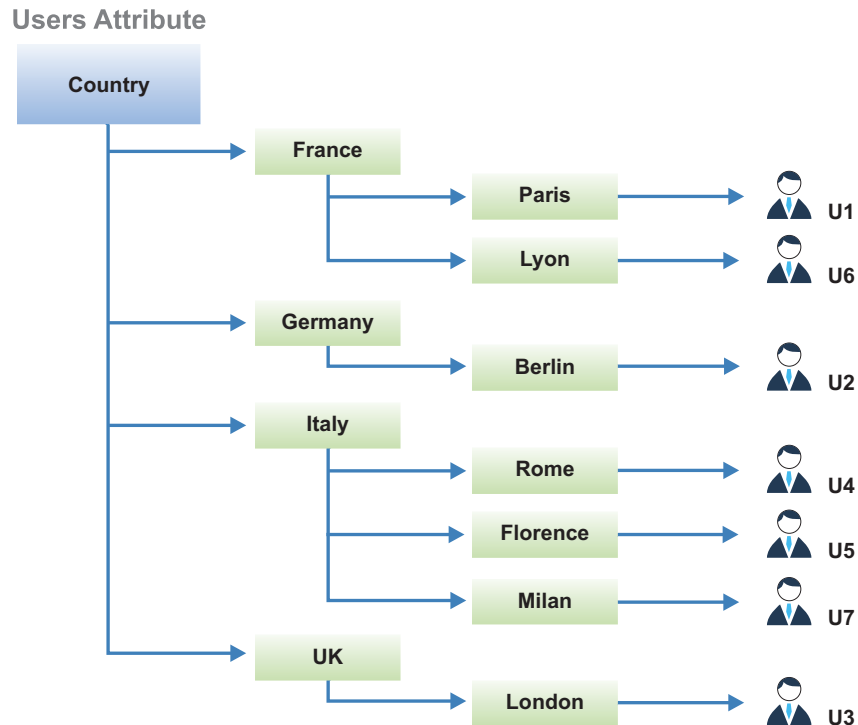


Figure 48. Example of polyarchy in which the attribute contains hierarchy path

This means that for user U1:

```
_COUNTRY=Country;France;Paris
```

while for user U5:

```
_COUNTRY=Country;Italy;Florence
```

In another example, if **\_LOCALITY** is the attribute selected to represent a hierarchy and we have two locations in Frankfurt (Frankfurt 1 and Frankfurt 2), we can create a virtual location named Frankfurt as a father of the two, otherwise it will be represented as a flat hierarchy:

```
_LOCALITY=Frankfurt;Frankfurt2
```

In the **Configure > Hierarchy** tab, you can build any hierarchy by clicking **Actions>Add** (left frame) and configuring the attributes shown in the **Details** tab (right).

The hierarchy is built by a job that can be scheduled with the **AttributeHierarchyRefresh** task (**Task Planner > Manage > Tasks**), and activated by the **Actions>Build** button.

The elements needed to define a new Hierarchy are described in the following table:

Hierarchy details	
Detail	Description
Name	Name used to identify the hierarchy.
Description	Brief description of the hierarchy.
Conf Type	<p>Manual: is built an empty hierarchy, only joined to the Name and listed in the combo-box Hierarchy available under <b>Manage &gt; Groups</b>.</p> <p>Simple: allows the selection from the Field combo-box of the user attribute on which the hierarchy is built. The available set of attributes is the same set involved in the virtualization process defined in <b>Settings &gt; Core Configurations &gt; User Virtual Attributes tab</b>.</p> <p>Advanced: allows the building of the attribute group according to a rule selectable by the Rule combo-box, with three different options:</p> <ul style="list-style-type: none"> <li>• Auto: The selected rule is used to build the attribute group and to join the users to the nodes of the hierarchy. The hierarchy is automatically updated by AttributeHierarchyRefresh</li> <li>• Once: The selected rule is used to build the attribute group "one-shot", without the refreshing action managed by AttributeHierarchyRefresh task.</li> </ul>
Value	<p>The available values are:</p> <ul style="list-style-type: none"> <li>• Single Value</li> <li>• Multi Value</li> <li>• Hierarchy</li> </ul>
Separator Char	This item must be indicated if the <b>Multi Value</b> (for example _PHONENUMBER) or the <b>Hierarchy</b> value is specified in the row above.
UserID Attribute (Authomatic Scope Assignment)	If this check box is ticked, the role selected into the <b>UserID Assigned Role</b> combo-box, is assigned automatically to the users involved in the attribute group selected in the left tab, with the scope policy defined by the check box <b>UserID Hierarchy</b> .
UserID Assigned Role	This combo-box hosts all the Administrative Roles available for the users involved in the attribute group.
UserID Hierarchy	<p>If this check box is ticked, the generic user, to the level K of the hierarchy, will see all the users on levels K+1, K+2,... up to the last level of the hierarchy. Otherwise, he will see only the user of level K+1.</p> <p><b>Note:</b> Root of the hierarchy is at level K=0</p>

After the building of the hierarchy, in the **Configure > Hierarchy > User** tab, you can view:

- The nodes of the hierarchy according to different views (**View** or **Search** tabs)
- The users joined to the node of the hierarchy selected in the **View** or **Search** tabs

## Rights Lookup

In this section it is possible to define the lookup tables sets for managing rights with lookup.

In the left frame you can filter by **Name** the list of tables (click **Filter/Hide Filter**).

In the **Actions** menu, through **Add/Remove** options you can add or remove tables.

For each table selected in the left frame, it is possible to add, in the right frame, a new value, adding a row through **Actions > Add** and setting the new value.

These values are used during the assignment of rights to a permission (see **Manage > Applications > Application Access > Rights**).

---

## Monitor

You can monitor some elements.

The functions that are available for monitoring some elements are contained in the following list.

- Reports
- Role Compare
- Scheduled Tasks
- TARGET inbound - Account events
- "TARGET inbound - Access events" on page 204
- OUT events
- IN - User events
- IN - Org. Unit events
- "INTERNAL events" on page 211

## Report

Scheduling and downloading are the main functions in Reports.

- Request schedules reports.
- Download downloads reports.

For unauthorized users, this menu is not available.

## Role Compare

With this tab you can compare roles to verify if there are redundancies amongst roles and to optimize their definitions. For example, if you find that two or more role definitions specify similar things without a real requirement, you can reduce the definitions to just one single role.

To compare roles, you are first asked to specify the scope of the roles that you want to compare:

1. In the **Scope** field, select OU or Application.
2. In the field below, that can be **OU** or **Application** based on your previous choice, enter the name of the OU or application whose roles you want to compare. Alternatively, click the elipsis (...) button to get a list from which you can select your entity. A click of the elipsis opens another window that, based on the scope you selected helps you select an application or view and search an Organization Unit.

If the scope is **OU**, you can flag the **Hierarchy** checkbox to have the roles of the Organization Unit listed in a hierarchical sequence.

After you specify the Organization Unit or the Application, all the defined roles associated within the entity are displayed in the list below. You can also use the filter fields to list specific roles and to sort roles in a particular order.

Roles are listed in tabular form displaying the following details:

*Table 76. Details of roles listed for comparison.*

Attribute	Description
Name	<p>The name of the role (entitlement) preceded by the symbol that indicates the type: Permission, IT Role, Business Role, External Role.</p> <p>If the role name is shown in red, the role cannot be used for comparison because it is not assigned.</p>
Application	<p>The name of the application (set of roles and permissions) to which the role belongs. This column is blank when the scope is OU, and shows the name of the selected application when the scope is Application.</p>
Direct Users	<p>The number of users to whom the role is assigned directly (that is, not as a child of another assigned role).</p>
Similarity	<p>When you run a comparison between a selected role and all the other roles in the list, this column becomes populated with the percentage similarity in direct users of the entitlement in the row with the comparison role. For example, a 100% value, means that the two entitlements (including all their permissions) are assigned to the same user.</p>
Permissions	<p>The number of permissions included in the entitlement.</p>
Similarity	<p>When you run a comparison between a selected role and all the other roles in the list, this column becomes populated with the percentage similarity in permissions of the entitlement in the row with the comparison role. For example, a 100% value, means that the two entitlements include exactly the same permissions.</p>



Table 76. Details of roles listed for comparison. (continued)

Attribute	Description
Assignments	The total number of direct and hierarchical (that is, as child role) assignments of the entitlement.
OUs	The number of Organization Units to which the entitlements are assigned through their user members.
OU Spread	A numeric index that provides an estimate of the homogeneous diffusion of a role in the hierarchical structure of an organization. If the spread value is very high, the role is not homogeneously scattered over a large number of OUs.
Applications	The number of applications that comprise this entitlement in their set of permissions and roles, if the scope is OU. If the scope is Application, the number is just 1.

To run the comparison, select the entitlement against which you want to compare the other entitlements in the list and click **Compare**. Then:

- The row of the entitlement is moved to the top and turns red
- The **Similarity** columns of all entitlements become populated with percentages in similarity of direct users or permissions
- The right panel becomes populated with a number of tabs that provide further details on the selected entitlement:

**Entitlement Details**

**Map of Permissions**

**Permissions**

**Applications**

**Users**

**Organization Units**

## Scheduled tasks

In this section are displayed all the scheduled tasks which are running or just started.

In the **Actions** menu, the **Remove** button allows you to remove the scheduled tasks from the list.

These tasks are scheduled using the Task Planner module.

## TARGET inbound - Account events

In this section you can monitor events, related to accounts, incoming from the target systems.

Events related to accounts on the targets can be filtered as described in the following table:

Table 77. Filters you can specify to list Target inbound - account events.

Filter	Description
Status	Event status can be one of the following values: <ul style="list-style-type: none"> <li>• Unprocessed</li> <li>• Success</li> <li>• Error</li> </ul>
Operation	Indicates the type of available operation: <ul style="list-style-type: none"> <li>• Add permissions</li> <li>• Remove permissions</li> <li>• Disable user</li> <li>• Enable user</li> <li>• Create user</li> <li>• Remove user</li> <li>• Add right</li> <li>• Remove right</li> <li>• Entitlement add child</li> <li>• Entitlement remove child</li> <li>• Custom</li> </ul>
Operation Code	Indicates the customized code of a specific event.  It is selectable only if the <b>Operation</b> filter is set on <b>Custom</b> .
Account ID	Identifier of the account involved in the event.
Marker	Marker of the event. It might coincide with the identifier of the target system.
Trace	Brief description of the error cause.
Process ID	An identifier assigned by the target system to one or more events.
Event Start-End Date	Filters defining the time period for searching events.

The target inbound - account events are listed in a table showing the following details:

Table 78. Target inbound - account event details.

Field	Description
ID	The event identifier, a sequential number.
Process ID	An identifier assigned by the target system to one or more events. This information can be used when writing rules to identify events or sets of events.
Account ID	The identifier of the account involved in the event.

Table 78. Target inbound - account event details. (continued)

Field	Description
Operation	The operation made on the account: <ul style="list-style-type: none"> <li>• Add permissions</li> <li>• Remove permissions</li> <li>• Disable user</li> <li>• Enable user</li> <li>• Create user</li> <li>• Remove user</li> <li>• Add right</li> <li>• Remove right</li> <li>• Entitlement add child</li> <li>• Entitlement remove child</li> <li>• Custom</li> </ul>
Status	The event status can be one of these values: <ul style="list-style-type: none"> <li>• Unprocessed</li> <li>• Success</li> <li>• Error</li> </ul>
Trace	A short description of the error.
Detail	Optionally provided by the target system.
Marker	The marker of the event. It may coincide with the identifier of the target system.
Permission	The permission that was added or removed.
Permission Type	The type of the permission that was added or removed.
Name	Personal data of the user subjected to a create, remove, enable, or disable user operation.
Surname	
Email	
DN	
Display Name	
Identity UID	
Event Date	The event generation date.
Process Date	The date in which the event must be processed by the RE (generally coincides with the event date but can be subsequent if the event processing was postponed).
Ownership	The user who caused the event on the external table.

The following options become available when you click **Actions**:

**Details**

Displays additional details of a selected event in the TargetEvent window.

**Re-Execute**

Runs again the operation of a selected event.

**Delete all filtered**

Removes all the events resulting from a specific filtered search.

**Remove**

Removes the selected event.

## TARGET inbound - Access events

In this section you can monitor events, related to operations of role creation or deletion, as well as of addition or removal of child roles, incoming from target systems.

Events related to the creation or deletion of roles incoming from (external) targets can be filtered as described in the following table:

*Table 79. Filters you can specify to list Target inbound - Access events.*

Filter	Description
Status	Event status can be one of the following values: <ul style="list-style-type: none"> <li>• Unprocessed</li> <li>• Success</li> <li>• Error</li> </ul>
Operation	Indicates the type of operation associated with the event: <ul style="list-style-type: none"> <li>• Create External Role</li> <li>• Delete External Role</li> <li>• Add External Role Child</li> <li>• Remove External Role Child</li> </ul>
Operation Code	Not used.
Process ID	An identifier assigned by the target system to one or more events.
Marker	Marker of the event. It might coincide with the identifier of the target system.
Trace	Brief description of the error cause.
Event Start-End Date	Filters defining the time period for searching events.

The target inbound - access events are listed in a table showing the following details:

*Table 80. Target inbound - access event details.*

Field	Description
ID	The event identifier, a sequential number.
Process ID	An identifier assigned by the target system to one or more events. This information can be used when writing rules to identify events or sets of events.
Operation	The operation associated with the event. Can be one of the following: <ul style="list-style-type: none"> <li>• Create External Role</li> <li>• Delete External Role</li> <li>• Add External Role Child</li> <li>• Remove External Role Child</li> </ul>
Status	The event status can be one of these values: <ul style="list-style-type: none"> <li>• Unprocessed</li> <li>• Success</li> <li>• Error</li> </ul>

Table 80. Target inbound - access event details. (continued)

Field	Description
Trace	A short description of the error.
Marker	The marker of the event. It may coincide with the identifier of the target system.
Master Application	The name of the application that includes the external role implicated in the event.
Master name	The name of the created or deleted external role for which the event was started.
Master type	The type of external role. It can be a permission or an external role.
Master entitlement type	The entitlement type identifier of the permission or external role.
Master Description	A short description of the permission or external role.
Child Marker	For events involving the addition or removal of an external role child, it is the marker of the event. It may coincide with the identifier of the target system.
Child Application	The name of the application that includes the external role child implicated in the event.
Child name	The name of the added or removed external role child for which the event was started.
Child type	The type of the external role child. It can be a permission or an external role.
Child entitlement type	The entitlement type identifier of the external role child.
Child Description	A short description of the external role child.
Event Date	The event generation date.
Process Date	The date in which the event must be processed by the RE (generally coincides with the event date but can be subsequent if the event processing was postponed).
Ownership	The user who caused the event on the external table.

The following options become available when you click **Actions**:

**Details**

Displays additional details of a selected event in the TargetEvent window.

**Re-Execute**

Runs again the operation of a selected event.

**Delete all filtered**

Removes all the events resulting from a specific filtered search.

**Remove**

Removes the selected event.

## OUT events

In this section you can monitor all events related to definitions of Users in output to external targets.

Output events can be filtered as described in the following table:

Table 81. OUT queue filters

Filter	Description
Status	Event status can be one of the following values: <ul style="list-style-type: none"> <li>• Unprocessed</li> <li>• Success</li> <li>• Error</li> </ul>
Operation	Indicates the type of available operation: <ul style="list-style-type: none"> <li>• Add permissions</li> <li>• Remove permissions</li> <li>• Disable user</li> <li>• Enable user</li> <li>• Create user</li> <li>• Remove user</li> <li>• Add right</li> <li>• Remove right</li> <li>• Entitlement add child</li> <li>• Entitlement remove child</li> <li>• Custom</li> </ul>
Operation Code	Indicates the customized code of a specific event.  It is selectable only if the <b>Operation</b> filter is set on <b>Custom</b> .
Account ID	Identifier of the account involved in the event.
Trace	Brief description of the error cause.
Marker	Marker of the event. It might coincide with the identifier of the target system.
Event Start-End Date	Filters defining the time period for searching events.

Every event is characterized by a the following attributes.

Table 82. Attributes of OUT events.

Field	Description
ID	Event identifier.
Account ID	Account identifier, related to the target system involved by the out event.
Master UID	Univocal identifier of the user.

Table 82. Attributes of OUT events. (continued)

Field	Description
Operation	Indicates the type of available operation: <ul style="list-style-type: none"> <li>• Add permissions</li> <li>• Remove permissions</li> <li>• Add delegation</li> <li>• Remove delegation</li> <li>• Disable user</li> <li>• Enable user</li> <li>• Create account</li> <li>• Remove account</li> <li>• Modify account</li> <li>• Change password</li> <li>• Add service</li> <li>• Remove service</li> <li>• Add resource</li> <li>• Remove resource</li> <li>• Add role to user</li> <li>• Remove role to user</li> </ul>
Status	Event status can assume only three values: <ul style="list-style-type: none"> <li>• Unprocessed</li> <li>• Success</li> <li>• Error</li> </ul>
ERC Status	The status of the User_ERC table. It can be: <ul style="list-style-type: none"> <li>• Unprocessed</li> <li>• Success</li> <li>• Error</li> </ul>
Trace	Brief description of the error cause.
Marker	Marker of the event. It might coincide with the identifier of the target system.
Free Attribute 1	Sensitive data 1.
Free Attribute 2	Sensitive data 2.
...	...
Free Attribute N	Sensitive data N.
Application	The name of the application impacted by the operation/event.
Code Operation	A code optionally assigned to the operation.
Event Date	Indicates the event generation date.
Process Date	Indicates the date in which the event must be processed by the RE (generally coincides with the event date but can be subsequent if the event processing was postponed).
Ownership	Indicates the user which caused the event on the external table.

The **Actions** menu includes the following buttons to manage OUT events:

**Re-Execute**

Reprocesses the operation associated with the selected event.

**Remove**

Deletes the selected event.

**IN - User events**

In this section you can monitor all events related to users in input from external target systems.

Input events can be filtered as described in the following table:

*Table 83. Filters you can specify to list user events in input from external target systems.*

Filter	Description
Status	Event status can assume one of the following three values: <ul style="list-style-type: none"> <li>• Unprocessed</li> <li>• Success</li> <li>• Error</li> </ul>
Operation	Indicates the type of operation associated with the event: <ul style="list-style-type: none"> <li>• Create User</li> <li>• Modify User</li> <li>• Remove User</li> <li>• Move User</li> <li>• Create User (Deferred)</li> <li>• Modify User (Deferred)</li> <li>• Remove User (Deferred)</li> <li>• Move User (Deferred)</li> <li>• Custom</li> </ul>
Operation Code	Not used.
Trace	Brief description of the error cause.
Event Start-End Date	Filters defining the time period for searching events.

The events related to users in input from external target systems are listed with the following attributes:

*Table 84. Details of User events in input from external target systems.*

Field	Description
ID	The event identifier, a sequential number.
User ERC	The code of the User_ERC table with the attributes of the user processed in the operation/event. The USER_ERC table contains a copy of user data from the external system and matches the PERSON table in the AG Core database.



Table 84. Details of User events in input from external target systems. (continued)

Field	Description
Operation	The operation associated with the event. Can be one of the following: <ul style="list-style-type: none"> <li>• Create User</li> <li>• Modify User</li> <li>• Remove User</li> <li>• Move User</li> <li>• Create User (Deferred)</li> <li>• Modify User (Deferred)</li> <li>• Remove User (Deferred)</li> <li>• Move User (Deferred)</li> <li>• Custom</li> </ul>
Status	The event status can be one of these values: <ul style="list-style-type: none"> <li>• Unprocessed</li> <li>• Success</li> <li>• Error</li> </ul>
Trace	A short description of the error.
Detail	Further information on the error that is optionally provided by the external system.
Identification Number	The ID of the user processed in the event.
OU Code	The Organization Unit associated with the user processed in the event.
Action Type	Fields optionally used by the external system to add information about the operation.
Action Reason	
Event Date	The event generation date.
Process Date	The date in which the event must be processed by the RE (generally coincides with the event date but can be subsequent if the event processing was postponed).
Ownership	The process that owns the event. It is usually is the name of the connector used with the target system.

The following options become available when you click **Actions**:

**Details**

Displays the details of the selected event in the IN Events window.

**User Data**

Displays system and personal data of the user processed in the selected event in the Details window.

**Re-Execute**

Runs again the operation of the selected event.

**Delete all filtered**

Removes all the events resulting from a specific filtered search.

**Remove**

Removes the selected event.

## IN - Org. Unit events

In this section you can monitor all events related to Organization Units in input from external target systems.

Input events can be filtered as described in the following table:

*Table 85. Filters you can specify to list Organization Unit events in input from external systems.*

Filter	Description
Status	Event status can assume one of the following three values: <ul style="list-style-type: none"> <li>• Unprocessed</li> <li>• Success</li> <li>• Error</li> </ul>
Operation	Indicates the type of operation associated with the event: <ul style="list-style-type: none"> <li>• Create OU</li> <li>• Modify OU</li> <li>• Remove OU</li> </ul>
Trace	Brief description of the error cause.
Event Start-End Date	Filters defining the time period for searching events.

The events related to Organization Units in input from external systems are listed with the following attributes:

*Table 86. Details of User events in input.*

Field	Description
ID	The event identifier, a sequential number.
OU ERC	The code of the OU_ERC table with the attributes of the Organization Unit processed in the operation/event. The OU_ERC table contains a copy of Organization Unit data from the external system and matches the Organization Unit table in the AG Core database.
Operation	The operation associated with the event. Can be one of the following: <ul style="list-style-type: none"> <li>• Create OU</li> <li>• Modify OU</li> <li>• Remove OU</li> </ul>
Status	The event status can be one of these values: <ul style="list-style-type: none"> <li>• Unprocessed</li> <li>• Success</li> <li>• Error</li> </ul>
Trace	A short description of the error.
Identification Number	The ID of the Organization Unit processed in the event.
OU Code	The name of the Organization Unit processed in the event.
Action Type	Fields optionally used by the external system to add information about the operation.
Action Reason	

Table 86. Details of User events in input. (continued)

Field	Description
Event Date	The event generation date.
Process Date	The date in which the event must be processed by the RE (generally coincides with the event date but can be subsequent if the event processing was postponed).
Ownership	The process that is owner of the event. It is usually is the name of the connector used with the target system.

The following options become available when you click **Actions**:

**Details**

Displays the details of the selected event in the IN Events window.

**Re-Execute**

Runs again the operation of the selected event.

**Delete all filtered**

Removes all the events resulting from a specific filtered search.

**Remove**

Removes the selected event.

## INTERNAL events

In this section you can monitor events triggered by operations run locally on the entities of your security model and impacting the AG Core database.

Internal events can be filtered as described in the following table:

Table 87. Filters you can specify to list internal events.

Filter	Description
Status	Event status can assume one of the following three values: <ul style="list-style-type: none"> <li>• Unprocessed</li> <li>• Success</li> <li>• Error</li> </ul>

Table 87. Filters you can specify to list internal events. (continued)

Filter	Description
Operation	<p>Indicates the type of operation associated with the event. It can be one of the following:</p> <ul style="list-style-type: none"> <li>• Create Application</li> <li>• Remove Application</li> <li>• Modify Application</li> <li>• Create Entitlement</li> <li>• Remove Entitlement</li> <li>• Modify Entitlement</li> <li>• Create User</li> <li>• Remove User</li> <li>• Modify User</li> <li>• Create OU</li> <li>• Remove OU</li> <li>• Modify OU</li> <li>• Change SOD Status</li> <li>• Add User Entitlement</li> <li>• Remove User Entitlement</li> </ul>
Entity Type	<p>The type of entity impacted by the event. It can be one of the following:</p> <ul style="list-style-type: none"> <li>• Application</li> <li>• Entitlement</li> <li>• OU</li> <li>• User</li> </ul>
Trace	A brief description of the error cause.
Event Start-End Date	Filters defining the time period for searching events.

The events related to operations run locally on the entities of your security model are listed with the following attributes:

Table 88. Details of internal events.

Field	Description
ID	The event identifier, a sequential number.

Table 88. Details of internal events. (continued)

Field	Description
Operation	The operation associated with the event. Can be one of the following: <ul style="list-style-type: none"> <li>• Create Application</li> <li>• Remove Application</li> <li>• Modify Application</li> <li>• Create Entitlement</li> <li>• Remove Entitlement</li> <li>• Modify Entitlement</li> <li>• Create User</li> <li>• Remove User</li> <li>• Modify User</li> <li>• Create OU</li> <li>• Remove OU</li> <li>• Modify OU</li> <li>• Change SoD Status</li> <li>• Add User Entitlement</li> <li>• Remove User Entitlement</li> </ul>
Status	The event status can be one of these values: <ul style="list-style-type: none"> <li>• Unprocessed</li> <li>• Success</li> <li>• Error</li> </ul>
Trace	A short description of the error.
Entity type	The type of entity impacted by the event. It can be one of the following: <ul style="list-style-type: none"> <li>• Application</li> <li>• Entitlement</li> <li>• OU</li> <li>• User</li> </ul>
Name	The name of the entity impacted by the event.
Description	A description of the entity impacted by the event.
Code	The identification of the entity impacted by the event.
Event Date	The event generation date.
Process Date	The processing date of the event (generally coincides with the event date but can be later if processing of the event was postponed).

The following options become available when you click **Actions**:

**Re-Execute**

Runs again the operation of the selected event.

**Delete all filtered**

Removes all the events resulting from a specific filtered search.

**Remove**

Removes the selected event.

---

## Tools

Several functions speed up and facilitate the tasks of the following modules:

- Bulk Data Load

### Bulk Data Load

You can load bulk data in the AG Core database.

You can run several types of bulk data-loading in the AG Core database.



The **Action** tab (left) shows the supported operations.

After you select an operation in **File Batch**, click one of the following options:

- **Download** to get a template (XLS file), related to the currently selected operation.
- **Browse** to search in the file system for an XLS file for the selected loading operation.

When the operation is completed, an information record is appended in the lower-right pane to the list of the previously completed operations.

In the same pane, you can click:

- **Input File**  to get the file used in the operation.
- **Log File**  to get the operation report.

The following procedures are available:

- Insert Applications
- Insert Resources
- Insert Entitlements
- Insert Organization Units
- Insert Users
- User-OU-Entitlement Assignments
- Remove Users
- Remove Organization Units
- Remove Entitlements
- Remove Applications
- Remove User-OU-Entitlement Assignments
- Remove Entitlements from OU
- Remove Resources
- Insert Property
- Insert Rights Look-up
- Add Resource To Org Unit
- Add Resources To User-Entitlement
- Add Internal Resources to User-Entitlement
- Remove Resources From Org Unit
- Remove Resources From User-Entitlement
- Remove Internal Resources From User-Entitlement
- Insert External Roles

- Remove External Roles

A generic record track distinguishes between **Mandatory** and **Optional** fields.

If a **Mandatory** field is empty or populated with unexpected values, the row is skipped unless otherwise specified in the documentation.

According to the data load behavior, populating an **Optional** field with unexpected or incorrect values could cause a row to be skipped.

Here the procedure for running a bulk data load.

### Insert Applications Record Track

This batch procedure can be used to insert Applications.

Insert Applications Track		
Information	Description	Validation
APPLICATION	Application identifier name.	Mandatory
DESCRIPTION	A free text field for describing the Application.	Optional
CONFIGURATION	Configuration identifier.	Optional
DISABLE_SYNC	Can assume the values TRUE or FALSE.	Optional
TARGET	Target identifier.	Optional

This batch procedure can be used to insert Applications. It verifies that the required fields are populated.

In the APPLICATION field, enter the Application name. If there is no existing Application with this name, the Application is added. If the Application already exists, the record is skipped.

If the CONFIGURATION field is empty, a default configuration is assigned to the Application. If the configuration does not exist, it is created.

If the value of DISABLE\_SYNC is TRUE, the synchronization is disabled. If the value is FALSE, empty, or if a wrong value is given, the synchronization is enabled.

The TARGET field must be populated with the name of the Target System.

If both the TARGET and CONFIGURATION fields are empty, a fictitious target named IDEAS is assigned.

If TARGET is empty and CONFIGURATION is populated, a target with the application name is created.

If TARGET is filled with a target identifier that does not exist, the target identifier is created.

### Insert Entitlements Record Track

Use this batch procedure to import entitlements into your security model.

This batch procedure can be used to enter/update Entitlements and organize them into a hierarchy. It verifies that Mandatory fields are populated.

For ALL Optional fields, if the NULL string is specified, the related item will be:

- set to the default value;
- cleaned, if a default value is not expected.


Table 89. Insert Entitlements record track

Information	Description	Validation
NAME	The name of the entitlement	Mandatory
CODE	The univocal identifier of the entitlement	Optional
DESCRIPTION	A description of the entitlement	Optional
TYPE	The type of entitlement. It can be one of the following: <ul style="list-style-type: none"> <li>• 1 (for Permission)</li> <li>• 2 (for IT role)</li> <li>• 3 (for Business role)</li> <li>• External_Role</li> </ul>	Mandatory
PERMISSION_TYPE	Permission Type identifier.	Mandatory for entitlement type 1
APPLICATION	The name of the application to which the entitlement belongs. The application must be already defined.	Mandatory for all entitlement types but 3
ADMINISTRATIVE		Optional
LANGUAGE	The localization language	Mandatory if localized version
PARENT_NAME	The name of the parent entitlement. If defined, the parent entitlement must be listed before as a role without parent.	Optional
PARENT_CODE	The code of the parent entitlement. If it exists, the parent entitlement must be listed before as a role without parent.	Optional
PARENT_TYPE	Parent Entitlement Type identifier. Allowed values are: <ul style="list-style-type: none"> <li>• 1 (for Permission)</li> <li>• 2 (for IT role)</li> <li>• 3 (for Business role)</li> <li>• External_Role</li> </ul> An external role can be parent only to other external roles and permissions.	Mandatory if PARENT_NAME or PARENT_CODE were entered.
PARENT_APPLICATION	The name of the application to which the parent entitlement belongs. The application must be already defined.	Mandatory if PARENT_NAME or PARENT_CODE were entered.



Table 89. Insert Entitlements record track (continued)

Information	Description	Validation
OWNER_CODE	The identifier code of the person who owns the entitlement. The code must be already defined.	Optional
SCOPE_TYPE	The scope type that defines the operational limitations of the entitlement.	Optional
ENTITLEMENT_FAMILY	The name of the entitlement family where the entitlement is classified.	Optional
BUSINESS_NAME	The name of the business activity with which the entitlement is associated.	Optional
BUSINESS_POLICY	The name of the business policy with which the entitlement is associated.	Optional

	<p><sup>1</sup><b>NOTE:</b> for Entitlements of TYPE=3, the APPLICATION field must be left blank. This field must be populated for the other types of entitlement.</p> <p><sup>2</sup> <b>NOTE:</b> for Entitlements of TYPE=1, the PERMISSION_TYPE field must be populated.</p> <p><sup>3</sup><b>NOTE:</b> PARENT_TYPE is Mandatory ONLY if PARENT_NAME or PARENT_CODE has been specified. The same policy applies to PARENT_APPLICATION.</p>
---	---

Depending on whether the **Entitlement Localization** is active or not active, you can specify the entitlements in different ways. See the IBM Security Governance installation procedure for details. The following table describes the options.

<sup>4</sup> Entitlement Localization options		
Concept	Description	
Localization Active	YES	NO
LANGUAGE	This field can be empty or host the language specification.	This field must be empty. If it is not empty, the entire row is skipped.
<sup>4</sup> CODE	This field is the unique identifier of the entitlement.  If CODE is not specified, the system provides an automatically generated CODE. In this sense, it might be considered an optional item of the record track.	This field must be empty. If it is not empty, the entire row is skipped.

<sup>4</sup> Entitlement Localization options		
Concept	Description	
NAME	<p>If LANGUAGE is empty or if the IL string is specified, the technical name of the entitlement is in NAME.</p> <p>If NAME is specified, the name of the entitlement, joined with the language that is specified in LANGUAGE, is in NAME.</p>	
Entitlement specification	<ul style="list-style-type: none"> <li>• NAME/CODE</li> <li>• TYPE</li> <li>• APPLICATION</li> <li>• PERMISSION_TYPE</li> </ul>	<ul style="list-style-type: none"> <li>• NAME/CODE</li> <li>• TYPE</li> <li>• APPLICATION</li> <li>• PERMISSION_TYPE</li> </ul>

The **TYPE** field contains the Entitlement Type.

The **APPLICATION** field contains the Entitlement Application name and is mandatory for Permissions, IT roles, and External roles.

Entitlement existence is verified using the given NAME/CODE and TYPE (for TYPE = 1 and 2, APPLICATION is also verified; for TYPE = 1 only, PERMISSION\_TYPE is also verified).

If there is already an Entitlement with the given NAME/CODE and TYPE-APPLICATION-PERMISSION\_TYPE, it is updated with any information present in the optional **DESCRIPTION** field. Otherwise the Entitlement is entered.

The **PARENT\_NAME**, **PARENT\_TYPE**, and **PARENT\_APPLICATION** fields are verified to ensure that the proposed hierarchy fulfills the Entitlement hierarchy definition. **PARENT\_TYPE** must thus be different than Permission and there must be a parent Entitlement with the given **PARENT\_NAME/PARENT\_CODE** and **PARENT\_TYPE** (TYPE = 2 also includes verification of **PARENT\_APPLICATION**).

Parent Entitlement verification applies either to preexisting Entitlements or to the entire XLS file. Therefore, Entitlements need not be entered into the XLS file in any particular order.

## Insert Organization Units Record Track

Table 90. Insert Organization Units Track

Information	Description	Validation
NAME	OU identifier name.	Mandatory
CODE	OU identifier code.	Mandatory
DESCRIPTION	A free text field for describing the OU.	Optional
PARENT_CODE	Parent OU identifier code.	Mandatory

This batch procedure can be used to insert/update Organization Units and organize them into a hierarchy. It verifies that Mandatory fields are populated.

The **CODE** field contains the OU Code. If there is no existing OU with this name, the OU is inserted. If an OU with this Code already exists, the OU is updated with the given Name and Description. The **PARENT\_CODE** field contains the code of the OU designated to be the Parent.

OUs are assigned to their respective Parent OUs. Presence of the Parent OU is verified with the given Parent Code.

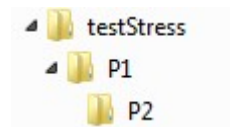
PARENT\_CODE verification applies either to a preexisting OU or to the entire XLS file. Therefore, OUs need not be inserted into the XLS file in any particular order. If the PARENT\_CODE field is empty, the OU is assigned to the root OU.

If a Parent OU with the given code does not exist, the OU is assigned to a technical OU (the code for a technical OU is "-undefined-"). The technical OU is created only at the first occurrence of this situation. The orphan OUs assigned to the technical OU will need to be properly repositioned within the OU hierarchy by the operator.

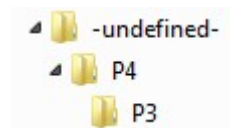
An example of the XLS file structure is shown below:

NAME	CODE	DESCRIPTION	PARENT_CODE
P3	Test_Stress	desc3	P4
P2	undefchild2	desc2	P1
P1	P1	desc1	testStress
P4	P4	desc4	bambex

Using the record track just shown, this first OU hierarchy will be built:



Another OU hierarchy will be built:



Since the bambex OU does not actually exist, this second one is required. P4 is thus assigned as a child of the “technical OU” named “-undefined-”.

### Insert Resources Record Track

This batch procedure can be used to insert/update Resources.

Insert Resources Track		
Information	Description	Validation
RESOURCE_NAME	Resource name.	Mandatory
RESOURCE_TYPE	Resource Type name.	Mandatory
RESOURCE_FAMILY	Resource Family name.	Mandatory
ATTR1	Customizable field for client purposes.	Optional

Insert Resources Track		
Information	Description	Validation
ATTR2	Customizable field for client purposes.	Optional

This batch procedure can be used to insert/update Resources.

It verifies that mandatory fields are populated as well as:

- The existence of the **RESOURCE\_TYPE** and **RESOURCE\_FAMILY** mandatory fields. If missing, they are inserted.
- The existence of a Resource with the given **RESOURCE\_NAME**, **RESOURCE\_TYPE**, and **RESOURCE\_FAMILY**. If such resource does not exist, it is inserted. Otherwise, the information for the resource is updated.

**ATTR1** and **ATTR2** are two customizable fields for client use and are useful for mapping resources to other optional fields (for example, **TEMPLATE** and **GENERIC\_RES\_REF** for the Access Provisioning (AP) Module).

An example of the XLS file structure is shown below:

RESOURCE_NAME	RESOURCE_TYPE	RESOURCE_FAMILY	ATTR1	ATTR2
TESTbatch	type_10	test_family		

## Insert Users Record Track

Use this batch procedure to insert and update users.

*Table 91. Insert Users record track.*

Information	Description	Validation
CODE	The user's identifying code.	Mandatory
NAME	The user's first name.	Mandatory
SURNAME	The user's last name.	Mandatory
SEX	The user's gender: <ul style="list-style-type: none"> <li>• 0: Male</li> <li>• 1: Female</li> </ul>	Optional
OU	The code of the organization unit where the user is assigned.	Optional
USER_TYPE	Describes the position of the user in the organization. For example, it can indicate the title of the user (User Manager, Security Officer, or more ), or, if the user is external, the type of relationship with the organization (Business Partner, Customer, Supplier).	Optional
EMAIL	The user's email address.	Optional
PHONE_NUMBER	The user's telephone number.	Optional
DN	The distinguished name of the user.	Optional

Table 91. Insert Users record track. (continued)

Information	Description	Validation
FISCAL_CODE	Any code or number issued by a national government (Fiscal code, SSN) that is used for the purpose of persona identification.	Optional
DATE_OF_BIRTH	Follows the format specified on the operating system.	Optional
PLACE_OF_BIRTH	User's place of birth and address information.	Optional
ADDRESS		Optional
CITY		Optional
STATE		Optional
COUNTRY		Optional
POSTAL_CODE		Optional
Additional columns may be added with user virtual attributes taken from external inventoried repositories.	Only User virtual attributes with names that do not start with an underscore (_) are allowed.	Optional

This batch procedure can be used to insert and update users. It verifies that the required fields are populated.

If the **OU** field contains a value, the procedure checks for the OU that matches the OU code entered. If the OU does not exist, the OU code value entered is ignored. A user with the matching **CODE** is then searched for.

If the user already exists, the user's information (**SURNAME, NAME, GENDER**) is updated. If no matching user is found, the user is created and added to the specified OU. If the OU does not exist, or if the OU field is empty, the user is not added to any OU.

If any of the loaded optional data is flawed, the user is still inserted and the error notified upon loading.

## Remove Applications Record Track

This batch procedure can be used to remove Applications.

Remove Applications Track		
Information	Description	Validation
APPLICATION	Application identifier name.	Mandatory
DESCRIPTION	A free text field used to describe the Application.	Unused
CONFIGURATION	Configuration identifier.	Unused
SYNCHRONIZED	Can be one of these values: <ul style="list-style-type: none"> <li><b>NO</b>: not synchronized</li> <li><b>M</b>: manually</li> <li><b>A</b>: automatically</li> </ul>	Unused
TARGET	Target identifier.	Unused

This batch procedure can be used to remove Applications. It verifies that the required fields are populated.

Enter the Application name in the **APPLICATION** field. If no Application is found with this name, the record is skipped. If the Application exists, the Application is removed.

An example of the XLS file structure is shown below:

APPLICATION	DESCRIPTION	CONFIGURATION	SYNCHRONIZED	TARGET
Application_1	Description_1	Configuration_1	no	Target_1
Application_2	Description_2	Configuration_2	M	Target_2
Application_3	Description_3	Configuration_3	A	Target_3

### Remove Entitlement from OU Record Track

This batch procedure can be used to remove an Entitlement from an Organization Unit.

Table 92. Remove Entitlements from OU Track

Information	Description	Validation
OU_CODE	OU identifier code.	Mandatory
ENTITLEMENT_NAME	Entitlement identifier name.	Mandatory
ENTITLEMENT_CODE	This field holds the univocal identifier of the Entitlement.	Optional
ENTITLEMENT_TYPE	Entitlement Type identifier. Allowed values are: <ul style="list-style-type: none"> <li>• 1 (for Permission)</li> <li>• 2 (for IT role)</li> <li>• 3 (for Business role)</li> <li>• External_Role</li> </ul>	Mandatory
ENTITLEMENT_APPLICATION	Entitlement Application identifier name.	Mandatory <sup>1</sup>
PERMISSION_TYPE	Permission Type identifier name.	Mandatory <sup>2</sup>


This batch procedure can be used to remove an Entitlement from an Organization Unit.

It verifies that the required fields are populated.

Depending on whether the **Entitlement Localization** is active or not active, you can specify the entitlements in different ways. See the IBM Security Governance installation procedure for details. The following table describes the options.

Entitlement Localization options		
Concept	Description	
Localization Active	YES	NO

Entitlement Localization options		
Concept	Description	
Entitlement specification	<p><b>ENTITLEMENT_CODE</b></p> <p>Or</p> <ul style="list-style-type: none"> <li>• <b>ENTITLEMENT_NAME</b></li> <li>• <b>ENTITLEMENT_TYPE</b></li> <li>• <b>ENTITLEMENT_APPLICATION</b></li> <li>• <b>PERMISSION_TYPE</b></li> </ul> <p>See Note<sup>1</sup> and Note<sup>2</sup>.</p> <p>If <b>ENTITLEMENT_CODE</b> is specified, it is the univocal identifier of the entitlement.</p> <p>The <b>ENTITLEMENT_NAME</b> is the technical name of the entitlement.</p>	<p>An entitlement must be specified by:</p> <ul style="list-style-type: none"> <li>• <b>ENTITLEMENT_NAME</b></li> <li>• <b>ENTITLEMENT_TYPE</b></li> <li>• <b>ENTITLEMENT_APPLICATION</b></li> <li>• <b>PERMISSION_TYPE</b></li> </ul> <p>See Note<sup>1</sup> and Note<sup>2</sup>.</p>

	<p><sup>1</sup></p> <p><b>NOTE:</b> If <b>ENTITLEMENT_TYPE</b> = 3, the <b>ENTITLEMENT_APPLICATION</b> field must be blank. Otherwise, it must be populated.</p> <p><sup>2</sup></p> <p><b>NOTE:</b> If <b>ENTITLEMENT_TYPE</b> = 1, the <b>PERMISSION_TYPE</b> field must be populated.</p>
---	--

The **OU\_CODE** field must contain an existing OU code. If not, the row is skipped.

Entitlement existence is verified using the values of **ENTITLEMENT\_NAME**, **ENTITLEMENT\_TYPE**, **ENTITLEMENT\_APPLICATION** (**ENTITLEMENT\_APPLICATION** is mandatory when **ENTITLEMENT\_TYPE**= 1, 2, or External\_Role) and **PERMISSION\_TYPE** (only when **ENTITLEMENT\_TYPE**= 1).

If there is no such Entitlement, the record is skipped. If the Entitlement exists and is assigned to the specified OU, the assignment is removed.

### Remove Entitlements Record Track

This batch procedure is used to remove Entitlements.

*Table 93. Remove Entitlements Track*


Information	Description	Validation
NAME	Entitlement identifier name.	Mandatory
ENTITLEMENT_CODE	This field hold the univocal identifier of the Entitlement.	Optional
DESCRIPTION	A free text field for describing the Entitlement.	Unused

Table 93. Remove Entitlements Track (continued)

Information	Description	Validation
TYPE	Entitlement Type Identifier. Allowed values are: <ul style="list-style-type: none"> <li>• 1 (for Permission)</li> <li>• 2 (for IT role)</li> <li>• 3 (for Business role)</li> <li>• External_Role</li> </ul>	Mandatory
PERMISSION_TYPE	Permission Type identifier.	Mandatory <sup>2</sup>
APPLICATION	Application identifier name.	Mandatory <sup>1</sup>
PARENT_NAME	Parent Entitlement identifier name.	Unused
PARENT_TYPE	Parent Entitlement Type identifier. Allowed values are: <ul style="list-style-type: none"> <li>• 1 (for Permission)</li> <li>• 2 (for IT role)</li> <li>• 3 (for Business role)</li> <li>• External_Role</li> </ul>	Unused
PARENT_APPLICATION	Parent Application identifier name.	Unused

This batch procedure is used to remove Entitlements. It verifies that the required fields are populated.

Table 94. Note about terms


	<p>For legacy reasons, the following terms can be assumed as equivalent:</p> <p><b>NAME</b> is equivalent to <b>ENTITLEMENT_NAME</b></p> <p><b>TYPE</b> is equivalent to <b>ENTITLEMENT_TYPE</b></p> <p><b>APPLICATION</b> is equivalent to <b>ENTITLEMENT_APPLICATION</b></p> <p>Note however that the Record Track <b>MUST BE</b> specified only by the keywords indicated in the Information column of the preceding table.</p>
---	--

Depending on whether the **Entitlement Localization** is active or not active, you can specify the entitlements in different ways. See the IBM Security Governance installation procedure for details. The following table describes the options.

Entitlement Localization options		
Concept	Description	
Localization Active	YES	NO



Entitlement Localization options		
Concept	Description	
Entitlement specification	<p><b>ENTITLEMENT_CODE</b></p> <p>Or</p> <ul style="list-style-type: none"> <li>• <b>ENTITLEMENT_NAME</b></li> <li>• <b>ENTITLEMENT_TYPE</b></li> <li>• <b>ENTITLEMENT_APPLICATION</b></li> <li>• <b>PERMISSION_TYPE</b></li> </ul> <p>See Note<sup>1</sup> and Note<sup>2</sup>.</p> <p>If <b>ENTITLEMENT_CODE</b> is specified, it is the univocal identifier of the entitlement.</p> <p>The <b>ENTITLEMENT_NAME</b> is the technical name of the entitlement.</p>	<p>An entitlement must be specified by:</p> <ul style="list-style-type: none"> <li>• <b>ENTITLEMENT_NAME</b></li> <li>• <b>ENTITLEMENT_TYPE</b></li> <li>• <b>ENTITLEMENT_APPLICATION</b></li> <li>• <b>PERMISSION_TYPE</b></li> </ul> <p>See Note<sup>1</sup> and Note<sup>2</sup>.</p>

	<p><sup>1</sup></p> <p><b>NOTE:</b> If <b>ENTITLEMENT_TYPE</b> = 3, the <b>ENTITLEMENT_APPLICATION</b> field must be blank. Otherwise, it must be populated.</p> <p><sup>2</sup></p> <p><b>NOTE:</b> If <b>ENTITLEMENT_TYPE</b> = 1, the <b>PERMISSION_TYPE</b> field must be populated.</p>
---	--

The **APPLICATION** field contains the Entitlement Application name and is mandatory only for Permissions, IT roles, and External roles.

The **PERMISSION\_TYPE** field contains the Entitlement Permission Type name and is mandatory only for Permissions.

The existence of an Entitlement is verified using the given **NAME** and **TYPE** (for **TYPE**= 1, 2, or External\_Role, **APPLICATION** is also verified; for **TYPE**= 1 only, **PERMISSION\_TYPE** is also verified). If there is already an Entitlement with the given **NAME** and **TYPE**, the Entitlement is removed. Otherwise the record is skipped.

The removal of an Entitlement implies a change in the hierarchy of Entitlements that is not managed by this batch procedure.

## Remove Organization Units Record Track

This batch procedure can be used to remove a set of Organization Units.

Remove Organization Units Track		
Information	Description	Validation
NAME	OU identifier name.	Unused
CODE	OU identifier code.	Mandatory
DESCRIPTION	A free text field for describing the OU.	Unused
PARENT_CODE	Parent OU identifier code.	Unused

This batch procedure can be used to remove a set of Organization Units. It verifies that the required fields are populated.

The **CODE** field contains the OU identifier code. If no OU exists with this **CODE**, the record is skipped. If an OU with this **CODE** does exist, its children are assigned to its parent OU and the OU is then removed.

The root OU cannot be removed.

An example of the XLS file structure is shown below:

NAME	CODE	DESCRIPTION	PARENT_CODE
P3	Test_Stress	desc3	P4
P2	undefchild2	desc2	P1
P1	P1	desc1	testStress
P4	P4	desc4	bambex

### Remove Resources Record Track

This batch procedure can be used to remove Resources.

Remove Resources Track		
Information	Description	Validation
RESOURCE_NAME	Resource name.	Mandatory
RESOURCE_TYPE	Resource Type name.	Mandatory
RESOURCE_FAMILY	Resource Family name.	Mandatory
ATTR1	Customizable field for client purposes.	Unused
ATTR2	Customizable field for client purposes.	Unused

This batch procedure can be used to remove Resources. It verifies that the required fields are populated.

It checks for a Resource with the given **RESOURCE\_NAME**, **RESOURCE\_TYPE**, and **RESOURCE\_FAMILY**. If there is no such Resource, the record is skipped. If the Resource exists, it is removed.

An example of the XLS file structure is shown below:

RESOURCE_NAME	RESOURCE_TYPE	RESOURCE_FAMILY	ATTR1	ATTR2
TESTbatch	type_10	test_family		

### Remove User-OU-Entitlement Assignments Record Track

This batch procedure can be used to manage Entitlement Assignment.

*Table 95. Remove User-OU-Entitlement Assignments Track*


Information	Description	Validation
USER_CODE	User identifier code.	Mandatory
USER_OU	User OU identifier code.	Optional
ENTITLEMENT_NAME	Entitlement identifier name.	Mandatory

Table 95. Remove User-OU-Entitlement Assignments Track (continued)

Information	Description	Validation
ENTITLEMENT_CODE	This field holds the univocal identifier of the Entitlement.	Optional
ENTITLEMENT_TYPE	Entitlement Type identifier. The allowed values are: <ul style="list-style-type: none"> <li>• 1 (for Permission)</li> <li>• 2 (for IT role)</li> <li>• 3 (for Business role)</li> <li>• External_Role</li> </ul>	Mandatory
ENTITLEMENT_APPLICATION	Entitlement Application identifier name.	Mandatory <sup>1</sup>
PERMISSION_TYPE	Permission Type identifier name.	Mandatory <sup>2</sup>

Depending on whether the **Entitlement Localization** is active or not active, you can specify the entitlements in different ways. See the IBM Security Governance installation procedure for details. The following table describes the options.

Entitlement Localization options		
Concept	Description	
Localization Active	YES	NO
Entitlement specification	<p><b>ENTITLEMENT_CODE</b></p> <p>Or</p> <ul style="list-style-type: none"> <li>• <b>ENTITLEMENT_NAME</b></li> <li>• <b>ENTITLEMENT_TYPE</b></li> <li>• <b>ENTITLEMENT_APPLICATION</b></li> <li>• <b>PERMISSION_TYPE</b></li> </ul> <p>See Note<sup>1</sup> and Note<sup>2</sup>.</p> <p>If <b>ENTITLEMENT_CODE</b> is specified, it is the univocal identifier of the entitlement.</p> <p>The <b>ENTITLEMENT_NAME</b> is the technical name of the entitlement.</p>	<p>An entitlement must be specified by:</p> <ul style="list-style-type: none"> <li>• <b>ENTITLEMENT_NAME</b></li> <li>• <b>ENTITLEMENT_TYPE</b></li> <li>• <b>ENTITLEMENT_APPLICATION</b></li> <li>• <b>PERMISSION_TYPE</b></li> </ul> <p>See Note<sup>1</sup> and Note<sup>2</sup>.</p>

	<p><sup>1</sup> <b>NOTE:</b> If <b>ENTITLEMENT_TYPE</b> = 3, the <b>ENTITLEMENT_APPLICATION</b> field must be blank. Otherwise, it must be populated.</p> <p><sup>2</sup> <b>NOTE:</b> If <b>ENTITLEMENT_TYPE</b> = 1, the <b>PERMISSION_TYPE</b> field must be populated.</p>
---	--

This batch procedure can be used to manage Entitlement Assignment. It verifies that the required fields are populated.

The procedure checks for a User with the given **USER\_CODE**. If the User is already assigned to an OU, the User's OU must match the value entered in the **USER\_OU** field. Otherwise, the row is skipped.

The **USER\_OU** field must contain an existing OU code. If it does not, the row is skipped.

The existence of the entitlement is verified using the values of **ENTITLEMENT\_NAME**, **ENTITLEMENT\_TYPE**, **ENTITLEMENT\_APPLICATION** (**ENTITLEMENT\_APPLICATION** is mandatory when **ENTITLEMENT\_TYPE**= 1, 2, or External\_Role) and **PERMISSION\_TYPE** (only when **ENTITLEMENT\_TYPE**= 1).

If there is no such Entitlement, the record is skipped.

If the Entitlement exists and is assigned to the specified User, the assignment is removed.

### Remove Users Record Track

This batch procedure can be used to remove Users.

Remove Users Track		
Information	Description	Validation
CODE	User identifier code.	Mandatory
SURNAME	User Surname.	Mandatory
NAME	User Name.	Mandatory
SEX	User's gender. Allowed values are: <ul style="list-style-type: none"> <li>• 0: Male</li> <li>• 1: Female</li> </ul>	Unused
OU	OU code.	Unused

This batch procedure can be used to remove Users. It verifies that the required fields are populated.

It searches for a User with the given **CODE**, **NAME**, and **SURNAME**. If found, the User is removed. Otherwise, the record is skipped.

An example of the XLS file structure is shown below:

CODE	SURNAME	NAME	SEX	OU
FTZ_R_0001	Fitzgerald	Robert	0	testStress
VHN_J_0002	Vahn	Jennifer	1	testStress
SLM_M_0003	Salomon	Mark	0	CheckOU
RMR_L_0004	Ramirez	Lorena	1	testStress
NDV_P_0005	Nedved	Pavel	0	CheckOU
SZY_G_0006	Szymanowsky	Gregor	0	testStress

## User-OU-Entitlement Assignments Record Track


This batch procedure can be used to manage Entitlement Assignments.


Table 96. User-OU-Entitlement Assignments Track

Information	Description	Validation
USER_CODE	User identifier code.	Optional
OU_CODE	OU identifier code.	Mandatory <sup>3</sup>
IN_HIER	Values can be <b>TRUE</b> or <b>FALSE</b> .	Optional
ENTITLEMENT_NAME	Entitlement identifier name.	Mandatory
ENTITLEMENT_CODE	This field holds the univocal identifier of the Entitlement.	Optional
ENTITLEMENT_TYPE	Can be one of the following: <ul style="list-style-type: none"> <li>• 1 (for Permission)</li> <li>• 2 (for IT role)</li> <li>• 3 (for Business role)</li> <li>• External_Role</li> </ul>	Mandatory
ENTITLEMENT_APPLICATION	Entitlement Application Identifier Name	Mandatory <sup>1</sup>
PERMISSION_TYPE	Permission Type identifier name	Mandatory <sup>2</sup>

Depending on whether the **Entitlement Localization** is active or not active, you can specify the entitlements in different ways. See the IBM Security Governance installation procedure for details. The following table describes the options.

Entitlement Localization options		
Concept	Description	
Localization Active	YES	NO
Entitlement specification	<p><b>ENTITLEMENT_CODE</b></p> <p>Or</p> <ul style="list-style-type: none"> <li>• <b>ENTITLEMENT_NAME</b></li> <li>• <b>ENTITLEMENT_TYPE</b></li> <li>• <b>ENTITLEMENT_APPLICATION</b></li> <li>• <b>PERMISSION_TYPE</b></li> </ul> <p>See Note<sup>1</sup> and Note<sup>2</sup>.</p> <p>If <b>ENTITLEMENT_CODE</b> is specified, it is the univocal identifier of the entitlement.</p> <p>The <b>ENTITLEMENT_NAME</b> is the technical name of the entitlement.</p>	<p>An entitlement must be specified by:</p> <ul style="list-style-type: none"> <li>• <b>ENTITLEMENT_NAME</b></li> <li>• <b>ENTITLEMENT_TYPE</b></li> <li>• <b>ENTITLEMENT_APPLICATION</b></li> <li>• <b>PERMISSION_TYPE</b></li> </ul> <p>See Note<sup>1</sup> and Note<sup>2</sup>.</p>

	1	<b>NOTE:</b> If <b>ENTITLEMENT_TYPE</b> = 3, the <b>ENTITLEMENT_APPLICATION</b> field must be blank. Otherwise, it must be populated.
	2	<b>NOTE:</b> If <b>ENTITLEMENT_TYPE</b> = 1, the <b>PERMISSION_TYPE</b> field must be populated.

	<sup>3</sup> <b>NOTE:</b> If <b>USER_CODE</b> is not present, <b>OU_CODE</b> MUST BE specified.
---	---

This batch procedure can be used to manage Entitlement Assignments. It verifies that the required fields are populated.

The procedure checks for a User with the given **USER\_CODE**. If the User is already assigned to an Organization Unit, the User's OU must match the given **OU\_CODE** field value. Otherwise, the row is skipped. If **USER\_CODE** is not populated, Entitlement is assigned only to **OU\_CODE**.

If the **IN\_HIER** field is TRUE, Entitlement is assigned in hierarchy.

If not already aggregated to an OU, the User is aggregated to the given User OU.

The **OU\_CODE** field must contain an existing OU code. If it does not, the row is skipped.

The existence of the Entitlement is verified using the values of **ENTITLEMENT\_NAME**, **ENTITLEMENT\_TYPE**, **ENTITLEMENT\_APPLICATION** (**ENTITLEMENT\_APPLICATION** is mandatory when **ENTITLEMENT\_TYPE**= 1, 2, or External\_Role) and **PERMISSION\_TYPE** (only when **ENTITLEMENT\_TYPE**= 1).

If there is no such Entitlement, the record is skipped. The following three aggregations are created:

- **Entitlement - Entitlement:** Entitlement is published and assignable to Users
- **Entitlement - OU:** Entitlement is available in an Organization Unit
- **Entitlement - User:** Entitlement is assigned to the User

### Add Resources to User/Entitlement Record Track


This batch procedure can be used to add Resources to an Entitlement already assigned to a User.

Add Resources to User/Entitlement Track		
Information	Description	Validation
USER_CODE	Code of the User.	Mandatory
ENTITLEMENT_NAME	Entitlement identifier name. If the <b>Entitlement Localization</b> option is active, this is the "technical name" of the Entitlement.	Mandatory

Add Resources to User/Entitlement Track		
Information	Description	Validation
ENTITLEMENT_CODE	Univocal identifier of an Entitlement.	Mandatory
ENTITLEMENT_TYPE	Entitlement Type identifier. The allowed values are: <ul style="list-style-type: none"> <li>• 1 (for Permission)</li> <li>• 2 (for IT role)</li> <li>• 3 (for Business role)</li> <li>• External_Role</li> </ul>	Mandatory
ENTITLEMENT_APPLICATION	Application identifier name.	Mandatory <sup>1</sup>
PERMISSION_TYPE	Permission Type identifier.	Mandatory <sup>2</sup>
RESOURCE_NAME	Resource name.	Mandatory
RESOURCE_TYPE	Resource Type name.	Mandatory
RESOURCE_FAMILY	Resource Family name.	Mandatory

This batch procedure can be used to add Resources to an Entitlement already assigned to a User.

It verifies that the required fields are populated; when a Mandatory field is missing, the row is skipped.

	<b>Note:</b> The Resource to be assigned to the Entitlement/User, MUST BE a Resource already assigned to the OU to which the User (USER_CODE) belongs.
---	--

Depending on whether the **Entitlement Localization** is active or not active, you can specify the entitlements in different ways. See the IBM Security Governance installation procedure for details. The following table describes the options.

Entitlement Localization options		
Concept	Description	
Localization Active	YES	NO

Entitlement Localization options	
Concept	Description
Entitlement specification	<p><b>ENTITLEMENT_CODE</b></p> <p>Or</p> <ul style="list-style-type: none"> <li>• <b>ENTITLEMENT_NAME</b></li> <li>• <b>ENTITLEMENT_TYPE</b></li> <li>• <b>ENTITLEMENT_APPLICATION</b></li> <li>• <b>PERMISSION_TYPE</b></li> </ul> <p>See Note<sup>1</sup> and Note<sup>2</sup>.</p> <p>If <b>ENTITLEMENT_CODE</b> is specified, it is the univocal identifier of the entitlement.</p> <p>The <b>ENTITLEMENT_NAME</b> is the technical name of the entitlement.</p>



<sup>1</sup>  
**NOTE:** If **ENTITLEMENT\_TYPE** = 3, the **ENTITLEMENT\_APPLICATION** field must be blank. Otherwise, it must be populated.

<sup>2</sup>  
**NOTE:** If **ENTITLEMENT\_TYPE** = 1, the **PERMISSION\_TYPE** field must be populated.

## Add Internal Resources to User/Entitlement Record Track

This batch procedure can be used to add Internal Resources to an Entitlement already assigned to a User.

Table 97. Add Internal Resources to User/Entitlement Track

Information	Description	Validation
USER_CODE	Code of the User.	Mandatory
ENTITLEMENT_NAME	Entitlement identifier name. If the <b>Entitlement Localization</b> option is active, this is the "technical name" of the Entitlement.	Mandatory
ENTITLEMENT_CODE	Univocal identifier of an Entitlement.	Mandatory
ENTITLEMENT_TYPE	Entitlement Type identifier. Allowed values are: <ul style="list-style-type: none"> <li>• 1 (for Permission)</li> <li>• 2 (for IT role)</li> <li>• 3 (for Business role)</li> <li>• External_Role</li> </ul>	Mandatory
ENTITLEMENT_APPLICATION	Application identifier name.	Mandatory <sup>1</sup>




Table 97. Add Internal Resources to User/Entitlement Track (continued)

Information	Description	Validation
PERMISSION_TYPE	Permission Type identifier.	Mandatory <sup>2</sup>
INT_RESOURCE_NAME	Internal Resource name.	Optional.
INT_RESOURCE_TYPE	Internal Resource Type name. Allowed values are: <ul style="list-style-type: none"> <li>• <b>OU</b>: the Resource is an Organization Unit</li> <li>• <b>E</b>: the Resource is an Entitlement</li> <li>• <b>A</b>: the Resource is an Application</li> <li>• <b>R</b>: the Resource is a Risk</li> </ul>	Mandatory
INT_RESOURCE_CODE	Univocal identifier of the Resource type specified in the row above.	Mandatory
RESOURCE_SPEC_1	Used if <b>INT_RESOURCE_TYPE = E</b>	Optional
RESOURCE_SPEC_2	Used if <b>INT_RESOURCE_TYPE = R or E</b>	Optional
RESOURCE_SPEC_3	Used if <b>INT_RESOURCE_TYPE = E</b>	Optional

This batch procedure can be used to add Internal Resources to an Entitlement already assigned to a User.

It verifies that the required fields are populated; if a Mandatory field is missing, the row is skipped.


Table 98. Note about resources

	<b>Note:</b> The Resource to be assigned to the Entitlement/User must be a Resource already assigned to the OU to which the User ( <b>USER_CODE</b> ) belongs.
---	--

Depending on whether the **Entitlement Localization** is active or not active, you can specify the entitlements in different ways. See the IBM Security Governance installation procedure for details. The following table describes the options.

Entitlement Localization options		
Concept	Description	
Localization Active	YES	NO

Entitlement Localization options		
Concept	Description	
Entitlement specification	<p><b>ENTITLEMENT_CODE</b></p> <p>Or</p> <ul style="list-style-type: none"> <li>• <b>ENTITLEMENT_NAME</b></li> <li>• <b>ENTITLEMENT_TYPE</b></li> <li>• <b>ENTITLEMENT_APPLICATION</b></li> <li>• <b>PERMISSION_TYPE</b></li> </ul> <p>See Note<sup>1</sup> and Note<sup>2</sup>.</p> <p>If <b>ENTITLEMENT_CODE</b> is specified, it is the univocal identifier of the entitlement.</p> <p>The <b>ENTITLEMENT_NAME</b> is the technical name of the entitlement.</p>	<p>An entitlement must be specified by:</p> <ul style="list-style-type: none"> <li>• <b>ENTITLEMENT_NAME</b></li> <li>• <b>ENTITLEMENT_TYPE</b></li> <li>• <b>ENTITLEMENT_APPLICATION</b></li> <li>• <b>PERMISSION_TYPE</b></li> </ul> <p>See Note<sup>1</sup> and Note<sup>2</sup>.</p>

	<p><sup>1</sup></p> <p><b>NOTE:</b> If <b>ENTITLEMENT_TYPE</b> = 3, the <b>ENTITLEMENT_APPLICATION</b> field must be blank. Otherwise, it must be populated.</p> <p><sup>2</sup></p> <p><b>NOTE:</b> If <b>ENTITLEMENT_TYPE</b> = 1, the <b>PERMISSION_TYPE</b> field must be populated.</p>
---	--

Depending on the specified **INT\_RESOURCE\_TYPE**, different combinations of parameters are allowed as shown in the table below:

*Table 99. Combinations of parameters available for adding Internal Resources*

Field	INT_RESOURCE_TYPE			
	OU	E	A	R
INT_RESOURCE_CODE	OU_CODE	ENTITLEMENT_CODE	N.A.	N.A.
INT_RESOURCE_NAME	N.A.	Entitlement name.	Application name.	Risk name.
RESOURCE_SPEC_1	N.A.	ENTITLEMENT_TYPE	N.A.	N.A.
RESOURCE_SPEC_2	N.A.	If <b>RESOURCE_SPEC_1</b> =1 (Permission) or <b>RESOURCE_SPEC_1</b> =2 (IT Role)  the Application name joined with the IT Role or Permission must be specified.	N.A.	Environment name.
RESOURCE_SPEC_3	N.A.	If <b>RESOURCE_SPEC_1</b> = 1 (Permission), the related Permission Type must be specified.	N.A.	N.A.

## Add Resources to OU Record Track

This batch procedure can be used to add Resources to an OU.

Add Resources to OU Track		
Information	Description	Validation
OU_CODE	Code of the OU target.	Mandatory
RESOURCE_NAME	Resource name.	Mandatory

Add Resources to OU Track		
Information	Description	Validation
RESOURCE_TYPE	Resource Type name.	Mandatory
RESOURCE_FAMILY	Resource Family name.	Mandatory
HIERARCHY	<p>The allowed values are:</p> <ul style="list-style-type: none"> <li>• <b>TRUE</b>: Resource is added in hierarchy</li> <li>• <b>FALSE</b>: Resource is added only to the OU indicated by <b>OU_CODE</b> (default value)</li> </ul>	Optional
INHERITANCE	<p>The allowed values are:</p> <ul style="list-style-type: none"> <li>• <b>TRUE</b>: The Resource is automatically available to any User assigned to the OU (<b>OU_CODE</b>)</li> <li>• <b>FALSE</b>: The Resource is not automatically available to Users of the OU (default value).</li> </ul>	Optional

This batch procedure can be used to add Resources to an OU.

It verifies that the required fields are populated; if a Mandatory field is missing, the row is skipped.

For **HIERARCHY** and **INHERITANCE** fields, an empty field is equivalent to **FALSE** value (default value).

### Remove Int Resources from User/Entitlement Record Track

Remove Profile from Activity Record Track ARC

This batch procedure can be used to remove Internal Resources from an entitlement already assigned to a user. The structure of the record track is the same as the one described in Add Internal Resources to User\_ Entitlement Record Track or in "Add Resources to OU Record Track" on page 234.

### Remove Resources from User/Entitlement Record Track

Remove Profile from Activity Record Track ARC

This batch procedure can be used to remove resources from an entitlement already assigned to a user. The structure of the record track is the same as the one described in "Add Resources to User/Entitlement Record Track" on page 230 and "Add Resources to OU Record Track" on page 234.

### Remove Resource from OU Record Track

Remove Profile from Activity Record Track ARC

This batch procedure can be used to remove Resource from an OU.

The structure of the record track is the same as the one described in “Add Resources to OU Record Track” on page 234 or in Add Permission to Activity Record Track.

## Insert Organization Units Record Track

Table 100. Insert Organization Units Track

Information	Description	Validation
NAME	OU identifier name.	Mandatory
CODE	OU identifier code.	Mandatory
DESCRIPTION	A free text field for describing the OU.	Optional
PARENT_CODE	Parent OU identifier code.	Mandatory

This batch procedure can be used to insert/update Organization Units and organize them into a hierarchy. It verifies that Mandatory fields are populated.

The **CODE** field contains the OU Code. If there is no existing OU with this name, the OU is inserted. If an OU with this Code already exists, the OU is updated with the given Name and Description. The **PARENT\_CODE** field contains the code of the OU designated to be the Parent.

OUs are assigned to their respective Parent OUs. Presence of the Parent OU is verified with the given Parent Code.

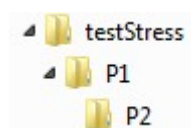
PARENT\_CODE verification applies either to a preexisting OU or to the entire XLS file. Therefore, OUs need not be inserted into the XLS file in any particular order. If the PARENT\_CODE field is empty, the OU is assigned to the root OU.

If a Parent OU with the given code does not exist, the OU is assigned to a technical OU (the code for a technical OU is "-undefined-"). The technical OU is created only at the first occurrence of this situation. The orphan OUs assigned to the technical OU will need to be properly repositioned within the OU hierarchy by the operator.

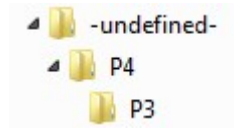
An example of the XLS file structure is shown below:

NAME	CODE	DESCRIPTION	PARENT_CODE
P3	Test_Stress	desc3	P4
P2	undefchild2	desc2	P1
P1	P1	desc1	testStress
P4	P4	desc4	bambex

Using the record track just shown, this first OU hierarchy will be built:



Another OU hierarchy will be built:



Since the bambex OU does not actually exist, this second one is required. P4 is thus assigned as a child of the “technical OU” named “-undefined-”.

## Insert Property Record Track

Table 101. Insert Property Record Track.

Information	Description	Validation
ENTITY_TYPE	Indicates the type of Entity to be associated with a set of properties. The possible values are: <ul style="list-style-type: none"> <li>• E: Entitlement</li> <li>• A: Application</li> </ul>	Mandatory
K1	Entity logic key.	Mandatory
K2	Entity logic key.	Mandatory
K3	Entity logic key.	Mandatory
NAME	Indicates the name of the property.	Mandatory
VALUE	Indicates the value of the NAME property .	Mandatory
MULTIVALUE	The possible values are: <ul style="list-style-type: none"> <li>• TRUE: Property is multi-value</li> <li>• FALSE: Property is single-value (default value)</li> </ul>	Optional
INHERITABLE	The possible values are: <ul style="list-style-type: none"> <li>• TRUE: Property is inheritable.</li> <li>• FALSE: Property is not inheritable (default value)</li> </ul>	Optional
ACTION	The DELETE tag indicates a property that is to be deleted.	Mandatory
ENTITLEMENT_CODE	This field holds the univocal identifier of the Entitlement.	Optional
EXTERNAL_ROLE	Specifies if the entitlement is an external role. Can be TRUE or FALSE (default).	Optional

This batch procedure can be used to insert/update Properties.

It verifies that mandatory fields are populated; if a mandatory field is missing, the row is skipped.

Properties support multivalued, so the same NAME can be repeated multiple times with different values.

The combinations of Logic Keys K1, K2 and K3 are shown in the table below:

Table 102. Entity Logic Keys combinations.

Entities\Keys	K1	K2	K3
Business Role	Name of the BRole	<i>empty</i>	<i>empty</i>
IT Role	Name of IT Role	Name of the Application	<i>empty</i>
Permission	Name of Permission	Name of the Application	Permission Type
Application	Name of the Application	<i>empty</i>	<i>empty</i>

The Entitlement associated with the Property can be specified by the (K1,K2,K3) combination or by the ENTITLEMENT\_CODE.

### Add Internal Resources to User/Entitlement Record Track

This batch procedure can be used to add Internal Resources to an Entitlement already assigned to a User.

Table 103. Add Internal Resources to User/Entitlement Track

Information	Description	Validation
USER_CODE	Code of the User.	Mandatory
ENTITLEMENT_NAME	Entitlement identifier name. If the <b>Entitlement Localization</b> option is active, this is the "technical name" of the Entitlement.	Mandatory
ENTITLEMENT_CODE	Univocal identifier of an Entitlement.	Mandatory
ENTITLEMENT_TYPE	Entitlement Type identifier. Allowed values are: <ul style="list-style-type: none"> <li>• 1 (for Permission)</li> <li>• 2 (for IT role)</li> <li>• 3 (for Business role)</li> <li>• External_Role</li> </ul>	Mandatory
ENTITLEMENT_APPLICATION	Application identifier name.	Mandatory <sup>1</sup>
PERMISSION_TYPE	Permission Type identifier.	Mandatory <sup>2</sup>
INT_RESOURCE_NAME	Internal Resource name.	Optional.


Table 103. Add Internal Resources to User/Entitlement Track (continued)

Information	Description	Validation
INT_RESOURCE_TYPE	Internal Resource Type name. Allowed values are: <ul style="list-style-type: none"> <li>• <b>OU</b>: the Resource is an Organization Unit</li> <li>• <b>E</b>: the Resource is an Entitlement</li> <li>• <b>A</b>: the Resource is an Application</li> <li>• <b>R</b>: the Resource is a Risk</li> </ul>	Mandatory
INT_RESOURCE_CODE	Univocal identifier of the Resource type specified in the row above.	Mandatory
RESOURCE_SPEC_1	Used if <b>INT_RESOURCE_TYPE = E</b>	Optional
RESOURCE_SPEC_2	Used if <b>INT_RESOURCE_TYPE = R or E</b>	Optional
RESOURCE_SPEC_3	Used if <b>INT_RESOURCE_TYPE = E</b>	Optional

This batch procedure can be used to add Internal Resources to an Entitlement already assigned to a User.

It verifies that the required fields are populated; if a Mandatory field is missing, the row is skipped.


Table 104. Note about resources

	<b>Note:</b> The Resource to be assigned to the Entitlement/User must be a Resource already assigned to the OU to which the User ( <b>USER_CODE</b> ) belongs.
---	--

Depending on whether the **Entitlement Localization** is active or not active, you can specify the entitlements in different ways. See the IBM Security Governance installation procedure for details. The following table describes the options.

Entitlement Localization options		
Concept	Description	
Localization Active	YES	NO

Entitlement Localization options		
Concept	Description	
Entitlement specification	<p><b>ENTITLEMENT_CODE</b></p> <p>Or</p> <ul style="list-style-type: none"> <li>• <b>ENTITLEMENT_NAME</b></li> <li>• <b>ENTITLEMENT_TYPE</b></li> <li>• <b>ENTITLEMENT_APPLICATION</b></li> <li>• <b>PERMISSION_TYPE</b></li> </ul> <p>See Note<sup>1</sup> and Note<sup>2</sup>.</p> <p>If <b>ENTITLEMENT_CODE</b> is specified, it is the univocal identifier of the entitlement.</p> <p>The <b>ENTITLEMENT_NAME</b> is the technical name of the entitlement.</p>	<p>An entitlement must be specified by:</p> <ul style="list-style-type: none"> <li>• <b>ENTITLEMENT_NAME</b></li> <li>• <b>ENTITLEMENT_TYPE</b></li> <li>• <b>ENTITLEMENT_APPLICATION</b></li> <li>• <b>PERMISSION_TYPE</b></li> </ul> <p>See Note<sup>1</sup> and Note<sup>2</sup>.</p>

	<p><sup>1</sup></p> <p><b>NOTE:</b> If <b>ENTITLEMENT_TYPE</b> = 3, the <b>ENTITLEMENT_APPLICATION</b> field must be blank. Otherwise, it must be populated.</p> <p><sup>2</sup></p> <p><b>NOTE:</b> If <b>ENTITLEMENT_TYPE</b> = 1, the <b>PERMISSION_TYPE</b> field must be populated.</p>
---	--

Depending on the specified **INT\_RESOURCE\_TYPE**, different combinations of parameters are allowed as shown in the table below:

*Table 105. Combinations of parameters available for adding Internal Resources*

Field	INT_RESOURCE_TYPE			
	OU	E	A	R
INT_RESOURCE_CODE	OU_CODE	ENTITLEMENT_CODE	N.A.	N.A.
INT_RESOURCE_NAME	N.A.	Entitlement name.	Application name.	Risk name.
RESOURCE_SPEC_1	N.A.	ENTITLEMENT_TYPE	N.A.	N.A.
RESOURCE_SPEC_2	N.A.	If <b>RESOURCE_SPEC_1</b> =1 (Permission) or <b>RESOURCE_SPEC_1</b> =2 (IT Role)  the Application name joined with the IT Role or Permission must be specified.	N.A.	Environment name.
RESOURCE_SPEC_3	N.A.	If <b>RESOURCE_SPEC_1</b> = 1 (Permission), the related Permission Type must be specified.	N.A.	N.A.

## Insert Rights Lookup Record Track

Insert Rights Lookup Track		
Information	Description	Validation
NAME	Indicates the name of the Right.	Mandatory
VALUE	Indicates the value of the Right NAME.	Mandatory



This batch procedure can be used to insert/update a set of values for every Right.

It verifies that Mandatory fields are populated; if some Mandatory field is missing, the row is skipped.

Typically, we have a set of rows (or more than one set) with:

- the same Name for every row of the set
- a distinct Value for every row of the set

### Insert External Roles record track

Use this batch procedure to import external roles and permissions into your security model.

*Table 106. Insert External Roles record track*

Information	Description	Validation
NAME	The name of the external role.	Mandatory
CODE	The univocal identifier of the external role.	Optional
DESCRIPTION	A description of the external role.	Optional
TYPE	The type of external role. It can be: <ul style="list-style-type: none"> <li>• Permission</li> <li>• External_Role</li> </ul>	Mandatory
PERMISSION_TYPE	Permission Type identifier for both external roles and permissions.	Mandatory
APPLICATION	The name of the application to which the external role belongs. The application must be already defined.	Mandatory
EXTERNAL_REF	The name used for the external role or permission on the external system.	Optional
FULFILLMENT	TRUE (the role is fulfilled) or FALSE (the role is not fulfilled).	Optional. Empty field is acknowledged as FALSE.
PUBLISH	TRUE (the role is published) or FALSE (the role is not published). Also FULFILMENT must be TRUE for the role or permission to be actually published.	Optional. Empty field is acknowledged as FALSE.
PARENT_NAME	The name of the parent external role. If it exists, the parent external role must be listed before as a role without parent.	Optional

Table 106. Insert External Roles record track (continued)

Information	Description	Validation
PARENT_CODE	The code of the parent external role. If it exists, the parent external role must be listed before as a role without parent.	Optional
PARENT_TYPE	Parent Entitlement Type identifier. This can be: External_Role	Mandatory if PARENT_NAME or PARENT_CODE were entered.
PARENT_PERMISSION_TYPE	The Permission Type identifier of the parent external role, if one was entered.	Mandatory if PARENT_NAME or PARENT_CODE were entered.
PARENT_APPLICATION	The name of the application to which the parent external role belongs. The application must be already defined.	Mandatory if PARENT_NAME or PARENT_CODE were entered.
OWNER_CODE	The identifier code of the person who owns the external role or permission. The code must be already defined.	Optional

An external role or permission is not inserted if it is found to be already present in the security model. It can still be published or inserted in a hierarchy.

External roles and permissions can be inserted in a hierarchy. However, neither external roles nor permissions can be added as children of a permission.

If both PARENT\_NAME and PARENT\_CODE are left blank, the external role or permission is inserted and possibly published, but is not associated to a hierarchy. If an external role or permission is to be associated to a hierarchy, and PARENT\_NAME is left blank, PARENT\_CODE becomes a mandatory field.

PUBLISH can be set to TRUE only if FULFILLMENT is TRUE or if the external role or permission is already fulfilled.

Either set of attributes TYPE, APPLICATION, PERMISSION\_TYPE, EXTERNAL\_REF (when defined) and TYPE, APPLICATION, PERMISSION\_TYPE, NAME defines a permission or an external role as a unique entity. While EXTERNAL\_REF cannot be modified locally, NAME can be changed.

### Remove External Roles record track

Use this batch procedure to remove external roles and permissions from your security model.

The line is skipped, when the external role or permission is not found.

Table 107. Remove External Roles record track

Information	Description	Validation
NAME	The name of the external role.	Mandatory if CODE is left blank

Table 107. Remove External Roles record track (continued)

Information	Description	Validation
CODE	The univocal identifier of the external role.	Optional
TYPE	The type of external role. It can be: <ul style="list-style-type: none"> <li>• Permission</li> <li>• External_Role</li> </ul>	Mandatory if CODE is left blank
PERMISSION_TYPE	Permission Type identifier.	Optional, unless it is defined and CODE is blank
APPLICATION	The name of the application to which the external role belongs. The application must be already defined.	Mandatory if CODE is blank
EXTERNAL_REF	The name used for the external role or permission on the external system.	Optional

If the EXTERNAL\_REF column is populated, the attribute is used in lieu of NAME.

---

## Settings

Use this area to configure basic features of Identity Governance and Intelligence.

This area features the following tabs:

### Core Configurations

Where you can configure several aspects related to the basic behavior of Identity Governance and Intelligence.

### Configure Password Service

Where you setup the Configure Password service for users who have lost their password to Identity Governance and Intelligence.

## Core configurations

In the core configuration area, you can configure several aspects related to the basic behavior of the IBM Security Identity Governance platform.

All elements that can be configured are located in the following tabs:

- General
- User Virtual Attributes
- “Internal Events” on page 250

## General

The general configuration attributes are described in the following table:

Table 108. General configuration attributes.

Attribute	Description
General	<b>Log Level</b> Four different log levels can be set: <ul style="list-style-type: none"> <li>• <b>Error:</b> Records errors only.</li> <li>• <b>Warning:</b> Records errors and indications of possible errors.</li> <li>• <b>Info:</b> Records errors, warnings, and information messages.</li> <li>• <b>Debug:</b> Records errors, warnings, information messages, and messages associated to the debugging phase.</li> </ul>
	<b>View Person's sensible data</b> If selected, all personal data is visible to Identity Governance and Intelligence modules; otherwise, it is hidden.
SoD/External SoD	<b>Enable Role Policy</b> If selected, all controls for role conflict (Access Risk Controls) are enabled, including controls for External SoD.
	<b>Enable external SoD</b> If selected, the information about risks associated to users will be provided by external systems.
	<b>Split Role into Permissions</b> If selected, the common hierarchical structure of a Role is split into a flat collection of component Permissions, before sending it to an external SoD engine.
	<b>Rest</b> With this radio button you can specify the ReST service address.
	<b>Class</b> With this radio button you can specify the Java Class used for managing external SoD.
Security	<b>Token Validity (minutes)</b> Indicates the time frame validity of the SAML token, expressed in minutes.  The SAML token contains sensitive information related to the user accessing the system, and is used for different steps of the authorization process.

Table 108. General configuration attributes. (continued)

Attribute		Description
Access	Login UserID	The credential requested in the login phase is the User ID.
	Login UserID and Password	The credentials requested in the login phase are User ID and password.
	Login DN	The credentials requested in the login phase include the distinguished name extracted from a digital certificate (generally stored into a smartcard).
	Login SAML	The credential requested in the login phase is a token SAML.
Auditing	Set Hour	If selected, sets the Start (hh:mm) attribute and changes the measurement unit from minutes to hours of the Repeat every attribute.
	Start (hh:mm)	Defines the time to start the daily audit task.
	Repeat every	Defines the snooze time (in seconds).
	Number of Lines	Number of lines involved in the audit process.

Click **Save** to record your selections.

**Important:** If you have enabled the **Enable external SoD** with the radio-button **Rest**, you have to update two **IBM Security Identity Governance Task Planner** tasks:

- NightShift
- Housekeeping

Proceed according to the procedure shown below:

1. Access to **IBM Security Identity Governance Task Planner** module
2. Select **Manage > Tasks**
3. Select **Actions > Add**
4. In the **Details** tab, set a name of the new task **SystemRiskAnalysis**
5. In the **Scheduler** combo box, select the scheduler **Singleton**
6. Click on **Save**
7. Repeat the steps 3, 4, 5 and 6 for the new task **BatchProcessedActionsAGC**
8. In the tab **Task**, select the task **NightShift**
9. Stop the task with **Actions > Stop**
10. Repeat the steps 8 and 9 for the task **Housekeeping**
11. Select the stopped task **NightShift**
12. In the central frame, select the tab **Job**.

13. Select the job **SystemRiskAnalisy**s and delete it with **Actions > Remove**
14. Select the stopped task **Housekeeping**
15. In the central frame, select the tab **Job**.
16. Select the job **BatchProcessedActionsAGC** and delete it with **Actions > Remove**
17. In the tab **Task**, select the task **SystemRiskAnalisy**s.
18. In the central frame, select the tab **Job**.
19. Select **Actions > Add**
20. In the Add a Job to a Task pop-up window, select the job **SystemRiskAnalisy**s
21. Click on **Ok**
22. Repeat the steps 17,18 and 19 for the task **BatchProcessedActionsAGC**
23. In the Add a Job to a Task pop-up window, select the job **BatchProcessedActionsAGC**
24. Click on **Ok**
25. In the **Task** tab, select the task **NightShift**
26. Start the task with **Actions > Start**
27. Repeat the steps 25 and 26 for the tasks **Housekeeping, SystemRiskAnalisy**s, **BatchProcessedActionsAGC**

**Important:** To update the risk patterns of the registered users after enabling or disabling **External SoD**, run the **Refresh Violation Detection** operation. To do this, select **IBM Security Identity Governance Access Risk Controls > Tools > Refresh Violation Detection**.

### **User virtual attributes**

Access Governance Core supports a policy for linking user data from external sources. This policy is called virtualization.

This section describes the virtualization process.

The left pane displays a list of the inventoried repositories:

- **UserErc:** is the main integration interface table of IGI platform.
- **S\_User:** is the table of the users of Access Request module.
- **Swim\_User:** disabled by default, is used by Access Request module.

**Note:** Do not remove these repositories. You can add other repositories, but the removal of these default repositories can compromise the virtual mapping functionalities.

The enabled repositories are displayed in green (disabled in red).

The enabled repositories are used by Access Governance Core.

The right pane contains the **Details** and the **Attribute Mapping** tabs.

When you select a repository in the left pane, the **Details** pane is automatically updated with the repository data.

Repository details are described in the next table:

Table 109. User virtual attributes - repository details.

Detail	Description
Name	Repository name
Description	Short description of the repository
Enabled	When this attribute is selected, the repository is accessible. When it is not selected, the repository cannot be accessed even if the connection parameters are configured correctly.
Type	Repository type. Currently, only the database type is available.
Connection	A connection to the database can be: <ul style="list-style-type: none"> <li>• Internal. PM (AG core module)</li> <li>• External.</li> </ul>
Connection Type	This attribute is displayed only if an external connection was chosen. It can be one of the following: <ul style="list-style-type: none"> <li>• JNDI.</li> <li>• Custom.</li> </ul>
JNDI Name	The JNDI name used for the connection to the database according to the configuration used on the application server in use. It is shown only if the JNDI external connection selected.
Driver	The database driver. It is shown only if a custom external connection selected.
URL	The URL used for connecting to the database. It is shown only if a custom external connection was selected.
UserId	The database User ID. It is shown only if a custom external connection was selected.
Password	The database password. It is shown only if a custom external connection was selected.
Table Name	The name of the table that is to be linked to the PERSON table as part of the customization task.
Database User	The user who is granted access to the database, if the authentication password to the database matches with the User ID.
Key Column	The name of the column in the PERSON table that must match with the column selected in the remote table.
Query File	An XML file containing one or more queries to the database hosting the remote table. These queries are used to collect data for building the customized table.

**Note:** For some repositories, only some of the above attributes are active and appear depending on the selection.

Each type of connection requires different parameters. The connection type is chosen in the intermediate part of the **Details** tab (Type and Connection fields), while all the parameters needed for the selected connection are displayed in the lower part of the same pane.

The virtualization process is based on the **Attribute Mapping** tab displayed below:




The main information of this panel is in the **Name** and **Labels** columns.

In **Name** you find the attributes related to the repository selected in the **Repository** tab.

If you need to add another attribute to this column, click **Actions > Add** and select the attribute from the **Select attribute to add** pop-up window.

For the UserErc repository only, if the **Select attribute to add** window does not include an attribute you might need, you must first create the new attribute in the Identity Governance and Intelligence data base. See “Adding columns to the UserErc table” on page 107 to learn how to do this.

In **Labels** you find the attributes related to system fields.

If you choose a label and click the nearby  **Select System Field** button, a **Select System Field** pop-up window opens, where you can set the system field that you want to associate to the **Name** on the same row.

For example, you can consider the **USER\_ERC** table as repository involved into the virtual mapping.

Each attribute can be set in two different modes:

#### **Mode 1**


The **USER\_ERC** attribute (listed under the column **Name**), is mapped with an attribute of **PERSON**. Changing the value of an attribute in one table causes the same change in the other table. To customize an attribute with Mode 1,




insert the name of the **PERSON** attribute to be associated, preceded by an underscore ("\_"), into the **Label** column.

## Mode 2


The attribute in **USER\_ERC** is only displayed among the users' external data, on the User Management page of the AG Core Console. To customize an attribute by using Mode 2, insert the attribute and assign it a name in the **Label** text-box. In this case, the change in **USER\_ERC** is also reflected in the external table.

If you choose a label and click the nearby  Attribute Localization button, an **Attribute Localization** pop-up window opens, where you can set the localization of the label.

The label can be associated to a set of values, related to the **Lookup** control column.

When you click the  Lookup button, a **Lookup Options** pop-up window opens.

There you can find several options provided by default (Internal) or freely configurable (Pop-up or Selectfield) (see **AGC > Configure > Rights Lookup**).

To delete a value you previously set for **Lookup** control, click  **Clear**.

A label can be also associated to a **Default Value** that can be set and shown to the user in Access Request workflow activities.

You can also decide if the label value is editable by selecting the related checkbox in the **Editable** column.

In the **UI Rendering** column, for every datum you have to specify the type of UI element that renders it, as shown in the following list:

- **Textfield**
- **Textarea**
- **Checkbox (true,false)**
- **Checkbox (1,0)**
- **Passwordfield**
- **Date**
- **Date-hours**
- **Date-hours-seconds**

### Note:

If you choose **Date**, **Date-hours** or **Date-hours-time** as rendering type and you set a default value in the **Default Value** position, the format of the default value must comply with the formats shared between all modules.

The product formats are:

- **Date:** dd/MM/yyyy
- **Date-hours:** dd/MM/yyyy HH:mm
- **Date-hours-time:** dd/MM/yyyy HH:mm:ss

To modify the product formats, read the indications provided for the Time and Date customization process.

Use the first checkbox in the left to select the corresponding row if you want to:

- Remove it, selecting **Actions > Remove**.
- Set as default, indicated with a green checkmark, selecting **Actions > Set Key** (single selection).

Select the **Visible** checkbox to specify that the data column must be displayed.

The **Up/Down** yellow arrows define in which order the data columns are displayed in the system.

Select the **Required** checkbox to specify that the data must exist in the column.

The checkbox is flagged and grayed out as not editable if you, after clicking **Actions > Add**, select attributes indicated with a green checkmark; that is, attributes required for the repository selected in the **Repository** tab.

If a **Required** checkbox is not flagged, you can select it to specify that the attribute is **required** for the remote table/system.

Select **Actions > Save** to enable your changes.

## Internal Events

Use this tab to specify if events should be triggered and recorded for local operations that involve the entities of your security model and have an impact on the AG Core database.

The event generation mechanism is used by default for operations (such as the creation of a user, the removal of an entitlement, or the modification of an application) that are run on external targets and need to be communicated to Identity Governance and Intelligence. An event is created and associated to every operation, and stored in a table in Identity Governance and Intelligence. This table can be accessed by the Rules engine and the events stored within can be subjected to additional processing.

Operations run locally on Identity Governance and Intelligence are by default not associated to events. They are saved directly on the database. However, you may want the event mechanism to be applied also to the operations that are run locally on the Identity Governance and Intelligence user interface. In this way, they can be processed by the Rules engine and undergo the same type of processing that is applied to external events.

If you want that events be created also for operations run from the Identity Governance and Intelligence interface, flag any or all of the following check boxes:

Table 110. Options for the creation of internal events associated to local operations.

Attribute		Description
Application	<b>Enable Internal Events</b>	Flag if you want an event to be created and stored in the Internal Events table every time one of the following actions is completed: <ul style="list-style-type: none"> <li>• Create Application</li> <li>• Remove Application</li> <li>• Modify Application</li> </ul>
Entitlement	<b>Enable Internal Events</b>	Flag if you want an event to be created and stored in the Internal Events table every time one of the following actions is completed: <ul style="list-style-type: none"> <li>• Create Entitlement</li> <li>• Remove Entitlement</li> <li>• Modify Entitlement</li> <li>• Add User Entitlement</li> <li>• Remove User Entitlement</li> </ul>
Organizational Unit	<b>Enable Internal Events</b>	Flag if you want an event to be created and stored in the Internal Events table every time one of the following actions is completed: <ul style="list-style-type: none"> <li>• Create OU</li> <li>• Remove OU</li> <li>• Modify OU</li> </ul>
User	<b>Enable Personal Data Internal Events</b>	Flag if you want an event to be created and stored in the Internal Events table every time one of the following actions is completed: <ul style="list-style-type: none"> <li>• Create User</li> <li>• Remove User</li> <li>• Modify User</li> </ul>
	<b>Enable SoD Status Change Internal Events</b>	Flag if you want an event to be created and stored in the Internal Events table every time the SoD status of a user is changed.

Click **Save** to enable your selections.

## Configure password service

Use this tab to create and manage the security questions for users who have lost or forgotten their password to access Identity Governance and Intelligence.

When a user forgets the Identity Governance and Intelligence password and must reset it, the user must answer the security questions in order to log in.

The answers must match the answers entered when the user logged in for the first time. If the answers are correct, the user is given a new password or allowed to reset it.

Use **Configure password service** to create and manage the set of security questions and to set up the details of the response mechanism.

Use the following tabs:

**Configure Forgotten Password service**

Enable the password service and specify the number of security questions that the user must answer.

**Security questions**

Add, change, or remove security questions in English and other languages.

**Configure Forgotten Password service**

Use this tab to set up the number of security questions that a user, who is requesting to access Identity Governance and Intelligence after being unable to provide his/her password, must answer correctly.

When a user forgets the password and must reset it, the user must answer security questions to verify its identity. Use this tab to configure the set of security questions that the user must answer to regain access.

In the **Admin configuration** section, select **Enable password service** to enable the following services:

**Forgot password**

Enables users to reset their Service Center password if they forget it. Users are authenticated with security questions, and either they can enter a new password or they receive a one-time password at their registered email address. Depending on the configuration setup, users might have the option to change their email address.

**Self Care**

Service Center module where users can change their passwords

**Password reset**

An Account Change process of the Access Requests module where a manager or entitled person can reset the password for a user

In the **Security questions configuration** section, enter the following information:

**Number of security questions asked at first login**

Number of security questions to ask a new user. The answers are used for verification when the user is unable to provide the login password.

**Number of security questions asked for reset**

Number of questions to ask a user who has forgotten a password. This number must be smaller or equal to the number of questions asked at first login.

**Number of failed attempts allowed**

If the user is unable to correctly answer all the questions asked for reset in the number of attempts specified here, the password is not provided. The user must follow a different process to ask for help. For example, the user might call the Help-desk, an administrator, or a manager.

**Note:** This option applies to the Forgot password and Self Care features. It does not affect Password reset.

#### **Minimum length of the answer**

The minimum number of characters required for every answer.

In the **Mode Configuration** section, specify how to proceed after the user successfully answered all the security questions asked.

#### **Allow user to change password immediately**

User is prompted to enter a new password and can login immediately.

#### **Send one-time password to known user address**

A new password is emailed to the user. The password is valid for only one login during which the user is prompted to enter a new password.

Select **Allow user to change email address** to let the user edit the address to which the password is to be sent.

### **Security questions**

Use the Security questions tab to work with security questions that a user must answer to receive or reset a password.

The window displays the available security questions. To view a particular question or groups of questions in the list, use the fields located above the **Search** button.

- To view questions in a particular language, click the arrow in **Active Language** to choose a language from a list. The default is the language setting for your Web browser.
- To view specific questions, search for words or strings that you know are in the questions. Enclose the search text between percent symbols (%).
- To find a particular question, you can also enter its **Localization Code**. A localization code is automatically created when the question is added.
- Use the **Active for user** pull-down list to choose Active, Inactive, or All questions. Active questions are questions in the current set.

The **Security Questions** section lists the questions. Unless you choose a different language in the Active Language filter, the questions are displayed in the default language of your Web browser. Questions not defined in the active language are shown in English and are followed by a warning that they are not available in the chosen language.

Click the ellipsis (...) next to a question to view it, edit it, or add a localized version.

Use the **Actions** menu to perform one of the following actions:

- **Add** a question.
- **Remove** a selected question. Use the check boxes to select questions.

Add new questions in English first. You can enter a localized version of a question only after the question is defined in English.

The **Active for user** check box makes a question available to users. When a new question is saved, the **Active for user** check box is clear. It is not available to users. To make a question available for use, select the check box. Before you edit a question, or add a locale, clear the check box. You do not need to clear the check box to remove a question.

When a question is removed or thoroughly modified, users who have that question in their Forgot password list are asked to answer a new question at their next login.

---

## Chapter 14. Introduction to Access Risk Controls

Access Risk Controls (ARC) module enforces segregation of duties (SoD) checks, based on an innovative relation established between two different layers: the business activities layer and the role-based access control (RBAC) model.

One of the major difficulties that a real organization encounters when implementing an RBAC-based IAG system, is mapping the entities planned within its business model, such as processes, activities, and permissions, with the entities outlined by the RBAC model, such as roles, users, and segregation of duties (SoD) rules.

This problem is particularly evident when transitioning from an existing authorization model, in which authorization profiles have been layered over time with a business-driven vision, to a RBAC model, which requires uniform organizational planning and centralized management of the entire authorization flow.

The Access Risk Controls engine is the tool capable of connecting these two models -- Business and RBAC. More specifically, the ARC module extends features of the RBAC model by introducing the "at-risk activities" concept.

It is always desirable, if not necessary, to prevent a member of the organization from taking on operational privilege that might cause a conflict of interest, and possibly have a detrimental effect on the organization.

For example, consider an employee whose task is to analyze the market searching for new products to add to the company production process.

For obvious reasons, the organization strongly advises that this person should not be simultaneously entrusted with signing of product purchase orders.

The general principle is that an individual employee should not be authorized to perform tasks which might damage the organization.

This aspect is one of the main elements that lead to the implementation of an IAG system.

In the RBAC model, this problem is modeled and managed using the segregation of duties (SoD) concept.

SoD imposes constraints so that a user with a certain role cannot take on another role whose nature conflicts with the one already assigned.

ARC embeds the management of SoD aspects into the more general concept of risk.

The ARC module provides a set of functions that enable:

- Definition of the entire set of activities necessary to complete each specific business process.
- Tracking the risks aggregated to a generic set of activities.

- Aggregation of each activity with the necessary set of authorization entitlements to perform the activity.
- Tracking the entire set of conflicts among the different authorization entitlements.
- Tracking a set of at-risk roles registered in the system.
- Tracking a set of illegal users registered in the system.

---

## Manage

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

- Business Activities
- Tech Transformation
- Mitigation Controls
- Risk Definitions
- Domains

### Business activities

This section contains all functions for the management of the business activity and for modeling a business activity tree structure.

In the left pane **Business Activity** two tabs are available.

In the **Tree View** tab, you can:

- Browse in the business activity tree for selecting the desired activity.
- Add or remove activities using the **Actions** menu.

In the **Search** tab, you have the filters to search for an activity (by clicking **Filter/Hide Filter**) and the **Actions>View** menu item for toggling to the **Tree View** tab.

The table below lists the available filters:

Business activity filters	
Filter	Description
<b>Name</b>	Name of the business activity.
<b>Identifier</b>	The univocal identifier of the business activity.
<b>Description</b>	Brief description of the business activity.


The content of the right frame changes depending on the tab selected in the upper side of the pane. When you access the business activity web interface, the **Details** tab is active by default. Under this tab are available two different accordion panes, selectable by clicking the pane title bar:

- **Activity details**
- **Activity property**

After an activity is selected in the left pane, the **Activity details** pane shows the related data contained in the AG Core database. The **Activity details** pane displays data, related to the selected activity, contained in the external repositories.



The table below lists the activity details:

Activity details	
Detail	Description
Parent Activity	Name of the parent activity (automatically set after the activity selection in the left frame).
Name	Name used within the organization to identify the activity.
ID Code	The univocal identifier of the activity.
Description	Brief description of the activity.
Owner	User who is responsible for the activity. Use the  <b>User</b> button on the right side of the attribute box to insert a user.


An activity can be aggregated to a set of properties that characterize it.

The Activity property pane displays properties that can add specific information about the selected activity.

For example, a property can have, as its value, an external link to the set of implementation regulations and standards compliance that must be implemented by that activity. Another example consists of considering the values of properties into the structure of a rule.

A property is identified by a pair of attributes <Name, Value>.

Properties can be easily added/removed/saved using the **Add** or **Remove** or **Save** items of the **Actions** menu in the upper right side of the pane.

	<p><b>Note:</b></p> <p>It is possible to have multi-values properties. Therefore, it is possible to specify a property <b>PROP_1</b> and associate it to a value <i>VALUE_1</i>.</p> <p>Add a new line, in the <b>Activity Property</b> pane, and specify the same property name (<b>PROP_1</b>) associated to a different value (<i>VALUE_2</i>).</p>
---	--


In the list below are shown the main operations related to the business activities:

- Details
- “Linked Permissions”
- Risk Memberships
- Applicable Domains

## Linked Permissions

In this section you may link Permissions to Activities.



As you select an activity in the left frame, the **Linked Permission** tab (right) is enabled and shows a tree view of the Permissions and/or Groups associated with the selected Activity.

	<p><b>Note:</b> The AND/OR condition is applied to all properties of Permissions and Groups and to everything is contained in the Groups; this condition is useful for the SoD analysis.</p>
---	--

From the **Linked Permission** tab it is possible to perform several operations, through the **Actions** buttons summarized below:

- **Add Group:** allows to add a root level Group identified as **PROFILE\_GROUP\_random\_number**, where **PROFILE\_GROUP\_** is a fixed string and **random\_number** is a random label composed by 5 ciphers. **This name is not modifiable!** A root level Group can contains Permissions and/or Groups (the Groups contained in the root level Group are identified only with the Group icon).
- **Add Perm (Permission):** allows to add 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 allows to defines the Rights values.
- **Remove:** allows to remove Permissions and Groups (the removal of a Group involves the instant removal of everything joined with the Group).
- **And/Or:** inverts the value of the boolean condition of the selected node (Groups, Permission and Rights).

For every button, a dedicated window opens and shows all the entities registered in the system and ready to be added. For example, for adding a Permission, clicking on the **Actions > Add Perm** button, the window Select Permission opens. In this window, the following filters can be used for Permissions search (click on **Filter/Hide Filter** button):

<b>Permission filters</b>	
<b>Filter</b>	<b>Description</b>
<b>Application</b>	Name of the Application for filtering Permissions. Use the  <b>Set Application</b> button on the right side of the attribute's box to set an Application.
<b>Type</b>	Type of filtered Permission. Use the  <b>Set Permission Type</b> button on the right side of the attribute's box to set a Permission Type.
<b>Name</b>	Permission name.

Permission filters	
Filter	Description
Status	<p>This filter can have four values:</p> <ul style="list-style-type: none"> <li>• <b>TBD:</b> when a Permission is not joined to any Activity but is not in the status Ignored or Missing Activity.</li> <li>• <b>Linked:</b> a Permission is joined to an Activity.</li> <li>• <b>Ignored:</b> when a Permission is not joined to any Activity.</li> <li>• <b>Missing Activities:</b> when the operator don't know to which Activities to join the Permission.</li> </ul>



## Business Activity Mapping

From this tab, you can associate the permissions to one or more activities.

The relationship between the activities and the permissions is "many to many".

An activity can be described using a set of aggregated permissions that are necessary for its implementation. In addition, a single permission can be aggregated to more than one activity.

In the **Permission** tab (left) you can search a specific permission according to the filters summarized in the table below (by clicking **Filter/Hide Filter**):

Permission filters	
Filter	Description
Application	Name of the application in which the illegal permissions are filtered. Use the  <b>Set Application</b> button on the right side of the attribute box to insert an application.
Type	Type of filtered permission. Use the  <b>Set Permission Type</b> button on the right side of the attribute box to insert a permission type.
Name	Permission name.
Status	<p>This filter can have four values:</p> <ul style="list-style-type: none"> <li>• <b>TBD:</b> when a permission is not associated to any activity but is not in the status Ignored or Missing Activity.</li> <li>• <b>Linked:</b> when a permission is associated to an activity</li> <li>• <b>Ignored:</b> when a permission is not associated to any activity</li> <li>• <b>Missing Activities:</b> when the operator does not know to which activities the permission should be associated.</li> </ul>

The results are displayed in the same pane according to the attributes summarized in the table below:

Permission attributes	
Attribute	Description
Status	Status of the permission.
Name	Name of the permission.
Type	Type of application.
Application	Name of the application.

From the **Permission** tab, clicking a permission, the **Details** tab (right) is enabled.

In the upper part of this pane is available the information about the selected permission and two check boxes that allow you to change 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.


To add an activity, click **Add** and, from the Add window, choose the desired activity from the **Tree view** tab or by clicking the **Search** tab and entering the filters for the search operation (by clicking **Filter/Hide Filter**).

Activity filters	
Filter	Description
Name	Activity name.
Identifier	Unambiguous identifier of the activity.
Description	Brief description of the activity.

To remove an activity, in the **Details** tab, from the list of the associated activities, select the desired activity, then click **Remove**.

When the permission-activity association is removed, the status of the permission changes back to TBD.

After the desired operation was performed, click **Save** in the bottom right part of the pane.

	<b>Note:</b> When a permission is in <b>Linked</b> status, it is not possible to change it to any other status. To modify the status of the Linked permission, you must remove the associated activity.
---	---

## Mitigation controls

Mitigations actions are used to define a set of suggested policies that can be activated to correct a conflicting situation, which is theoretically prevented by the risk violation detection.

Each action describes a procedure that the responsible administrator can activate when faced with an identified conflict that must be handled appropriately.

The control action can be performed automatically or manually by an authorized operator.



**Note:** In the current version, none of the Mitigations actions are aggregated to specific automatic procedure.

The **Mitigation** tab contains the list of mitigation actions listed by the system. Select a mitigation control to view its details as displayed in the **Control Details** accordion pane (hosted in the **Mitigation details** tab). In the **Control Properties** accordion pane (at the bottom right of the same tab), are listed the **Mitigation properties**; the administrator can add the properties. This step is not mandatory.

The filters that can be used to perform a mitigation search are **Name** and **Description**. The **Controls** details are indicated in the table below:

Controls details	
Detail	Description
<b>Name</b>	Name of the mitigation action.
<b>Proc. Code</b>	Numeric code associated with the mitigation.
<b>Description</b>	Brief description of the mitigation.
<b>Extended Description</b>	Extended description.
<b>Link</b>	This attribute can be used to indicate an external link.

In the **Mitigation** tab, a mitigation control can be added or removed by clicking **Add** or **Remove**. In the list below are shown the main operations related to the mitigation controls:

- Mitigation details
- Applicable Risks
- Applicable Domains
- Assigned Users

### Applicable risks

In this section are available the procedures used to aggregate risks to mitigations.

In the **Applicable Risks** tab are listed all the risks already aggregated to the mitigation control just selected in the **Mitigation** tab, on the left. In the same pane you can remove a risk by clicking **Remove**. Clicking **Add** button, the Add risk window opens and allows you to add a risk to a mitigation control. By clicking **Risk** in the Add risks window, you can view the activities aggregated to the selected risk.

In the Add risks window, the following filters can be used to perform a risk search (by clicking **Filter/Hide Filter**):

Risk filters	
Filter	Description
<b>Name</b>	Name of the risk
<b>Description</b>	Brief description of the risk
<b>Status</b>	Status of the risk: <ul style="list-style-type: none"> <li>• <b>Assigned Risk:</b> Risk already assigned to the mitigation.</li> <li>• <b>Not Assigned Risk:</b> Risk not assigned to the mitigation yet.</li> </ul>
<b>Type</b>	Types of risk inventoried in the system.

By clicking **Risk** in the **Applicable Risks** tab, you can view the activities aggregated to the selected risk.

## Applicable domains

In this section are available the procedures used to aggregate domains to a mitigation.

In the **Applicable Domains** tab are listed all the domains already aggregated to the mitigation control selected in the **Mitigation** tab, on the left. In the same tab, you can remove a domain by clicking **Remove**.

Clicking **Add**, the Add domain window opens displaying the list of all domains listed in the system. From this window, you can add a domain to a mitigation control by clicking **Ok**. In the Add domains window, the **Name** (name of the domain) and **Description** (description of the domain) filters can be used to perform a domain search (by clicking **Filter/Hide Filter**).

## Assigned users

In this section are available the procedures used to view users with assigned mitigations.

The filters that can be used to perform a user search (by clicking **Filter/Hide Filter**) are described in the following table:

User filters	
Filter	Description
<b>Search Identity</b>	This field can contain the name, the surname or the User ID of the user.
<b>Associated</b>	This check box is always selected. The search action is performed only on the user already aggregated to an OU.
<b>Organization Unit</b>	OU to which the user belongs.
<b>Hierarchy</b>	If this check box is selected, the operation is executed starting from the selected OU root down through all branches of the subtree that originate from that root.

## Risk definition


The **Risk** tab contains the list of risks defined on the system.

In the **Risk** tab, the following filters can be used for the risk search (by clicking **Filter/Hide Filter**):

Risk filters	
Filter	Description
<b>Name</b>	Risk name.
<b>Description</b>	Description of the risk nature.
<b>Status</b>	Risk status: <ul style="list-style-type: none"> <li>• <b>Assigned Risk:</b> Risk already assigned to the mitigation.</li> <li>• <b>Not Assigned Risk:</b> Risk not assigned to the mitigation yet.</li> </ul>
<b>Type</b>	Type of risk.

In the **Risk** tab, a risk can be added or removed by clicking **Add** or **Remove**.

Select a risk to view its details in the **Risk Details** tab. The Risk details are described in the table below:

Risk details	
Detail	Description
<b>Name</b>	Risk name
<b>Description</b>	Description of the risk nature
<b>Type</b>	Type of risk
<b>Scope Type</b>	Type of visibility scope: <ul style="list-style-type: none"> <li>• <b>Model:</b> Risk is assigned as a user role.</li> <li>• <b>Scope:</b> Risk is assigned directly to a user (owner).</li> <li>• <b>Both:</b> Risk can be assigned using a model or a scope</li> </ul>
<b>Level</b>	Level of risk (measured from 0 to 9)
<b>Impact</b>	Description of the risk impact
<b>Likelihood</b>	Value between 0 and 1
<b>Tolerance</b>	Description of the risk tolerance
<b>Trend</b>	Description of the risk trend
<b>Risk acceptance rational</b>	Description of the manageable risk acceptance. Risk acceptance is a value < tolerance
<b>Owner</b>	Name of the person responsible for an activity in a company. Use the  <b>User</b> button on the right side of the attribute box to insert a user (owner)
<b>Creation Date</b>	Date of the risk creation (dd/mm/yyyy; hh/mm/ss)

In the list below are shown the main operations related to the risk definition:

- Risk details
- Activity
- Applicable Mitigation Controls
- Users

## Activity

In the **Activity** tab are listed all the activities already aggregated to the risk selected in the **Risk** tab, on the left. In the same pane, you can remove an activity by clicking **Remove**. By clicking **View** in the **Activity** tab, you can view the exact position of the selected activity in the tree structure.

By clicking **Add** in the Add window that opens, you can view all the activities listed in the system (**Tree view** tab or **Search** tab). From this window it is possible to add an activity to a risk by clicking **Ok**. In the Add window, the following filters can be used to perform an activity search (by clicking **Filter/Hide Filter**):

Activity filters	
Name	Description
Name	Name of the business activity.
Identifier	The univocal identifier of the business activity.
Description	Brief description of the business activity.

## Applicable mitigation controls

In the **Applicable Mitigation Controls** tab are listed all the mitigation controls already aggregated to the risk selected in the **Risk** tab, on the left. In the same pane, you can remove a mitigation control by clicking **Remove**.

By clicking **Add**, the Add window that appears contains the list of all the mitigation controls listed in the system. From this window, you can add a mitigation control to a risk by clicking **Ok**. In the Add window, the **Name** (name of the mitigation) and **Description** (description of the mitigation) filters can be used to perform a risk search (by clicking **Filter/Hide Filter**).

## Users

From the **Users** tab you can view the list of users already aggregated to the risk selected in the **Risk** tab. In this tab, the following filters can be used to perform a search operation (by clicking **Filter/Hide Filter**):

User filters	
Filter	Description
Search Identity	This field can contain the name, the surname or the User ID of the user.
Associated	This check box is always selected. The search action is performed only on the user already aggregated to an OU.
Organization Unit	OU to which the user belongs.



User filters	
Filter	Description
Hierarchy	If this check box is selected, the operation is executed starting from the selected OU root down through all branches of the subtree that originate from that root.

## Domains

In this section you can define a theoretically unlimited number of domains.

The **Domain** tab contains the list of domains registered in the system. Select a domain to view its details in the **Details** tab.

In the **Domain** tab, a domain can be added or removed.

The filters available for a domain search are name and description (by clicking **Filter/Hide Filter**).

The domain details are described in the table below:

Domain details	
Detail	Description
Type	Type of domain.
Name	Name of the mitigation action.
Description	Brief description of the mitigation.
Extended Description	Extended description.
Note	This attribute can be used to indicate a specific message.

In the list below are shown the main operations related to the domains:

- Details
- Permissions
- Applications
- Mitigation Controls
- Activities



## Permissions

In this section are available the procedures used to aggregate permissions to domains.

In the **Permissions** tab are listed all the permissions already aggregated to the domain selected in the **Domain** tab. In the same pane, you can add or remove a permission by clicking **Add** or **Remove**.

Clicking **Add**, the Add window that opens contains the list of all the permissions listed in the system.

In the **Permissions** tab and in the Add window, the following filters can be used to perform a permission search (by clicking **Filter/Hide Filter**):

Permissions filters	
Filter	Description
Application	Application of the permission. Use the  <b>Set Application</b> button on the right side of the attribute box to insert an application.
Name	Name of the permission.
Type	Type of permission. Use the  <b>Set Permission Type</b> button on the right side of the attribute box to insert a type.

## Applications

In the **Applications** tab are listed all the applications already aggregated to the domain selected in the **Domain** tab.

In the same tab, you can add or remove an application by clicking **Add** or **Remove**.

Clicking **Add**, the Add window that opens contains the list of all the applications listed in the system.

In the **Applications** tab and in the Add window, the **Name** (name of the application) filter can be used to perform an application search (by clicking **Filter/Hide Filter**).

## Mitigation controls

In the **Applicable Domains** accordion pane are listed all the mitigations already aggregated to the domain selected in the **Domain** tab.

In the same pane, you can remove a mitigation by clicking **Remove**. The **Add** accordion pane contains the list of all the mitigations listed in the system. From this pane, you can add a mitigation to a domain by clicking **Add**.

The filters available for a mitigation search are **Name** and **Description** (by clicking **Filter/Hide Filter**).

## Activities

This section allows you to view the activities aggregated to a domain.

In the **Activities** tab are listed all the activities already aggregated to the domain selected in the **Domain** tab, on the left. In this tab, the following filters can be used to perform an activity search (by clicking **Filter/Hide Filter**):

Activity filters	
Filter	Description
Name	Name of the activity.
Code	Univocal identifier of the business activity.
Description	Description of the activity.

---

## Configure

Use the following functions for configuring the listed elements:

- Configurations

### Configurations


Different configurations can be activated for testing different authorizations patterns.

A configuration is built by:

- A set of business activities
- A set of conflicts associated to the activities
- A set of domains

In the **Configuration** tab is listed all the configurations available.

The filters **Name** and **Description** can be used for the configuration search (by clicking **Filter/Hide Filter**).

Select a configuration and click **Actions > Current** for setting the  active configuration.

Click **Actions > Add** for adding a configuration.

The new configuration can be empty or copied from an existing configuration.

In this last one case, you can decide whether to copy the entire configuration or select only some elements:

- Only the activities
- The activities and all the associated conflicts
- Some specific domain or all registered domains

---

## Monitor

Monitoring elements

The functions that are available for monitoring some elements are contained in the following list.

- Dashboard
- Risk Violations
- Scheduled Tasks
- Configuration Comparison
- Reports

### 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 49. Summary of permissions statuses

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

	<b>Note:</b> The data beyond the green status bar refers to the number of the permissions and not to the association between entities.
---	--

The following filters are available by clicking **Filter/Hide Filter**:

Dashboard Filters	
Filter	Description
Application	Clicking  <b>Application</b> 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  <b>Activity</b> opens the Activities window. You can select activities from the <b>Activity tree</b> tab or search from the <b>Activity</b> tab.
Permission	Name of the permission.
Status	Status of the permission <ul style="list-style-type: none"><li>• <b>To be Defined</b></li><li>• <b>Linked</b></li><li>• <b>Ignored</b></li><li>• <b>Missing Activity</b></li></ul>

The results are displayed in the same page and summarize the associations made according to the following attributes:

Dashboard Details	
Detail	Description
Application	Name of the application.
Permission	Name of the permission.
Status	Status of the permission.
Activity	Activity that is associated with the permission.

If the same permission is joined to more than one activity, the permission is displayed several times.

Figure 50. 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

## Risk violations

This section shows the set of ARC violations that can be evaluated by the ARC administrator.

The main sections are listed below:

- User Violations
- Entitlement Violations

**Note:** Before you begin to work in these sections, you should update the analysis on violations in section **Tools > Refresh Violation Detection**.

### User violations





This section allows you to view:

- Information on risky or conflicting activities related to the user considered.
- Mitigation actions that can be aggregated to a user and/or with a set of risky/conflicting activities aggregated to the user.
- Domains and activities that are aggregated to a user.

In the **User Violations** tab are displayed all the conflicting users listed by the system.

A user is considered "conflicting" if it has two or more entitlements that are in conflict.

In this tab, the following filters can be used for the user search (by clicking **Filter/Hide Filter**):

Conflicting user filters	
Filter	Description
Organization Unit	OU to which the user belongs. Use the  <b>Organization Unit</b> button on the right side of the attribute box to insert an OU.
Hierarchy	If this check box is selected, the operation is executed starting from the selected OU root and down through the entire subtree originating from the root.
Search Identity	This field can contain the name, and the surname or the User ID.
DN	Distinguished name of the user.
Search Type	Type of search: <ul style="list-style-type: none"> <li>• <b>All</b>: the search is executed on all users.</li> <li>• <b>With violations</b>: the search is executed on conflicting users.</li> <li>• <b>With mitigated violations</b>: the search is executed on conflicting user with compensated conflicts.</li> <li>• <b>With unmitigated violations</b>: the search is executed on conflicting user with uncompensated conflicts.</li> </ul>
Conflict level	Level of conflict, which can have one of the following three values: <div style="display: flex; flex-direction: column; align-items: flex-start; margin-top: 10px;"> <div style="display: flex; align-items: center; margin-bottom: 10px;">  <span>High</span> </div> <div style="display: flex; align-items: center; margin-bottom: 10px;">  <span>Medium</span> </div> <div style="display: flex; align-items: center;">  <span>Low</span> </div> </div> <p>These filters are not selectable if the <b>Search Type</b> filter is set to <b>All</b>.</p>

In the list below are described the main operations related to the user violations:

- Risk info
- Assignment details
- Mitigation Controls

### Assignment details

The **Domain** accordion pane list all the domains already aggregated to the user selected in the **User Violations** tab, on the left, while the **Activity** accordion pane contains the list of all the activities aggregated to the user.

Clicking on **View**, you can view the exact position of the activity in the tree structure.

In these accordion panes, the following filters can be used to search information (by clicking **Filter/Hide Filter**):

Domains/Activities search filters	
Name	Description
Name	Name of the domain/activity.
Description	Description of the domain/activity.

## Mitigation Controls

After completing the analysis on a conflicting user, some mitigation actions can be aggregated to that user.

In the **Mitigations** tab is displayed a list of conflicting activities in which the user is involved (upper part).




In the bottom part of the tab, you can find all the mitigation controls already aggregated to the user risk. You can add or remove a mitigation.

## Entitlement violations

This section allows you to display and analyze the conflicting entitlements that have been assigned compared to the activities and domains involved.

A conflicting entitlement allows for the execution of conflicting activities. In this tab, the following filters can be used for the entitlement search (by clicking **Filter/Hide Filter**):

Conflicting entitlement filters	
Filter	Description
Type	Choose one of the following type of entitlement: <ul style="list-style-type: none"> <li>• <b>Permission</b></li> <li>• <b>IT role</b></li> <li>• <b>Business role</b></li> </ul>
Application	Application name according to which conflicting entitlements are filtered.
Name	Entitlement name.
Search type	Choose between: <ul style="list-style-type: none"> <li>• <b>All</b>: the search is executed on all entitlements.</li> <li>• <b>With Violations</b>: the search is executed only on conflicting entitlements.</li> </ul>

Conflicting entitlement filters	
Filter	Description
Conflict level	<p>Description of the level of conflict, which can have one of the following three values:</p> <p> Low</p> <p> Medium</p> <p> High</p> <p>These filters are not selectable if the <b>Search type</b> filter is set to <b>All</b>.</p>

The main operations related to user violations are:

- Risk info
- Assignment details

### Assignment details

In the **Domain** accordion pane are listed all the domains already aggregated to the entitlement selected in the **Entitlement Violations** tab, on the left.

The **Activity** accordion pane contains the list of all the activities aggregated to the entitlement selected in the **Entitlement Violations** tab, on the left. Clicking on **View** you can view the exact position of the activity in the tree structure. In these accordion panes, the following filters can be used to perform a search (by clicking **Filter/Hide Filter**):

Domains/activities filters	
Filter	Description
Name	Name of the domain/activity.
Identifier	The univocal identifier of the business activity.
Description	Description of the domain/activity.

### Scheduled tasks

In this section are described all the scheduled tasks running or just started.

These tasks are scheduled using the Chapter 20, "Introduction to Task Planner," on page 545 module.



### Configuration comparison

In this section, you can compare two different configurations, and check whether or not the changes performed in a specific configuration alter the model compared to the operating configuration.



In the **Configuration** tab are displayed all the configurations listed by the system.

By selecting the **Compare Configuration** pane and choosing the **Comparative Configuration**, in the **Configurations** tab on the right is displayed the information about the configuration users and the entitlement analysis.

The  icon shows that the analysis completed successfully, the  icon shows that the analysis failed. The bordered green configuration is the operating configuration information.

In the list below are described the main operations related to the mitigation controls:

- Configurations
- Comparison Dashboards
- Comparison Details

## Comparison dashboards

Four different default dashboards of two configurations are displayed.

- **Conflicting Business role**
- **Conflicting IT role**
- **Conflicting Permission**
- **Conflicting User**

These dashboards show the structure of the compared configuration.

## Comparison details

In this section you can compare detailed reports on paired configurations.

In this situation, more information is provided about changes of numbers and types of conflicts on a single ARC model entity present in both configurations. The **Comparison Details** tab allows you to access the following two tabs:

- **User**
- **Entitlement**

In the **User** tab, you can define the filters to identify the set of conflicting users registered on the system, according to the attributes indicated in the table below:

Conflicting user filters	
Filter	Description
Organization Unit	OU to which the user belongs.
Hierarchy	Selecting this check box, sets the operation to start executing from the root of the selected OU and down through the hierarchy originating from that root.
Search Identity	This field can host the name, and the surname or the User ID.
DN	Distinguished name of the user.

Conflicting user filters		
Filter	Description	
Conflicting status	All	All possible conflicting states.
	Unaltered	The user remains with the same number of risks in both configurations.
	Altered	Every user with a modified number of risks ( <b>Enhanced, Worsened</b> ).
	Enhanced	In the operating configuration, the user has a lower number of risks compared to the comparative configuration.
	Worsened	In the operating configuration, the user has a higher number of risks compared to the comparative configuration.

The risk level distribution provides a view of the qualitative mix of risk levels among the total number of risks.

For example: a user has 11 total risks, 4 have a low risk level and 7 have a high risk level. Therefore, the user is characterized by the low/high qualitative mix of risk levels.

In the **Entitlement** tab, you can define the filters to identify the set of conflicting entitlements registered on the system, according to the attributes indicated in the table below:

Conflicting entitlement filters	
Filter	Description
Type	Choose one of the following type of entitlement: <ul style="list-style-type: none"> <li>• Permission</li> <li>• IT role</li> <li>• Business role</li> </ul>
Application	Application name by which the conflicting entitlements are filtered.
Name	Entitlement name.

Conflicting entitlement filters		
Filter	Description	
Conflicting status	All	All possible conflicting status.
	Unaltered	The entitlement remains in a conflicting status with the same qualitative mixed conflict level values (High, Medium, Low), in both configurations.
	Altered	Every user with a modified number of risks ( <b>Enhanced</b> , <b>Worsened</b> ).
	Enhanced	In the operating configuration, the entitlement has a lower number of risks compared to the comparative configuration.
	Worsened	In the operating configuration, the entitlement has a higher number of risks compared to the comparative configuration.

The concept of risk level distribution, which was addressed in the **User** tab, applies also here.

## Report

You can request and download reports.

Scheduling and downloading are the main functions in Reports.

- Request schedules reports.
- Download downloads reports.

For unauthorized users, this menu is not available.

---

## Tools

Tools help to speed up and facilitate some tasks.

Several functions speed up and facilitate the tasks of the following modules:

- Refresh Violations Detection
- Bulk Data Load

### Bulk Data Load

You can load large amounts of data.

You can run several types of bulk data-loading in the AG Core database.



The **Action** tab (left) shows the supported operations.

After you select an operation in **File Batch**, click one of the following options:

- **Download** to get a template (XLS file), related to the currently selected operation.
- **Browse** to search in the file system for an XLS file for the selected loading operation.

When the operation is completed, an information record is appended in the lower-right pane to the list of the previously completed operations.

In the same pane, you can click:

- **Input File**  to get the file used in the operation.
- **Log File**  to get the operation report.

The following procedures are available:

- Add Permission to Activity
- Add Permission to Domain
- Remove Permission from Activity
- Insert Activities Hierarchy
- Risk Definition
- Remediations to Risks
- Remove Risks
- Remove Activities
- Business Activity Mapping Bulk Load
- Business Activity Mapping Import

A generic record track distinguishes between **Mandatory** and **Optional** fields.

If a Mandatory field is empty or populated with unexpected values, the row is skipped unless specified otherwise in the documentation.

According to the data load behavior, populating an Optional field with unexpected or wrong values could cause a row to be skipped.

Here the procedure for running a bulk data load.

### Add permission to activity record track

This batch procedure can be used to aggregate a permission to an activity. It verifies that the mandatory fields are populated.

Add permission to activity track		
Information	Description	Validation
APPLICATION	Application name	Mandatory
PERMISSION_TYPE	Permission type identifier	Optional
PERMISSION	Permission name	Mandatory
PERMISSION_CODE	Univocal identifier of a permission	Optional
ACTIVITY_REF	Reference to activity on sheet 2 of the XLS file	Mandatory
CODE	Activity code	Mandatory
ACTIVITY	Activity name	Mandatory

Add permission to activity track		
Information	Description	Validation
ENVIRONMENT	Environment name	Optional

The XLS source file is organized into two sheets.

The ACTIVITY\_REF column on sheet 1 refers to the same column on sheet 2.

Values possibly contained in the ACTIVITY\_REF column on sheet 1 must also be present in the same column on sheet 2. Conversely, the ACTIVITY\_REF column on sheet 2 might contain values that are not present or referenced in sheet 1.

The APPLICATION field contains the name of the application.

If there is no such application, the row is skipped.

The PERMISSION field contains the name of the permission. A permission with this name, that is aggregated to the above application, must exist. If not, the row is skipped.

PERMISSION\_TYPE is an optional field.

However, according to the best practices, this value should be specified to avoid the ambiguity of permissions having the same name (PERMISSION) but different types (PERMISSION\_TYPE) .

The following scenario is correct:

PERMISSION = P1 ; PERMISSION\_TYPE = T1

PERMISSION = P1; PERMISSION\_TYPE = T2

but

PERMISSION = P1 ; PERMISSION\_TYPE = T1

PERMISSION = P1; PERMISSION\_TYPE =undefined

is ambiguous, resulting in the record being skipped and the logging of a warning message:

Permission not unique.

You can specify PERMISSION\_CODE and leave empty APPLICATION, PERMISSION\_TYPE and PERMISSION.

Conversely, PERMISSION\_CODE can be empty if you fill the columns APPLICATION, PERMISSION\_TYPE and PERMISSION.

Activity existence is verified using the given code (CODE field) and name (ACTIVITY field). If there is no such activity, the row is skipped.

The optional ENVIRONMENT field contains the name of the environment.

Environment existence is verified using the given name.

If the ENVIRONMENT field is empty, the default environment is used.

### Add permission to domain record track

This batch procedure can be used to aggregate a permission to a domain. It verifies that the mandatory fields are populated.

Add permission to domain track		
Information	Description	Validation
APPLICATION	Application name.	Mandatory
PERMISSION_TYPE	Permission type identifier.	Optional
PERMISSION	Permission name.	Mandatory
PERMISSION_CODE	Univocal identifier of a permission.	Optional
DOMAIN	Domain name.	Mandatory
ENVIRONMENT	Environment name.	Optional

The APPLICATION field contains the name of the application. If there is no such application, the row is skipped.

PERMISSION\_TYPE is an optional field.

However, according to the best practices, this value should be specified to avoid the ambiguity of permission having the same name (PERMISSION) but different types (PERMISSION\_TYPE).

The following scenario is correct:

PERMISSION = P1; PERMISSION\_TYPE = T1

PERMISSION = P1; PERMISSION\_TYPE = T2

but

PERMISSION = P1; PERMISSION\_TYPE = T1

PERMISSION = P1; PERMISSION\_TYPE = undefined

is ambiguous, resulting in the record being skipped and the logging of a warning message:

```
-Permission not unique-.
```

The PERMISSION field contains the name of the permission.

A permission with this name, that is aggregated to the above application, must exist. If not, the row is skipped.

You can specify PERMISSION\_CODE and leave empty APPLICATION, PERMISSION\_TYPE and PERMISSION.

Conversely, PERMISSION\_CODE can be empty if you fill the columns APPLICATION, PERMISSION\_TYPE and PERMISSION.

The optional ENVIRONMENT field contains the name of the environment. The environment existence is verified using the given name. If the ENVIRONMENT field is empty, the default environment is used.

The DOMAIN field contains the name of the domain. Domain existence is verified using the given domain name. If no such domain exists, it is created in the default environment.

### Remove permission from activity record track

This batch procedure can be used to remove a permission from an activity.

The structure of the record track is described in Add Permission to Activity.

Also in this case, you can specify PERMISSION\_CODE and leave empty APPLICATION, PERMISSION\_TYPE and PERMISSION.

Conversely, PERMISSION\_CODE can be empty if you fill the columns APPLICATION, PERMISSION\_TYPE and PERMISSION.

### Insert activity hierarchy record track

This batch procedure can be used to insert activities. It verifies that the mandatory fields are populated.

Insert activity hierarchy track		
Information	Description	Validation
CODE	Activity code	Mandatory
ACTIVITY	Activity name	Mandatory
ENVIRONMENT	Environment identifier name	Optional
DESCRIPTION	Activity description	Optional
PARENT_CODE	Activity parent code	Optional

The ENVIRONMENT field is optional. If this field is populated, the existence of an environment with the specified name is verified. Otherwise, the row is skipped. If left blank, the default environment is used (Working Environment).

The CODE and ACTIVITY fields contain the activity code and name, respectively.

The existence of an activity with the given code is verified. If the given name does not match the activity name, the row is skipped. If there is no such activity, it will be inserted.

The PARENT\_CODE field is used for positioning the activity in the hierarchy.

If this field is left blank, the activity will be inserted as a child of the root activity.

If there is no such activity associated to the given parent code, the activity is inserted as a child of a technical activity called "Undefined", which will be created as needed.

CODE	ACTIVITY	ENVIRONMENT	DESCRIPTION
AA1234	Test Web 1	ESERCIZIO	Description Test We
BB1234	Test Web 2	ESERCIZIO	Description Test We
CC1234	Test Web 3	ESERCIZIO	Description Test We
DD1234	Test Web 4	ESERCIZIO	Description Test We
EE1234	Test Web 5	ESERCIZIO	Description Test We

### Risk definition record track

This batch procedure can be used to insert risks and aggregate activities to them. It verifies that the mandatory fields are populated.

Risk definition track		
Information	Description	Validation
RISK_NAME	Risk identifier name	Mandatory
DESCRIPTION	Risk description	Optional
TYPE	Risk type. Default values are: <ul style="list-style-type: none"> <li>• SOD</li> <li>• RISK</li> </ul>	Mandatory
LEVEL	Risk level. Allowed values are: <ul style="list-style-type: none"> <li>• HIGH</li> <li>• MEDIUM</li> <li>• LOW</li> </ul>	Mandatory
ENVIRONMENT	Environment identifier name	Optional
ACTIVITY_CODE	Activity identifier code	Mandatory
HIERARCHY	Hierarchy check. Default values are: <ul style="list-style-type: none"> <li>• YES</li> <li>• NO</li> </ul>	Optional

The ENVIRONMENT field is optional. If this field is populated, the existence of an environment with the specified name is verified. Otherwise, the row is skipped. If left blank, the default environment is used.

The RISK\_NAME field contains the name of the risk. If this field is left blank, the row is skipped. Otherwise, if no such risk exists in the selected environment, it is created. The TYPE and LEVEL fields are used for risk insertion.

SOD and RISK are the default values for the TYPE field. The operator can use previously inserted custom risk types. If the custom risk type is not found in the system, the row is skipped and the risk is not inserted.

HIGH, MEDIUM and LOW are default values for the LEVEL field. Anything different from these values automatically sets the risk level to LOW.

To aggregate activities to the risk, the existence of the activity specified in the ACTIVITY\_CODE field is verified. If the field is blank, the row is skipped.



If no such activity is found, aggregation is skipped but the risk is still inserted.

The HIERARCHY field is an optional field that can be used to specify whether the activity-risk aggregation is hierarchical or individual.

If the field value is set to YES, the aggregation involves the specified activity and its subbranches.

If the field value is set to NO, the aggregation involves only the specified activity.

RISK_NAME	DESCRIPTION	TYPE	LEVEL	ENVIR
Risk Test 5	Description Test 5	SOD	HIGH	
Risk Test 1	Description Test 1	SOD	MEDIUM	
Risk Test 2	Description Test 2	RISK	LOW	ESERC
Risk Test 3	Description Test 3	SOD	HIGH	
Risk Test 4	Description Test 4	RISK	MEDIUM	ESERC
Risk Test 4		SOD	MEDIUM	
Risk Test 4		RISK	MEDIUM	

### Remediation to risk record track

This batch procedure can be used to insert remediation aggregated to the risk. It verifies that the mandatory fields are populated.

Remediation to risk track		
Information	Description	Validation
REMEDATION	Remediation name	Mandatory
CODE	Remediation code	Mandatory
DESCRIPTION	Remediation description (short)	Optional
EXT_DESCR	Remediation description (extended)	Optional
RISK_NAME	Risk name	Mandatory
ENVIRONMENT	Name of environment in which the risk has been defined	Optional

The CODE and REMEDIATION fields contain the remediation code and name, respectively.

The existence of a remediation with the given code is verified. If there is no remediation, it will be inserted.

In the RISK\_NAME field, enter the risk name. If there is no existing remediation with this name, the record is skipped.

The ENVIRONMENT field is optional. If this field is populated, the existence of an environment with the specified name is verified. Otherwise, the row is skipped.

If left blank, the default environment is used (Working environment).

### Remove risk record track

This batch procedure can be used to delete risks. It verifies that the mandatory fields are correctly populated.

Remove risk track		
Information	Description	Validation
RISK_NAME	Risk identifier name	Mandatory
DESCRIPTION	Risk description	Not used
TYPE	Risk type	Not used
LEVEL	Risk level	Not used
ENVIRONMENT	Environment identifier name	Optional
ACTIVITY_CODE	Activity identifier code	Not used
HIERARCHY	Hierarchy check	Not used

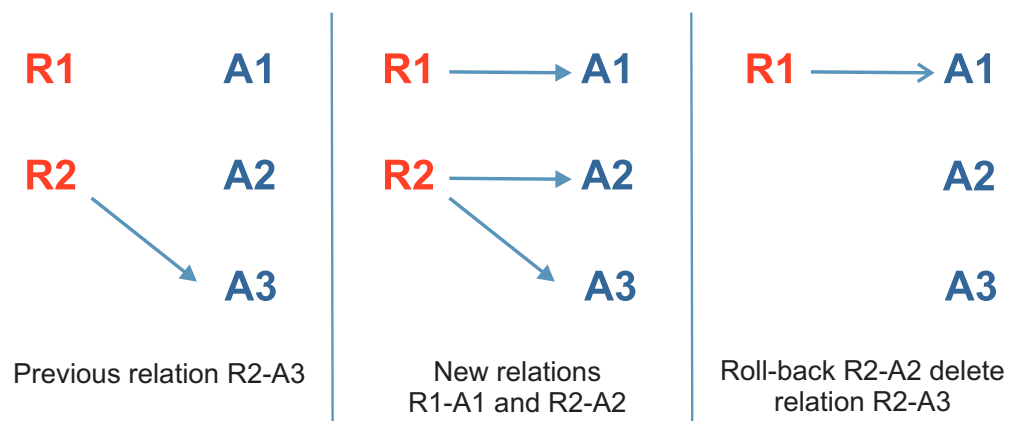
The ENVIRONMENT field is optional. If this field is populated, the existence of an environment with the specified name is verified. Otherwise, the row is skipped. If left blank, the default environment is used.

The RISK\_NAME field contains the name of the risk. If the risk does exist in the selected environment, it is deleted along with all its activity aggregations.

**Note:**

The record track indicated in the table above is the same as that of the risk definition record track. It is not recommended to use this bulk procedure as a rollback action for the risk definition procedure.

The figure below displays a tricky situation where the removal of risk R2 can have a deceptive side effect:



A rollback action on R2 (on R2-A2 just defined) has a side effect on a relation R2-A3, which was already present before the definition of R2-A2 occurred.

### Remove activities record track

This batch procedure can be used to delete activities. It verifies that the mandatory fields are correctly populated.

<b>Remove activities track</b>		
<b>Information</b>	<b>Description</b>	<b>Validation</b>
CODE	Activity code	Mandatory
ACTIVITY	Activity name	Not used
ENVIRONMENT	Environment identifier name	Optional
DESCRIPTION	Activity description	Not used
PARENT_CODE	Activity parent code	Not used

The ENVIRONMENT field is optional. If this field is populated, the existence of an environment with the specified name is verified. Otherwise, the row is skipped. If left blank, the default environment is used.

The CODE field contains the code of the activity to delete. If the existence of an activity with the given code is verified, the activity is deleted.

### **Business activity mapping bulk load record track**

This process provides mapping between activities and permissions.

Permissions can be aggregated into groups.

Permissions of a group can be associated in a AND/OR logical relation.

Groups can be nested up to any level and also nested groups can be associated in a AND/OR logical relation.

This batch procedure can be used to load permissions, permission rights, groups, subgroups, group AND/OR types and group hierarchies.

It can be used:

- After you install Identity Governance and Intelligence.
- At the start up of the project.
- Any time during the production lifetime.

Data imported to Identity Governance and Intelligence is automatically converted into a mapped structure connected to the already available business activity tree structure.

Data should be loaded into an empty structure: if there are some mapping already defined, this will not be removed. The result will be the merging of the two structures.

The business activity tree must be already defined, and all activities linked by the activity business mapping must already be in the system.

If an activity business mapping object in the input excel file (such as an activity or a permission) is not present in the already available target environment, an exception is generated, and the loading process fails.

If there are conflicts with existing objects in the TT, the process does not overwrite the existing structure but renames the conflicting objects to allow anyway the loading of the TT structure. The result is the integration of the two TT structures.

The process verifies that the mandatory fields are populated.

Technical transformation bulk load track		
Information	Description	Validation
ENVIRONMENT	Working environment on which the TT structure is loaded.	Mandatory
ACTIVITY_CODE	Activity (from the activity tree) of the TT to be loaded.	Mandatory
ROOT	If a group hierarchy is present, the root group of the hierarchy.	Optional
COND	And/Or condition. The value OR is the default, also for "single" items.	Optional
ENT_REF	Unique reference of the item in this position.	Mandatory
ENT_PARENT_REF	Direct hierarchical parent of the item.	
TYPE	Allowed values are: <ul style="list-style-type: none"> <li>• Group</li> <li>• Permission</li> <li>• Right</li> <li>• Right Value</li> </ul> For permissions directly linked to the activity, this field must be empty.	Mandatory
PERMISSION	Name of the permission.	Optional
PERMISSION_APP	Application related to the permission. It is empty for groups, subgroups, rights and right values.	Optional
PERMISSION_TYPE	Permission type (as configured in AG Core). It is empty for groups, subgroups, rights and right values.	Optional
RIGHT	Right possibly associated to the permission (if any).	Optional
RIGHT_VALUE	Actual value of the right (if any).	Optional

The ROOT column can be empty only for permissions that are directly linked to the activity.

For data linked to the activity through a structure, the name of the first level group ( the group directly linked to the activity) must be set.

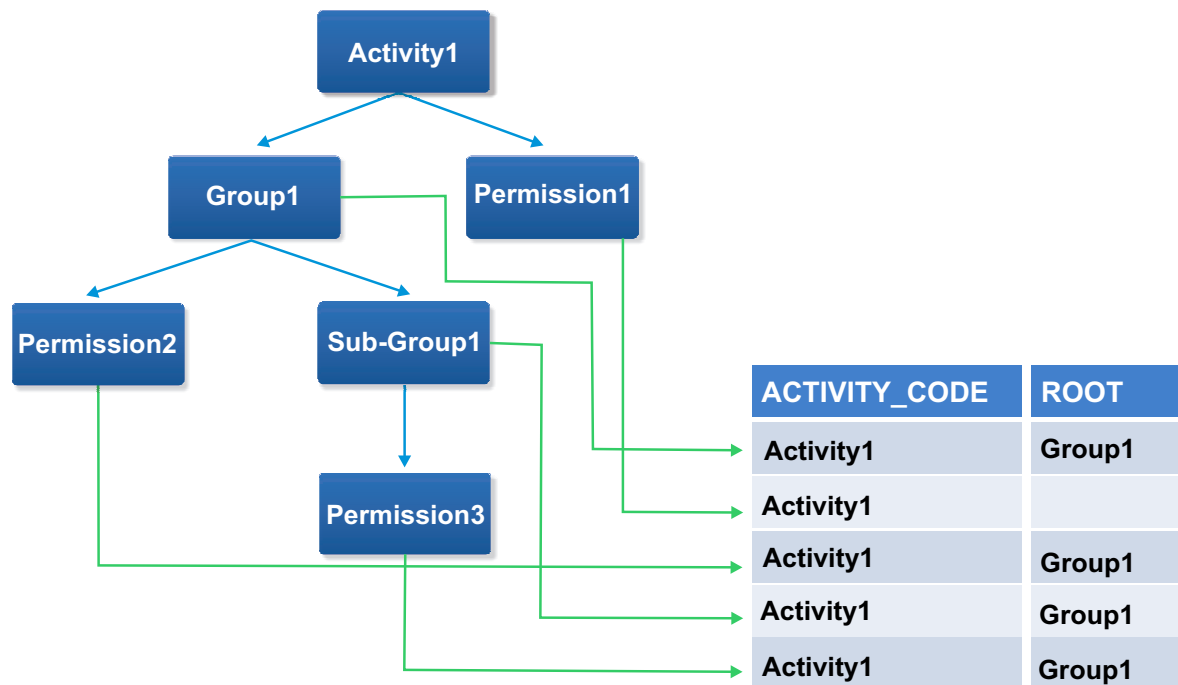


Figure 51. Graphical representation of Activities-permissions mapping (1).

The COND column can be empty only for permissions that are directly linked to the activity.

In case of a group and a subgroup, the cell content must reflect the selected logic: AND or OR.

For permissions linked to a group or subgroups and for rights and right values, the cell must be set to OR.

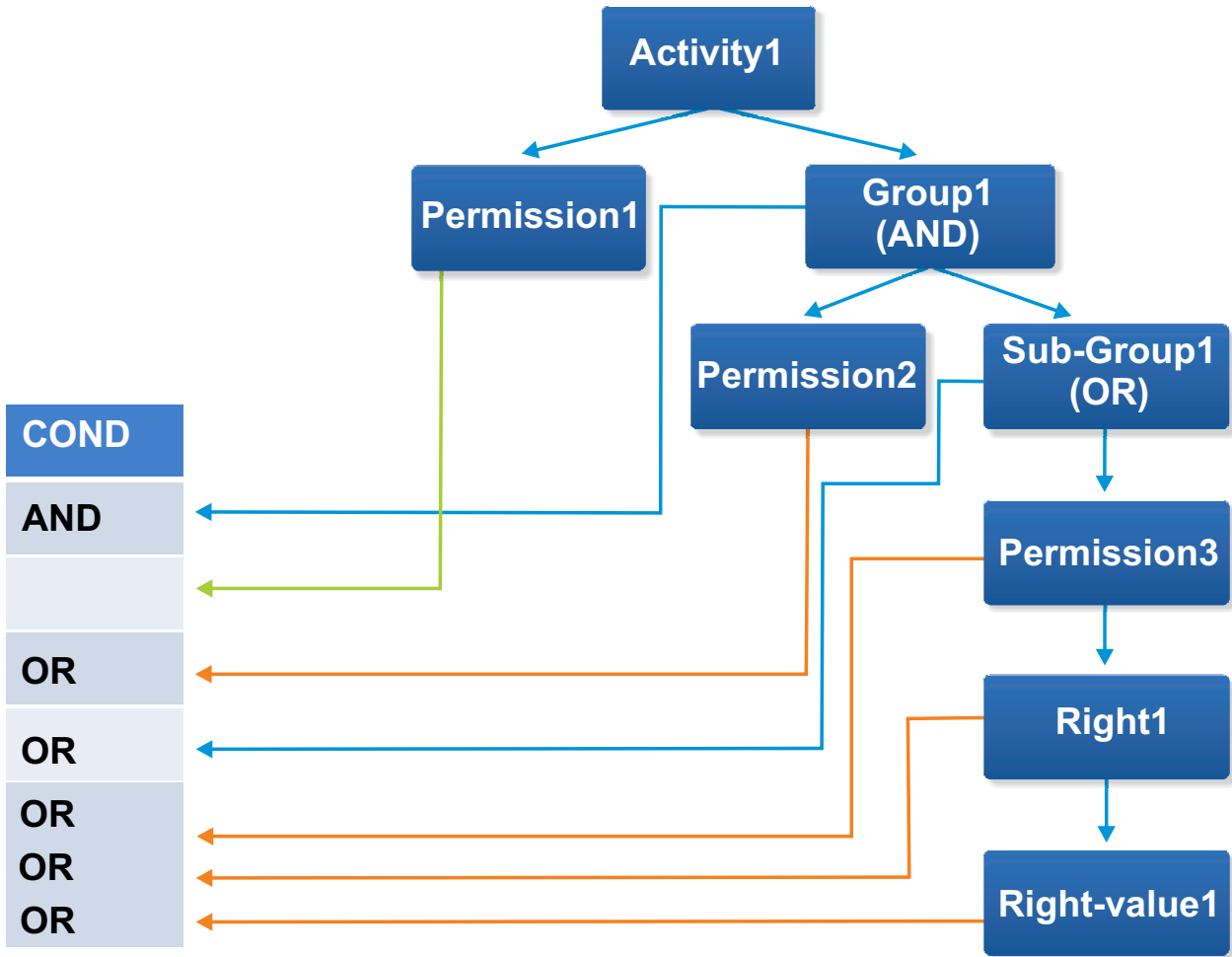


Figure 52. Graphical representation of Activities-permissions mapping (2).

ENT\_REF is a unique reference of an item (Group, subgroup, permission, right or right value)

It is mandatory as it is required to identify that item in that precise position inside the TT structure.

For example *Permission1* (PERMISSION column) might be present in several parts of the tree, while the ENT\_REF info allows the precise identification of *Permission1* in that specific position.

According to the value of TYPE, is mandatory to fill the columns shown in the table below:

Column set according TYPE	
Filter	Column set
Group	ENT_REF
Permission	ENT_REF - PERMISSION
Right	ENT_REF - RIGHT
Right Value	ENT_REF - RIGHT VALUE

To check on the outcome of a bulk load, in the ARC web interface:

1. Select Manage/Business Activities
2. Select the ACTIVITY\_CODE activity
3. In the right frame, select the **Linked Permissions** tab
4. Check if the permissions/groups structure linked to that activity is as expected.

If you need to, fix exceptions and reload data according to the same record track.

Generally, the most common error is:

Object not found

that refers to a missing permission of an activity.

### **Business Activity Mapping import record track**

This process needs to be fed by the output file of the related report Export Tech Transformation.

This report is reachable by clicking **Monitor > Reports** in the web interface.

In the left frame, select **Status > Export > Export Tech Transformation** and run the report shown in the wizard in the right frame.

The output file (Export Tech Transformation[DD-MM-YYYY HH-MM-SS].XLSX) can be used for importing a set of Business Activity Mapping data from a system to another.

## **Refresh violation detection**

In this section, you can check the progress of the analysis of two specific sets of model entities: users and roles.

This analysis is performed in the operating configuration currently selected, therefore it is executed on all domains related to this configuration.

The configuration can be changed by performing the Configuration operation, selecting **Actions > Current**.

A configuration can comprise several domains. A domain can have several activities aggregated to it, and every activity is aggregated to a set of permissions.

After any modify of the domain structure, you have to run a complete analysis on all available entities before any refresh violation detection operation.

This will upgrade the conflicting relationships between the model elements on all domains related to the mentioned configuration.

All operations available here can be carried out simultaneously. The analysis can be started (**Start** button) or stopped (**Stop** button).

**Note:** If this operation is not active (click **Refresh** to update the green progress bar), the **Task Housekeeping** might be stopped (see the administration module **Task Planner**, by selecting **IBM Security Identity Governance Task Planner > Manage > Task**).





---

## Chapter 15. Introduction to Process Designer

The PD module helps you design and define the authorization processes.

Process Designer provides a modeler capable of outlining every type of workflow finalized for implementing custom authorization processes, that can be accessed from the Access Requests front end module of IBM Security Identity Governance and Intelligence.

The Process Designer strength lies in its ability to describe an authorization process using an instrument of visual design, that supports the administrator from the beginning of the process to the end, which is marked by the automatic production of front end graphical pages associated with every single activity.

This module, together with Access Governance Core (AGC), which implements the role-based access control engine of IBM Security Identity Governance and Intelligence, provides all the tools and functions needed for managing effectively:

- Requests to access the system application
- Allocation/revocation of authorization profiles
- Password lifecycle
- Notifications that are sent to users during different phases of the authorization process
- Temporary delegations of personal roles associated with users of the system
- Definition of the visibility range associated with an administrative figure.

Process Designer is a highly configurable module that can be used by system integrators or administrators of an organization to plan an authorization workflow.

For every administrative figure (IAM actors), it is possible to define a visibility range that only includes parts of the organization (hierarchy of organizational units and its associated users) that are directly involved and the applications with which it can deliver the necessary authorization.

The integrated workflow engine in this module enables you to create appropriate combinations of authorization actions, with the aim of defining groups of permissions (condensed into roles) for every single user registered by the system.

You can create approval processes for the allocation or revocation of a user role, established by different intermediate levels, each one pertaining to a distinct actor within the process.

Access Requests directly communicates with the Access Governance Core for the allocation and the revocation of user roles and for the propagation of permissions on potential target systems.

An example of the structure of a possible authorization flow, implemented by Process Designer, is shown in the following diagram:

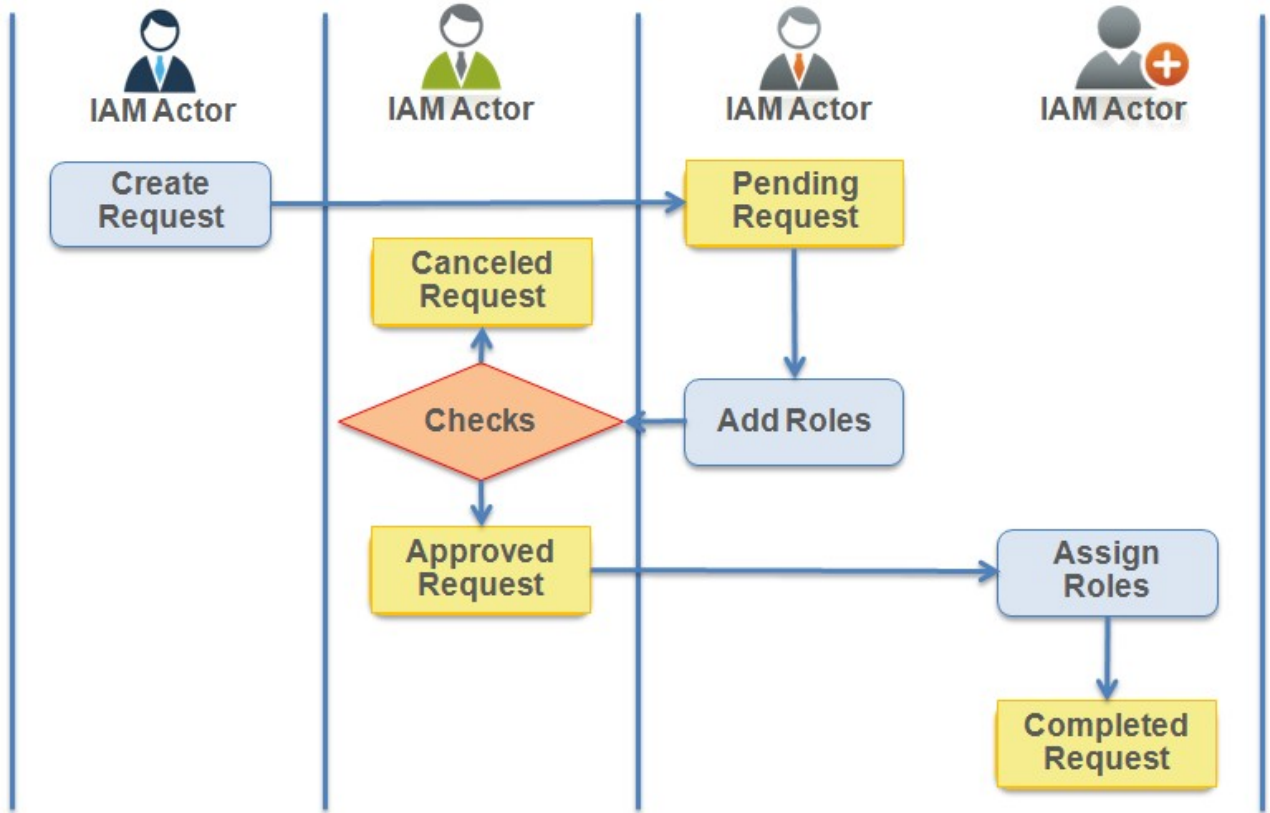


Figure 53. Workflow based on four IAM actors

## Authorization process roadmap

The provisioning of access permissions to resources and applications of an organization require a well-defined authorization procedure.

This procedure begins with the generation of a request that some IAM actors take responsibility for; they, in turn, provide additional information and/or authorizations until a final set of conditions is confirmed, according to which the request is processed.

After that, the final user receives the permission (or has it revoked) to access the relevant applications/resources.

In the role-based access control IAM model developed by the IBM Security Identity Governance platform, enabling/disabling user access to an application/resource matches with the allocation/revocation of one or more roles for that user.

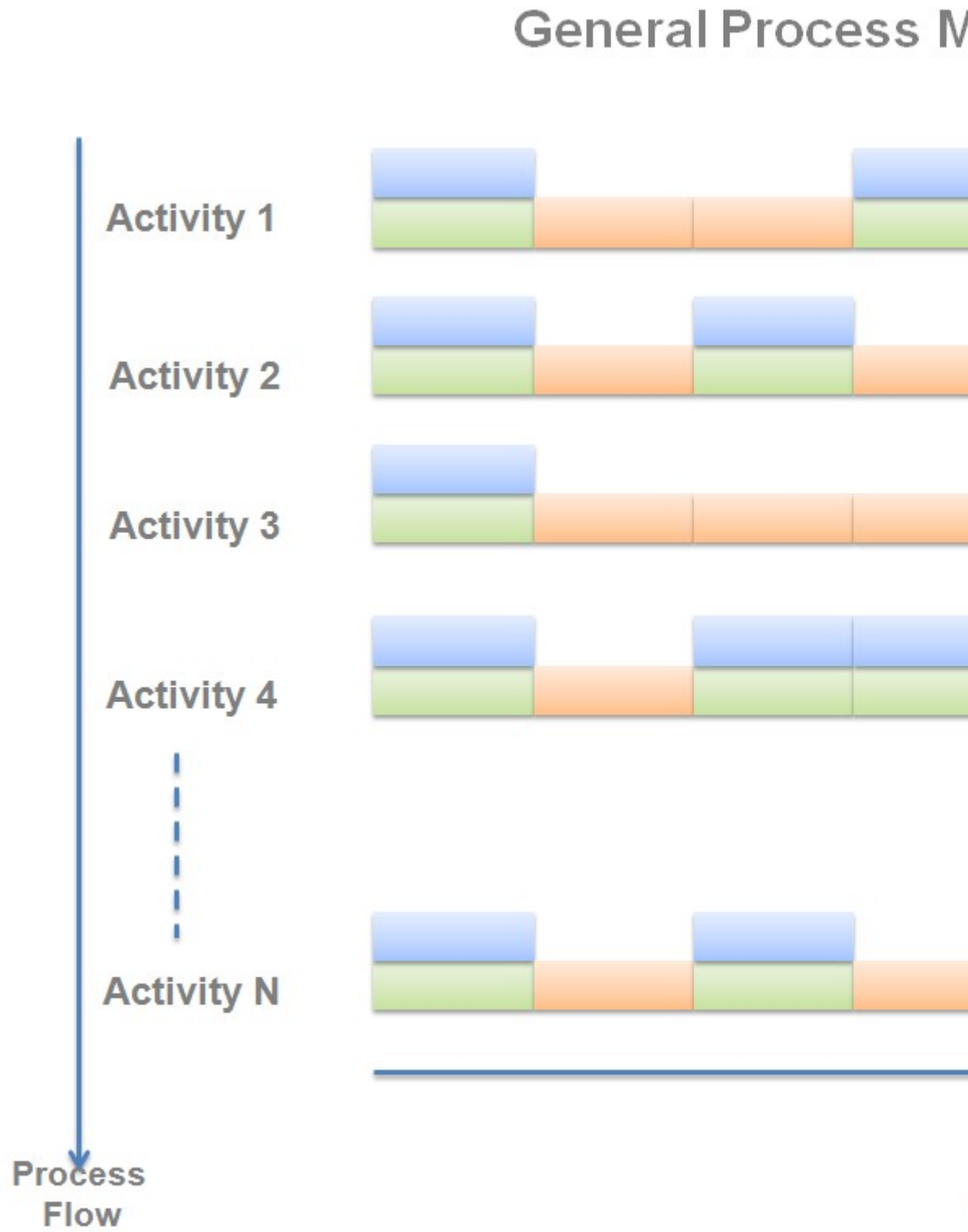
This authorization procedure is structured as a process, which consists of N activities, that in turn run the lifecycle of a request.

From the administrator point of view, designing a process means design a sequence of steps.

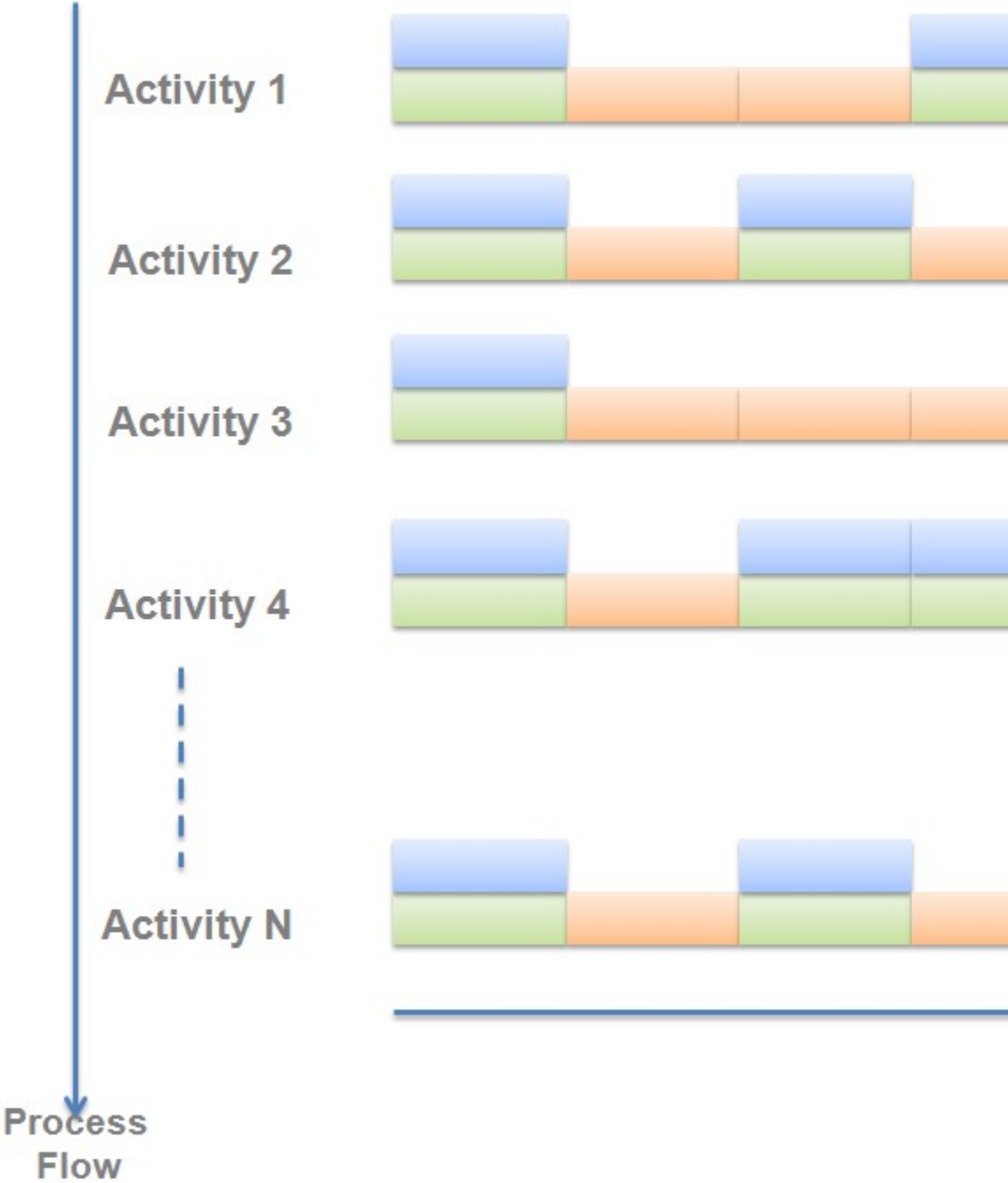
Each step matches with the production of an activity.

Every activity will be supported by one or more web pages which represent the graphical front end for the I/O operation which the activity needs. An activity is linked to a role that detects the IAM actor responsible for that activity.

The result of this work is represented by an authorization workflow, conceptually displayed in the following diagram:



# General Process



Using Process Designer visual wizard, you can define all aspects of an authorization process.

The list below suggests a reference roadmap that follows a best practice to define a process:

1. Define a set of activities.
2. Define a process, structured as a group of activities.
3. Associate an Admin role to each Activity.
4. Associate the operating menu with each bundle role-activity.
5. Change the process status and setting it on line.

---

## Modeling an activity

An activity is an aggregation of functional attributes.

An activity is characterized by a set of attributes that define all its aspects.

An activity can be schematically represented as a function with N attributes, depending on the value of its attributes:

$$\text{ACTIVITY} = f (\text{ATTR}_1, \text{ATTR}_2, \text{ATTR}_3, \dots, \text{ATTR}_N \dots)$$

The attributes can be classified as identifying attributes and operating attributes, as shown in the following table:

*Table 111. Activity attributes*

Attributes	Category	Description
Identifying attributes	Type	Type of process that involves the activity
	Mode	Category of action of the activity
	Name	Name of the activity
	Context	Set of homogeneous functions used to manage an authorization process
	Functionality	Name of the function related to the Context field set

Table 111. Activity attributes (continued)

Attributes	Category	Description
Operating attributes	Beneficiary	Visibility for users who are affected by the request
	Delegator	Visibility for users who delegated the request
	Application	Visibility set by application access. Only administrators with access to the specified applications can see the request.
	Entitlement	Visibility set by entitlement access. Only administrators with access to the specified entitlements can see the request.
	Request Scope	Type of request
	Required Data	Specifies data required for an activity
	Email Data	Specifies email template to use
	Entity Scope	Model entity scope of a specified activity

Use the Activity details pane to model activities.

## Type attribute

The Type attribute specifies the type of process to use with the activity.

Table 112. Type attribute values

Type	Description
Direct	Process that consists of a single EXE activity
Workflow	Process that consists of an appropriate set of GEN, AUTH and EXE activities
Escalation	Process that consists of an appropriate AUTH activity

## Mode attribute

The following table describes the Mode attribute:

Table 113. Mode attribute values

Category	Description
GEN: Generation	Generation request activity. This activity typically opens an authorization workflow.
AUTH: Authorization	Authorization activity. This activity is typically assigned to a IAG officer for authorizing a request.

Table 113. Mode attribute values (continued)

Category	Description
EXE: Execute	Activity that executes what was indicated in the previously authorized request or a one-shot action.

## Context attribute

The following table describes the context attributes of an activity:

Table 114. Context attribute values

Context	Description
Account Change	Related to account creation operations
Admin Access Change	Related to operations for the modification of the administrative role
Admin Delegation Change	Related to administration delegation operations
Delegation Change	Related to delegation renewal operations
User Management	Related to creating and modifying a model entity User
Entitlement Management	Related to creating and modifying a model entity Entitlement
Incompatibility Management	Related to incompatibility management operations
Request Report	Related to the request report operations
User Access Request	Related to the activities used to manage a user transfer

## Functionality attribute

Each Functionality value corresponds to a Context value, Type value, and Mode value.

Table 115. Functionality attribute values

Context	Type	Mode	Functionality	Description
Incompatibility Management	Escalation	AUTH	Authorize Incompatibility In Delegation	Authorize Incompatibility Request
Account Change	Workflow	GEN	Detailed Request	Account Change
	Workflow	AUTH	Request Authorization	Authorization
	Workflow	EXE	Request Execution	Account Change Assignment



Table 115. Functionality attribute values (continued)

Context	Type	Mode	Functionality	Description
<b>User Access Change</b>	Workflow	GEN	Formal Request	Formal Request
	Workflow	AUTH	Request Authorization	Request Authorization
	Workflow	AUTH	External Request Authorization	Authorize Request with external system
	Workflow	EXE	Request Execution	Role Assignment
<b>Admin Access Change</b>	Workflow	GEN	Formal Request	Formal Request
	Workflow	AUTH	Request Authorization	Request Authorization
	Workflow	EXE	Request Execution	Request Execution
<b>Delegation Change</b>	Workflow	GEN	Application Filtered Request	Delegation filtered by Application
	Workflow	AUTH	Request Authorization	Authorization
	Workflow	EXE	Request Execution	Delegation Assignment
<b>Admin Delegation Change</b>	Workflow	GEN	Formal Request	Formal Request
	Workflow	AUTH	Request Authorization	Request Authorization
	Workflow	EXE	Request Execution	Request Execution
<b>User Management</b>	Workflow	GEN	Insert User	Insert User Request
	Workflow	AUTH	Insert User	Insert User Request Authorization
	Workflow	EXE	Execute Insert User	Insert User Request Execution
	Workflow	GEN	Update User	Update User Request
	Workflow	AUTH	Update User	Update User Request Authorization
	Workflow	EXE	Execute Update User	Update User Request Execution

Table 115. Functionality attribute values (continued)

Context	Type	Mode	Functionality	Description
Entitlement Management	Workflow	GEN	Insert Entitlement	Insert Entitlement Request
	Workflow	AUTH	Authorize Insert Entitlement	Authorize Insert Entitlement Request
	Workflow	EXE	Execute Insert Entitlement	Execute Insert Entitlement Request
	Workflow	GEN	Update Entitlement	Update Entitlement Request
	Workflow	AUTH	Authorize Entitlement Update	Authorize Entitlement Update Request
	Workflow	EXE	Execute Insert User	Insert Entitlement Request
Request Report	Direct	EXE	Request Report	Request Report
	Direct	EXE	Daily Work	Daily Work

## Operating attributes

Operating attributes determine the behavior of an activity.

Operating attributes are shown in the following tabs:

- Beneficiary
- Delegator
- Application
- Entitlement
- Request Scope
- Required Data
- Email data
- Entity Scope

### Beneficiary tab

This attribute specifies sets of users associated with different scopes in the organizational structure.

Table 116. Visibility levels by Beneficiary

Visibility type		Description
By Organization Unit Tree	All Users	Visible to all the OUs in the realm (all users in the organization)
	Actor	Visible only to the IAM actor involved in the activity (logged in user)
	All Users belonging to an OU	Visible to a selected OU, thus to the users associated with that OU
	All Users belonging to an OU (including hierarchy)	Visible to a selected OU and the entire sub-tree, thus to all users associated with the hierarchy
	All Users belonging to logged OU	Visible to all OUs that are visible to the IAM actor involved in the activity
	All Users belonging to logged OU (including hierarchy)	Visible to all OUs visible to the IAM actor involved in the activity and to the entire sub-tree, thus to all users associated with the hierarchy
	All Users belonging to logged Hierarchy	Visible to all groups of a specific hierarchy that are visible to the IAM actor involved in the activity

### Delegator tab

A delegator assigns its own access rights to another user for a limited time. The scope criteria are the same as the ones described in Beneficiary.

This type of visibility is involved in processes of delegation.

### Application tab

An application represents an external system connected to the IAM system. A single target (for example, Active Directory) can manage more than one application.

An IAM actor in the authorization process usually acts only on a subset of applications (Application scope).

The Process Designer administrator sets the application visibility for every IAM actor involved in the process.

The following table lists the different levels of user visibility that you can specify on applications:

Table 117. Visibility levels by application

Visibility type	Description
All Applications	All applications registered

Table 117. Visibility levels by application (continued)

Visibility type	Description
<b>Specific Applications</b>	Group of applications selected by clicking <b>Specific Applications</b>
<b>User owned Applications</b>	Owned applications only

## Entitlement tab

Entitlements determine access to applications.

An IAM actor that manages the authorization process, usually acts only on a subset of entitlements (entitlement scope).

The Process Designer administrator sets the entitlement visibility levels for every IAM actor involved in the process.

Table 118. Visibility levels

Visibility type	Description
<b>All Entitlements</b>	All entitlements registered
<b>Specific Entitlements</b>	A group of entitlements selected by clicking <b>Specific Entitlements</b>
<b>User owned Entitlements</b>	Owned entitlements only

## Request scope tab

For some activities, you can select **Request type** and **Request status** as additional filters to use. They specify the **Request scope**. The activity can only manage requests of the indicated type and status.

If the **Ownership** check box is selected, the IAM actor can manage owned requests.

A parent request can generate child requests. Each has its own independent flow and status. The parent request state depends on the state of its child requests.

The parent request is completed if its child requests have been completed. The parent request status is partially completed until the child requests are completed.

## Required data tab

Data needed to configure the activity is specified in the **Required Data** tab.

The filter value is set in the **Required Data Value** field.

Table 119. Activity identifiable attributes: required data

Field	Description
<b>Active Data</b>	Check box to activate the data filter
<b>Required Data</b>	Name of the data filter
<b>Required Data value</b>	Value of the data filter. The value can be edited
<b>Description</b>	Description of the data filter

The required data depends on the activity that you are configuring.

Table 120. Required data items

Required Data	Assignable Values	Description
<b>Role Operation</b>	<ul style="list-style-type: none"> <li>• Assign</li> <li>• Remove</li> <li>• Renew</li> </ul>	Select the operation related to the entitlement involved in the activity.
<b>Account Operation</b>	<ul style="list-style-type: none"> <li>• Change Password</li> <li>• Suspend/Restore</li> </ul>	Select the operation related to the account password.
<b>User identification</b>	<ul style="list-style-type: none"> <li>• None</li> <li>• Security questions</li> <li>• Security questions or by other means</li> </ul>	<p>Specify how to verify the identity of a user needing a password change or account restoration.</p> <p><b>None</b> Is not verified. The identity verification step is omitted in Access Requests.</p> <p><b>Security questions</b> Must be verified by asking security questions and matching the answers with answers provided at first login.</p> <p><b>Security questions or by other means</b> Is verified either by the answer to security questions or by some other process. The wizard step that displays the questions in Access Requests includes also a check box that can be selected to skip the security questions.</p>
<b>Applicant's IGI password</b>	<ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul>	<p>If true, the applicant is requested to enter his/her password.</p> <p>In this context, applicant is a manager or Help-desk who makes the request for a user (the beneficiary).</p>

Table 120. Required data items (continued)

Required Data	Assignable Values	Description
<b>Change password mode</b>	<ul style="list-style-type: none"> <li>Entered by applicant</li> <li>Entered by applicant with no show/hide option</li> <li>Created by system</li> </ul>	Select one of the following: <ul style="list-style-type: none"> <li>The applicant enters a new password for the beneficiary and:               <ul style="list-style-type: none"> <li>The password characters are concealed when the applicant types them.</li> <li>Applicant can choose between showing or hiding the password characters as they are being typed.</li> </ul> </li> <li>The password is created automatically when the applicant clicks <b>Generate</b>.</li> </ul>
<b>Email password to beneficiary</b>	<ul style="list-style-type: none"> <li>Do not email</li> <li>To editable address</li> <li>Only if address exists</li> </ul>	Specify a rule for emailing the new password to the beneficiary. The password: <ul style="list-style-type: none"> <li>Is not to be emailed. Other means of communication are used.</li> <li>Is to be emailed to an address that the applicant can enter or edit.</li> <li>Is to be emailed only if the beneficiary's email address is recorded.</li> </ul>
<b>Suspend/Restore account suspending codes</b>	<ul style="list-style-type: none"> <li>Authoritative</li> <li>Expire</li> <li>Maintenance</li> <li>Security</li> <li>Technical</li> <li>Terminated</li> </ul>	Select a subset of Account suspending codes to use.
<b>Entity Operation</b>	N.A.	Select the entity operation to use.
<b>Role Type Assignable</b>	<ul style="list-style-type: none"> <li>Business Role</li> <li>Application Role</li> <li>Permissions</li> <li>External Role</li> </ul>	Select the entitlement type to use.
<b>IT Autopopulate Operation</b>	<ul style="list-style-type: none"> <li>true</li> <li>false</li> </ul>	Autopopulate Application Entitlements.
<b>IT Open Filter Operation</b>	<ul style="list-style-type: none"> <li>true</li> <li>false</li> </ul>	Set open filter for Application Search form.
<b>Entity Data Type</b>	<ul style="list-style-type: none"> <li>Details</li> <li>Structure</li> </ul>	Select the entity data type to use.

Table 120. Required data items (continued)

Required Data	Assignable Values	Description
<b>Self Authorization</b>	<ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul>	If true, self authorization is enabled (when the beneficiary is the Authorizer).
<b>Branch one shot Authorization</b>	<ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul>	If true, one-shot authorization is enabled, otherwise parallel authorization (Business Role) is used.
<b>Split Entitlement</b>	<ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul>	If true, the entitlement involved in the request is split in its own Permissions.
<b>External Authorization</b>	Free text	External call for authorization. You can specify a ReST implementation with a URL or a Java implementation with a Java class name.
<b>Enable Like Mike</b>	<ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul>	If true, the AR workflow panel includes the ability to select Like Mike functionality. You can assign the entitlements of one user directly to another use.

## Email data tab

For some activities, you can define the action of sending an email.

In this tab click **Template email** to choose the email template to use. Click **Preview** to see the template. Templates are managed in **Access Governance Core > Configure > Email**.

## Entity Scope

For some activities of type GEN, if you choose the context **Entity Change**, you define the data model entity by clicking **Entity**.

Click **Repository** to define the target repository where you read the user attributes.

Repositories are managed in **Access Governance Core > Settings > User Virtual Attributes**.

When you choose a repository and click **Load**, repository attributes are shown at the bottom of the panel.

Table 121. Repository attributes

Attribute	Description
<b>Visibility</b>	If selected, the related field in the <b>Field</b> column is visible in output.
<b>Mandatory</b>	If selected, it is a mandatory field.

Table 121. Repository attributes (continued)

Attribute	Description
<b>Order</b>	Select a field and use the Up and Down arrows to position it in the list.
<b>Field</b>	Field to be shown/hidden. See <b>Visibility</b> .
<b>Localization</b>	All fields can be localized. For this localization task, see <b>Access Governance Core &gt; Settings &gt; Core Configuration &gt; User Virtual Attributes</b> .
<b>Default Value</b>	Select <b>Editable</b> to allow a user to specify a default value.
<b>Editable</b>	If selected, this field is editable in the output panel (Access Request activity).
<b>UI Rendering</b>	Specifies the rendering of the related <b>Field</b> . See <b>Access Governance Core &gt; Settings &gt; Core Configuration &gt; User Virtual Attributes</b> . The available controls are: <ul style="list-style-type: none"> <li>• <b>Textfield</b></li> <li>• <b>Textarea</b></li> <li>• <b>Checkbox (true, false)</b></li> <li>• <b>Checkbox (1, 0)</b></li> <li>• <b>Passwordfield</b></li> <li>• <b>Date</b></li> <li>• <b>Date-hours</b></li> <li>• <b>Date-hours-seconds</b></li> </ul>

## Manage

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

- Process
- Activity

## Activity

From this tab, you can define the activities that can be associated to a process.

To know the attributes of an activity, see Modeling an Activity.

In the **Activity** tab on the left, you can identify all the activities registered in the system.

To find a specific activity, click **Filter/Hide Filter** and use the filters described in the table below:

Activity filter	
Filter	Description
<b>Name</b>	Activity name



Activity filter	
Filter	Description
<b>Mode</b>	Activity mode: <ul style="list-style-type: none"> <li>• <b>Generation</b></li> <li>• <b>Authorization</b></li> <li>• <b>Execute</b></li> </ul>
<b>Type of Activity</b> (derived by the type of processes)	Activity type: <ul style="list-style-type: none"> <li>• <b>Direct</b></li> <li>• <b>Workflow</b></li> <li>• <b>Escalation</b></li> </ul>

In the same tab, from the **Action** menu, you can select the operations listed below:

- Synchronize all
- Copy
- Add
- Remove

## Synchronize all

The Process Designer and the Access Request modules use two different databases.

After defining the activities with the Process Designer, it is also necessary to propagate the changes to the Access Requests database.

Using the **Actions > Synch all** button, you can synchronize one or more activities, previously selected from the list shown in the left **Activity** tab.

## Copy

Use this function to clone an activity before modify it, rather than making changes to the original version of the activity.

When many changes are required in an activity, this option becomes less useful and it probably makes more sense to perform a Add operation.

Proceed as follows:

1. In the **Activity** tab, select the activity to be copied.
2. Click **Actions > Copy**
3. In the **Activity Copy** tab, edit at least the fields **Name** and **Description**.
4. Click **Save**.

## Add

The definition of an activity involves the definition of its identifying and operating attributes.

A solid knowledge of the concepts described in Modeling an Activity can facilitate this task.

Proceed as follows:

1. In the **Activity** tab, click **Actions > Add**

2. In the window Select Activity Modality, you can choose the type and mode, then click **Ok**.
3. In the upper side of the **Insert Activity** tabInsert Activity pane, set the required attributes. The selectable values of **Context** depend on the type and mode already set. Also, the **Functionality** value is filled according to the value specified in **Context** . For more details, see Modeling an Activity.
4. After the attributes have been defined, in the lower section of the pane the **Activity Scope** tabs are shown. This set of tabs can vary according to the selected activity, thus according to the couple **Context -Functionality**.
5. Click **Save**.

## Remove

Proceed as follows:

1. In the **Activity** tab, select the activity to be removed.
2. Click **Actions > Remove**.
3. Click **Ok** to confirm the operation.

### Note:

You cannot delete an activity already linked to a process.

The web interface shows a specific diagnostic message that informs you about the inability to remove the activity.

Before removing an Activity, can be useful to have a clear knowledge of how many processes hosts the Activity that you want remove.

After have selected the Activity in the left tab, click the **Processes using this activity** tab (right), where are listed all processes linked to the selected activity.

Clicking on **Show Process**, you are redirect on **Manage > Process** tab, for having the full view of the process and of the position of the activity into the process.

If you need to modify an activity, you can simply select the activity, modify its attributes into the **Activity details** tab and click on **Save**.

## Process



The design of an authorization process proceed with a visual tool assisted through a wizard.

For managing a process you need to be confident with several concepts.

In the **Process** tab, on the left, you can identify all the processes registered in the system.




A process is characterized by a set of main attributes, shown in the **Details** tab and described in the table below:

Process attributes	
Attribute	Description
Name	The name of the process. If the process name is in italics, the process is not synchronized.

Process attributes		
Attribute	Description	
<b>Code</b>	Numerical and univocal code associated to the process, for logging and reporting activities.	
<b>Context</b>	A context identifies a set of homogeneous functions used to manage an authorization process.	
<b>Type</b>	Workflow	A process composed of an appropriate combination of GEN, AUTH and EXE activities.
	Escalation	A process composed by a sequence of AUTH activities (at least, only one AUTH activity).
	Direct	A process composed of a single EXE activity.
<b>Status</b>	Off Line	 A process is <b>Off Line</b> during its initial planning stages, which include the design and configurations of activities, followed by the association of any activity with one or more IAM actors. From this state, the only transition allowed is to <b>On Line</b> state.
	On Line	A process is in this state when it is ready to be run. From this state, the only transition allowed is to <b>Maintenance</b> state.
	Maintenance	 A process is in this state when some modifications must be made to the starting structure of the process or to the configuration of one or more activities. From this state, the only transition allowed is to <b>On Line</b> state.

Three of these attributes (**Name**, **Type**, **Status**) are also used for filtering processes.

The available activity types that you can define for building a process, are described in the table below:

Activity block-types		
Icon	Type	Description
	Generation (GEN)	Request generation function to obtain something such as a VPN access, a role on a target system or an account or different credentials.
	Authorization (AUTH)	Serial approval function for a previously entered request.
	Execution (EXE)	Function that runs the requested operation.  Not used for target systems that are automatically synchronized with the IAM system; however, it is necessary if the activity on the target is manually fulfilled. The execution step automatically produces an event for the operator who manually acts on the target. This might be used to trigger external applications such as help desk applications.

In the **Process** tab, from the **Action** menu, you can select the operations listed below:

- Copy
- Add
- Remove
- “Export” on page 309
- “Import” on page 309
- Maintenance
- Online

**Note:** Copy and Add operations are especially involved in the configuration of a process.

## Remove

Proceed as follows:

1. In the **Process** tab, select the a Process to be removed.
2. Click **Actions** > **Remove**.
3. Click **Ok** to confirm the operation.

**Note:**

You cannot delete an **On Line** process.

## Export

Proceed as follows:

1. In the **Process** tab select the process to be exported.
2. Click **Actions** > **Export** button.
3. If the process is in status **On Line** or in **Maintenance**, in the Assign - Process name window are shown roles assigned to the activities; click **Ok**.
4. A system-based window opens and allows you to save/open the .zip file that contains the XML file that describes the process.
5. Click **Ok** in the window that shows the outcome of the operation.


## Import

Proceed as follows:

1. Click **Import** .
2. In the window Select file to be imported, click **Browse** and select the file to import.
3. Click **Ok** in the window that shows the outcome of the operation.


## Maintenance

Proceed as follows:

1. In the **Process** tab select a process.
2. If the process is **On Line**, click **Actions** > **Maintenance** button.
3. The status icon of the process is updated to  **Maintenance**.

## Online

Proceed as follows:




1. In the **Process** tab select a process.
2. If the process is in  **Maintenance**, click **Actions** > **On Line** button.
3. The status icon of the process is updated to **On Line**.


## Process configuration

The effective design of a process proceeds through the **Configuration tab**.

The available activities that you can use for building a process, are described next.

A **Workflow Process** is built with:

1. A starting GEN activity (block  ).
2. A free number (also 0) of AUTH activities (block  ).
3. A final and single EXE block (block  ).


A **Direct Process** is built with a single EXE block (block ).

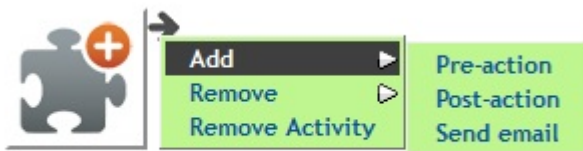
An **Escalation Process** is built with a free number (at least 1) of AUTH activities

(block ).

An extension can be added to each activity, which makes the behavior of an activity more flexible.

Different types of extensions are available.

Right-click the  button, to choose an extension option from the list on the right side of the process block:



#### Generate Revoke Request

Figure 54. Choose an activity extension on GEN block

In **Process > Actions** menu, select any of the operations listed below:

- Copy
- Add

### Copy

While the process is online, you may find it necessary to make changes to it.

It is best to always make a copy of the process before modifying it.

This function is useful so that you can clone a process that needs to be modified, rather than changing the process directly.

In this way, the original process can be maintained online, while you modify the copied instance.

**Note:** When a process is copied, its activities are copied accordingly.

Copying a process does not include:

- A copy of the roles associated with activities that form a process (see **Process > Assign**).
- A copy of the user menu associated with roles and activities (see **Configure > Menu**).

For this reason, after copying a process ensure that you associate the roles to the activities and create the menu for linking activities.

Proceed as follows:





1. In the **Process** tab, select the process to be copied.
2. Click **Actions > Copy**
3. In the **Details** tab, change the **Name** and the **Description** of the process. The system, automatically, changes the process name from *Process Name* to *Process Name-Copy*
4. Click **Save**.

## Add

Throughout the process definition phases, the vertical bar of the block types displays only the selectable blocks, based on the progress of the configuration procedure.

The specific insertion constraints are automatically managed by visual Process Designer.

To define a process, proceed as follows:

1. In the **Process** tab, click **Actions > Add**.
2. In the **Details** tab, set the main attributes for the new process and click **Next**.
3. Depending on the process type specified in the previous step, the **Configuration** tab is populated with a set of activity icons.
4. If needed (**Workflow** process), click the GEN activity block type () to open the Activity window.
5. In this window, you can:
  - Create a filter in the activities set, choosing a registered context from the **Context** combo-box.
  - Click one of the activities listed to select it.
  - Click **Details** to view the configuration of the activity.
  - Click **Create** to create a new activity (see how to configure an Activity).
6. Click **Ok** to close the Activity window and confirm the previous operations.
7. Click  if you need to add one or more extensions to the activity you just defined.
8. Click the AUTH block type () if you need to open the Activity window (**Workflow** or **Escalation** processes).
9. Repeat steps 5, 6, and 7 for this block.
10. Repeat steps 8 and 9 for every AUTH activity added to the process.
11. Click the EXE activity block type () if you need to open the Activity window (**Workflow** or **Direct** processes).
12. Repeat steps 5, 6, and 7 for this block.
13. Click **Save**.

In a Workflow process, the GEN activity sets the context. All the activities that can be selected in the steps that follow, will have the same activity context as the one defined in the first step.

## Note:

- Each block that describes the flow of a process must be associated with a specific activity context.
- If the association of the activity is not performed, it is anyway possible to select the next block.
- The new activity will be added to the list of existing activities.

When you have finished building the process in the **Configuration** tab, click one of the following:

- **Previous** to return to the **Details** tab.
- **Next** to assign a role (with the **Assign** tab) to any activity of the process you just built.

## Assign

In this section you can associate an administrative role to an activity of a process.

The administrative roles are registered in the system through Access Governance Core module (see **Access Governance Core > Configure > Admin Roles**).

If you decide that a new administrative role is needed within a company process, it can be created and configured through the UI indicated above.

Under the **Assign** tab you can find a variable number of tabs, corresponding to the sequence of activities of the Process.

Using the **Assign** tab, you can associate one or more administrative role to each activity of a Process, previously selected in the left frame.

Every activity of the Process **have to be assigned at least one administrative role**, otherwise a diagnostic message is shown when the process status is set to **Online**.

Only one role can be assigned to an AUTH activity, whereas to the other types of activities, more roles can be associated.

The main operations available are listed below:

- Add
- Remove
- Activities associated to an Admin Role

### Add a role to an activity

This operation allows you to link the activity to the a specific administrative role and can be run only on processes that are in offline or maintenance status.

Proceed as follows:

1. Select a process from the list displayed in the **Process** left tab.
2. In the **Assign** tab, in the right frame, select one of the tab displayed (one for each activity of the selected process).
3. If the activity is already associated to one or more roles, these roles will be listed.
4. For adding a role, select **Actions > Add** button.
5. In the Roles pane select the right set of filters (**Filter** button) and click **Search** to find all available roles.



6. Select one or more Roles from the list ([Ctrl] or [Shift] keys for a multiple selection).
7. Click **Ok**.

### Remove a role from an activity

This operation can only be executed on the processes that are in offline or maintenance status.

Proceed as follows:

1. Select a process from the list displayed in the **Process** left tab.
2. In the **Assign** tab, in the right frame, select one of the tab displayed (one for each activity of the selected process).
3. In the list of roles, select one or more Roles from the list ([Ctrl] or [Shift] keys for a multiple selection).
4. For removing a role, select **Actions** > **Remove** button.
5. The role selected in step 2 will be removed from the list displayed.

### Managing activities associated to an Admin Role

Selecting one of listed roles, a tree structure is shown in the right-most frame of the tab.

In this tree structure, the root is the role selected and the leafs (only one level) are the activities associated to that role.

The list of leafs can display more than one instance of the same activity. This is because you can have several processes, with activities that have the same name, associated to the selected role.

At the bottom side of the right-most panel you can run one or more of the following actions:

- Click **Localize** to localize the label of a selected node.
- Click **Move Up/Move Down** to reposition a selected node.
- Click **Remove** to delete a selected node.
- Click **Save** to validate any sequence of previous actions.

In addition, selecting one activity, through a mouse right-click button, a service menu opens with some functions already indicated above (**Move Up/Down** and **Localize**).

Through the function **Details**, the Details pop-up shows data related to the activity.

If you want to hide one or more activities, tick the check box **Menu Link Disabled**, changing from green to gray the selection color of the activity.

Proceed as follows:

---

## Configure

Use the following functions for configuring the listed elements:

- Menu
- Rules

## Menu

After a process was defined and structured into a group of activities, each activity is associated to an administrative role.

To run such activities, any authorized user (thus, any user with a specific administrative role) have to access to a front end web that support the execution of this set of activities.

The **Menu** operation allows you to associate, to each administrative role, a group of activities associated with that role.

This menu is interpreted by the page constructor engine of Process Designer to assemble the front end graphic that will support each user in the management of the different activities (Access Request module).

Consider a process called P1, which is composed by the activities GEN1, AUTH1, EXE1.

Similarly, we can have a process called P2, made up of: GEN2, AUTH2, EXE2.

Assume that you have associated the activities AUTH 1 and AUTH 2 to an administrative role ADMIN\_ROLE\_1.

If the user Mike Brown has the role ADMIN\_ROLE\_1, the front end web shows to him the activities AUTH 1 and AUTH 2.

**Note:** The following indications can be implemented only for the processes that are found in the offline or maintenance status.

On the left tab **Process** you find the list of all registered process.

Click **Filter/Hide Filter** and enter the filter data, then click **Search**.

After selecting a process, in the right tab **Menu** are available two combo box, **Roles** and **Activities**.

In the **Roles** combo box are listed all administrative roles involved in the process previously selected.

Selecting one of listed roles, a tree structure is shown where the root is the role selected and the leafs (only one level) are the activities associated to that role.

The list of leafs can display more than one instance of the same activity. This is because you can have several processes, with activities that have the same name, associated to the selected role.

In the **Activities** combo box are listed all the activities involved in the process selected.

Selecting one of listed activities, in the tree on the left is highlighted the instance involved in the process previously selected (other instances possibly present are related to other processes).

If the activity selected is not present, you can add it to the hierarchy with the **Add** button.

At the bottom side of the **Menu** tab you can run one or more of the following actions:

- Click **Localize** to localize the label of a selected node.
- Click **Move Up/Move Down** to reposition a selected node.
- Click **Remove** to delete a selected node.
- Click **Save** to validate any sequence of previous actions.

In addition, selecting one activity, through a mouse right-click button, a service menu opens with some functions already indicated above (**Move Up/Down** and **Localize**).

Through the function **Details**, the Details pop-up shows data related to the activity.

If you want to hide one or more activities, tick the check box **Menu Link Disabled**, changing from green to gray the selection color of the activity.

## Rules

Rules are used to define event management based on event type or for the automation particular policies.

The seven Rule Class concepts are summarized below:

- **Live events:** Rules triggered by Event Queues (for more information about Events, see Events in Integration Interface. These types of events are processed in real time. Their purpose is to control the input/output data flow.
- **Deferred events:** Rules triggered by the Event Queue IN. These types of events are processed by scheduling (see Task Planner). Their purpose is to aggregate events.
- **Authorization Digest:** Rules triggered by changes in the User data set. These types of events are processed in real time. Their purpose is to validate enforcements.
- **Account:** Rules for the creation of a user account.
- **Attestation:** Rules automatically applied in campaigns of attestation.
- **Hierarchy:** Rules for the automatic building of hierarchies based on user attributes.

You can select the class of Rules in the filter section (click **Filter** button).

The filtering approach requires the selection of a **Rule Class** and, according to the class, you can select from **Queues** or **Rule Sequence (Flow)** combo boxes.

The **Actions** menu of the tab **Rules** in the left frame lists the following actions:

### Import

For importing the XML representation of a Rule or of a Rule Sequence (Rule Flow).

**Export** For exporting a Rule or a Rule Sequence (Rule Flow).

**Add** Adds a Group of Rules (function maintained for legacy reason).

### Remove

Removes a Rule or a Group of rules (for Groups, function maintained for legacy reason).

**Enable/Disable**

Enable or disable a Rule execution into a sequence.

**Move Up/Down**

Move the Rule up/down in the Rule sequence.

In the right frame you can find two main accordion panes:

**Rules Package**

In this accordion pane are available all functions for manage a Rule selected in the left frame.

**Package Imports**

In this accordion pane are present all functions for managing packages of rules.

**Rules Package**

In this accordion pane are available all functions for managing Rules through the Rules editor.

According to the selection on the left tab **Rules**, a set of rule are listed in this pane.

The **Actions** menu hosts the following actions:

**Verify** For checking the formal structure of the code involved in a rule (needs the selection of one of the rule listed).



**Modify**

For modifying the rule, opening the Rules editor pop-up window.

**Delete** For deleting selected rule.

**Create** For creating a new rule.

**Add**

This function add a rule selected by the list to a  **Group** (legacy versions) or  **Rule Sequence** selected in the **Rules** tab, on the left.

**Rules Editor**

The Rules Editor speeds up the writing of code contained in a Rule.

The figure below shows the Rules Editor panel:

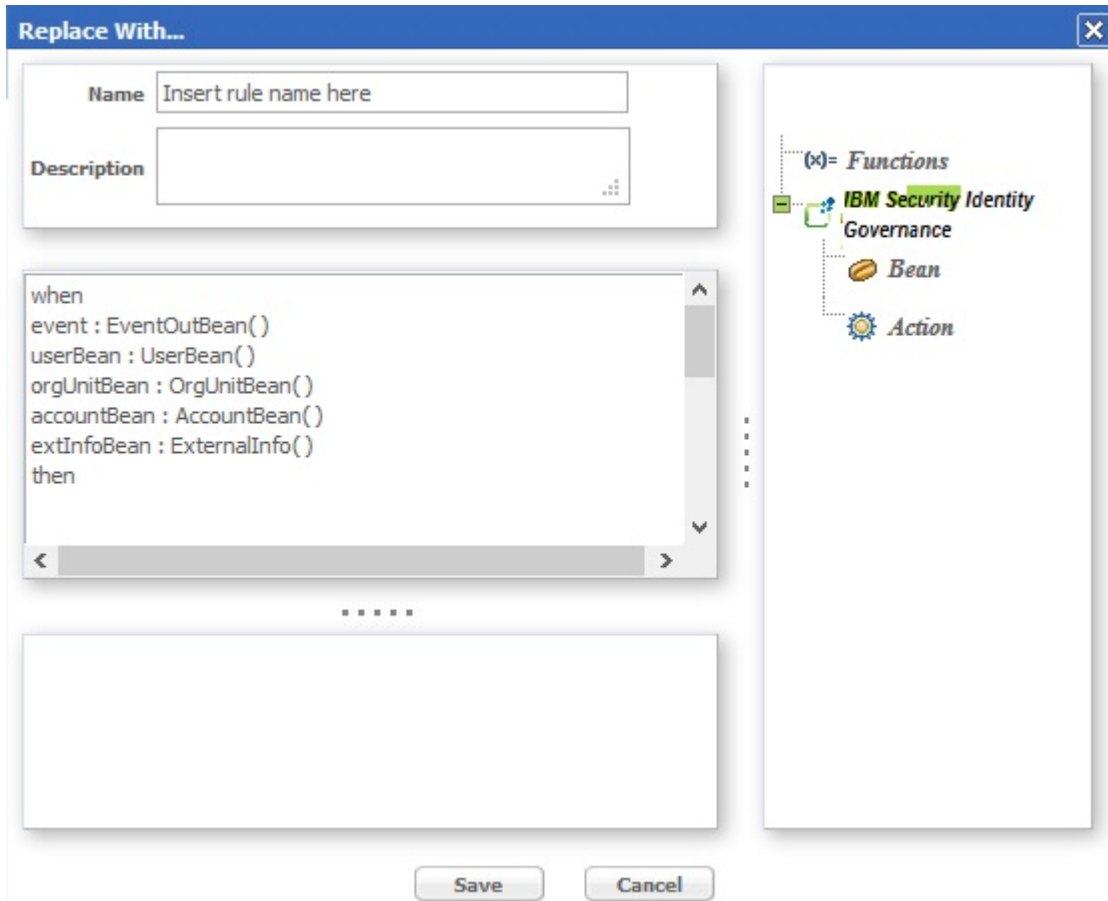













Figure 55. The Rules Editor panel.

The table below shows the symbols of several buttons and icons present in the Rules editor:

Table 122. Symbols of the Rules editor.

Icon	Description
	Import a Java class
	Java class
	New variable
	New function
	Bean
	Action
	Associated rule: rule that is associated to a rules group
	Split: used to construct flow processes in situations that require a branch point.
	Constraints
	Rules group
	Flow process

All the Rules must have the following structure:

- **Condition Area** (between “when” and “then”)
- **Action Area** (immediately after “then”).

The word **when** identifies the beginning of the conditions area.

Any number of conditions can be inserted and the actions will be executed only if all the conditions are verified (logic AND between each condition)

The word **then** identifies the beginning of the actions area.

Actions are written in normal Java code; all classes making up the libraries delivered with the product are available for writing actions.

A complete list and descriptions are available in the **Replace with...**

The conditions are written according to Drools syntax.

Every condition verifies, within the Working Memory, whether or not there are one or more objects identified by the Beans. If such objects are actually found, the actions described above will be executed on them.

The **Replace with...** window contains the code obtained from the Editor.

From the frame on the right side of the window, predefined code blocks can be selected and placed directly into the **Replace with...**

The objects are grouped in a hierarchy and managed through a tree structure.

The **Object** frame contains the nodes corresponding to the higher level object categories. The two initial main categories are:

- Functions
- Ideas

Based on the selection, the objects can be **Functions**, **Bean** or **Action** and their methods are visible below the selected object (fourth level of the tree):

Now, select a leaf object (a method) and insert it into the **Replace With...** frame (left) using the **Actions>Add** button.

This operation can be performed to modify or create a Rule.

**Note:** The name of a Bean can be written without its system path **ONLY** if it has been imported into the Package that contains the Rule.

## Functions

The Functions category contains functions for fundamental Rule-writing constructs; the same frame lists the following four elements:

- if
- ifelse
- ifelseif

- for

Select one of the functions and click **Add** to insert the related parametric code into the **Replace with...** frame, at the end of the already-listed code. The parameters to edit are easily recognized because they are between two '\$' symbols.

For example, in the IF ELSE construct, you have to edit the parameters CONDITION1, ACTION1 and ACTION2.

Proceed in one of two ways to edit the parameters:

- Directly write the code instead of the corresponding symbolic string (e.g., CONDITION1 included between two '\$' characters);
- Use the editor again.

In this last case, click **Field > Bean > AccountBean** and select one of the objects listed, then click **Add**:

Selecting \$ACTION2\$ places the selected code block in the position that was covered by \$ACTION2\$. If none of the parameters in the window are selected, click **Ok** to place the code block at the end of the already-present code. To eliminate a potentially wrong insertion, cancel the corresponding code directly in the **Replace With...** frame.

## Bean and Action Elements

The IBM Security Identity Governance folder contains the following two folders:

- Bean
- Action

These folders contain ALL the Beans and Actions imported into the Rules Package; in particular, the Bean folder contains the Beans imported into the Package that are part of the libraries delivered with the product. Client users of the AG Core can create additional personalized Beans.

This paragraph analyzes how to use a Bean in the Bean folder. By selecting Bean, the content of the Bean folder is presented in the form of a tree, where every Bean is a node and its child nodes represent its methods.

After selecting the Bean, click Add to insert it into the **Replace With...** frame.

Be sure to insert a semicolon (;) at the end of each line and put the code in order.

Be sure to assign the String parameter a string that makes sense.

The Action folders contain ALL Actions imported into the Package of the selected Rule; in particular, the Action folder contains all Actions imported into the Package that are part of the libraries delivered with the product.

The procedure for inserting Actions (even custom Actions) is exactly the same as that for inserting Beans.

## Package Import

From the tabs bar, select **Configure > Rules** then click on the **Package Import** accordion pane on the right.

Configuring a Package consists of declaring certain objects available to all Rules in the Package.

Such a declaration consists of specifying an appropriate Java code in the allotted text box.

To make configuration of the Packages easier, insert blocks of predefined code (on the right side of the frame there is a small vertical toolbar with buttons).

The following actions are available for each Package:

- Import specific classes
- Insert variables
- Insert functions

The Rules programmer can write the Rule's code to directly call the objects that are set up for the Package containing the Rule.

Importing a class into a Package adds a class to a Rule without having to specify the entire path.

For example, after importing the class `UserBean()` into the Package, it is possible to directly write `UserBean()` instead of `com.engiweb.profilemanager.common.bean.UserBean()`.

## Package Editor

An administrator familiar with programming languages can insert any object in the Package by writing the code directly in the text box.

A Package Editor is also available to assist administrators to accomplish this task.


The Editor uses the following buttons, located on the right-hand side of the text box:

-  New Import
-  New Variable
-  New Function

Variables usually support objects that are already instanced with global visibility to all the Rules of the Package; if, for example, there is an object that contains all the parameters required to connect to the DB, the object can be assigned to an "sql" variable (always visible to the Package's Rules) and can be used in the Rule code, as shown in figure above.

Lastly, it is possible to create Functions that always have global visibility to all the rules of a package. For example, if several rules request an operation for the arithmetic average of two numbers, this can be created directly in the Package instead of in each single rule.

## Import a Class

To import a class, click on  **New Import** button in the vertical toolbar on the right-hand side of the Package Imports pane.




The Classes window opens (figure below) with a list of available classes

Choose a class, then click **Ok**.

The Java code corresponding to the selected class is written in the text area on the right-hand side of the Replace With... window.

### Enter a New Variable

To insert a new variable, click on  **New Variable** in the vertical toolbar on the right-hand side of the Package Imports accordion pane.

The text box displays the code corresponding to the declaration of a new variable.

The code is parametric and thus must be edited in the allotted spaces, defined by the characters <>.

Insert the object (specify entire system path) in the space <your class here>.

Insert a variable name in the space <variable name>; this name can then be used in every Rule of the Package.

### Enter a New Function

To insert a new function click on  **New Function** in the vertical toolbar on the right-hand side of the Package Imports accordion pane.

The text box displays the code corresponding to the declaration of a new variable.


The code is parametric and thus must be edited in the allotted spaces, defined by the characters <>.

Edit the parameters as follows:

- Replace <return Type> with the type of objects that result from processing the function (e.g. an integer, a string, a class, etc.).
- Replace <args here> with the list of parameters given to the function at input.
- {} needs to contain the body of the function, i.e., all the code that implements the function.

### How to Schedule a Rules Flow

It is possible to link a Rules Flow to a scheduled Job. The IBM Security Identity Governance Task Planner is the module dedicated to scheduling several types of Jobs that optimize different tasks in the IBM Security Identity Governance Platform. The Flows that can be scheduled belong to the Rule Classes Advanced or/and Deferred Events.

After creating a Flow Process, open the upper toolbar and click on the  button related to the IBM Security Identity Governance Task Planner.

In the Task Planner module, from the tabs bar, select **Manage > Job** Classes to access the Job Classes GUI.

From the list of Job Classes, choose the AdvancedRuleFlow or DeferredEventsRuleFlow (depending on what is needed) then select the Jobs tab and choose a relevant Job from the list produced.

Click on the >Job button in the Jobs frame, then populate the fields with the values of the chosen Job Class.

---

## Monitor

The functions that are available for monitoring some elements are contained in the following list.

- Requests
- Global Statistics

## Statistics

This is the default entry point of the Process Designer module.

From this section, you can access the:

- Global Statistics
- Requests

### Global statistics

The **Global Statistics** web interface is composed by the following panes:

- Activity
- Template
- Localization Code
- Process
- Template Type
- Functionality

In some panes, the **Clear** button is available. Click it to remove items from the database.

### Requests

The requests web interface is shown below:

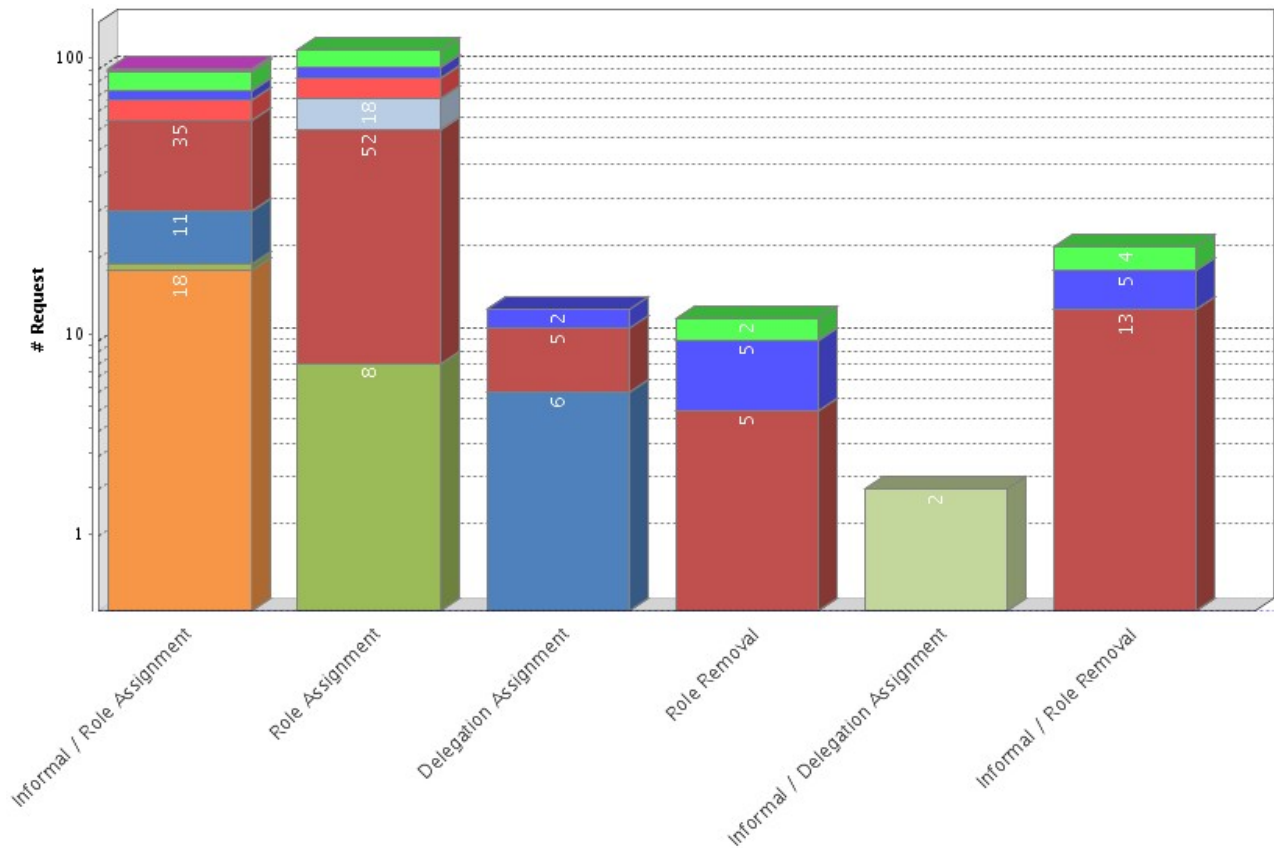


Figure 56. The Requests web interface of Process Designer.

The requests web interface is composed by two axes:

- Request
- Type of request

The Request axis defines the quantity of the requests in an x state.

The Type of request axis defines the type of the requests.

The colors are used to show the state of the request as described in the colors legend below:

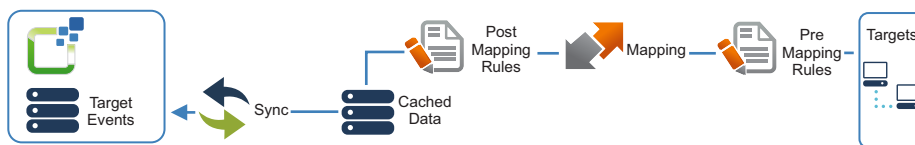


Figure 57. Colors show the state of request.

## Settings

The following functions are available for setting values of some elements of the module:

- Language management
- “Entity display” on page 324

## Language management

In this section, the PD administrator can modify the default language used to load the label groups associated with the various application objects.

The settings described in this section are not related to the language settings of the browser. The browser language affect the labels on the tab bar only.

The **Languages in use (Browser)** text box displays the language that is currently set for the browser.

The **Default Language** text box displays the language that is currently set.


To modify the language, proceed as follows:

1. Click **Change** near the **Default Language** text box.
2. Choose one of the languages from the Default Language window.
3. Click **Ok** to confirm the selected default language.

To add languages to the list of available languages (from right to left), proceed as follows:

1. Select the desired language from the available languages list box on the right.
2. Click **Add to Table** to move the selected language to the **Languages in use** list box on the left.

To remove a language from the list of languages in use (from left to right), proceed as follows:

1. Select the desired language from the languages in use list box on the left.
2. Click  **Remove Languages** to move the selected language to the **Available languages** list box on the right.

## Entity display

For some attributes of some ISIG model entities, it is possible to choose if the attribute will be shown (and in which position) in Access Request processes.

On the left tab **Entities** are listed the model entities available for settings.

Selecting one entity form the list, in the right tab **Entity Fields** you find all related fields.

Ticking the check-box **Visible** you can determine if the field it's shown into the Access Request processes.

Through the arrows **Position** you can determine the relative position of the field.

---

## Chapter 16. Introduction to Enterprise Connectors

Enterprise Connectors (ERC) is the module delegated to achieve the alignment between the centralized database of IBM Security Identity Governance and Intelligence and the peripheral target systems.

A generic organization decides to adopt IBM Security Identity Governance and Intelligence after experiencing the difficulties found in managing different and heterogeneous IAM systems, layered over time, sometimes without a clear vision of the integration issues.

Usually, the final result of a “patchwork strategy”, is a multi-repository system that stores the authorization attributes of the organization, based on different data models and approaches, with different authorization systems that cannot be easily interfaced.

During the transition phase from an existing (and often chaotic) authorization model to an RBAC model such as IBM Security Identity Governance and Intelligence, it is not possible to abruptly switch off all the other existing IAM systems and to use only the AG Core centralized repository.

Ensuring business continuity is always a priority for large organizations but, during the transition phase to Identity Governance and Intelligence, this requires additional effort since:

- The Identity Governance and Intelligence platform must be integrated with the current layout of the enterprise.
- Tuning and customization activities are possibly needed.
- Staff needs to be trained on the features and characteristics of Identity Governance and Intelligence.

During the transition phase it is important that the following objectives be harmonized:

- Granting the normal behavior of all the business activities of the organization, maintaining all the preexisting IAM systems (targets) active.
- Updating the AG Core centralized repository of Identity Governance and Intelligence and keeping it aligned with the peripheral target systems.

Also after the transition phase is over, when all authorization issues are filtered and managed by the AG Core centralized repository, it may be necessary to maintain a relevant number of target systems active. This is the most common situation, when more than one target system is linked to the AG Core of Identity Governance and Intelligence.

Enterprise Connectors (ERC) is the module of the IBM Security Identity Governance and Intelligence platform that answers the following concerns:

- Synchronizing the AG Core repository with a target system when on the target system identity attributes are modified.
- Replicating on a target system changes that were made in the AG Core repository.

A connector *connects* the AG Core centralized repository with a particular IAM system, so that identity governance data can be imported and kept synchronized. In particular, the ERC module provides a set of functions that enable an administrator to:

- Define a connector
- Define a connector's channel mode
- Define the configuration rules for a specific connector
- Start and stop a connector, either manually or by schedule

---

## The Identity Governance and Intelligence ERC model

The Integration Interface (II) of Identity Governance and Intelligence provides an efficient way to connect the AG Core module with a wide range of external target systems.

The figure below displays the structure of II:



Figure 58. The structure of the Integration Interface.

The ERC module is the logical layer that is positioned between the target systems and II, as displayed below:



Figure 59. The ERC layer.

In the figure above, you can easily distinguish three different logical channels colored in light green (**Read From** channel), light orange (**Write To** channel) and light blue (**Reconciliation** channel).

The standard structure of a connector block is displayed below:

Figure 60. The general structure of a connector block.

A connector consists of three basic blocks:

- Target driver
- Connector core
- Identity Governance and Intelligence (IDEAS) driver

The target driver is the boundary element between Identity Governance and Intelligence and the external targets.

This block hosts all configurations settings needed to communicate with a specific target system.

The connector core block hosts the connector engine, mainly characterized by a set of rules.

The Identity Governance and Intelligence (IDEAS) driver is the interface between the connector core and the II.

## Channel mode of the connector

For any connector, you must define at least one channel mode.

It is possible, however, to define a connector that operates in every channel mode. The channel modes are:

- Write to
- Read from
- Reconciliation

### Write to

This channel option allows you to propagate to a generic target system every change registered into the AG Core repository. The logical workflow of this channel mode is displayed below:



Figure 61. The logical workflow of the Write to channel mode.

### Read from

This channel option allows you to read the input events and user data coming from the generic target system. The logical workflow of this channel mode is displayed below:



Figure 62. The logical workflow of the Read from channel mode.

### Reconciliation

This channel option allows you to realign the data changed in a generic target system with the data registered into the AG Core repository. The logical workflow of this channel mode is displayed below:

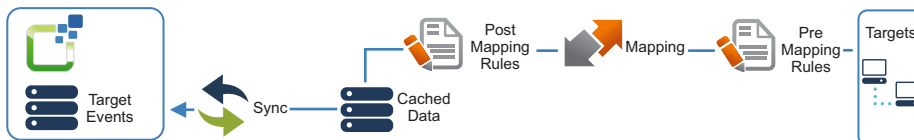


Figure 63. The logical workflow of the Reconciliation channel mode.

---

## Building a connector

A short roadmap to build a connector is provided.

You can build a connector using the ECONN module with only four basic steps:

1. Configure a driver.
2. Link the connector to the driver configured in step 1.
3. Choose one or more channel modes for the connector, according to step 2.
4. Set the appropriate mapping for the connector.

### Driver configuration

In the ERC model, there are two types of drivers:

#### Target driver

Is the boundary element between IBM Security Identity Governance and the external environment, and is part of a connector block.

#### IBM Security Identity Governance driver

Is the boundary element between a generic connector block and the IBM Security Identity Governance II.

IBM Security Identity Governance driver is a built-in default driver ECONN module. For the IBM Security Identity Governance driver, no configuration activities are needed.

A generic target driver must be accurately configured:

- To get data from an external target system (Read from channel).
- To send data to an external target system (Write to channel).

ECONN allows the management of a multi-target driver.

A driver is identified by three sets of data:

- Driver details
- Driver properties
- Driver attributes

### Multi-target driver

This option is very useful in very common situation, when is present a specific type of target system (for example, Active Directory) and several instances of AD, possibly running on workstations.

In this case, the driver configuration is characterized by:

- A set of common data that can be shared among all instances.
- A reduced subset of data related to the specific instance (for example, the IP address or the SSL certificate).

In this situation, it can be useful to specify the driver common data once and to clone it for several instances. Therefore, for every instance will be easy to specify only the specific data subset for the specific instance.

The logical structure of a multi-target driver is displayed below:



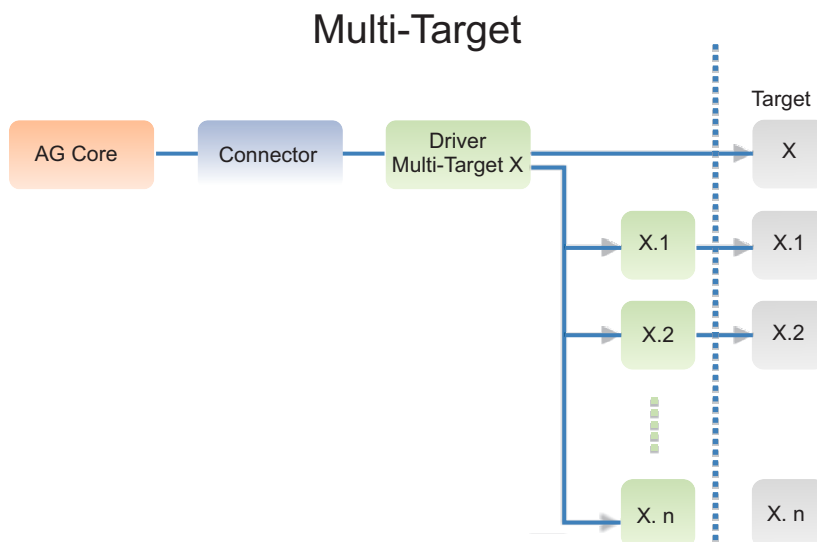


Figure 64. General structure of a multi-target driver.

### Adding a new connector

To add a new connector means, basically, to link a connector module to a specific driver. This operation allows you to establish the real implementation of a communication channel between a target system and IBM Security Identity Governance II (see The IBM Security Identity Governance Connector model).

For details about the actions needed, see “Manage connectors.”

---

## Manage connectors


Use this tab to define and manage connectors, their driver, and channel mode.

The Connectors frame on the left displays a list of defined connectors. You can select the **Filter** button and enter the following information to refine the list of connectors or to find specific ones:

Table 123. Available filters to search connectors

Filter	Description
<b>Name</b>	The name of the connector
<b>Enabled</b>	<b>Yes</b> The connector is enabled <b>No</b> The connector is not enabled

The list of connectors shows a connector name and:

- Whether the connector is enabled (  ) or not (blank). An enabled connector is ready to run.
- The channel mode of the connector. A channel is the logical representation of the communication path that can be established between the AG Core module (through an annexed connector) and a generic target system. There are three channel modes, represented as:


**WTO** Write to: Used to send data from the AG Core repository to a target.

**RFROM**

Read from: Used to import data from a target to the AG Core repository.

## RECON

Reconciliation: Used to re-align data that for some reason was changed in a target system with the data recorded in the AG Core repository.

A connector can operate in any or all of these modes, depending also on its type. The channel modes enabled for a connector are marked by the  icon.

You can click the **Actions** button to select any of the following:

**Add** Opens the Connector Details panes in edit mode enabling you to enter a new connector definition. To add a new connector implies linking a connector module to a specific driver. This operation results in the implementation of a communication channel between a target system and IBM Security Identity Governance and Intelligence.

The **Channel Mode** check boxes are not displayed the first time you define the details of a new connector. You must first save the new connector and then select it in Edit mode for the check boxes to display.

## Remove

Deletes a selected connector definition

## Import

Imports a connector definition as an XML file.

The XML file name format is:

*ConnectorName.dd\_mm\_yyyy hh.mm.ss.xml*

**Export** Exports a selected connector definition as an XML file.

The XML file name format is:

*ConnectorName.dd\_mm\_yyyy hh.mm.ss.xml*

When you select a connector in the list, the **Connector Details** frame on the right shows the following connector properties:

Table 124. Connector details

Detail	Description
<b>Enabled</b>	When checked, it shows that the connector is ready to run.
<b>Channel Mode</b>	A checkbox is displayed for every channel mode available. There can be up to three channel modes, depending on the type of connector. A check mark indicates that the connector is ready to run in the specific channel mode. All channel modes can be enabled concurrently.
<b>Name</b>	The name of the connector.
<b>Description</b>	An optional description that states the function of the connector.
<b>Type</b>	The connector type. The following connector types are ready for use: Active Directory, CSV, IDEAS, JBDC, LDAP, SAPHR, SAPR3, Unix, WorkGroup, XLS, XML.
<b>Driver Class</b>	The name of the associated driver, based on the connector type.
<b>Trace ON</b>	When this check box is flagged, the connector is traced and logged in the <i>connector_name.log</i> file.

Table 124. Connector details (continued)

Detail	Description
<b>Trace Level</b>	<p>This text box is enabled when you flag the Trace ON checkbox. Choose one of these trace levels:</p> <p><b>INFO</b> Records informational messages that highlight the progress of the application at coarse-grained level.</p> <p><b>DEBUG</b> Records fine-grained informational events that are most useful to debug an application.</p> <p><b>ERROR</b> Records error events that might still allow the application to continue running.</p>
<b>History ON</b>	Flag this checkbox to save usage history of this connector.

The **Global Config** accordion pane lists a number of connector properties that apply to all connectors, independently of their type. These properties are shown with their default values. You can change these values, or use the **Actions** button to remove any of them or to add new ones, making sure that none of these changes upset the performance of the connector.

Table 125. Global configuration properties for connectors.

Property Name	Default Value	Description
rightNameValueSeparator	=	The character used for separating a name and its corresponding value in
reconciliationCode	1	A counter that is updated by the system each time reconciliation takes place. You can reset the number to a value of your preference.
ModifyToAdd	true	During the reconciliation process, adds a record in the database in lieu of modifying it as done in the target. For example, if a record was modified in the target, but the record is not found in the AGC database, the record is created in the database. If the value is set to false, an error is logged when the record is not found.
disableMapping	false	Change to true to disable the mapping of connector object class fields.
Manage Event Target on error	false	Change to true to be able to manually handle error events generated by the target.

The details and properties of a selected connector are displayed in browse mode only. Click **Edit** at the bottom of the window if you want to modify them.

To complete or view all connector-related information, continue to the following tabs:

- Driver Configuration
- Driver Attributes List
- Tabs corresponding to the enabled channels (Read From, Write To, or Reconciliation)

## Driver configuration

Enter in this panel the properties of the driver that the connector runs on.

The properties differ according to the type of driver, but they generally specify information such as:

- Details for connecting with the target
- Identification data
- Details on the format used to send and receive data

This panel includes the following accordion panes:

**Driver** Lists the properties of the driver that runs the connector selected in the left pane.

### Fanout

If you have more than one instance of the target system, this is where you can specify driver properties for the additional instances.

These panes are described next.

## Driver

This pane is displayed in Browse mode when you select the Driver Configuration tab, unless you are defining a new connector. Click **Edit** if you need to update values.

The Driver pane collects the following information:

### Events Marker



This dropdown list shows the event marker selected for this driver. An event marker represents the target system linked by this driver (and connector) as the sender or recipient of events to or from Identity Governance and Intelligence. Event markers are defined in the **Manage > Account** panel of the Access Governance Core module. Each marker is closely associated to the account linked with an application. With an exception for the IDEAS event marker, an event marker cannot be associated with more than one driver.

When you access this pane in Edit mode, click the arrow to list the available markers.

### Driver Properties frame

Displays a list of driver properties as shown in the following table. The properties shown are specific to each type of driver.

Table 126. Driver properties

Name	Description
<b>Mandatory</b>	If the  icon is shown, you are required to provide a value for the property in the row.
<b>Name</b>	The name of the property.
<b>Value</b>	A working value for the property.
<b>Description</b>	Position your mouse on the  icon so that a tooltip displays a description of the requested value.

The following buttons enable you to specific actions:

- Reset** Resets the driver cache. Select it to delete the hash file of the driver. This action can be run only on drivers that do not use a trigger.
- Conn.** Checks the state of the connection configured for the driver.
- Query** Checks the driver query values.
- Dump** Applies to drivers used in Reconciliation mode. An operating system window is opened to save the file created with the values of the Reconciliation process.

## Fanout

Expand this pane to configure properties for additional instances of the target addressed by this driver and connector.

This option is useful to address multiple instances of a target system (for example, Active Directory) that run on different computers. In this case, the driver configuration is characterized by a set of common data that can be shared for all instances and by a subset of data related to the specific instance (for example, the IP address or SSL certificate). This pane is where you specify the data subset for the specific instances.

To specify the properties for additional target instances, click **Actions** and select **Add**. The following items appear in the attached table:

Table 127. Adding targets

Event Marker	Enabled	Operations	Properties
The events marker associated with the target instance.	Click to enable the driver to run for the target instance.	The same operations available in the Driver pane.	Click <b>Conf.</b> to display the <b>Driver properties</b> window. This is similar to the Driver Properties frame in the Driver pane and specific to the instance.

Click **Actions** > **Save** when you are finished. You can add as many rows as there are instances.

To remove the driver configuration of a particular target instance, flag the associated checkbox and select **Actions** > **Remove**.

## Driver Attributes List

In this panel you enter the Object Class nodes and Object Class Field nodes that you will later map within the channel modes of the connector.

Object Class nodes and Object Class Field nodes make up the structure in which information, such as user names, roles, groups, accounts, passwords, and any other type of data used in your security model is mapped in the model. An Object Class node contains several Object Class Field nodes and every node displays its fields in a tree structure in this pane.

The IDEAS driver already comes with its own list of attributes, but you can define additional attributes to this driver as well as to all the other drivers that you use. You can also edit and remove these attributes to comply with the changes of your security model.

With a connector selected in the left pane, you can click **Actions > Add** to add:

- A New Object Class node
- An Object Class Field node

If you click **Add** with nothing selected in the Driver Attributes List panel, you are shown the Add node window with the following fields:

*Table 128. New Object Class node attributes.*

Name	Description
Name	The name of the Object Class node
Description	A description of the Object Class node

If you click **Add** with a selected Object Class node, the Add node window gives you the choice of specifying the attributes of another Object Class node or those of a field of the selected node (Add Object Class Field node to *node\_name*). If you opt for adding an Object Class Field node, the attributes you must specify are:

*Table 129. Object Class Field node attributes.*

Name	Description
Name	The name of the Object Class Field node
Description	A description of the Object Class Field node
Type	Click the arrow to display a list of Java data codes to choose from
Multivalued	Flag this check box if the field will have more than one value

The Object Class Field nodes are added as hierarchy leafs to the Object Class node. You can add as many field nodes to an Object Class node as required. Ultimately, each Object Class node is displayed with all its field nodes in a tree structure.

If you click **Actions > Automatic Add** for a selected Object Class node, depending on the driver configuration the Object Class Field nodes are added based on the driver properties.

To edit or remove an Object Class node or an Object Class Field node, select the object and click the appropriate item in the **Actions** menu.

**Remember:** Before you modify the Type of an Object Class Field node, verify that the new value is compatible with the mapped value in the **Connectors > Channels > Mapping** button.

## Channels and Rules

This is where you map the Object Class fields stored in the AG Core repository of Identity Governance and Intelligence with those of the target system. It is also where you define and manage rules that make adjustments to the data exchanged between the two parties to adapt it to the data layout of each system.

After selecting a connector (left), you can click on the related channel tabs on the right:

### Channel-Write To

Propagates every change registered into the AG Core repository to the target system.

### Channel-Read From

Reads the events and user data arriving from the target system and bound for the AG Core repository.

### Channel-Reconciliation

Realigns the data changed (for various reasons) in the target system and the data recorded in the AG Core repository.

**Important:** Each connector can have one or more configured channels. The display of one or more Channel tabs depends on the configuration of the selected connector (driver).

Every channel is provided with an infographic made up by icons that you select to take specific actions:

- Events Queue: available for every channel (Write To, Read From, and Reconciliation).
- Pre Mapping Rules: available for every channel.
- Mapping: available for every channel.
- Post Mapping Rules: available for every channel.
- Response Rules: available only for the Write To channel.
- Target: available for every channel.
- Sync.: available only for the Reconciliation channel.
- Cache: available only for the Reconciliation channel.

The infographic provided for every channel suggests the logical workflow of the channel.

## Events Queue

Click the **Events Queue** icon, to view the list of authorization events that transited through your selected connector. The following window opens, depending on the channel mode:

### Target Events Queue

For Read From and Reconciliation channels

### IDEAS Out Events

For Write To channels

The window displays all or some of the following fields, depending on the driver configuration:

Table 130. Event fields

Field	Description	Events Queue window	
		IDEAS Out Events (WTO)	Target Events Queue (RFROM and RECON)
<b>ID</b>	Event identifier.	x	
<b>Account ID</b>	The identifier of the account associated with the application impacted by the event.		x
<b>Application</b>	The name of the application impacted by the event.	x	
<b>Operation Cod</b>	Operation identifier.	x	
<b>Operation</b>	Indicates the type of operation made.	x	x
<b>Target</b>	The name of the target system to which the outbound event is directed.	x	
<b>Status</b>	The state of the event. It can be one of the following: <ul style="list-style-type: none"> <li>• Unprocessed</li> <li>• Success</li> <li>• Error</li> </ul>	x	x
<b>User ID</b>	The identifier of the user affected by the event.	x	
<b>Trace</b>	A description of the error.		x
<b>Event Marker</b>	The marker of the event. It may coincide with the identifier of the target system.		x
<b>Permission</b>	Indicates the assigned/removed permission.		x
<b>Permission Type</b>	Indicates the type of assigned/removed permission.		x
<b>Free Attribute 1</b>	Sensitive data 1.	x	x
<b>Free Attribute 2</b>	Sensitive data 2.	x	x
<b>...</b>	...	x	x
<b>Free Attribute N</b>	Sensitive data N.	x	x
<b>Event Date or Date Event</b>	Indicates the event generation date.	x	x
<b>Process Date</b>	Indicates the date in which the event must be processed by the RE (generally coincides with the event date but can be subsequent if the event processing was postponed).		x
<b>Ownership</b>	Indicates the user who caused the event on the external table.		x

Click **Ok** to close the window.



## Pre Mapping and Post Mapping Rules

Pre Mapping Rules are used to prepare data inbound from a target driver (in the Read From and Reconciliation channels) or outbound from the Identity Governance and Intelligence driver (in the Write To channel) for the application of the Mapping process. For example, you write a pre mapping rule for the Write To channel that changes an event or sets a particular value for it and then writes on the log the content of the event.

Conversely, Post Mapping Rules are used to adjust data, after the completion of the Mapping process, before it is stored in the AG Core repository of Identity Governance and Intelligence (Read From and Reconciliation channels) or sent to the target driver (Write To channel).

Select the **Pre Mapping Rules** and **Post Mapping Rules** icons to specify actions on data or events before and after the Mapping process takes place. As you do so, the icon you selected is highlighted and the following panes are displayed below:

- The pane on the left contains a **Run** tab that lists one or more packages of rules charted in a tree structure. The rules are either imported from another Identity Governance and Intelligence module or created within the Rules Package on the right.

The pane includes an Actions button with the following items:

*Table 131. Rule Package Actions*

Action	Description
Import	Imports a rule class or rule flow previously exported from Access Governance Core or Process Designer. Opens the Import Rule Class/Flow window where you choose the item to import and select the rules file with the help of a Browse option.
Export	Not used.
Modify	Not used.
Enable/Disable	Not used.
Up	Moves the selected rule one place up in the rule package tree.
Down	Moves the selected rule one place down in the rule package tree.
Remove	Removes the selected rule from the package tree.

- The Rules Package accordion pane on the right lists the rules defined within the pane with the help of the “Rules” on page 186.

The pane includes an Actions button with the following items:

*Table 132. Rules Package pane Actions*

Action	Description
Verify	Checks the integrity of the rules listed in the pane.
Modify	Opens the selected rule for editing in the “Rules” on page 186.
Delete	Removes the selected rule from the pane.
Create	Opens the “Rules” on page 186 for the definition of a rule.
Cr. Def	Not used.
Add	Adds a selected rule to the tree structure of a selected package in the left pane.

- The Package Imports accordion pane, also on the right, contains the Java code of the rules package selected in the left pane.

The Java code is shown in the “Package Editor” on page 191 text box, where you can edit the Java code to change the configuration of the rules package.

Configuring a package consists in declaring certain objects and making them available to all the rules of the package. This is accomplished by specifying the appropriate Java code in the allotted text box.

The “Package Editor” on page 191 assists you in changing the Java code by enabling you to add blocks of predefined code. These blocks are made available by three buttons located on the right-hand side of the text box. The buttons start the following actions:

#### **New Import**

Imports a rule class selected from a list. Importing a class in a package adds a class to a rule without having to specify the entire path. For example, after importing the class `UserBean()` into the package, it is possible to directly write `UserBean()` instead of `com.engiweb.profilemanager.common.bean.UserBean()`.

#### **New Variable**

Adds a variable block at the end of the code.

#### **New Function**

Adds a function block at the end of the code.

More helpful information about rule building is described in the Rule Classes section **AGC > Configure > Rules**.

## **Mapping**

In this part of the infographic, you map the Object Class fields of Identity Governance and Intelligence with those of the target system.

Click the **Mapping** icon in the infographic displayed for your selected channel to view the two panes with the Object Class fields you want to map. The IDEAS pane lists the Object Class fields of the particular authorization event on Identity Governance and Intelligence, while the TARGET pane lists those on the target system. The panes vary depending on the channel mode:


- In the Write To channel mode, the Object Class fields of TARGET (**Operation** = Source) are mapped on the ones of IDEAS (**Operation** = Destination).
- In the Read from and Reconciliation channel modes, the Object Class fields of IDEAS (**Operation** = Source) are mapped on the ones of TARGET (**Operation** = Destination).

The pane where **Operation** equals Source shows the following columns:

*Table 133. Mapping pane columns when Operation = Source.*

Column	Description
Field	The name of the Object Class field mapped to the fields of the <b>Operation</b> = Destination pane. The fields can be selected individually by flagging the nearby checkbox or globally by flagging the checkbox next to <b>Field</b> .
Operation	Source

Table 133. Mapping pane columns when Operation = Source. (continued)

Column	Description
Type	Can be: <ul style="list-style-type: none"> <li>• Mapped</li> <li>• Not Mapped</li> </ul> Mapped fields are placed on top of the list.
Value	If <b>Type</b> = Not Mapped, it is blank. Otherwise, it is the name of the Object Class field on the counterpart that this field is mapped to: <ul style="list-style-type: none"> <li>• For an Identity Governance and Intelligence field mapped to a target field, <b>Value</b> is the name of the target field preceded by the name of the driver.</li> <li>• For a target field mapped to a Identity Governance and Intelligence field, <b>Value</b> is the name of the Identity Governance and Intelligence field preceded by the Object Class name.</li> </ul>
Key	 The icon displayed next to one of the fields shows that the field is used as the matching key for the mapping process. <p>This matching enables an event to check that the current object exists on the application target, according to the relation defined between Object Class Fields and Value.</p>

In this pane click **Actions** to do any of the following:

**Set Key**

Makes a flagged field the matching key for the mapping process.

**Change Map**

Displays a list of defined Object Class Nodes where you choose the node whose fields you want to use for mapping.

**Custom Map**

Opens a window where you can enter a constant value or variable attribute field as the **Value** of a selected field.



**Reset** Resets the flagged fields to the Not Mapped **Type**.

The pane where **Operation** equals Destination shows the following columns:

Table 134. Mapping pane columns when Operation = Destination.

Column	Description
Operation	Destination
Name	The name of the Object Class field mapped upon by one of the fields of the <b>Operation</b> = Source pane.
Type	The Java data code of the Object Class field. For example, <code>java.lang.String</code> .

Table 134. Mapping pane columns when Operation = Destination. (continued)

Column	Description
Multi	 <p>The  icon displayed next to a name shows that the field can have more than one value.</p>

To map a field:

1. Click the **Source** button next to the field that you want to map.
2. In the adjacent pane, click the **Destination** button next to the field that you want to match.

As a result, the attributes of the mapped fields will populate the corresponding fields whenever an exchange of data occurs between Identity Governance and Intelligence and the target system.

## Response Rules

This step is similar to the one described in Pre/Post Mapping Rules.

The Response Rules section shows the outcome of the action run on the target. It enables you to view the status of the target following the completion of that particular action.

To learn the result of an operation, you need a rule that handles the results of the procedure. This type of rule helps you control the objects addressed by the rule.

Select **Actions > Create** in the Rules Package accordion pane to define rules that enable you to learn the results of operations.

To learn more about how to build rules, see **AGC > Configure > Rules**.

## Target

Click this icon to view information about the target driver. This information is also available when you click **driver Configuration** on a selected connector.

## Synchronize (Sync.)

This icon, available only in the **Channel-Reconciliation** tab, is currently not active.

## Cache

Click the **Cache** icon to view the data used for the Reconciliation process and read by the target.

Use any of the following filters (after selecting **Filter**) to find a target cache:

Table 135. Target Cache filters



Filter	Description
Account	Account ID on Identity Governance and Intelligence.
Permission	The name of the permission of the account.

Table 135. Target Cache filters (continued)

Filter	Description
Status	Flag this checkbox to search for inactive target caches only.

The target caches are listed in the **Target Cache** tab. The primary target cache attributes displayed are:

Table 136. Main Target Cache attributes

Attribute	Description
Account	The user ID on Identity Governance and Intelligence.
Permission	The name of the permission of the account.
Events Marker	The events marker associated with the target.
Load Date	The data loading date.
Status	 : the account is active.  : the account is not active.

## Monitor

The functions that are available for monitoring some elements are contained in the following list.

- Connector Status
- Reconciliation Status

### Connectors status

This section enables you to start, stop, and schedule your defined connectors.



The Connector Status pane contains the list of inventoried connectors and filters for the connectors search (click **Filter/Hide Filter**), as summarized in the table below:

Table 137. Connector filters

Filter	Description
Name	The name of the connector.
Active	<b>Yes</b> The connector is currently active. <b>No</b> The connector is not currently active.

The results produced are characterized by the attributes summarized in the table below:

Table 138. Connector attributes

Attribute	Description
Active	<p><b>Local/External Scheduling</b> The connector is running in Local/External scheduling.</p> <p><b>Stopped</b> The connector is stopped.</p>
Name	The name of the connector.
WTO	If the  icon is shown, the Write to channel is enabled.
RFROM	If the  icon is shown, the Read from channel is enabled.
Status	<p>The available status for the connectors are:</p> <p><b>Running</b> The connector is running.</p> <p><b>Pending</b> The connector is waiting to be started.</p> <p><b>Error</b> There was an error while the connector was running</p> <p><b>Stopped</b> The connector is stopped.</p>
Last Run / Start	The last start date of the connector ( <i>dd-Month-yyyy; hh:mm:ss</i> ).

To start or stop a connector, select the connector and click **Start** or **Stop** in the **Actions** menu.

The **Connector Status Details** tab includes the following boxes:

#### Details

Shows the following information:

Table 139. Details box attributes.

Attribute	Description
Name	The name of the connector.
Description	A description of the connector.
Message	The message that you want to be displayed when an error occurs in the execution.
Last Run/Start	The last start date of the connector ( <i>dd-Month-yyyy; hh:mm:ss</i> )
Last Run/Elapsed	The elapsed time of execution ( <i>hh:mm:ss</i> ).

#### Scheduling

Is where you enter the following information if you want to schedule connector runs:

Table 140. Scheduling box attributes

Attribute	Description
Local Scheduling/ External Scheduling	<p>Selecting the <b>Local Scheduling</b> radio button, the runs are scheduled from the <b>Connector Status</b> tab.</p> <p>Selecting the <b>External Scheduling</b> radio button, the runs are scheduled from the Task Planner module and all the options that follow become unavailable in this pane.</p>

Table 140. Scheduling box attributes (continued)

Attribute	Description
Frequency	Use this combo box to set the frequency of the connector runs.
Immediately	Select this check box to start the connector immediately. This selection overrides any date you specify in the field below.
Date	Select the date ( <i>dd/mm/yyyy</i> ) and time ( <i>hh:mm</i> ) of the connector start.

Click **Edit** to modify the content of these boxes. Then click **Save** to enable your selections.

The **Connector History** tab is where you can view a history of the outcomes of the past runs of a selected connector, based on the channel mode.

You can enter the following information to filter your search for past runs:

Table 141. Connector History filters

Filter	Description
Start Date from	Shows all runs started from this date onwards.
Start Date to	Shows all runs started until this date.
Result	Can be: <ul style="list-style-type: none"> <li>• Blank (all)</li> <li>• Completed</li> <li>• Error</li> </ul>

The list of connector runs in Reconciliation mode is shown in the following columns:

Table 142. Connector History attributes

Attribute	Description
Channel Mode	Can be Write to or Read from.
Result	Completed or Error.
Message	The message displayed in the <b>Message</b> text box.
Start Date	The starting date and time the connector run started.
Elapsed Time	The completion (if successful) or ending (if in error) time of the run.

To delete a particular run history line from the list, select the line and click **Actions > Remove**. To delete all run histories, click **Actions > Remove All**.

## Reconciliation status

This section enables you to start and schedule connectors in Reconciliation mode.

The Reconciliation Status pane contains the list of inventoried connectors and filters for the connectors search (click **Filter/Hide Filter**), as summarized in the table below:

Table 143. Connector filters

Filter	Description
Name	The name of the connector.
Active	<b>Yes</b> The connector is currently active. <b>No</b> The connector is not currently active.

The results produced are characterized by the attributes summarized in the table below:

Table 144. Connector attributes

Attribute	Description
Active	<b>Local/External Scheduling</b> The connector is running in Local/External scheduling. <b>Stopped</b> The connector is stopped.
Name	The name of the connector.
Status	The available status for the connectors are: <b>Running</b> The connector is running. <b>Pending</b> The connector is waiting to be started. <b>Error</b> There was an error while the connector was running <b>Stopped</b> The connector is stopped.
Last Run / Start	The last start date of the connector ( <i>dd-Month-yyyy; hh:mm:ss</i> ).

To start or stop a connector, select the connector and click **Start** or **Stop** in the **Actions** menu.

The **Reconciliation Status Details** tab includes the following boxes:

#### Details

Shows the following information:

Table 145. Details box attributes.

Attribute	Description
Name	The name of the connector.
Description	A description of the connector.
Message	The message that you want to be displayed when an error occurs in the execution.
Last Run/Start	The last start date of the connector ( <i>dd-Month-yyyy; hh:mm:ss</i> )
Last Run/Elapsed	The elapsed time of execution ( <i>hh:mm:ss</i> ).

#### Scheduling

Is where you enter the following information if you want to schedule connector runs:



Table 146. Scheduling box attributes

Attribute	Description
Local Scheduling/ External Scheduling	Selecting the <b>Local Scheduling</b> radio button, the runs are scheduled from the <b>Connector Status</b> tab.  Selecting the <b>External Scheduling</b> radio button, the runs are scheduled from the Task Planner module and all the options that follow become unavailable in this pane.
Frequency	Use this combo box to set the frequency of the connector runs.
Immediately	Select this check box to start the connector immediately. This selection overrides any date you specify in the field below.
Date	Select the date ( <i>dd/mm/yyyy</i> ) and time ( <i>hh:mm</i> ) of the connector start.

### Advanced Settings

Is where you specify the following advanced settings for local scheduling:

Table 147. Advanced Settings box attributes

Attribute	Description
Mode	Select one of the following:  <b>Synchronization</b> Generates a short report and places it in the <b>Message</b> text box. In addition, the detailed list of associated events can be viewed in one of these places: <ul style="list-style-type: none"> <li>• By selecting <b>Manage &gt; Connectors &gt; Channel-Reconciliation &gt; Events Queue</b> after selecting the connector.</li> <li>• By going to <b>AGCore &gt; Monitor &gt; Target Queue</b>.</li> </ul> <b>Simulation</b> Generates the report and places it in the <b>Message</b> text box.
Used Data	Select one of the following actions on the cached data after it is processed:  <b>Refresh from Target</b> Processed data is deleted from the cache table of the connectors and reloaded from the target.  <b>Cached data</b> Processed data is maintained.

Click **Edit** to modify the content of these boxes. Then click **Save** to enable your selections.

The **Connector History** tab is where you can view a history of the outcomes of the past runs of a selected connector, based on the channel mode.

You can enter the following information to filter your search for past runs:

Table 148. Connector History filters

Filter	Description
Start Date from	Shows all runs started from this date onwards.
Start Date to	Shows all runs started until this date.
Result	Can be: <ul style="list-style-type: none"> <li>• Blank (all)</li> <li>• Completed</li> <li>• Error</li> </ul>

The list of connector runs in Reconciliation mode is shown in the following columns:

Table 149. Connector History attributes

Attribute	Description
Channel Mode	Reconciliation.
Result	Completed or Error.
Message	The message displayed in the <b>Message</b> text box.
Start Date	The starting date and time the connector run started.
Elapsed Time	The completion (if successful) or ending (if in error) time of the run.

To delete a particular run history line from the list, select the line and click **Actions > Remove**. To delete all run histories, click **Actions > Remove All**.

---

## Settings

In this panel you can update the Object Class nodes and Object Class Field nodes of the IDEAS driver which map the layout of data in your Identity Governance and Intelligence security model.

Object Class nodes and Object Class Field nodes make up the structure in which information, such as user names, roles, groups, accounts, passwords, and any other type of data used in your security model is mapped in the model. An Object Class node contains several Object Class Field nodes and every Object Class displays its fields in a tree structure in this pane.

The IDEAS driver already comes with its own list of attributes, but you can define additional attributes to this driver, as well as edit and remove these attributes to comply with the changes of your security model.

The Settings panel displays the list of the Object Class nodes defined in the IDEAS driver. Each Object Class node can be expanded to display its Object Class Field nodes. The information is shown in the following way:

Table 150. Settings > IDEAS driver panel layout.

Name	Description
Field Name	The name of the Object Class nodes and, when expanded, of their Object Class Field nodes.
Description	A description of the Object Class node.
Type	The Java data codes of the Object Class Field nodes.
Is Multivalued	Shows if the field can have more than one value. Can be true or false.

Click **Actions** > **Add** to add:

- A New Object Class node
- An Object Class Field node

as follows:

- If you click **Add** with no selected Object Class nodes in the list, you are shown the Add node window with the following fields:

Table 151. New Object Class node attributes.

Name	Description
Name	The name of the Object Class
Description	A description of the Object Class

- If you click **Add** with a selected Object Class node, the Add node window gives you the choice of specifying the attributes of another Object Class node or those of a field of the selected node (Add Object Class Field node to *node\_name*). If you opt for adding an Object Class Field node, the attributes you must specify are:

Table 152. Object Class Field node attributes.

Name	Description
Name	The name of the Object Class Field node
Description	A description of the Object Class Field node
Type	Click the arrow to display a list of Java data codes to choose from
Multivalued	Flag this check box if the field will have more than one value

The Object Class Fields are added as hierarchy leafs to the Object Class node. You can add as many fields to an Object Class node as required. Ultimately, each Object Class node is displayed with all its fields in a tree structure.

To edit or remove an Object Class node or an Object Class Field node, select the object and click the appropriate item in the **Actions** menu.

If you click **Actions** > **Automatic Add**, the list is updated with the latest changes in the layout of the AG Core repository.

## Introduction to IRA agent

The Remote Agent (IRA) is part of the Identity Governance and Intelligence platform that lets you receive user events on Windows Active Directory (AD) and Workgroup (WG) from the AD and WG Identity Governance and Intelligence connectors. These events are related to creation/deletion/modification operations of user data.

The component, from the architectural point of view, is a server that listens the connectors and performs the required operations from IBM Security Identity Governance.

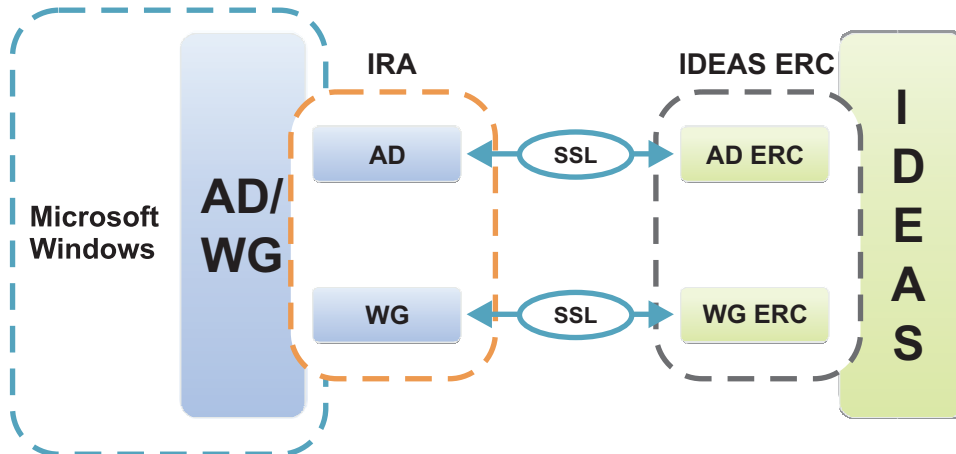


Figure 65. The communication process between AD/WG and Identity Governance and Intelligence.

Several levels of security are provided:

- Define the source IP address
- Choose the IBM Security Identity Governance password for authentication to IDEAS
- Enable the encryption SSL channel

# Security Level










	1	2	3
Single IP			
IRA Auth			
SSL			

Figure 66. Security levels.

For further details, see:

- Prerequisites HW/SW
- Setup options
- Install procedure (example)
- Uninstallation procedure

## Prerequisites

Before proceeding with the installation of IBM Security Identity Governance IRA on the host workstation where AD/WG is located, it is recommended to verify the base hardware and software requirements.

The base hardware and software requirements are described in the tables below:

Hardware requirements		
Element	Description	Note
Server	RAM > = 4 GB	Not applicable
	CPU Cores > = 2	Not applicable
	Storage: 30 MB	Not applicable

Software Requirements		
Element	Description	Note
Operating System	Microsoft Windows 2003 Standard Server SP2	Not applicable
	Microsoft Windows 2008 R2 Standard SP1	
Microsoft .NET	.NET Framework 3.5 SP1	Not applicable

## IRA setup and patches

Two different types of setup are provided, one for the management of the target Active Directory, and one for Workgroups.

Each of them with two versions depending on the type of platform, 32- or 64-bit.

The version of the Active Directory matches, in terms of setup, with the previous version 4.2.1. For this reason, the patches are only for Active Directory versions 32- and 64-bit.

The available setups are four:

- Active Directory 32-bit
- Active Directory 64-bit
- Workgroup 32-bit
- Workgroup 64-bit

Each setup has an associated GUID product. None of these setups can be run on a workstation if another version was previously installed.


	<p><b>Note:</b> Every setup must be used for the first installation.</p> <p>If there is a previous version already installed, an error message is displayed.</p>
---	--


Table 153. IRA setups.

Setup name	Description
setupirac32AD.exe	Installs the Active Directory version for 32-bit workstations.
setupirac64AD.exe	Installs the Active Directory version for 64-bit workstations.
setupirac32WG.exe	Installs the Workgroup version for 32-bit workstations.
setupirac64WG.exe	Installs the Workgroup version for 64-bit workstations.

The following are the IRA patches:

Table 154. IRA patches.

Patches name	Description
patchirac32AD.exe	Updates the Active Directory version for 32-bit workstations.
patchirac64AD.exe	Updates the Active Directory version for 64-bit workstations.

	<p><b>Note:</b> Patches can only be used to update a previous installation.</p> <p>If no version of IRA is installed, an error message is displayed.</p>
---	--

To distinguish the different options available for setup and patches, see the sections below:

- First installation
- Patch updates

### First installation

The first installation is always made in two steps; the basic setup (setup X.0) and the latest patch (patch X.N).

If the patch installed is not the latest, you can directly install the latest patch.

### Patch updates

After the first installation, the version evolution of IRA is managed using a patching process, displayed in the figure:

# Patch Updates

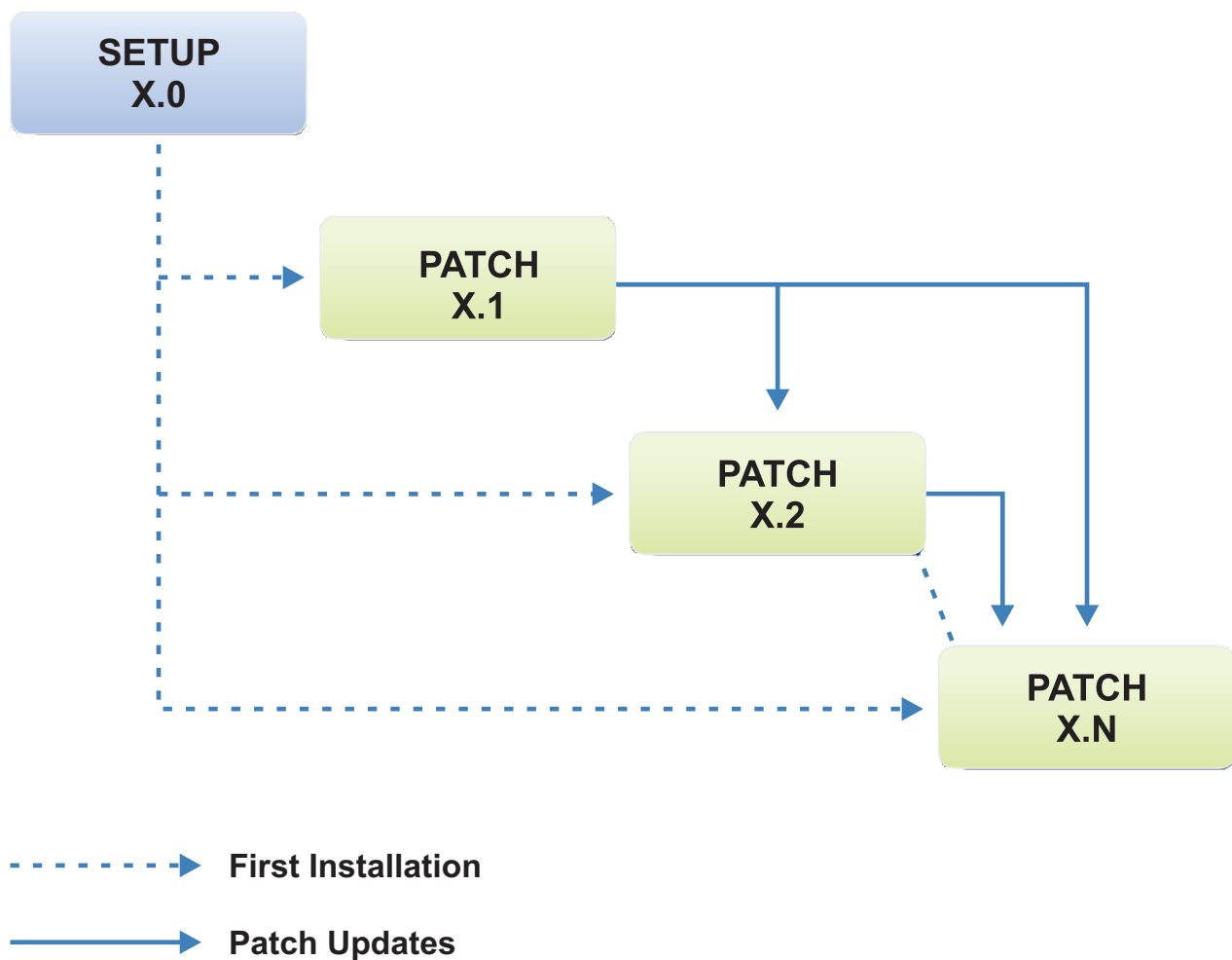


Figure 67. Patch updates.

## Installation procedure

This section shows an example of a remote agent setup.

The following is a setup example for the Identity Governance and Intelligence (IDEAS) remote agent (x64) for Active Directory (setupirac64AD.exe):

1. Click setupirac64AD.exe. The first Warning window opens.
2. Click **Yes** to confirm the operation. The second Warning window opens.
3. Click **Yes** to confirm the operation. The Identity Governance and Intelligence Remote Agent for Active Directory - Installation Shield Wizard window opens.
4. Click **Next** to move to the second step.

Click **Change** if you want to change the default directory, thus click **Next** to move to the third step.

5. Tick the check-box **IBM Security Identity Governance remote agent (core)**

**Note:** IRA contains an optional module (to be selected during the set up) that allows IBM Security Identity Governance to implement the system password change notification. This option requires the Microsoft Windows Password-Filters option. If the administrator decides to install the password change notification service, it is recommended to reboot the workstation both during installation and uninstall phases.

6. Click **Next**, thus click **Install** to start the installation.

After the installation completes, click **Finish** for terminating the installation process.

## Remote agent for active directory

The Remote Agent for Active Directory window is described.

After selecting the IRA console from **Starts**, the Remote Agent for Active Directory window displays:




Figure 68. The Remote Agent for Active Directory window.

From this window, the administrator can perform the following main operations:

- Add Service
- Edit
- Start/Stop
- Properties
- Refresh
- About
- Close

Table 155. Administrator actions

Note	Text
	<b>Note:</b> For some platforms, you might need to start the IRA console by clicking "Run as Admin".



## Add service


Clicking **Add** on the right part of the window, the Add Service window displays. You can fill the fields described in the table below:

Table 156. Add Service window fields

Field name	Description	
<b>Remote Agent ID</b>	Univocal identifier of the remote agent (settled by default).	
<b>Description</b>	Brief description of the remote agent (mandatory).	
<b>Communication</b>	<b>Client</b>	IP of the IBM Security Identity Governance server (mandatory if the <b>All</b> check box is not selected).
	<b>All</b>	Selecting this check box is not mandatory to specify the IP address of the IBM Security Identity Governance server (the <b>Client</b> field will be disabled).
	<b>Port</b>	Listening port of the IBM Security Identity Governance server (mandatory).
<b>Service Account Properties</b>	<b>Modify service account properties</b>	Selecting this check box allows you to modify the service account properties.
	<b>Domain Name</b>	Name of the domain.
	<b>User Name</b>	Name of the administrator.
	<b>Password</b>	Enter the administrator password.
	<b>Confirm</b>	Confirm the password.
<b>Remote Agent Password</b>	<b>Password</b>	Remote agent password (mandatory).
	<b>Confirm</b>	Confirm the password (mandatory).
<b>Secure Socket Layer (SSL)</b>	<b>SSL</b>	Select this check box to enable the server certificate fields.
	<b>SSL Server Certificate Common Name</b>	Enter the certificate name.
	<b>Select Certificate</b>	Click this button to choose the available certificates from the list of the certificate store MY of the workstation.
<b>Log File</b>	<b>Log</b>	Select the check box to enable the <b>Log File</b> field.
	<b>Log File</b>	Enter the path name of the log file.
	<b>Folder button</b>	Click this button to choose the folder where to save the log file. This sets the name of a log file (ira_N.log).

Add service fields

Table 157. Add service fields

Note	Text
	<p><b>Note:</b></p> <p>The IBM Security Identity Governance ERC administrator must enter the same <b>Remote Agent Password</b> in the <b>Driver Connector property</b> fields.</p> <p>From the IBM Security Identity Governance ERC module, select:</p> <p><b>IBM Security Identity Governance ERC &gt; Manage &gt; Connectors &gt; Driver Configuration &gt; Driver.</b></p> <p>Properties involved are:</p> <ul style="list-style-type: none"><li>• adRemoteConnectionPassword for AD IBM Security Identity Governance ERC</li><li>• wgRemoteConnectionPassword for WG IBM Security Identity Governance ERC</li></ul>

Click **Ok** to confirm the operation.


### Edit

Click **Edit** to modify the service properties.


### Delete


Click **Delete** to remove one or more services.

Table 158. Remove services

Note	Text
	<p><b>Note:</b> Before deleting a service, it is not necessary to turn it off.</p>

### Start/Stop

Click **Start** to turn on the service. The service status is characterized by a  green icon.



Click **Stop** to turn off the service. The service status is characterized by a  red icon.

When a service is stopped, an Information window displays.

### Properties

Clicking **Properties**, the Service Properties window displays. You cannot modify any properties.



## Refresh

Clicking **Refresh**, you can update the graphical status of the service ( / ) in case of errors or if someone stopped/started the service from Windows.

## About

Click **About** to view the version and copyright information.

## Close

Click **Close** for closing the IRA console. This action does not affect the status of the service (**Started**  or **Stopped** ).



---

## Chapter 17. Introduction to Access Optimizer

Access Optimizer (AO) is a powerful and comprehensive tool for risk analysis and role mining in medium and big size companies.

IBM Security Identity Governance and Intelligence Access Optimizer (AO) is a powerful and comprehensive tool for risk analysis and role mining in medium and big size companies.

Access Optimizer is fully integrated with IBM Security Identity Governance and Intelligence role management facilities, to support continuous role development and optimization as business processes evolve. New roles can be automatically passed to a role management workflow where the role is approved and deployed to production.

The main advantages of the Access Optimizer engine are:

- Innovative pre-mining analysis finalized to generate intuitive business roles.
- Cost driven role mining with a rich set of parameters to tune the role mining process, minimizing the administrative cost of generated roles.
- Interactive graphical optimization to visually optimize roles with useful information to facilitate coverage analysis of user-privilege relations to identify potential side effects of analysis changes.
- Role lifecycle support integrated with role management for role deployment to production.
- Comprehensive management of risk analysis focused on identifying a certain type of risk for the company to find the right solutions.

---

### Architecture and components

This section describes the main blocks of the Access Optimizer (AO) architecture and specifies the essential peculiarities of each component module.

The following figure summarizes the overall architecture of the AO module:

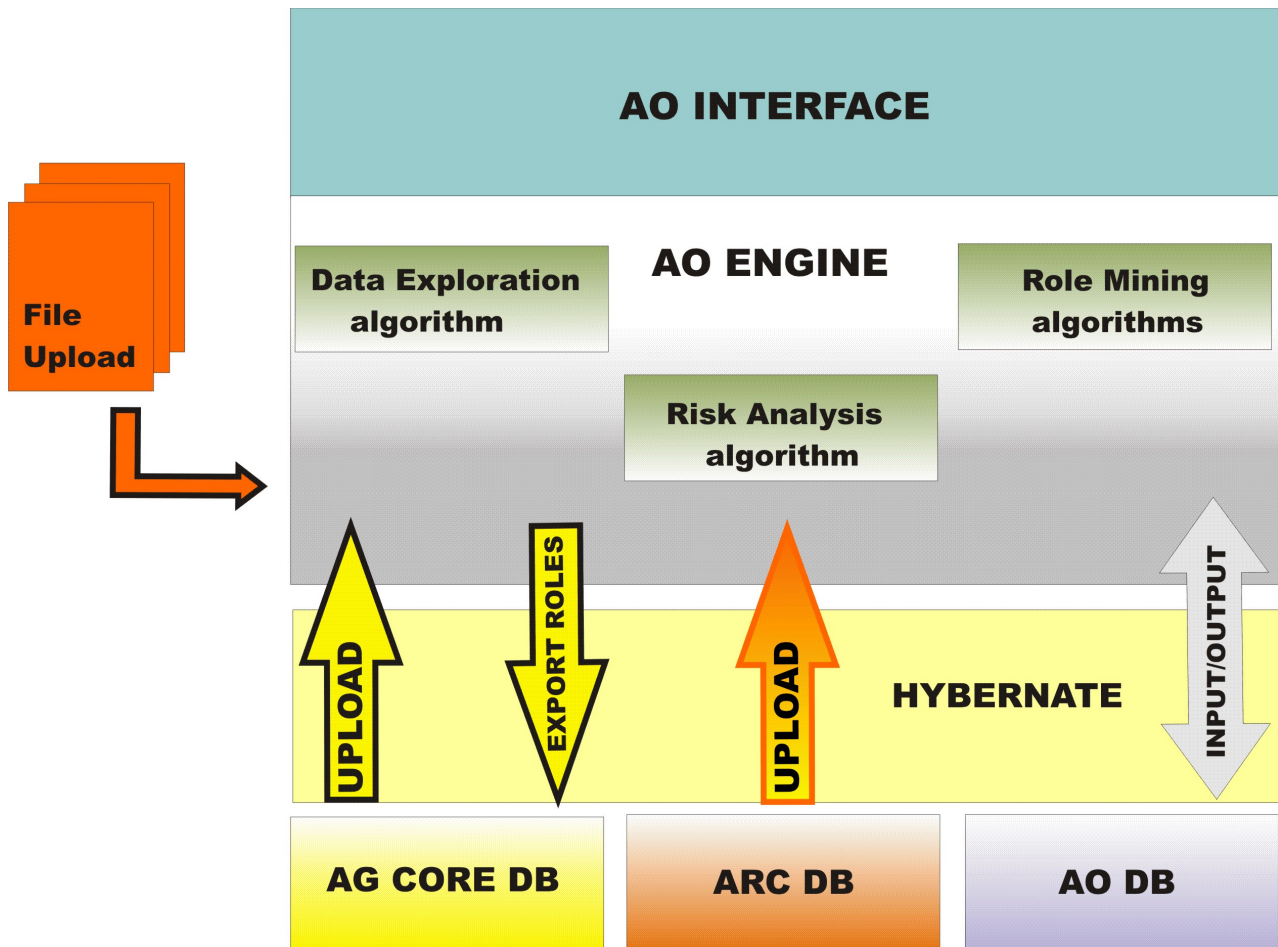


Figure 69. Access Optimizer: Components and architecture.

The following sections describe the features of all modules displayed in the figure above. The main sections are listed below:

- AO Module
- AO Engine
- Access Governance Core Module
- Access Risk Controls Module
- Hibernate Layer

### AO module

The AO module represents the user interface for administering the AO functionality.

More specifically, using this interface you can:

- Load the model dimensions (mainly organization units, users, entitlements, applications and assignments)
- Configure a large set of data model attributes
- Perform the data exploration processes
- Perform risk analysis processes
- Perform role mining processes

- Export the validated candidate roles to the main Access Governance core repository.

For more details about the main characteristics of this module, see *Access Optimizer: Guide to Modeling*.

### **AO engine**

The AO engine implements the data exploration, risk analysis and role mining processes, based on advanced algorithms.

### **Access Governance core module (AG Core)**

The Access Governance core (AG Core) is the Identity Governance and Intelligence module that manages digital identities, and delineates and implements access rights/control.

### **Access risk controls module**

Access risk controls (ARC) is the Identity Governance and Intelligence module that, in the context of authorization definition based on the AG Core RBAC model, implements SOD mechanisms based on the concept of conflicting roles.

### **Hibernate layer**

Hibernate is an ORM (Object Relational Mapping) framework that manages information persistence in the database.

ORM is a group of management methods and techniques that enable an object-oriented paradigm to interact with a relational paradigm of the Relational Database Management Systems (RDBMS). The goal of ORM is to program this interaction using a pure object-oriented paradigm that conceals the relational paradigm translation from the developer.

---

## **The Access Risk approach**

Granting access to resources in a medium or large company can raise the probability of incurring into several types of threats.

To measure and reduce such probability, the Identity Governance and Intelligence model follows the Access Risk approach.

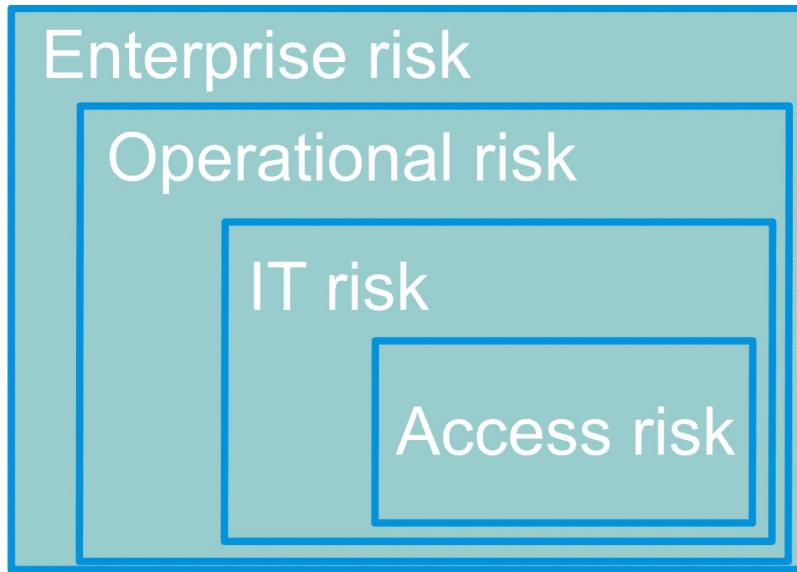


Figure 70. The Access Risk approach.

The Access Risk approach relies on a tagging process of the potential risks related to assigned accesses whereby the key entities managed by the IAG solution are assigned a score. The process provides the capability to drive the most effective remediation measures.

Assigning a score to an access risk, the Access Risk analysis process makes the risk measurable and likely to be mitigated.

Access Risk scoring is based on a viable methodology for modeling, measuring, and reducing the threats to an access, as the next figure shows:

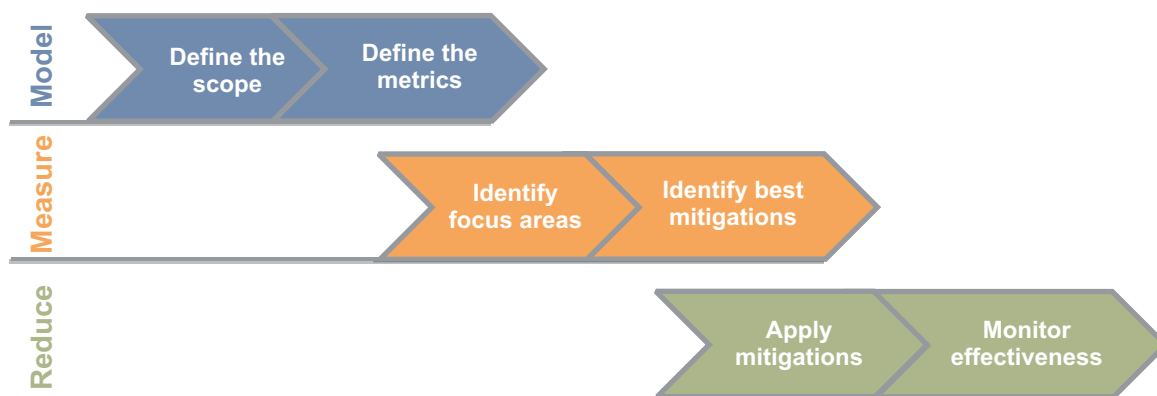


Figure 71. The Access Risk scoring model.

To enable actionable Access Risk scoring, it is necessary to explore the access risk space from the following standpoints:

**Data sets**

Define the data partition (define the scope and identify the focus area).



### Risk Models

Blend access risk contribution types (define the metrics, identify the best mitigation, and apply mitigations).

**Time** Trend analysis and drilldown snapshot (apply mitigations and monitor effectiveness).

The next figure schematically explains the Access risk space:

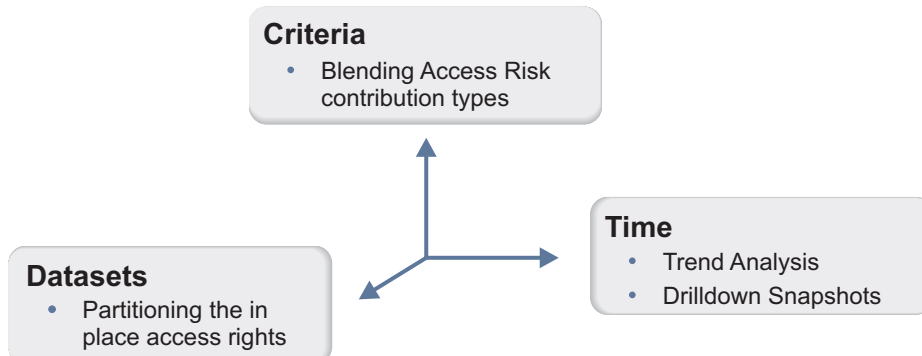


Figure 72. The Access risk space.

The following sections provide a detailed explanation of what it means to explore the access risk space with a viable methodology:

- “Defining an Access data set”
- “Measuring access risk criteria” on page 363
- “Reducing risk distribution” on page 367
- “Monitoring access risk trend over time” on page 367

### Defining an Access data set

The first step is to define the relevant perspectives through the data definition.

The next figure shows an example of data definition:

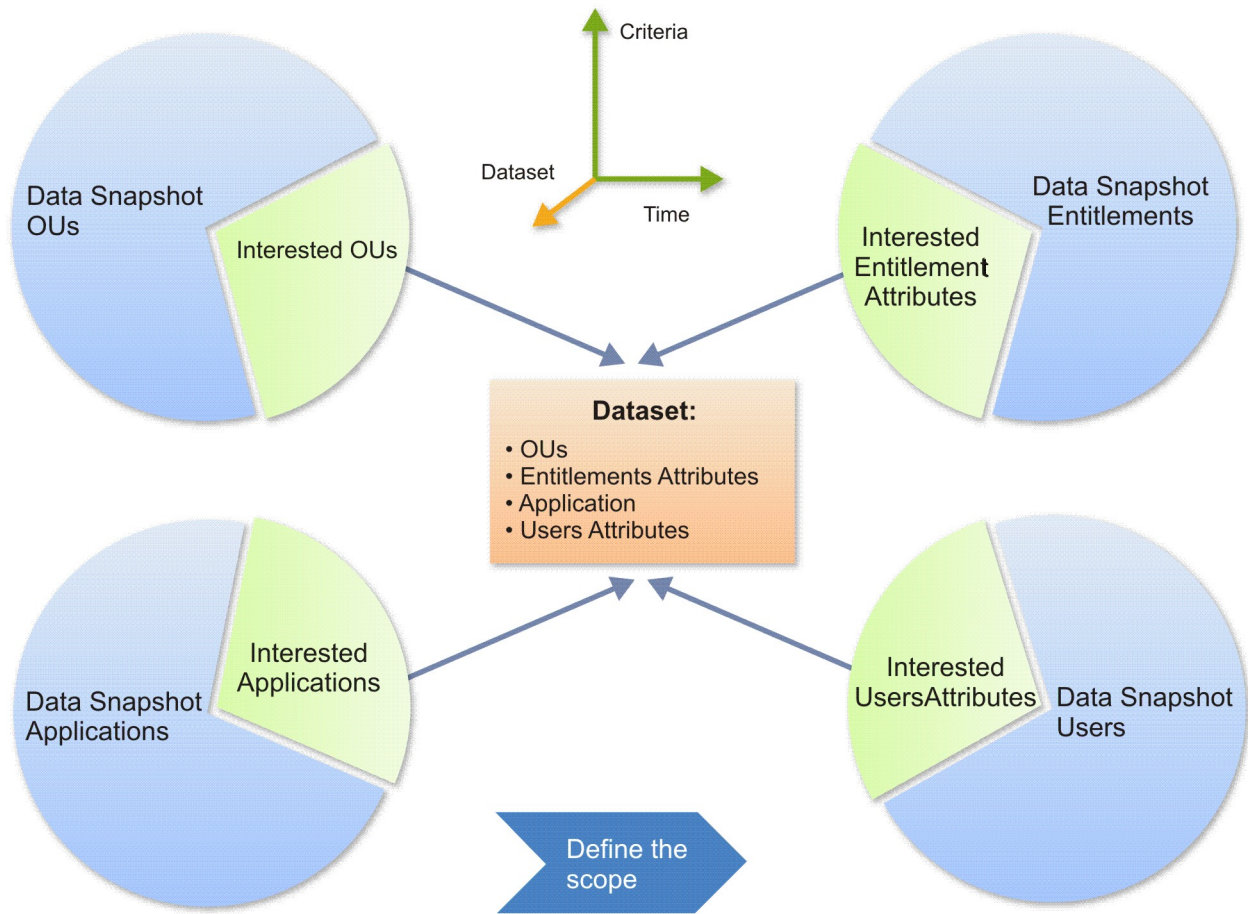


Figure 73. Define a data set.

The figure shows that the relevant OUs, applications, user attributes, and/or entitlement attributes elected for analysis can be grouped in a data set named Access data set. You can define the Access data set by placing the items that you want to inspect in a White List, while placing the elements that you want to exclude from inspection in a Black List. This is shown in the next figure:

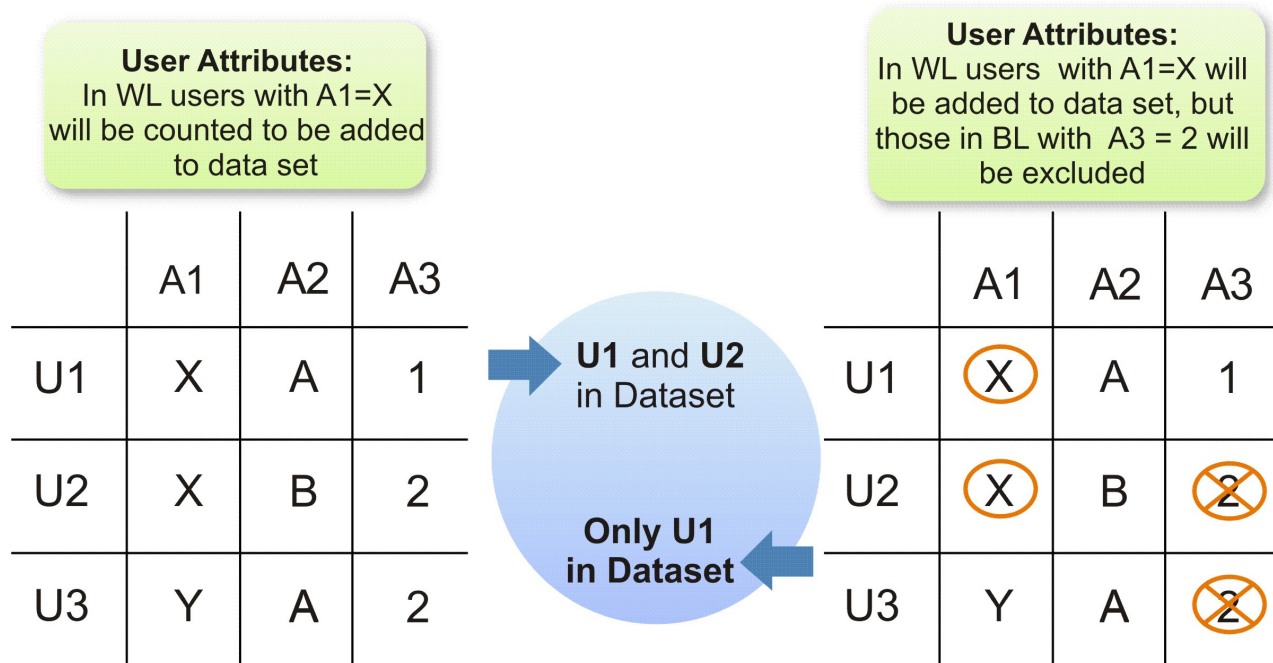


Figure 74. Using black and white lists to define a data set.

The figure shows how to build an Access data set that contains all the users that have the A1=X attribute. To achieve this, in the white list specify all users for whom attribute A1=X. In this way, users U1 and U2 are selected to be included in the data set, as the matrix in the left shows.

Another example is shown by the matrix on the right of the figure, where the Access data set is to include all users with attribute A1=X with the exception of those with attribute A3=2. To achieve this, in the white list specify all users for whom attribute A1=X, and in the black list specify all users for whom attribute A3=2. In this case, user U2 is not added to the data set because, although it has A1=X in the white list, it has A3=2 in the black list. The data set will therefore include only user U1 as it is the only user whose attributes match the desired specifications.

In Access Optimizer you can apply this process to the data (OUs, applications, user attributes, entitlement attributes) on which you want to run a risk analysis. In this way, the risk analysis is performed on an Access data set that includes only the items filtered by the white and black lists.

**Note:** For any given item (OU, application, user, entitlement) you cannot specify the same filter in both white and black lists. If you do so, the filter is ignored when the data is analyzed.

## Measuring access risk criteria

To help the administrator choose the best access risk criteria, Access Optimizer is provided with a predefined catalog.

The predefined catalog is described in the table below:

Table 159. Predefined access risk criteria.

Risk criteria	Description
<b>All Relevances</b>	Global risk score on the assignments to identify critical data sets.
<b>Not Recertified</b>	Higher risk score on assignments not recently certified.
<b>Power Users</b>	Higher risk score on users with critical permissions. (bound to many business activities).
<b>SoD Risk</b>	Higher risk score on users with many SoD conflicts.
<b>The Almightyies</b>	Higher risk score on entitlements bound to many business activities, assigned to users with many SoD conflicts but not recently certified.
<b>The Exceptions</b>	Higher risk score on assignments too different from their peers.
<b>The Others</b>	Higher risk score on assignments too different from their peers and not recently certified.

These criteria are a compound of metrics that optimize the risk analysis. Metrics are all configurable and removable. The only exception is the first criteria, All Relevances, which comprises all available risk criteria metric objects.

The compound metric objects are:

- **User Relevance:** relevant information about the user's attributes.
- **Entitlement Relevance:** relevant information about the entitlement's attributes.
- **Assignment Relevance:** relevant information about the assignment's attributes.

You can also customize new risk criteria and relevance depending on your needs. You can use the following filters to search relevant information about these entities:

Table 160. Relevance filters

Filter	Description	ON	OFF
<b>User relevance</b>	Number of assigned permissions	Evaluated in the risk analysis.	Not evaluated in the risk analysis.
	Number of SoD violations		
<b>Entitlement relevance</b>	Number of assigned business activities		
	Number of SoD constraints		
<b>Assignment relevance</b>	Similarity divergence		
	Last certification age		

The access risk models and metrics definitions help the administrator identify the highest access risk place, or focus area, and how the risk spans over different partitions (Access distribution).

The next figure shows an example of what it means to identify the focus area:

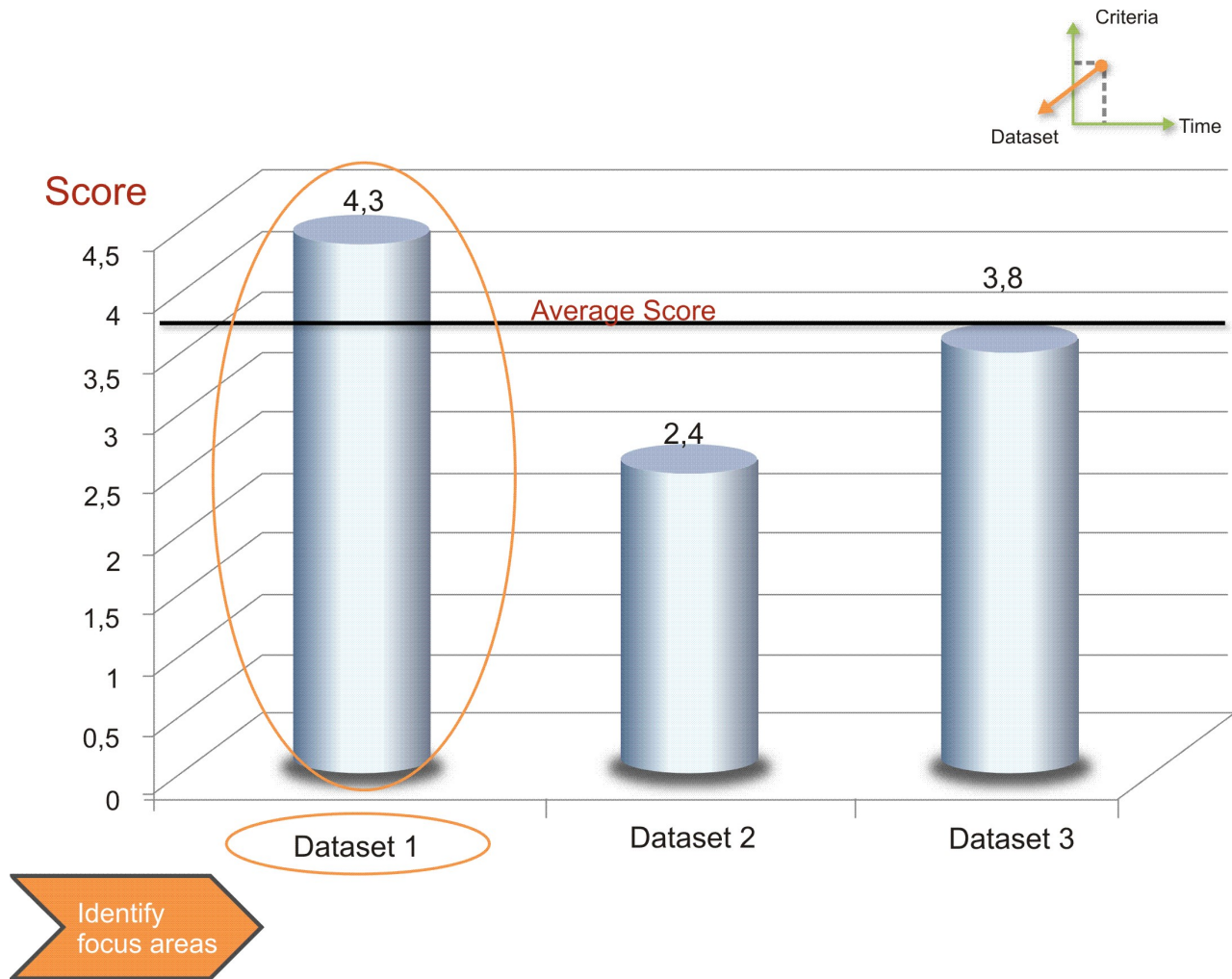


Figure 75. Identify focus area.

In this way, the administrator can immediately visualize the focus Area in data set 1 but, after the focus area is identified, the administrator also needs to investigate the cause of the threat. He or she needs to analyze the interested focus area and compare the different risk criteria.

After the data set is analyzed based on the applied risk criteria, the administrator can see in which of the criteria the highest average risk resides, and identify the best mitigations to apply.

Following the example, the next figure shows that data set 1 has the highest average risk in the SoD risk.

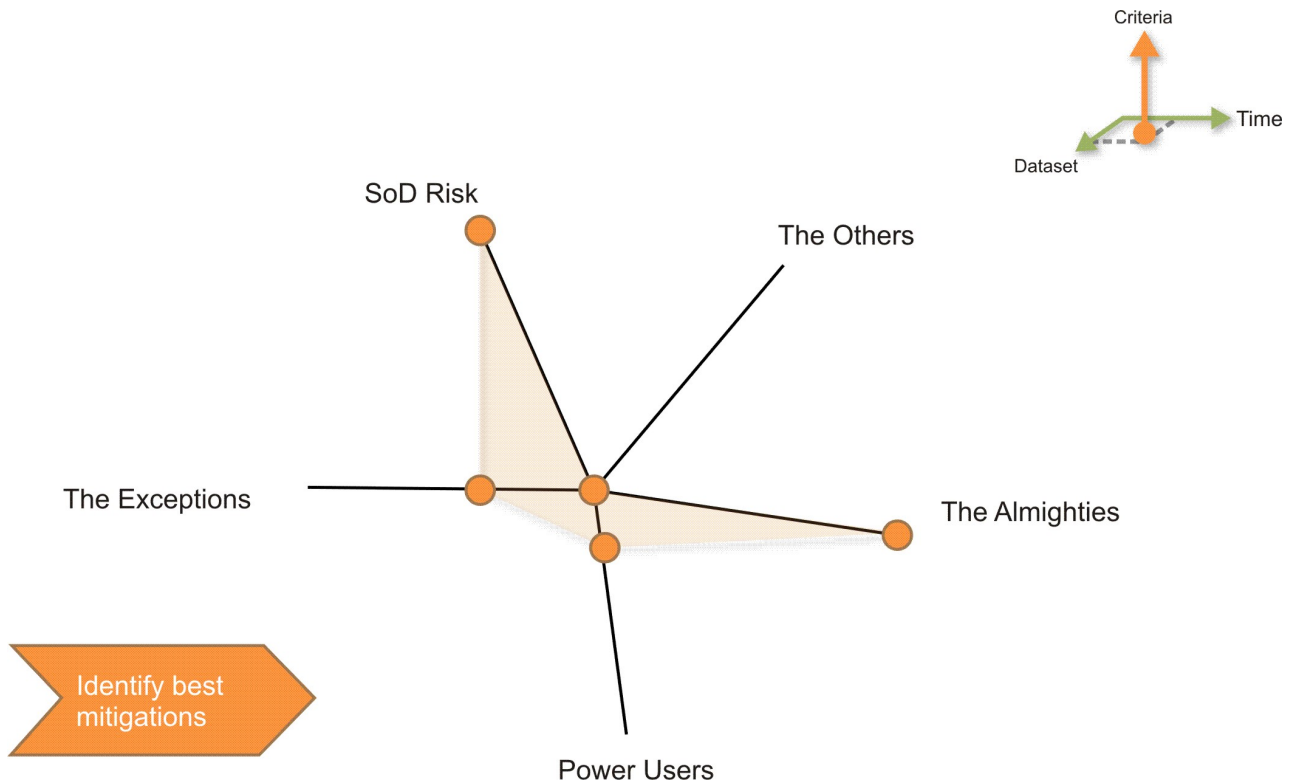


Figure 76. Identifying where the highest risk is.

This means that there are many SoD conflicts in data set 1. Now that the administrator knows where to operate, he or she can choose the best risk mitigating actions.

The most common measures for mitigation are the certification or mitigation campaigns, depending on the risk typology. The access risk criteria configuration suggests the most effective reduction approach. The table below lists a suggested reduction approach for every relevance:

Table 161. The Relevance Reduction Approach.

Name	Description	Suggested reduction approach
User relevance	Number of assigned permissions	Not applicable
	Number of SoD violations	SoD campaign
Entitlement relevance	Number of assigned business activities	Not applicable
	Number of SoD constraints	SoD campaign
Assignments relevance	Similarity divergence	Access certification
	Last certification age	Access certification

**Note:** To get meaningful data, you need to compare snapshots or data sets that contain the same data, updated from time to time. When data is first loaded, a trend graphic is not present.



## Reducing risk distribution

After identifying the type of risk and determining the best solution to minimize it, the administrator must have the detail of how the risk is distributed amongst users and entitlements.

For this, Access Optimizer can provide Maps, where the rows are entitlements and the columns are users, that show the distribution and the magnitude of risk, which can then be easily identified by the administrator.

The next figure shows an example of a risk distribution map:

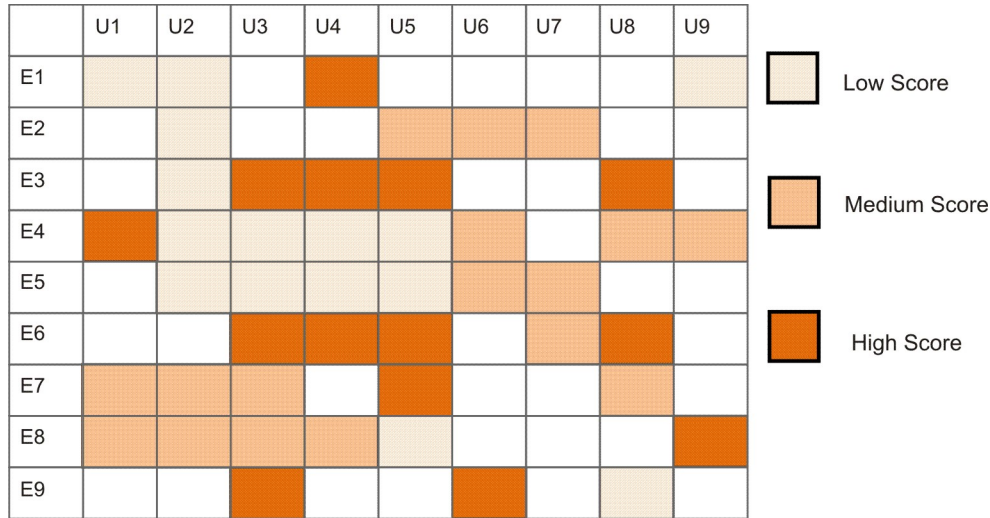


Figure 77. Risk degree and distribution.

The administrator can thus ascertain what combinations of users and entitlements bear the highest risk and require action. He/she can run attestation campaigns on the high risk section only, to gain complete control of the situation and easily manage the risks.

## Monitoring access risk trend over time

By periodically inspecting the access risk space (or access distribution), the administrator can monitor the levels of risk over time, and ascertain the effectiveness of the risk mitigation actions he/she applied.

The following figure shows an example of how the administrator can monitor the presence of risk over time:

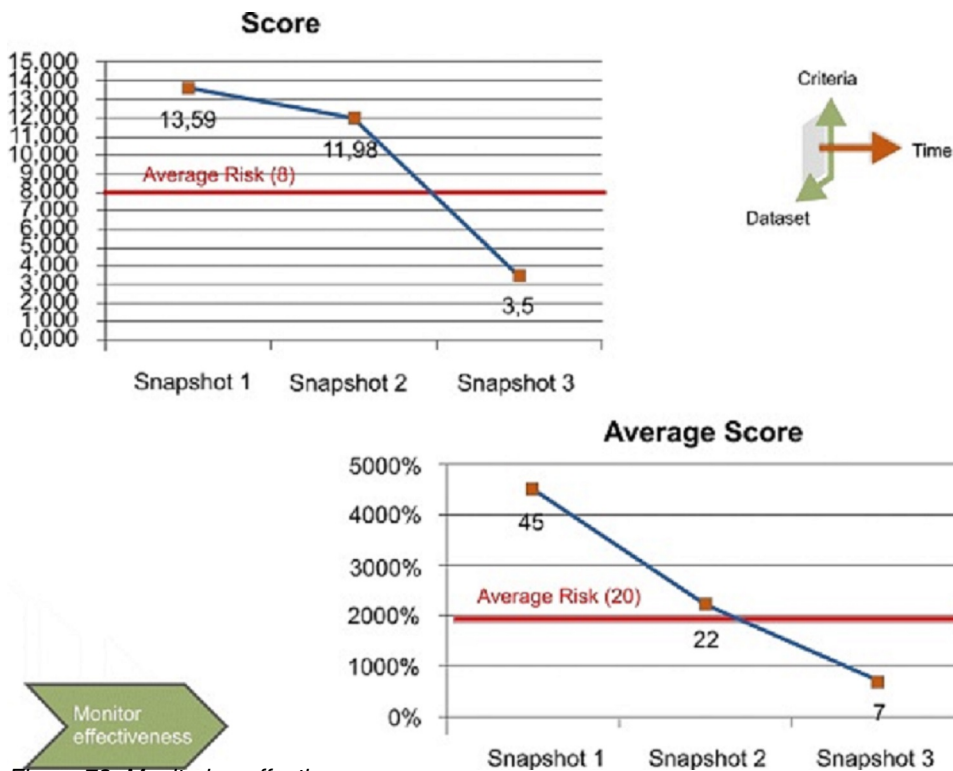


Figure 78. Monitoring effectiveness.

To get this kind of graphic, the administrator must compare more snapshots over time (always updated).

The figure shows that there are three snapshots:

- The first snapshot is taken when the data is first loaded.
- The second one is taken after the data was updated over time with a resulting gradual decrease of risk.
- The third one shows a further reduction of risk.

This means that the administrator mitigated the risk with the appropriate measures and, over time, saw a significant decrease in risk. In this way, the administrator can drive and track the reduction of access risk over time.

**Note:** To get meaningful data, the administrator needs to compare snapshots or data sets that contain the same data, updated from time to time. When data is first loaded, a trend graphic is not present.

## Role mining guidelines

This section describes important role mining modeling concepts, including concerns related to configuration issues that can influence how you interpret the results produced by the role mining algorithms.

The role engineer must have a clear objective for the role mining process to be effective.

Candidate roles can be considered well-formed only when correlated with:

- The characteristics of the input data.
- The role engineer's objective.



In the basic roadmap for Access Optimizer, the role mining step can be exploited with the iterative approach listed below:

1. Run data exploration (**Manage > Data Exploration**).
2. Choose one of the result sets produced in step 1.
3. Run the Optimal Role-set algorithm.
4. Analyze the candidate roles proposed by the results of the previous step.
5. Return to step 3 to refine the analysis.

When you follow the basic roadmap, carefully examine the results provided by step 4.

These main aspects are listed below and described later:

- Minability
- Direct/Hierarchical assignments: Entitlement Type
- Spread
- Farness

## Optimal Role-Set algorithm

This section explains the default parameter values of the Optimal Role-set algorithm. These default values will appear in every new Request operation (**Monitor > Report > Request**).

The Optimal Role-set parameters are described in the table below:

*Table 162. Optimal Role-Set parameters*

Parameter	Description
<b>Minimum Number of Users per Role</b>	Minimum number of users to whom a candidate role can be assigned
<b>Minimum Number of Entitlements per Role</b>	Minimum number of entitlements that can be associated to a profile included in a candidate role
<b>Maximum Number of Roles</b>	Maximum number of candidate roles
<b>Role to User Assignments</b>	Tendency to associate many/few users with a role
<b>Role to Entitlement Assignments</b>	Tendency to construct "large/small" candidate roles, grouping many/few entitlements into a Role
<b>User to Entitlement Assignments</b>	Tendency to associate many/few entitlements with a user (through a subset of candidate roles)
<b>OU Spread</b>	Spread is a numeric index that provides an estimate of the "homogeneous diffusion" of a role in the hierarchical structure of an organization
<b>Application Number</b>	Tendency to associate many/few applications to a user (through a subset of candidate roles)
<b>Entitlement Type Number</b>	Tendency to associate many/few entitlement types to a user (through a subset of candidate roles)

Table 162. Optimal Role-Set parameters (continued)

Parameter	Description
User Attributes	These are listed only if configured in the User Attributes section.
Entitlements Attributes	These are listed only if configured in the Entitlements Attributes section.

## The Minability index

This index, ranging from 0 to 100, represents the main output of the data exploration algorithm.

The Minability index measures the ability to create roles easily and efficiently by aggregating several assignments under a single role. This implies that when assignments are densely aggregated, the role can be identified more easily (High minability). If assignments are scattered throughout the map, it becomes more difficult to choose a meaningful set of assignments to create a candidate role (Low minability).

Generally, high minability values correspond to large aggregations of assignments. This is shown by large and unbroken blocks of assignments in the Entitlements map.

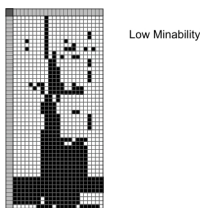


Figure 79. High/Low minability

It is best to avoid examining maps with very high numbers (thousands) of entitlements and users, as you would not obtain very useful information.

## Direct or hierarchal assignments: concept of entitlement type

The Identity Governance and Intelligence data model is based on the concept of hierarchical entitlements.

There are several types of entitlements. They are:

### Permission

It is the basic authorization object. It is defined as a permitted action on a protected object (such as reading and writing a local files or creating a connection).

### IT Role

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

- IT Role(s)
- Permission(s)

### 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 Role(s)
- Permission(s)

**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 within the same organization unit. It can contain:

- Business Role(s)
- IT Role(s)
- External Role(s)
- Permission(s)

A business role (BRole) can be hierarchically formed by business roles, IT roles, external roles, and permissions. An IT role can be formed by IT roles and permissions. An external role can include other external roles and permissions.

The generic hierarchical structure of an entitlement is shown in the following figure.

## Entitlement: Hierarchical Structure

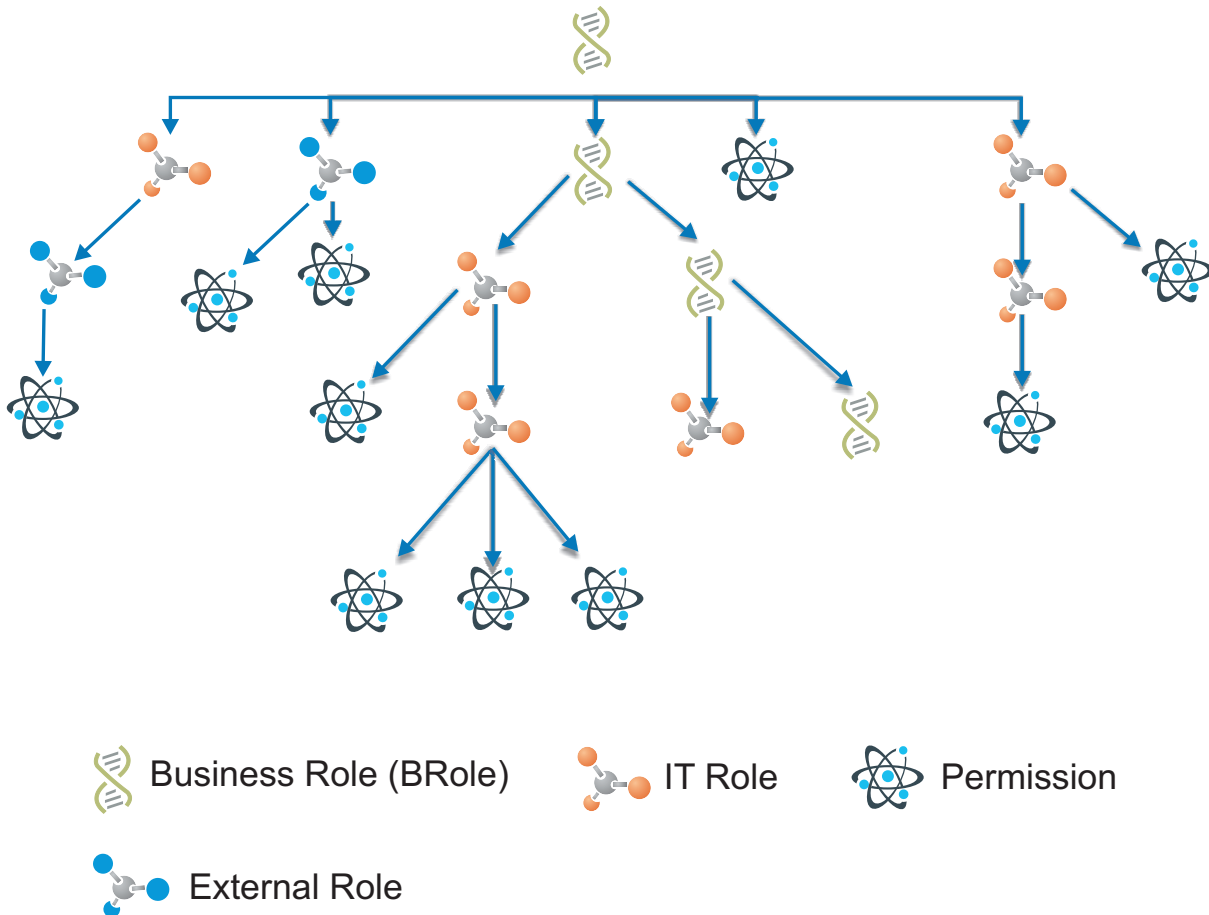


Figure 80. Structure of a generic entitlement

The IBM Security Identity Governance and Intelligence entitlements model does not limit the number of hierarchy levels.

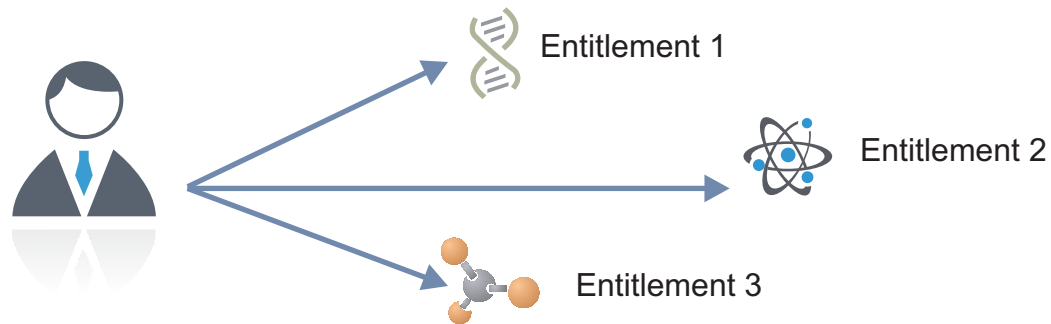
Permissions represent the basic elements on which authorizations are built. The permissions of an application are mapped with target system authorizations that are directly assigned to the users.

In IBM Security Identity Governance and Intelligence you can select  $N$  permissions that are filtered by an application in several sections. The IT Role object collects a set of permissions that are related to the same application.

You can have two types of scenarios.

- an entitlement that is assigned in a direct mode (direct assignment)
- an entitlement that is in a hierarchical structure (hierarchical assignment) is assigned in a hierarchical mode.

## Direct Assignment



## Hierarchical Assignment

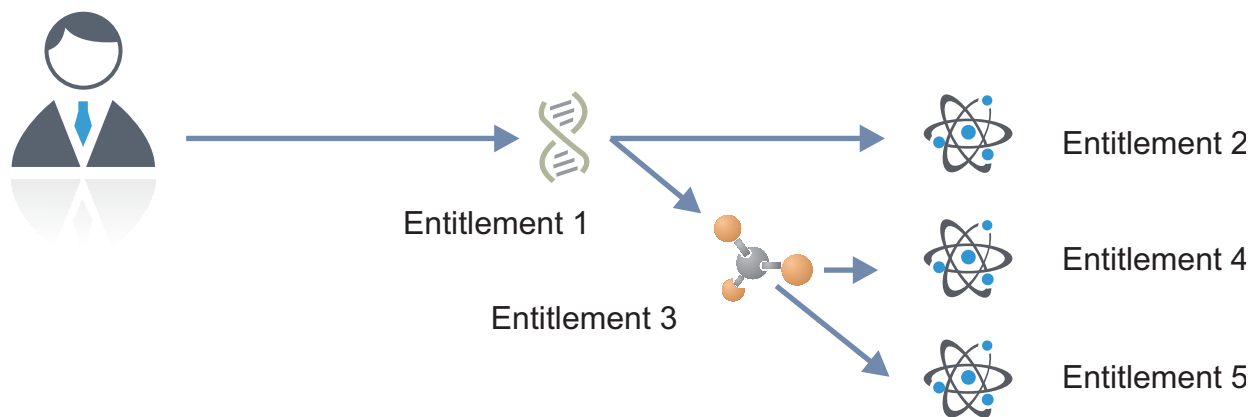


Figure 81. Direct and hierarchical assignment

If you assign the Entitlement 2 (Permission 2) to a user, you directly assign the Entitlement 2 only.

If you assign the Entitlement 1 (Business Role 1) to a user, you directly assign the Entitlement 1. Hierarchically, the user is assigned the Entitlements 2 - 5. This must be taken into consideration during the role engineering activity.

The permissions grouped in an external role are by definition handled by hierarchical assignment, since they cannot be granted individually.

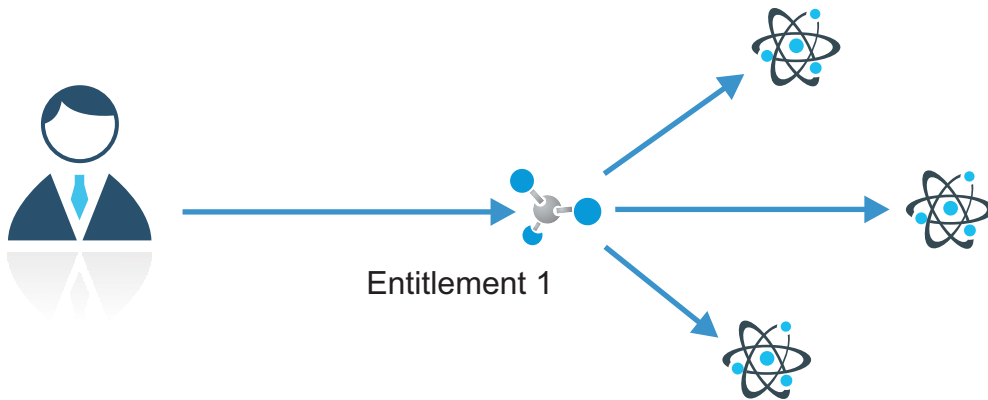


Figure 82. Hierarchical assignment for external roles

During the request construction, the selection of the **Only direct assignments** check box limits the analysis to direct assignments only. If the check box is not selected, inherited entitlements will also be included. This check box is available for all algorithms (data exploration, optimal role set) of the Access Optimizer module.

### **Hierarchical assignments: a blue spotted map**

In the roles map, entitlements hierarchically inherited from another entitlement are highlighted in blue. The involved assignment, instead of being represented by a black box, is outlined in blue.

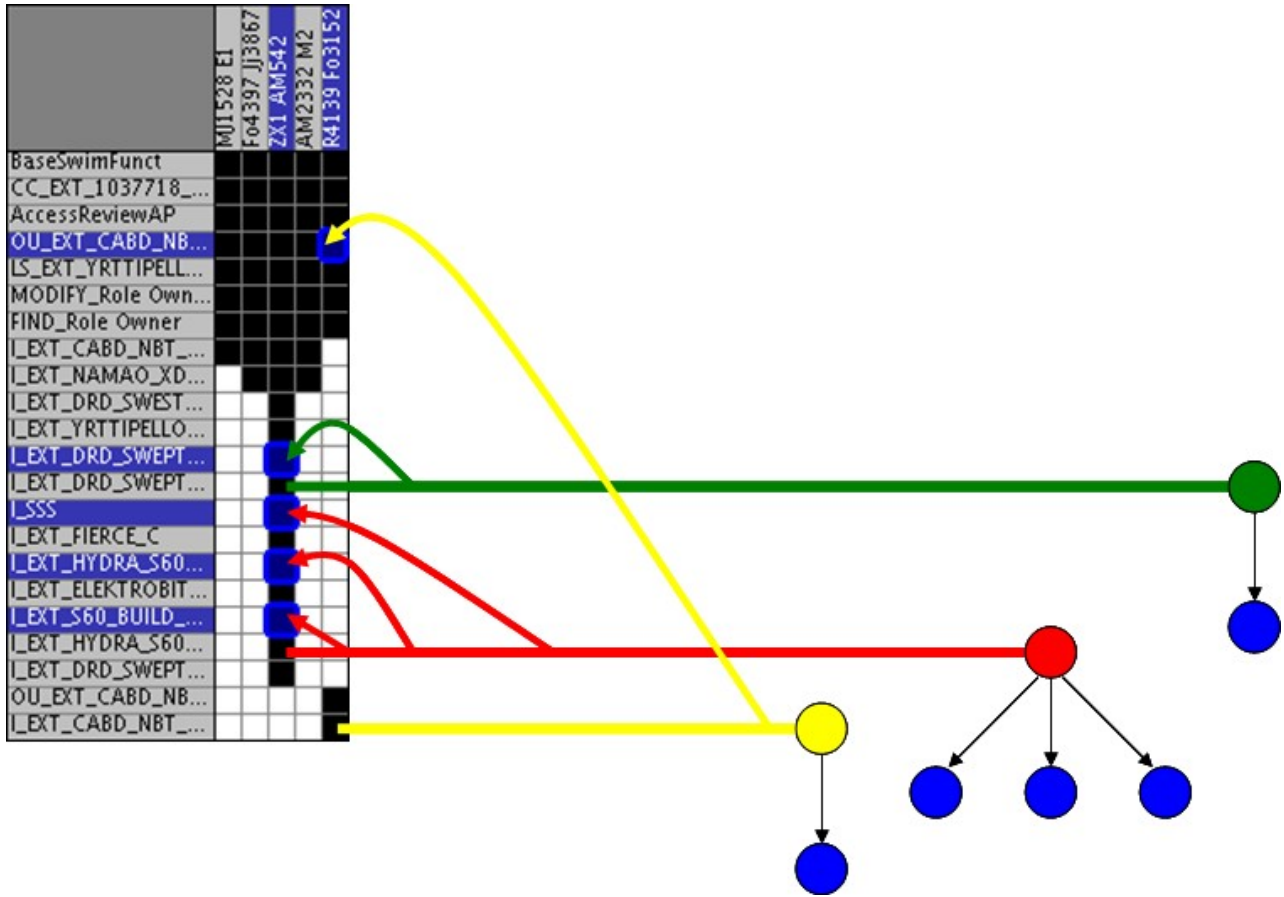


Figure 83. Blue entitlements inherited from others (Yellow, red and green entitlements)

Positioning the mouse pointer on a box outlined in blue triggers a dedicated tooltip which highlights the position coordinates and identifies the parent entitlement, in the form:

**User:** User name, user surname [User code]

**Entitlement:** Entitlement name | Entitlement type | Application name

**Inherited from:** Parent entitlement name | Parent entitlement type | Parent application name

The figure above contains five blue entitlements.

One entitlement has a yellow parent and one a green parent.

The three remaining blue entitlements are all inherited from a red parent.

The creation of the blue spotted map is enabled/disabled by a dedicated check box.

Only direct assignments are available for the following algorithms:

- Data exploration
- Entitlement clusters





If the spread value of a role is very high, the role is not homogeneously scattered over a large number of OUs. In the figure, the spread of Role 4 is very high because Role 4 is associated with users that are not homogeneously scattered throughout the organization tree. This does not provide useful information about the significance of Role 4. In other words, if this role was assigned randomly, no interesting conclusions can be drawn about its actual value in relation to the OUs where it is found, nor in relation to the users registered in these OUs.

Role 2 shows a distribution similar to Role 1, but is not present in any of the OUs of the subtree under consideration. Its spread value is likely greater than 0, so that  $\text{spread } 2 > \text{spread } 1 = 0$

Role 3 has a fairly heterogeneous distribution within the right subtree. This indicates that  $\text{spread } 3 < \text{spread } 4$ , because Role 4 has a heterogeneous distribution throughout the entire organization.

Therefore, if a role has a spread index equal to 0 (or almost 0) compared to a subtree of the organization hierarchy, there is a high concentration of users with that role in the subtree. Moreover, the role is probably “quite suitable” for the users of that subtree.

For example, role INTERNET\_ACCESS is a default role that must be assigned to all users. In this case, the spread is 0 because, since the role is assigned to all users, it is homogeneously distributed over all the OUs of the organization.

**Note:** The spread index can be calculated for every attribute distributed in a hierarchical organization. It is not limited to candidate roles.

## 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.

This index has 0 as its minimum value and no maximum value. It is calculated using the centroid of distribution of Organization units having a fixed entitlement/candidate role.

Calculate the Farness index to answer a question such as: Starting from a generic OU, how many moves are needed along the organization tree to reach the centroid of distribution based on the same entitlement/candidate role of the starting OU?

The following diagrams help explain this concept.

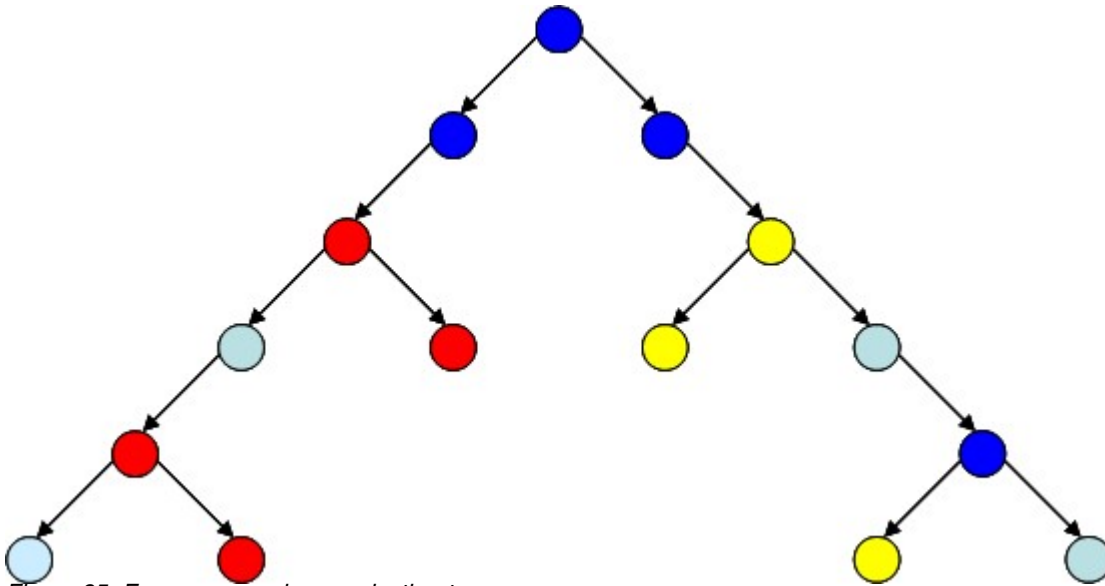


Figure 85. Farness: sample organization tree.

The nodes in this organization tree are colored in correspondence with different entitlements. Take the light-blue entitlement and find where the light-blue centroid of the tree is found.

In this very simple and symmetric tree, the centroid of distribution is easy to locate, as shown below:

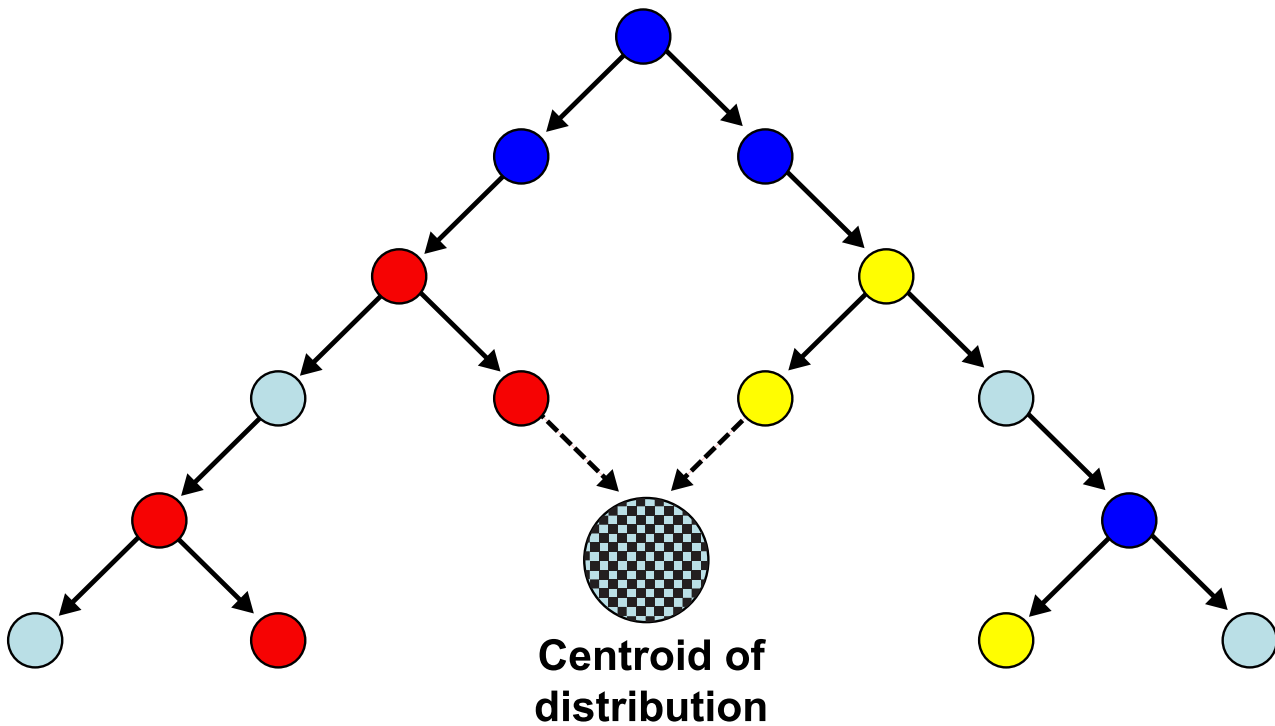


Figure 86. Farness: "virtual" centroid of distribution.

**Note:** The centroid is a virtual entity that can rarely be matched in a real OU.

After the centroid is located, the minimum farness - the shortest possible path from the generic OU to the centroid of the hierarchy - is easy to find. In the organization tree of the previous figure the minimum farness is equal to 3.

The example just shown is a very simplified scheme that is valid only when all OUs have the same number of users. When you try to locate a centroid of distribution, it is very important to acknowledge that different OUs may include very different amounts of users.

The next figure displays an unbalanced organization tree with many closely grouped and highly populated OUs (colored in blue) on the right side of the tree. This is a more realistic scenario.

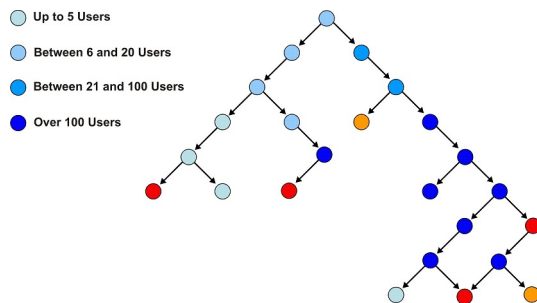


Figure 87. Farness: unbalanced distribution tree

A reasonable position for the virtual centroid of this distribution is:

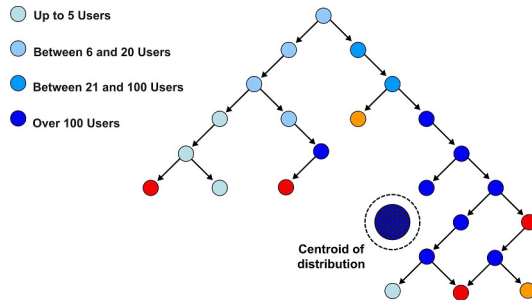


Figure 88. Farness: "virtual" centroid of the unbalanced distribution tree

After locating the centroid, you can calculate the minimum farness by finding the shortest path between the generic OU and the centroid for any blue family OU. The concept of Farness relates to the concept of Spread. Spread is the variance of the farness values calculated for all the involved OUs .

In other words, calculating farness means calculating the distance between an OU and the centroid of the hierarchy, rather than between an OU and a specific attribute such as an entitlement or a candidate role. Spread identifies the diffusion of that attribute throughout the entire hierarchy.

---

## Maps

The visual map of roles and risks is described.

The Identity Governance and Intelligence model uses a "visual map" layout to represent:

- Entitlement-user assignments
- Levels of risk present in entitlement-user assignments

Do become familiar with this visual support before you start working with the Access Optimizer functions, which are all based on the visual map paradigm.

- Role Map
- Map
- Map Management

## Role map

A role map represents entitlement-user assignments.

Good familiarity with role maps is required to:

- Investigate the set of results calculated by the role mining engine.
- Be able to best modify the input data to refine the obtained results set.

The following is an example of a Role map:

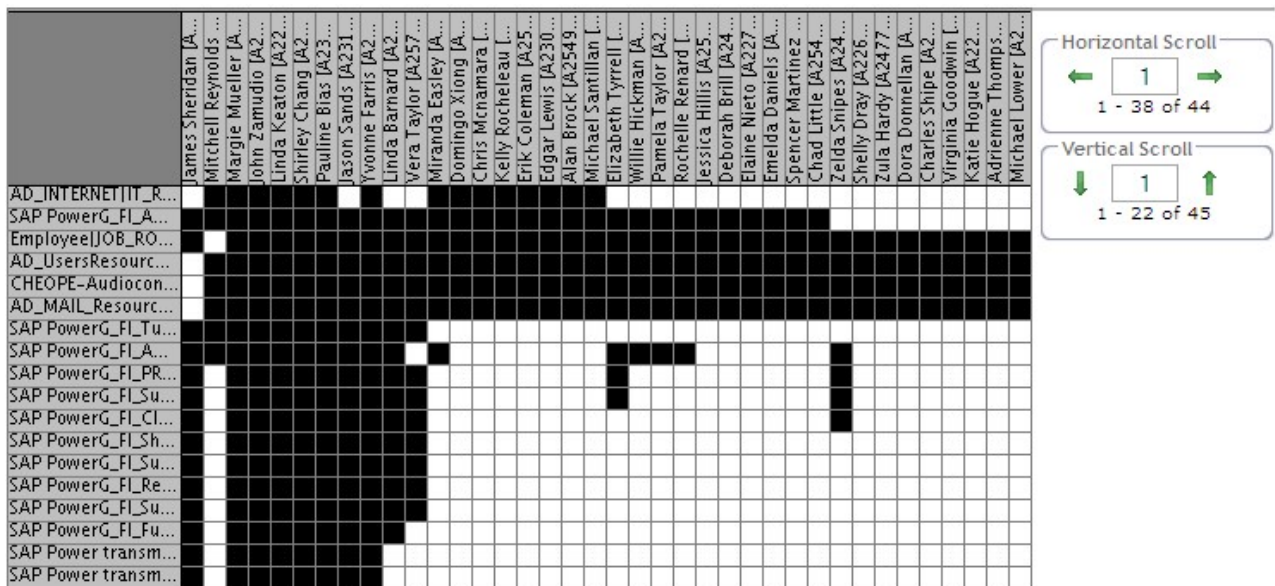


Figure 89. Role map example.

In the map, the vertical axis shows the entitlements whereas the horizontal axis shows the users. The black boxes show when an entitlement is assigned to a user.

If the map is too large to be displayed entirely, use the **Horizontal/Vertical** scrolls, on the right side of the map.

To navigate the map, either click the arrows (← / → or/and ↓ / ↑), or write the desired number directly in the text area and then click the arrows.

Although not all the possible configuration maps can be covered, the more significant role maps are described in the next sections:

- Default Role

- Candidate Roles
- Select Area on the Map
- Exception/Missing filters
- Searching "Out Roles" in the Map
- Zoom on the Map

### Default Role

A Default Role is automatically assigned to all the users of a specific OU.

For example, if in an OU characterized by N entitlements and M users a number of K entitlements is assigned to all M Users, these K Entitlements can indicate a Default Role that can be assigned to all the users of that OU.

In the following map, the same five entitlements are assigned to all the users (7) of the Organization unit.

**Users**

	ZX1 Agya2826	ZX1 Agya3022	ZX1 Agya5011	ZX1 Agya2828	ZX1 Agya3021	ZX1 Agya3020	ZX1 Aj731
<b>Entitlements</b>							
CC_EXT_5248551_...							
I_EXT_EXCLUDED_...							
I_EXT_CN_BJ_PCP_...							
I_EXT_NOKIA_IT_C...							
I_EXT_CN_BJ_PCP_...							
OU_EXT_IT_SBC_0...							
I_S_EXT_183_TIAN...							
I_EXT_CN_BJ_PCP_...							
OU_EXT_M_DSNM_...							
I_EXT_WE_LOGISTI...							
CC_EXT_5105322_...							

Figure 90. A default Role configuration.

The resulting 35 distinct assignments (black boxes) are outlined by the red rectangle. This configuration strongly suggests creating a default role that includes these five entitlements.

The next map presents a similar situation but the last user is assigned only two of the five entitlements.

## Users

Entitlements	ZX1 Agya2826	ZX1 Agya3022	ZX1 Agya5011	ZX1 Agya2828	ZX1 Agya3021	ZX1 Agya3020	ZX1 A1731	
	CC_EXT_5248551_...							
	I_EXT_EXCLUDED_...							
	I_EXT_CN_BJ_PCP_...							
	I_EXT_NOKIA_IT_C...							
	I_EXT_CN_BJ_PCP_...							
	OU_EXT_IT_SBC_0...							
	I_S_EXT_183_TIAN...							
	I_EXT_CN_BJ_PCP_...							
	OU_EXT_M_DSNM_...							
I_EXT_WE_LOGISTI...								
CC_EXT_5105322_...								

Figure 91. Missing Entitlements configuration.

This leads to the definition of a different default role that includes only the two entitlements the users have in common.

	ZX1 Agya2826	ZX1 Agya3022	ZX1 Agya5011	ZX1 Agya2828	ZX1 Agya3021	ZX1 Agya3020	ZX1 A1731
CC_EXT_5248551_...							
I_EXT_EXCLUDED_...							
I_EXT_CN_BJ_PCP_...							
I_EXT_NOKIA_IT_C...							
I_EXT_CN_BJ_PCP_...							
OU_EXT_IT_SBC_0...							
I_S_EXT_183_TIAN...							
I_EXT_CN_BJ_PCP_...							
OU_EXT_M_DSNM_...							
I_EXT_WE_LOGISTI...							
CC_EXT_5105322_...							

Figure 92. Another Default Role configuration.

## Candidate Roles

The Role Mining analysis output is generally built on a set of "Candidate Roles" represented by the black/white box combinations in the map.

The next three figures show examples of output formed by three Candidate Roles.

The first Candidate Role is shown below:

Name	Exp.	Rep.	Users	Entitlements	Assignments
role_1	?	?	1	6	6
role_10	?	?	7	2	14
role_11	?	?	6	3	18

	ZX1_Agya2826	ZX1_Agya3022	ZX1_Agya5011	ZX1_Agya2828	ZX1_Agya3021	ZX1_Agya3020	ZX1_Aj731
CC_EXT_5248551_...							
L_EXT_EXCLUDED_...							
L_EXT_CN_BJ_PCP_...							
L_EXT_NOKIA_IT_C...							
L_EXT_CN_BJ_PCP_...							
OU_EXT_IT_SBC_O...							
LS_EXT_183_TIAN...							
L_EXT_CN_BJ_PCP_...							
OU_EXT_M_DSNM_...							
L_EXT_WE_LOGISTI...							
CC_EXT_5105322_...							

Figure 93. Candidate Role n° 1.

In this situation, a specific Candidate Role built on 6 Entitlements is shaded in brown and can be assigned to only one User.

The second Candidate Role is shown below:

Name	Exp.	Rep.	Users	Entitlements	Assignments
role_1	?	?	1	6	6
role_10	?	?	7	2	14
role_11	?	?	6	3	18

	ZX1_Agya2826	ZX1_Agya3022	ZX1_Agya5011	ZX1_Agya2828	ZX1_Agya3021	ZX1_Agya3020	ZX1_Aj731
CC_EXT_5248551_...							
L_EXT_EXCLUDED_...							
L_EXT_CN_BJ_PCP_...							
L_EXT_NOKIA_IT_C...							
L_EXT_CN_BJ_PCP_...							
OU_EXT_IT_SBC_O...							
LS_EXT_183_TIAN...							
L_EXT_CN_BJ_PCP_...							
OU_EXT_M_DSNM_...							
L_EXT_WE_LOGISTI...							
CC_EXT_5105322_...							

Figure 94. Candidate Role n° 2.

This situation involves 14 assignments, with two Entitlements assigned TO ALL CONSIDERED USERS. Could this be a Default Role? Most likely, even if the Role is only composed of two Entitlements.

The third Candidate Role is shown below:



Name	Exp.	Rep.	Users	Entitlements	Assignments
role_1			1	6	6
role_10			7	2	14
role_11			6	3	18

	ZX1_Agya2826	ZX1_Agya3022	ZX1_Agya5011	ZX1_Agya2828	ZX1_Agya3021	ZX1_Agya3020	ZX1_AJ731
CC_EXT_5248551_...							
I_EXT_EXCLUDED_...							
I_EXT_CN_BJ_PCP_...							
I_EXT_NOKIA_IT_C...							
I_EXT_CN_BJ_PCP_...							
OU_EXT_IT_SBC_O...							
LS_EXT_183_TIAN...							
I_EXT_CN_BJ_PCP_...							
OU_EXT_M_DSNM_...							
I_EXT_WE_LOGISTI...							
CC_EXT_5105322_...							

Figure 95. Candidate Role n° 3.

This can be considered a very common situation, in which K of N (K<N) Entitlements are assigned to H of M (H<M) Users. In this case, 3 of 11 Entitlements are assigned (brown area) to 6 of 7 Users.

	H877 Bz546	H3835 Cx2684	ZX1_AJ650	P278 Jane3193	Kv1037 J4934	H5890 Jane1921	Op3918 EI	ZX1 LN25	ZX1 LN24	ZX1 We4782	ZX1 We1763	ZX1 LN2729
I_EXT_PRM_PPMC_...												
I_EXT_BI_ALL												
I_EXT_SCPR_USERS												
I_EXT_SCPR_APP_...												
I_EXT_CE_USERS_P...												
LN_CDO												
I_EXT_CS_PILOT_IT												
I_EXT_TSWR_R												
BaseSwimFunct												
AccessReviewAP												
MODIFY_Role Own...												
FIND_Role Owner												
LS_EXT_VIALE_LAN...												
LS_VIALE_LANCET...												
I_EXT_NOKIA_ITAL...												
I_EXT_NOKIA_ITAL...												
I_NOKIAALL_LTY1...												
I_EXT_WAH_PRM_...												
I_EMEA_IT_SITE_M...												
I_EXT_PROJECTS_C...												
I_EXT_VMT_USERS												
I_EXT_NBI_IMAFVC...												

	H877 Bz546	H3835 Cx2684	ZX1_AJ650	P278 Jane3193	Kv1037 J4934	H5890 Jane1921	Op3918 EI	ZX1 LN25	ZX1 LN24	ZX1 We4782	ZX1 We1763	ZX1 LN2729
I_EXT_PRM_PPMC_...												
I_EXT_BI_ALL												
I_EXT_SCPR_USERS												
I_EXT_SCPR_APP_...												
I_EXT_CE_USERS_P...												
LN_CDO												
I_EXT_CS_PILOT_IT												
I_EXT_TSWR_R												
BaseSwimFunct												
AccessReviewAP												
MODIFY_Role Own...												
FIND_Role Owner												
LS_EXT_VIALE_LAN...												
LS_VIALE_LANCET...												
I_EXT_NOKIA_ITAL...												
I_EXT_NOKIA_ITAL...												
I_NOKIAALL_LTY1...												
I_EXT_WAH_PRM_...												
I_EMEA_IT_SITE_M...												
I_EXT_PROJECTS_C...												
I_EXT_VMT_USERS												
I_EXT_NBI_IMAFVC...												

Figure 96. Two more examples of Candidate Roles.

The above figure shows an example of another two Candidate Roles.

In the interesting "L" configuration shown below, 8 Entitlements and 4201 Users are displayed. The first two Entitlements are assigned to ALL 4201 Users, while the other six are assigned only to the first two Users. With the scroll positioned on the right side of the Map, it is possible to show all the other assignments.



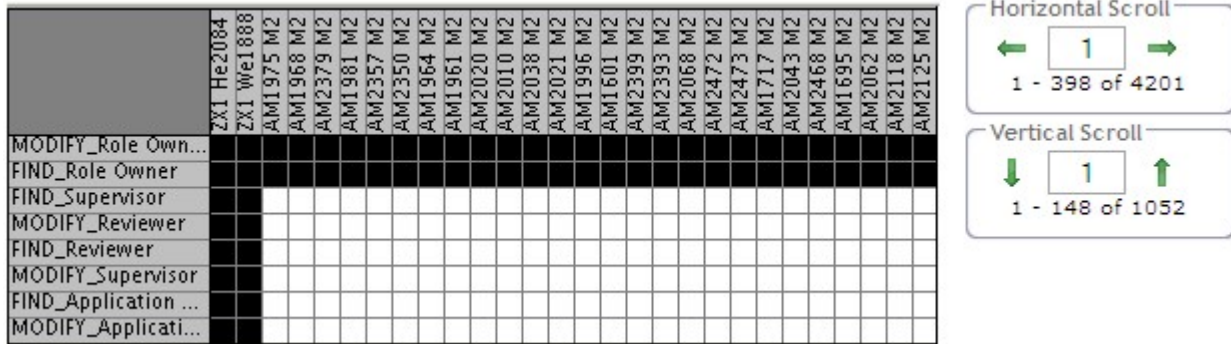


Figure 97. "L" Map.

The Map resolution can always be adjusted using the zoom buttons (**Zoom In/Zoom Out**) (see Map management/functionality).

**Note:** When moving the mouse pointer to a specific position on the Map, a dedicated tooltip appears, highlighting the position's coordinates in the form:

**User :** User name | User surname [User code]

**Entitlement :** Entitlement name | Entitlement type | Application name

### Select Area on the Map

You can analyze user entitlement assignments

One of the approaches to analyze the User-Entitlement assignment, is the selection of an area on the Map.

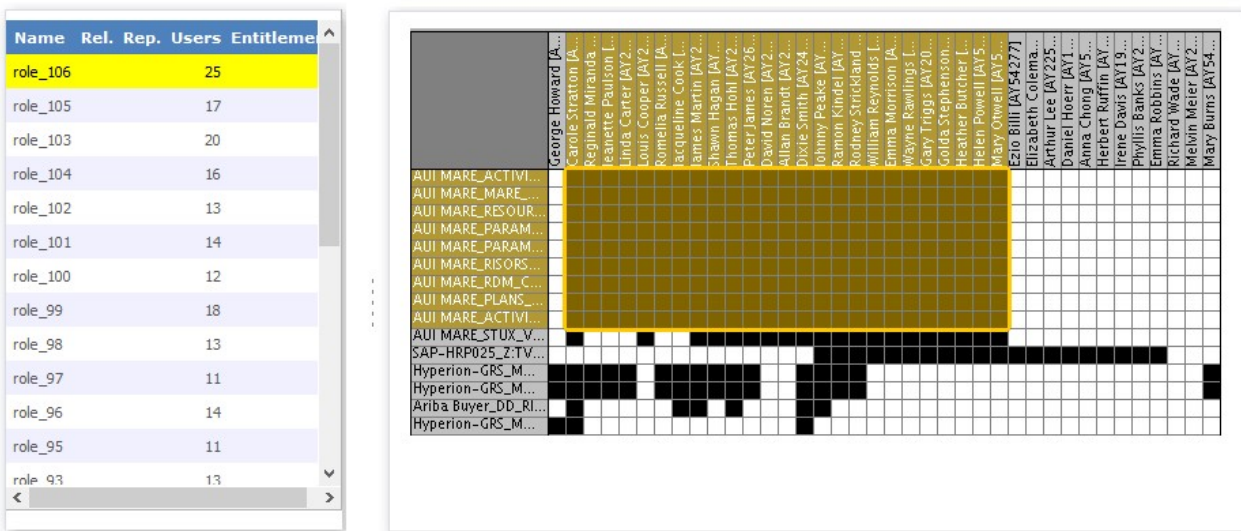


Figure 98. Selection of an area on the Map.

In the figure above is displayed a generic example of the select area operation; this operation is possible by the **Select Area** button.

When the selected area corresponds to a specific Role, in the **Role Search** frame (left), automatically the Role is highlighted in light orange. This feature, make possible to easily identify the Roles already defined.

Another possibility that offer this feature is the easily reorganization of the black blocks in the Map, as shown in the figure below:



Figure 99. Selection of an area and reorganization of it on the Map.

In the figure above, the map has been reorganized based on the selection of the highlighted blocks (Select Area). In this way, the map is built around the Role highlighted.

If it is decided to select one other area and then reorganize again, the map will change again and so on. This operation is possible, after selecting the area, by clicking the **Reshuffle** button.

This feature does not compromise the original meaning of the Map, but allows the Administrator to visualize the different organizations of the existing Roles. It is

possible to group not only the black blocks in an area, but also the white blocks. This operation permits you to use the **Exceptions/Missing** filters.

### Exception and Missing filters

The Exception/Missing assignments analysis is one of the graphic analysis approaches available; they can be considered a "noise analysis" aimed at reaching the "core" assignments by either erasing a subset of "weak assignments" (Exception filter) or adding a subset of "interesting assignments" (Missing filter).

A generic Role Map is shown in the figure below:

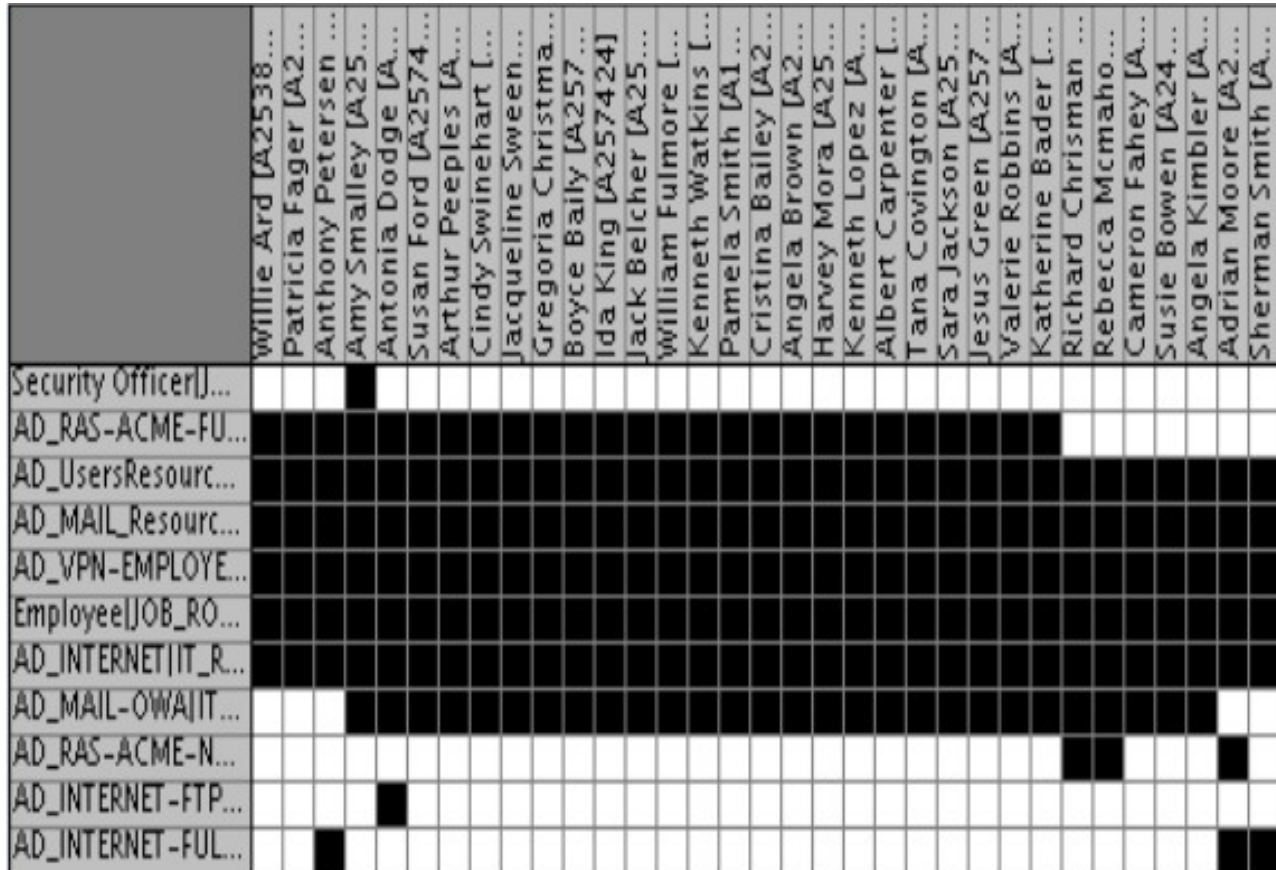


Figure 100. Exceptions Role analysis.

There are two distinct scroll in the upper portion of the **Role Map** frame; the **Exceptions** scroll on the left and the **Missing** scroll on the right.

The **Exceptions** scroll provides a dynamic filter to identify assignments which are more "uneven" and "dissimilar" in relation to the starting Role Map.

Using the  symbol to change the scroll value (from 0 to 100), or writing in the text area the desired exceptions number and clicking the up/down arrow (automatic Exception), shows the "peripheral" assignments in the Role Map configuration. It could be more efficient to segregate such assignments into a well defined Role rather than in the "core zone" of the Map, where "well aggregated" assignments are concentrated.

Thus, assignments which are possibly more efficient segregate into a well-defined Role rather than into the Map's "core zone" concentrated, "well-aggregated" assignments having low red levels ("weak" red).

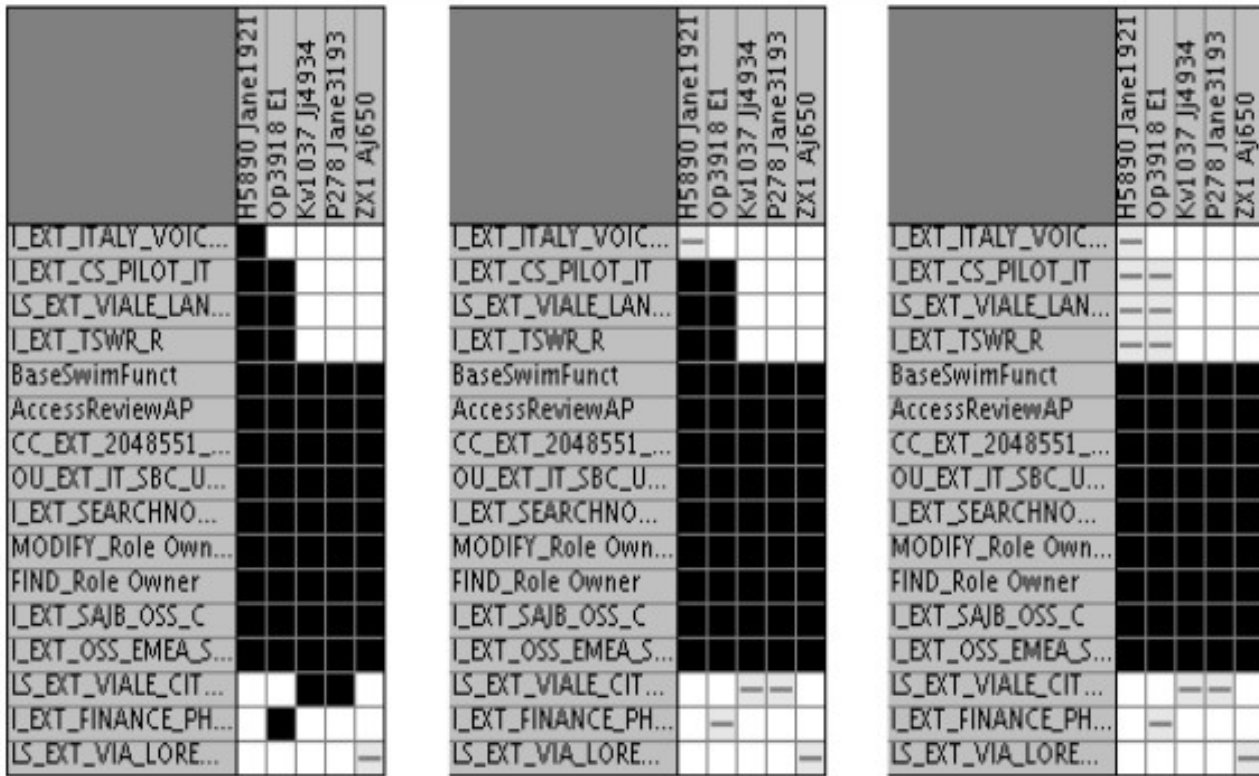


Figure 101. Exception Role analysis: three distinct values.

In the above figure, three distinct values of the **Exceptions** scroll are shown from left to right.

In the left column of the above figure (Exception =10) only one assignment is highlighted in the bottom-right corner of the Map. Those isolated assignments are clearly suitable to be collapsed into a single Entitlement Role.

More assignments are shown by Exception =20.

Exception =50 shows assignments outside the main black-box rectangle -- separate from the ideal "Default Role".

What happens if Exception =100? The result is shown in the next figure:


	H5890 Jane1921	Op3918 E1	Kv1037 Jj4934	P278 Jane3193	ZX1 Aj650
I_EXT_ITALY_VOIC...	—	—	—	—	—
I_EXT_CS_PILOT_IT	—	—	—	—	—
LS_EXT_VIALE_LAN...	—	—	—	—	—
I_EXT_TSWR_R	—	—	—	—	—
BaseSwimFunct	■	—	—	—	—
AccessReviewAP	■	—	—	—	—
CC_EXT_2048551_...	■	—	—	—	—
OU_EXT_IT_SBC_U...	■	—	—	—	—
I_EXT_SEARCHNO...	■	—	—	—	—
MODIFY_Role Own...	■	—	—	—	—
FIND_Role Owner	■	—	—	—	—
I_EXT_SAJB_OSS_C	■	—	—	—	—
I_EXT_OSS_EMEA_S...	■	—	—	—	—
LS_EXT_VIALE_CIT...	—	—	—	—	—
I_EXT_FINANCE_PH...	—	—	—	—	—
LS_EXT_VIA_LORE...	—	—	—	—	—

Figure 102. Exception Role analysis: the "black core" of the Candidate Role.

How must this Map be interpreted?

This is the "core" of the Map where the most meaningful assignments are concentrated.

The RC engine seems to suggest this particular Role, which includes the same Entitlements as the Default Role, but differs in the fact that it is assigned only to two Users. It is quite evident that Exception =100 results in a Candidate Role covering fewer Users than the Exception =50 option.


The same effect will be obtained by directly selecting a black assignment (clicking on it with the left mouse button) and clicking on the  **Remove Assignments** button.

Considering the "noise" concept mentioned earlier, erasing too much noise (high Exception index value), poses the risk of also erasing a lot of good signal!

The figure on the next page provides a qualitative description of this mechanism using the **Exception** index values.

The **Missing** scroll provides a dynamic filter to identify assignments that are "closer" and more "alike" in relation to the starting Role Map.



Using the  symbol to change the scroll value (from 0 to 100) or writing in the text area the desired exceptions number and clicking the up/down arrow (automatic Missing), shows assignments that are "closer" to the Role Map configuration. It would probably be useful to add such assignments to the "core zone" of the Map where there is a "well aggregated" concentration of assignments.

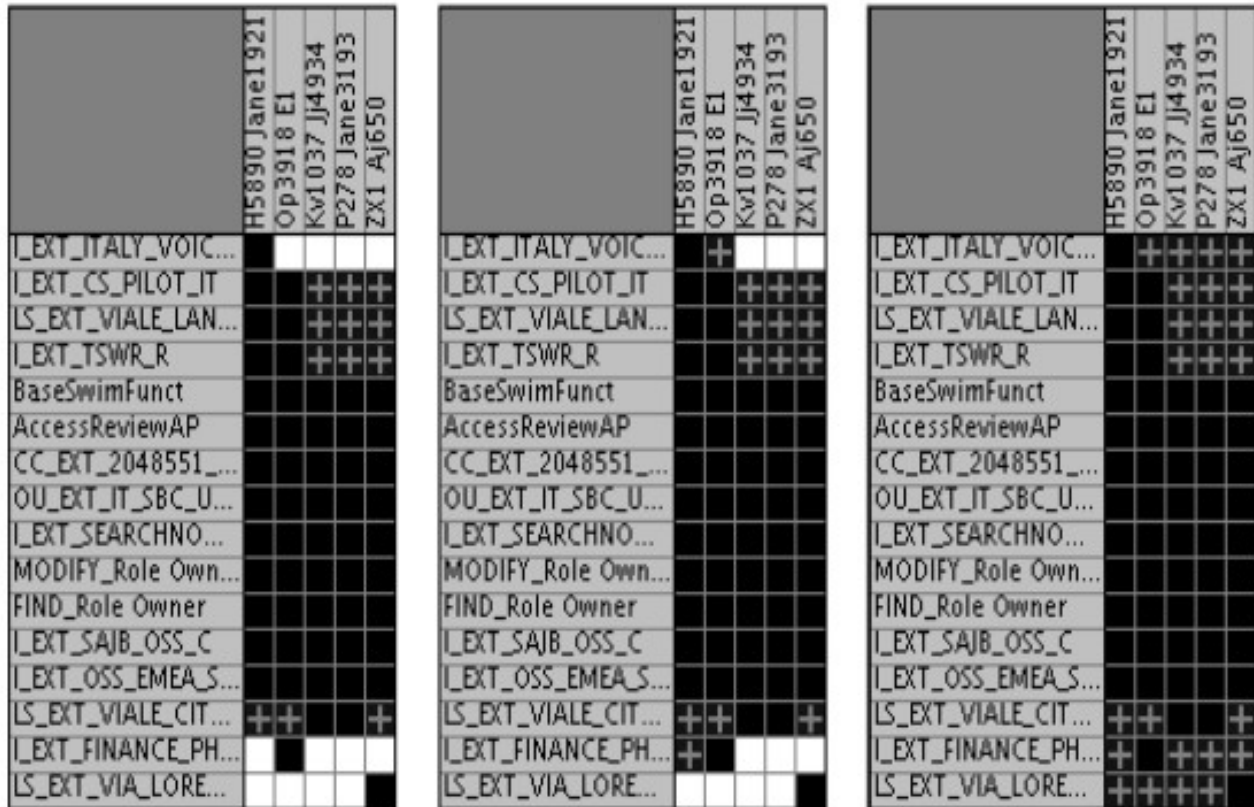


Figure 103. Missing Role analysis: three distinct values.

**Note:** If the Map produced is too large, the automatic Exceptions/Missing modulation is not available.

In the above figure, three distinct values of the **Missing** scroll are shown from left to right.

In the left column of the above figure (Missing =55) nine assignments are highlighted in the upper portion of the Map and another three at the bottom of the Map.

With Missing =75, another two assignments are added without any significant changes in the quality of the solution when compared with the previous configuration.

With Missing =95, the entire Map goes black!

How must this Map set be interpreted?

To obtain an appreciable improvement over the starting configuration, the not so "near" assignments must be selected (Missing =>55).



In this last option, creating a more powerful Candidate Role implies the need for a new authorization workflow process once the Candidate Role is exported to the system.

**Note:** These functionalities must be used very carefully!

If too many assignments are deleted (☐ symbol) near the "core" of the map (see Figure 3.21) and too many assignments are added (⊕ symbol) to the same area of the map, a "conceptual mismatch" can occur, tending to overturn the result of the analysis!

The **Exception/Missing** scrolls **MUST BE USED VERY CAREFULLY!**

By deleting some assignments (☐ symbol in Figure 3.23) and invoking a New Request operation, the RC Engine generates a new Map. In this instance, using the same Missing index value as the original Map does not result in the same ⊕ distribution.

This means there is a dynamic and mutual relationship between both the presence and absence of ☐ / ⊕ symbols.

**CAUTION:**  
**IF Exception = Missing = 1**

... the result is the "negative" of the original Map (Exception = Missing = 0).

**This is a situation of ALL "noise" and NO "signal"!**

**This is the worst case of all!**

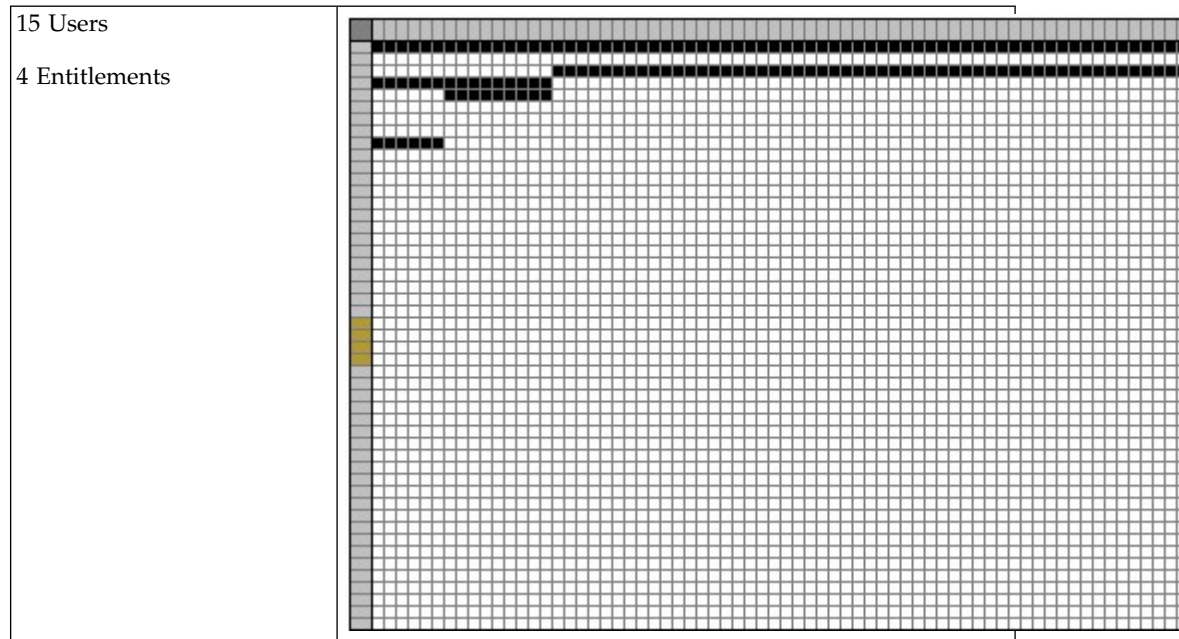
### **Searching "out Roles" in the Map**

When the Role Map is built with a lot of Users and Entitlements it can be difficult to detect the graphic structure of a Role. For a very large Map, it is not always easy to recognize a Role by selecting it from the list in the left-hand frame. For example, in a map that has 375 Roles built on 1060 Entitlements and distributed on a set of 4204 Users.

Selecting a Role in the **Role Search** frame returns this fragment of the Map:



Table 163. Candidate Role



In this Map the position of the 4 Entitlements can be identified in the left-hand, vertical, gray column.

BUT WHERE ARE THE USERS?

Finding them requires some work with the horizontal scroll or, more easily, clicking on the Role Search button positioned on the upper-right toolbar of the GUI:

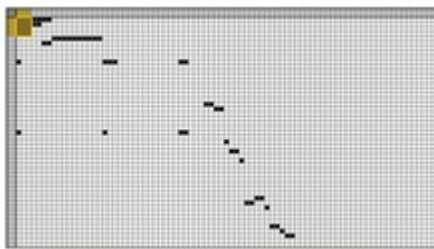


Figure 105. Recognized role.

The four Entitlements and the first three Users are Located in the top-left corner of the Map. The other 12 Users are now more easily found by scrolling horizontally through the first 4 rows at the top of the Map.

### Zoom on the Map

Maps in the AA Module can be viewed at three distinct zoom levels.

By default, the base Map is always shown.

In the panel below, the upper figure displays the Map at the base resolution:





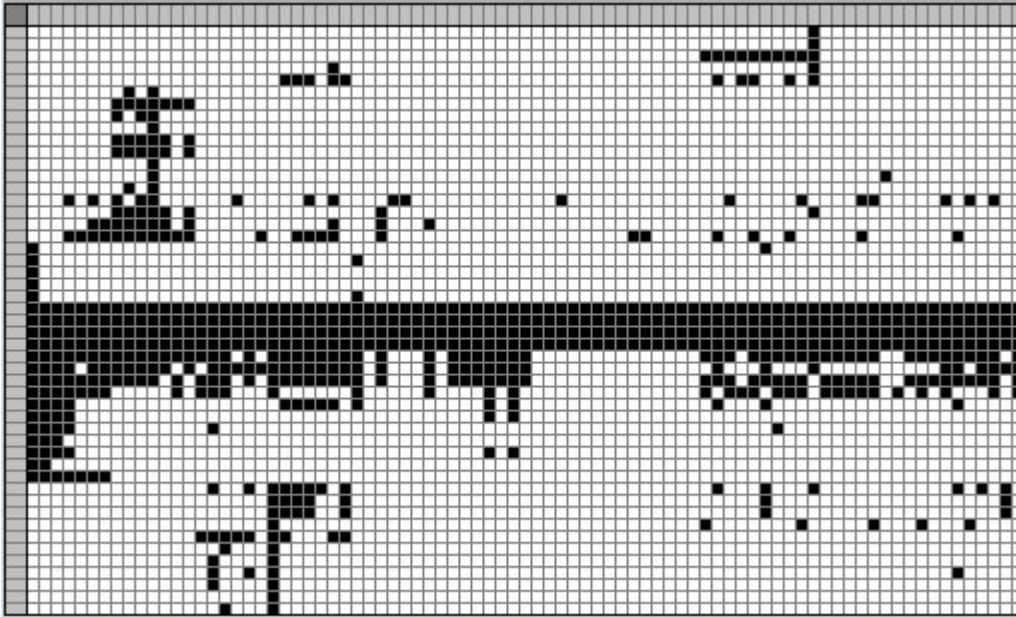


Figure 109. “Scattered” Map: Zoomed In (150% enlargement)

## Risk Map

The Map represents the score in the entitlements-users assignments.

A high level of familiarity with the Map is a must in order to:

- Investigate the result set produced by the analysis process.
- Make decisions about Attestation Campaign on input data to refine the obtained result set.

A set of entitlements is listed on one axis of the map and a set of users on the other. The red dot represents the risk on the assignment of the entitlements to a user.

Map is colored with 256 different levels of red, depending on the risk level present in that assignment.

From the same Map window, you can launch the Review Campaign. It is possible to exclude from campaigns the assignments with low risk level and consider only the high risk assignments.

The attestation campaigns made by the AO module will go into the AG Core database, where they will be processed and made available.


For viewing the campaign status on the AG Core administration module, from the tabs bar, click:

**Configure > Certification > Campaigns.**

## Map management

In this section are listed all common buttons available for any map of the AA module, role and risk maps.



- **Zoom in/Zoom out:** the zoom action modifies the resolution of the map.**Zoom in/Zoom out:** the zoom action modifies the resolution of the map. For more details, see *Zoom on the Map*.
- **Exclude Campaigns:** the **Risk Threshold** combo box allows you to change the value from 5% to 100%. According to the value of the combo box, clicking **Exclude**, a subset of risky assignments in the Risk Map will change from red squares into the  symbol.
- **Exclude:** by directly selecting a red assignment (clicking it with the left mouse button) and clicking **Exclude**, the assignments will be removed from the selected area.
- **Review Campaigns:** allows you to open the Attestation Campaign window. For more details about this topic, see *Risk Map*.

**Remember:**

- When you move the mouse pointer to a specific position on the map, a dedicated tooltip displays, highlighting the position coordinates in the form:

User: user name | user surname [user code]

Entitlement: entitlement name | entitlement type | application name

- You can manually add/remove missing/exception assignments after an exception/missing modulation which is an automatic operation.

By inverting the order of the operation typology and performing the manual operation before the automatic operation, the fixed settings of the manual operation are lost.

---

## Access Optimizer: Guide to modeling

Access Optimizer is a role engineering tool that combines the concept of risk analysis with the process of role mining.

The goal is to

- Automate the cumbersome and inefficient process of manual role creation
- Contribute to the ongoing lifecycle management process with operations aimed at controlling the amount of risk

In this manner, roles can be implemented to obtain the best results in governance, risk management, and compliance.

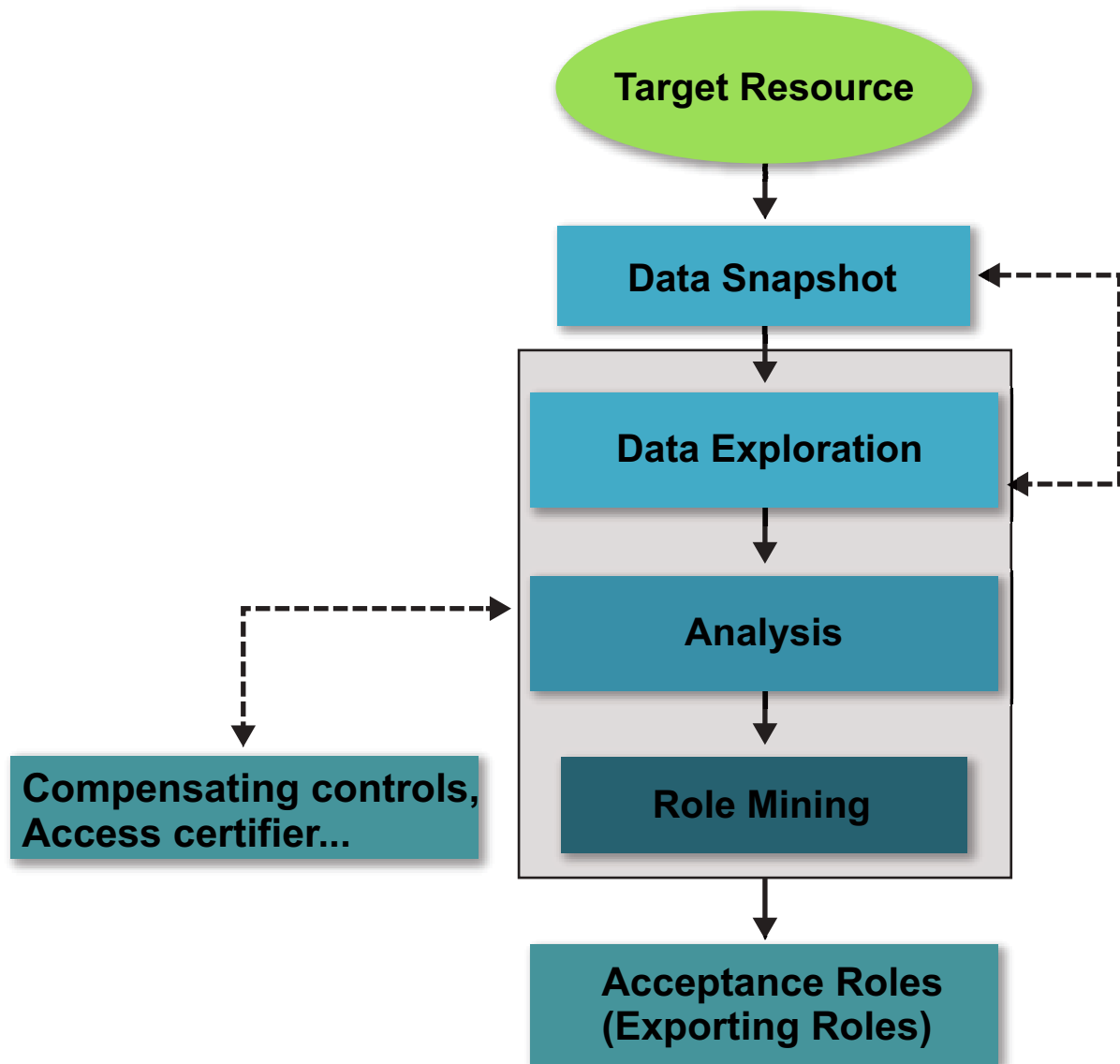


Figure 111. Main workflow.

Access Optimizer uses a set of advanced algorithms to create a map of users and permissions (entitlements). With a full set of visual tools, role recognition becomes much easier. All key aspects of the role engineering process are described in the following sections.

- “Phase 1: Data snapshot”
- “Phase 2: Data exploration algorithm” on page 400
- “Phase 3: Risk analysis process” on page 401
- “Phase 4: Role mining algorithm” on page 401
- “Phase 5: Role acceptance” on page 402

## Phase 1: Data snapshot

In this phase, select the set of access permissions that best represents all the examined IT subsystems to identify the right set of candidate roles.

The selection criteria can be based on target systems and user attributes (for example, all the users who belong to a certain OU).

After identification, the data must be collected from all the sources.

The following entities and relations are loaded:

**Organization Units**

The units that make up the organization being examined.

**Users** The users who belong to the organization.

**Applications**

The applications that are run in the organization.

**Entitlements**

The entitlements (permissions) registered in the organization.

**Entitlement Hierarchy**

The hierarchy among the entitlements registered in the organization.

**Assignments**

All user-entitlement assignments.

These operations are available from Bulk Data Load>Data Snapshot.

The data is loaded from either of two sources:

- A flat file.
- The IAG-DB (AGCore database), a centralized warehouse of the IBM Security Identity Governance platform.

## Phase 2: Data exploration algorithm

The goal of role mining is to create/design roles, which means identify a set of entitlements that must be assigned to a set of users.

Even for a medium scale company, it is impossible to find all the interesting roles by analyzing the whole set of user-entitlement assignments.

For a better data subset detection, the access analytics offers a pre-mining phase based on business information such as:

- Users (OUs + 10 user attributes independently selectable)
- Entitlements (Applications + entitlement type + 10 entitlement attributes independently selectable)

After uploading the data performing the data snapshot operation, the data exploration algorithm must be run for all user-entitlement assignments registered in the organization information system. This phase allows you to understand the quality of the expected role patterns by defining a set of filters to identify the best problem partition.

The algorithm allows for data filtering based on a large set of criteria.

For example, the data exploration procedure can be run:

- on all data
- on a specific OU or on a specific subtree of the organization's hierarchy
- on a specific attribute within the set of available attributes
- other data

Generally, it is recommended to run the first instance of this phase on all data.



The pre-analysis computes one special index, the Minability, which guides the analyst in selecting the filters for the subsequent analysis. This index allows for further, more precise risk analysis and role mining processes based on other algorithms and well-shaped areas to best create roles. This activity of "pre-mining" is aimed at reducing subsequent role engineering effort.

For every result set, an advanced graphical role map is provided along with a set of specific statistical data.

### Phase 3: Risk analysis process

The risk analysis process is described.

The process consists of two phases:

- Step 1: Analysis
- Steps after Step 1 (2, 3, and so on)

The next figure below the recommended roadmap to follow for the first and for all following analysis:

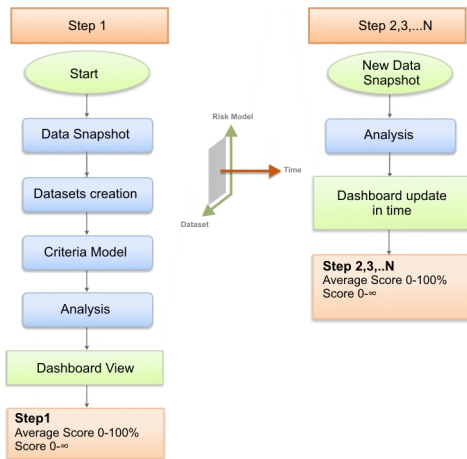


Figure 112. The Risk Analysis process.

After uploading the data from the database or from a file using the data snapshot operation and the data exploration operation, and before you start the risk analysis process, you should create a data subset via a Dataset, by applying specific Risk Criteria.

After detecting an interesting result set, the algorithm provides two indexes for determining its risk: Average risk and risk quantity.

This index helps you keep under control the amount of risk and the relative increase or decrease in time. For every result set, an advanced graphical dashboard is provided along with a set of specific statistical data.

### Phase 4: Role mining algorithm

The role mining process have to be preceded by a pre-mining phase of Data Exploration.

The Data Exploration phase is based on the data snapshot previously set.

You have to run a new Data Exploration after every change of the data snapshot.

## Optimal role set

This algorithm analyzes the data to find the best (optimal) roles based on the assigned criteria such as input data.

The optimal role set determines the best roles from the analyzed data, maximizing or minimizing the criteria of the chosen aggregation (for example, contextually maximize the number of users with a certain assigned entitlement, minimize the number of roles per user, and so on) .

It can generate a very big number of candidate roles.

Therefore, it is always useful to consult the data exploration output, choosing carefully the initial data set to analyze.

## Phase 5: Role acceptance

Before deployment into the production system, correctness and relevance of the identified roles should be checked.

In many organizations, this activity involves both the business and IT departments. After the approval phase, roles can be imported into the IBM Security Identity Governance AG Core main repository.

---

## Manage

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

- Data Exploration
- Role Mining

## Data Exploration analysis and details

This section helps you run the main operations involved with creating and managing an analysis.

An *analysis* is the object that contains all the data required for a data analysis. Analyses are listed under the **Analysis** tab.

An analysis is identified by a set of fields arranged in a row.

Click **Filter** to filter rows of analyses using the items described in the following table:

Table 164. Analysis filters.






Filter	Description
<b>Analysis Description</b>	A descriptive text of the analysis.
<b>Organization Unit</b>	Click  <b>Browse</b> to choose the OU in the analysis.
<b>Application</b>	Click  <b>Browse</b> to choose the Application in the analysis.

Table 164. Analysis filters. (continued)

Filter	Description
<b>Entitlement Type</b>	Indicates the entitlement types. <ul style="list-style-type: none"> <li>• Permission</li> <li>• IT Role</li> <li>• Business Role</li> <li>• External Role</li> </ul>
<b>Status</b>	Indicates the status of the analysis. <ul style="list-style-type: none"> <li>• Indicates in progress.</li> <li>•  Indicates complete.</li> <li>•  Indicates an error.</li> <li>•  Indicates invalidated due to a new bulk load.</li> </ul>
<b>User/Entitlement Attributes</b>	If present, according to the current configuration.

The details included in an Analysis row are the same as those described in the preceding table, with the addition of more items.


Click  **Info** to display all the information of an analysis. The details that characterize an analysis are described next.

Table 165. Analysis details.

Attribute	Description
<b>Analysis</b>	<ul style="list-style-type: none"> <li>• <b>Code</b> is a number that is automatically attached to the request.</li> <li>• <b>Analysis Description</b> describes the request.</li> <li>• <b>Start Time</b> is expressed in configurable format.</li> <li>• <b>End Time</b> is expressed in configurable format.</li> <li>• <b>Processing Time</b> is the time that is required to process the request.</li> </ul>


Table 165. Analysis details. (continued)

Attribute	Description
Data Filters	<ul style="list-style-type: none"> <li>• <b>Only direct assignment</b> specifies whether the analysis is based only on entitlements that are directly assigned to users.</li> <li>• <b>OU</b> is the OU name.</li> <li>• <b>Hierarchy</b> specifies that the analysis involves all the OUs starting from the root OU.</li> <li>• <b>Application</b> is the application name.</li> <li>• <b>Entitlements Type</b> can be any of the following types: <ul style="list-style-type: none"> <li>– Permission</li> <li>– IT Role</li> <li>– Business Role</li> <li>– External Role</li> </ul> </li> <li>• <b>User Attributes or Entitlement Attributes</b>, if present, according to User – Entitlement Attributes.</li> </ul>
Analysis Type	<ul style="list-style-type: none"> <li>• <b>Type</b> is the label name.</li> <li>• <b>Depth</b> is the position of the OU in the hierarchy. (All or 0...6 depth level)</li> </ul>

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

**Add** Select to define an analysis.




**Remove**  
Select to delete an analysis row.

Click  **Details** to display a panel that includes 3 frames.

In the top part of the panel, the **Back** button enables you to return to the Analysis view.

In the left frame, the **Partitions** tab hosts all the partitions generated during the analysis, according to the attributes summarized below:

Table 166. Partition attributes.

Attribute	Description
Name	The name of the partition.
Minability	Minability values.
Subset	Entities of the partition.
Status	<p>The status of the request. It can be:</p> <ul style="list-style-type: none"> <li>•  : Complete</li> <li>•  : Error</li> <li>•  : Warning</li> </ul>

When you select a partition, the center pane is populated with the subsets of the selected partition. From the center pane you can search (click **Filter/Hide Filter**) partition subsets using their Name as a filter.

From this pane, you can click **Actions > Massive Role Minig** to run a new operation on the entire data exploration partition.

From the tabs on the right pane, you can view the subset data in detail:

- Map (open by default)
- Entitlements/Users
- Entitlements/Users Statistics

## Entitlements/Users

Select the **Entitlements/Users** tab to display the entitlements/users aggregated to the partition selected in the central pane.

The columns displayed for an entitlement/user are configured in the **Settings > Attributes** tab.

## Entitlements/Users Statistics

Select the **Entitlements/Users Statistics** tab to display a histogram-based graphic that shows statistics about the entitlement/users of the selected partition.

In these tabs, you can search Entitlements/Users Statistics (click **Filter/Hide Filter**) using the filters summarized in the next table:

*Table 167. Entitlements/Users Statistics filters.*

Attribute	Description
<b>Order by</b>	This combo box helps you choose the visualization order of the column attributes
<b>Descendant/Ascendat</b>	This combo box helps you choose the sorting order of the data attributes
<b>Attribute 0... Attribute 9</b> (for Users)	Attributes configured in the User – Entitlement Attributes section
<b>Attribute 0... Attribute 9</b> (for Entitlements)	Attributes configured in the Entitlement attributes section

## Role mining

The output of this phase is mainly represented by a set of candidate roles.

During this analysis, the following algorithms can be applied:

- “Optimal Role-Set algorithm” on page 369





The **Analysis** tab displays already made role mining analysis. This pane includes the following buttons:

- **Filter/Hide Filter:** shows/hides the Filters option
- **Search:** finds the results of role mining analyses
- **Add:** makes a new request

- **Remove:** deletes requests

You can use the following filters to search for the results of a role mining request:

Table 168. Role mining search filters.

Filter	Description
<b>Request Description</b>	A description of the request.
<b>Type</b>	The type of request can be one of the following: <ul style="list-style-type: none"> <li>• <b>Optimal Role-set</b></li> </ul>
<b>Organization Unit</b>	The name of the root OU in the hierarchy.. Select <b>Hier</b> to include all the Organization Unit starting from the root <b>OU</b> .
<b>Application</b>	Name of the application.
<b>Entitlement Type</b>	The entitlement can be one of the following: <ul style="list-style-type: none"> <li>•  : <b>Permission</b></li> <li>•  : <b>IT role</b></li> <li>•  : <b>Business role</b></li> <li>•  : <b>External role</b></li> </ul>
<b>Status</b>	The status of the request.
<b>Attribute 0... Attribute 9 (for Users)</b>	Attributes configured in the User attributes section.
<b>Attribute 0... Attribute 9 (for Entitlements)</b>	Attributes configured in the Entitlements attributes section.

A request for a role mining analysis has the following attributes:

Table 169. Role mining analysis attributes.










Attribute	Description
<b>Code</b>	A progressive code number that is automatically attached to the request.
<b>Request Description</b>	A description of the request.
<b>Status</b>	The status of the request can be: <ul style="list-style-type: none"> <li>•  : <b>Complete</b></li> <li>•  : <b>In progress</b></li> <li>•  : <b>Error</b></li> <li>•  : <b>Warning</b></li> <li>•  : <b>Deleting</b></li> </ul>
<b>Type</b>	The request type can be: <ul style="list-style-type: none"> <li>• <b>Data Exploration</b></li> <li>• <b>Optimal Role-set</b></li> </ul>
<b>Direct</b>	Indicates that the only direct assignments option was specified for the request.

Table 169. Role mining analysis attributes. (continued)

Attribute	Description
<b>Organization Unit</b>	The name of the root OU in the hierarchy.. Select <b>Hier</b> to include all the Organization Unit starting from the root OU.
<b>Application</b>	Name of the application.
<b>Entitlement Type</b>	The entitlement can be one of the following: <ul style="list-style-type: none"> <li>•  : <b>Permission</b></li> <li>•  : <b>IT role</b></li> <li>•  : <b>Business role</b></li> <li>•  : <b>External role</b></li> </ul>
<b>Attribute 0... Attribute 9 (for Users)</b>	Attributes configured in the User attributes section.
<b>Attribute 0... Attribute 9 (for Entitlements)</b>	Attributes configured in the Entitlements attributes section.

You can set a specific algorithm type for every new role mining request, based on the following parameters:

Table 170. Optimal role-set parameters.

Attribute	Description
<b>Minimum Number of Users per Role</b>	The minimum number of users that can be aggregated for a candidate role
<b>Minimum Number of Entitlements per Role</b>	The minimum number of profiles that can be aggregated to a profile included in a candidate role
<b>Maximum Number of Roles</b>	The maximum number of candidate roles
<b>Role to User Assignments</b>	The tendency to associate many or few users to a role
<b>Role to Entitlement Assignments</b>	The tendency to create large or small candidate roles, by grouping many or few entitlements in a role
<b>User to Entitlement Assignments</b>	The tendency to associate many or few entitlements to a user (using a subset of candidate roles)
<b>OU Spread</b>	Spread 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 inclination towards obtaining a very scattered or localized role distribution in the OU hierarchy. See Spread.
<b>Application Number</b>	The tendency to associate many or few applications to a user (using a subset of candidate roles)
<b>Entitlement Type Number</b>	The tendency to associate many or few types of entitlements to a user (using a subset of candidate roles)

Table 170. Optimal role-set parameters. (continued)

Attribute	Description

Click **Details** to display the following tabs:

- **Details** (opened by default)
- Statistics
- Map
- Roles
- Entitlements

The **Details** tab shows the details of a selected data exploration operation according to the attributes described in the next table:

Table 171. Data exploration details.

Attribute	Description
<b>Request</b>	Includes the following: <ul style="list-style-type: none"> <li>• <b>Code:</b> The code number attached to the request</li> <li>• <b>Request Description:</b> A description of the request</li> <li>• <b>Start Time:</b> The time when execution of the request was started in the <i>dd/mm/yyyy</i> and <i>hh/mm/ss</i> format</li> <li>• <b>End Time:</b> The time when execution of the request was finished in the <i>dd/mm/yyyy</i> and <i>hh/mm/ss</i> format</li> <li>• <b>Processing Time:</b> The time required to process the request</li> </ul>
<b>Data Filters</b>	Includes the following: <ul style="list-style-type: none"> <li>• <b>Only direct assignment</b></li> <li>• <b>OU name</b></li> <li>• <b>Hierarchy</b></li> <li>• <b>Application name</b></li> <li>• <b>Entitlements Type:</b> Permission/ IT role/Business role</li> <li>• <b>Users/ Entitlements Attributes</b></li> </ul>
<b>Request Type</b>	Includes the following: <ul style="list-style-type: none"> <li>• <b>Algorithm type:</b> Data exploration, Optimal role set</li> <li>• <b>Type:</b> Label name</li> <li>• <b>Depth:</b> Hierarchy OU position (All or 0..6 depth level)</li> </ul>

## 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 172. Dashboard set.

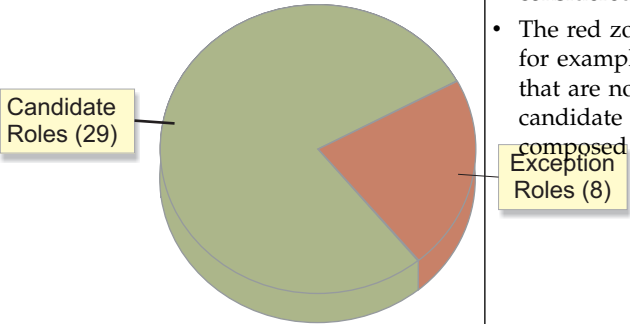
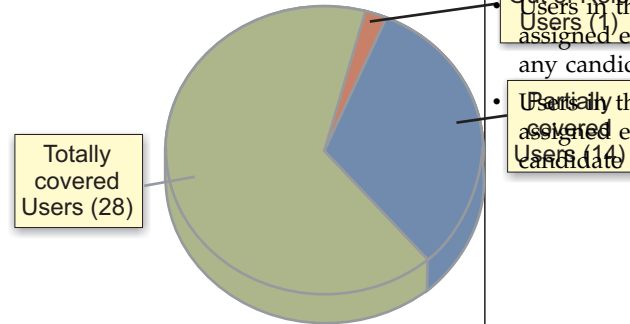
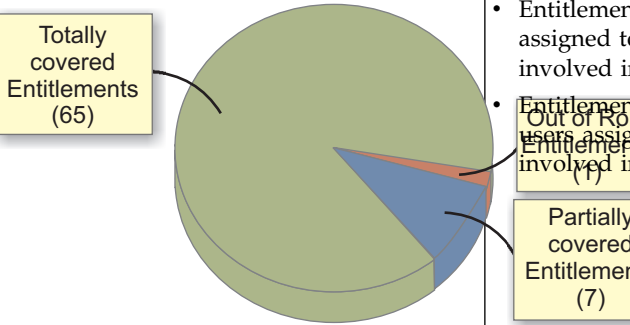
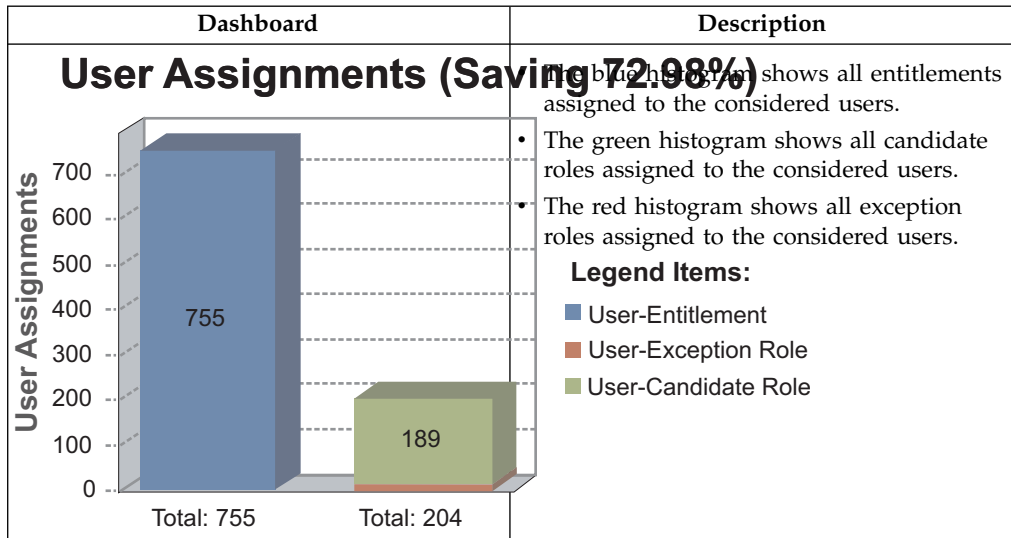
Dashboard	Description
<p data-bbox="651 380 954 428"><b>Total Roles (37)</b></p>  <p data-bbox="479 575 613 638">Candidate Roles (29)</p> <p data-bbox="987 617 1105 680">Exception Roles (8)</p>	<ul style="list-style-type: none"> <li>• The green zone represents the collection of candidate roles, for example roles whose adoption into the organization can be considered useful.</li> <li>• 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.</li> </ul>
<p data-bbox="597 842 997 890"><b>Analyzed Users (43)</b></p>  <p data-bbox="488 1079 623 1163">Totally covered Users (28)</p> <p data-bbox="987 932 1105 995">Out of Role Users (1)</p> <p data-bbox="987 1037 1105 1100">Partially covered Users (14)</p>	<ul style="list-style-type: none"> <li>• Users in the green zone: each of their assigned entitlements is involved in at least one candidate role.</li> <li>• Users in the blue zone: some of their assigned entitlements are not involved in any candidate role.</li> <li>• Users in the red zone: none of their assigned entitlements belong to any candidate role.</li> </ul>
<p data-bbox="542 1297 1081 1346"><b>Analyzed Entitlements (73)</b></p>  <p data-bbox="479 1415 630 1541">Totally covered Entitlements (65)</p> <p data-bbox="987 1499 1105 1562">Out of Role Entitlements (1)</p> <p data-bbox="987 1604 1105 1709">Partially covered Entitlements (7)</p>	<ul style="list-style-type: none"> <li>• Entitlements in the green zone: each user assigned to these entitlements is involved in at least one candidate role.</li> <li>• Entitlements in the blue zone: some users assigned to these entitlements are not involved in any candidate role.</li> <li>• Entitlements in the red zone: none of the users assigned to these entitlements are involved in any candidate role.</li> </ul>

Table 172. Dashboard set. (continued)



### 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 173. Role statistics filters.

Filter	Description
<b>Name</b>	Name(s) of role(s) involved in the request.
<b>Order By</b>	You can sort the displayed data in ascending or descending order, based on the data elements provided. You can start with <b>Users</b> .
<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>	
<b>Users</b>	Users involved in the request
<b>Entitlements</b>	Entitlements involved in the request
<b>Spread</b>	OU spread
<b>Org Units</b>	OUs involved in the request
<b>Entitlement Types</b>	The entitlement can be one of the following: <ul style="list-style-type: none"> <li> : <b>Permission</b></li> <li> : <b>IT role</b></li> <li> : <b>Business role</b></li> <li> : <b>External role</b></li> </ul>
<b>Applications</b>	Applications involved in the request
<b>User Attribute 0 ... Attribute 9</b>	Only user attributes specified in the request are available
<b>Entitlement Attribute 0 ... Attribute 9</b>	Only entitlement attributes specified in the request are available

Table 173. Role statistics filters. (continued)

Filter	Description
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.

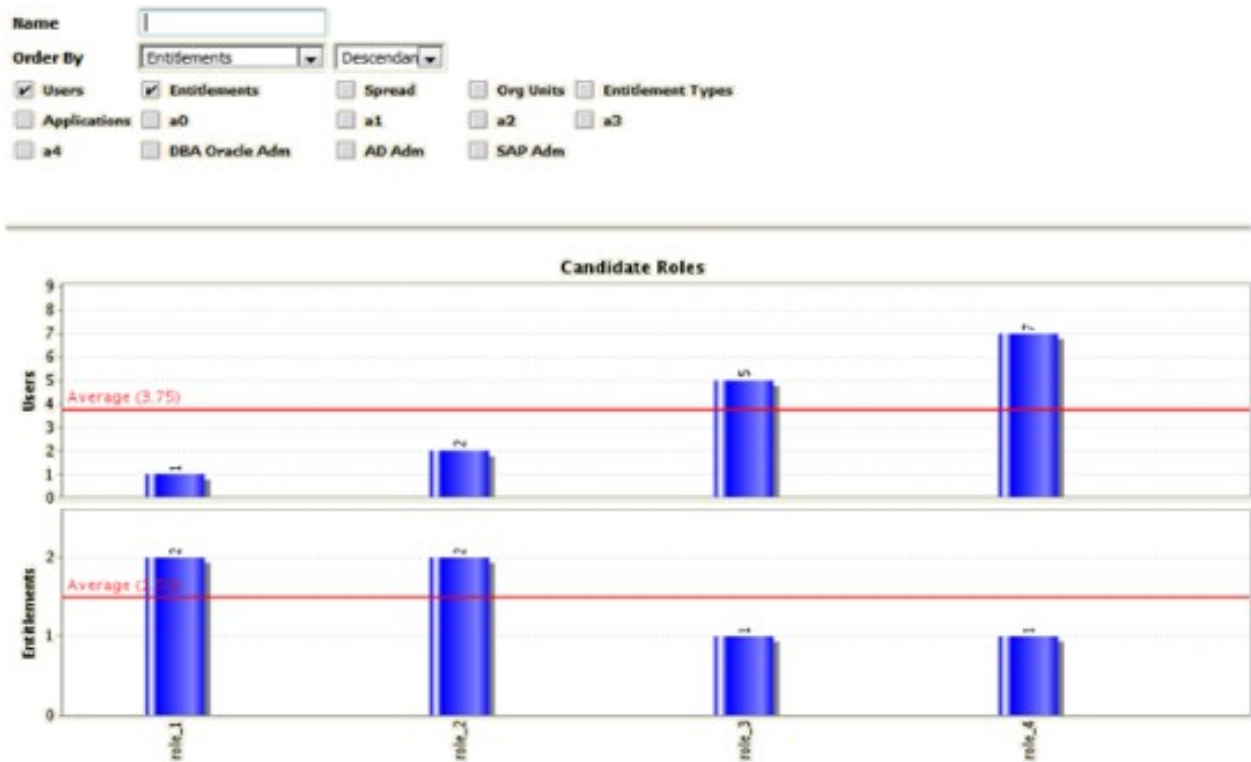


Figure 113. Example of Statistics with User and Entitlements check boxes selected.

### 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.

## Roles Candidates exporting states

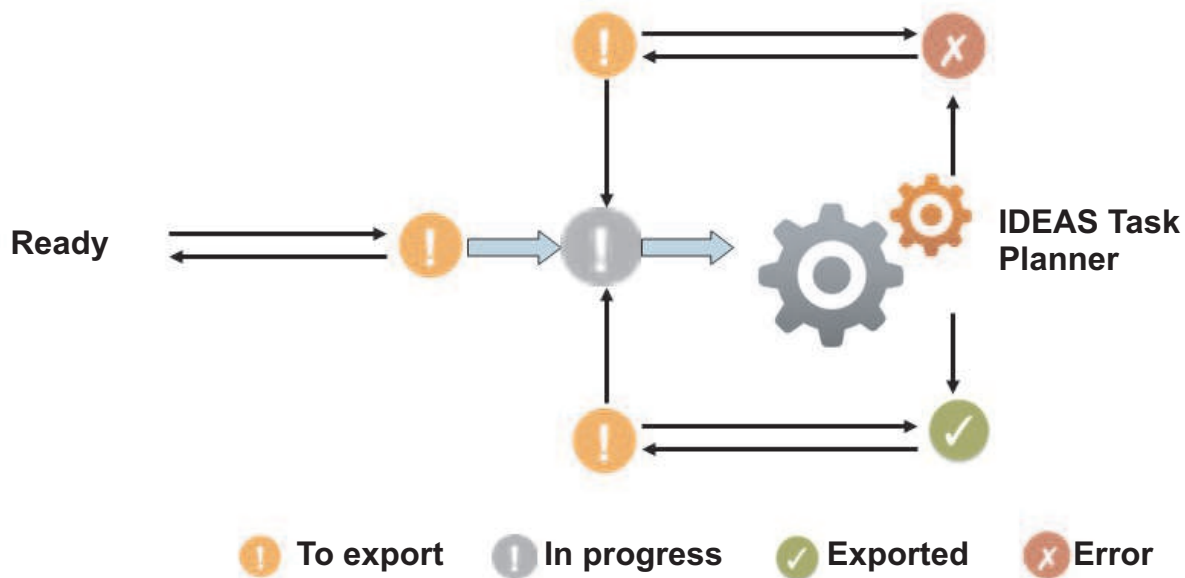


Figure 114. Possible states of candidate roles.

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 174. Entitlement details.

Detail	Description
<b>Role Name</b>	Name of role
<b>Rep. Status</b>	Status of the role
<b>Application</b>	Name of the application.
<b>Application Support (%)</b>	Percentage of application to be assigned to the candidate roles, from the entire set of entitlements involved in the analysis.
<b>Entitlements</b>	Name of the entitlement.
<b>Entitlements Support (%)</b>	Percentage of entitlements to be assigned to the candidate roles, from the entire set of entitlements involved in the analysis.
<b>Users</b>	Number of users assigned to the selected role.

Table 174. Entitlement details. (continued)

Detail	Description
<b>User Support (%)</b>	Percentage of users to be assigned to the role, from the entire set of users involved in the analysis.
<b>Org Units</b>	Number of organization units involved in the selected role.
<b>Org Unit Support (%)</b>	Percentage of organization units to be assigned to the role, from the entire set of organization units involved in the analysis.
<b>OU Spread</b>	OU Spread indicates the inclination towards obtaining a very scattered or localized entitlement distribution in the OU hierarchy. See Spread.
<b>Minimum Farness</b>	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.
<b>Average Farness</b>	Average distance of all OUs from the centroid of distribution. See Farness.
<b>Average Coverage (%)</b>	Average percentage of OUs assigned with the entitlement.
<b>Maximum Coverage (%)</b>	Maximum percentage of OUs assigned with the entitlement.
<b>Attribute 0... Attribute 9</b> (for Entitlements)	Attributes configured in the section Entitlement attributes.

In the "Role map" on page 380, 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 175. Entitlement filters

Attribute	Description
<b>Name</b>	Indicates the name of the entitlement.

Table 175. Entitlement filters (continued)

Attribute	Description
<b>Entitlement Type</b>	The entitlement can be one of the following: <ul style="list-style-type: none"> <li> : <b>Permission</b></li> <li> : <b>IT role</b></li> <li> : <b>Business role</b></li> <li> : <b>External role</b></li> </ul>
<b>Application</b>	Name of the application.
<b>User Coverage</b>	This filter can assume three different values: <ul style="list-style-type: none"> <li> Out of Role: the entitlement cannot be assigned to any qualified user using the candidate roles.</li> <li> Partially covered: the entitlement can be assigned only to a subset of qualified users using the candidate roles.</li> <li> Covered: the entitlement can be assigned to all qualified users using the candidate roles.</li> </ul>

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 176. Entitlement details

Attribute	Description
<b>Application</b>	Name of the application.
<b>Entitlement Name</b>	Name of the entitlement.
<b>Users</b>	Number of users assigned to the selected entitlement.
<b>User Support (%)</b>	Percentage of users that have the entitlement from the entire set of users that must have the entitlement.
<b>Covered Users</b>	Number of users covered with the entitlement.
<b>User Coverage (%)</b>	Percentage of users in the OU who are assigned to the entitlement.
<b>Org Units</b>	Number of organization units involved in the selected entitlement.
<b>Org Unit Support (%)</b>	Percentage of organization units to be assigned to the entitlement, from the entire set of organization units involved in the analysis.
<b>Covered Org Units</b>	Number of organization units covered with the Role entitlement.

Table 176. Entitlement details (continued)

Attribute	Description
Org Unit Coverage(%)	Percentage of organization units that are assigned with the entitlement, from the entire set of organization units that must be assigned with the entitlement.
OU Spread	OU Spread indicates the inclination towards obtaining a very scattered or localized entitlement distribution in the OU hierarchy. See Spread.
Minimum Farness	Minimum distance between an OU and the centroid of distribution, rather than between an OU and a particular attribute such as an entitlement. See Farness.
Average Farness	Average distance of all OUs from the centroid of distribution. See Farness.
Average Coverage (%)	Average percentage of OUs assigned with the entitlement.
Maximum Coverage (%)	Maximum percentage of OUs assigned with the entitlement.
Attribute 0... Attribute 9 (for Entitlements)	Attributes configured in the Entitlement attributes section.

The other operations for Entitlements analysis are:

- Users aggregated with the selected Entitlement
- OUs aggregated with the selected Entitlement

### Users aggregated with the selected entitlement

The **Users** tab lists all candidate roles containing the entitlement previously selected in the **Entitlements** tab.

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

Table 177. 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"> <li>•  Scheduled to be exported</li> <li>•  Exportation in progress</li> <li>•  Successfully exported</li> <li>•  Error</li> </ul>
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.



Table 177. Candidate Role attributes (continued)

Attribute	Description
<b>OU Spread</b>	“Spread” on page 376 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.
<b>Org Units</b>	Indicates the number of OUs for the selected candidate role.
<b>Applications</b>	Indicates the number of applications for the selected candidate role.
<b>Entitlement Type</b>	Entitlement types include the following ones: <ul style="list-style-type: none"> <li> <b>Permission</b></li> <li> <b>IT role</b></li> <li> <b>Business role</b></li> <li> <b>External role</b></li> </ul>
<b>Attribute 0... Attribute 9</b> (for Users)	Attributes that are configured in the User Attributes section.
<b>Attribute 0... Attribute 9</b> (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 178. User attributes

Attribute	Description
In/Out	The user status can be one of the following: <ul style="list-style-type: none"> <li> In Role (Role aggregated to the User)</li> <li> Out of Role (Role not aggregated to the User)</li> </ul>
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 179. Candidate Role attributes

Attribute	Description
<b>Role Name</b>	Indicates the name of the role.
<b>Exportation (Report/Release)</b>	The role can have one of the following statuses: <ul style="list-style-type: none"> <li> <b>Scheduled to be exported</b></li> <li> <b>Exportation in progress</b></li> <li> <b>Successfully exported</b></li> <li> <b>Error</b></li> </ul>
<b>Users</b>	Indicates the number of users for the selected candidate role.
<b>Entitlements</b>	Indicates the number of entitlements for the selected candidate role.
<b>Assignments</b>	Indicates the number of user-entitlement assignments for the selected candidate role.
<b>OU Spread</b>	“Spread” on page 376 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.
<b>Org Units</b>	Indicates the number of OUs for the selected candidate role.
<b>Applications</b>	Indicates the number of applications for the selected candidate role.
<b>Entitlement Type</b>	Entitlement types include the following ones: <ul style="list-style-type: none"> <li> <b>Permission</b></li> <li> <b>IT role</b></li> <li> <b>Business role</b></li> <li> <b>External role</b></li> </ul>
<b>Attribute 0... Attribute 9</b> (for Users)	Attributes that are configured in the User Attributes section.
<b>Attribute 0... Attribute 9</b> (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 180. OU attributes.

Attribute	Description
In/Out	The OU status can be one of the following: <ul style="list-style-type: none"> <li> In Role (Role aggregated to the OU)</li> <li> Out of Role (Role not aggregated to the OU)</li> </ul>
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.

### 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 181. User filters.

Attribute	Description
Master UID	Univocal identifier of the User
Last Name	Surname of the User.
First Name	Name of the User.
Organization Unit	Indicates the OU in which the User is registered.
Hier.	Flag this check box to get the tree view of the Organization unit.

Table 181. User filters. (continued)

Attribute	Description
<b>Entitlement Coverage</b>	<p>This filter can assume three distinct values:</p> <ul style="list-style-type: none"> <li>  <b>Out of Role:</b> the User is not aggregated to any Entitlement through the Candidate Roles.         </li> <li>  <b>Partially covered:</b> the User is aggregated only to a subset of Entitlements through the Candidate Roles.         </li> <li>  <b>Covered:</b> the User is aggregated to ALL Entitlements through the Candidate Roles.         </li> </ul>

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 182. User details.

<b>User</b>	
Attribute	Description
<b>Last Name</b>	Indicates the User's last name
<b>Name</b>	Indicates the User's name
<b>User ID</b>	Indicates the User's User ID
<b>Organization Unit</b>	Indicates the OU in which the User is registered
<b>Entitlements</b>	
<b>Entitlements</b>	Indicates the number of Entitlements assigned to the selected User
<b>Entitlement Support (%)</b>	Indicates the percentage of Entitlements that should be assigned to the User from the entire set of Entitlements involved in the Request
<b>Covered Entitlements</b>	Indicates the number of Entitlements assigned to the User
<b>Entitlement Coverage (%)</b>	Indicates the percentage of Entitlements actually assigned to the User from the entire set of Entitlements that should be assigned to the User
<b>Applications</b>	
<b>Applications</b>	Indicates the number of Applications involving the selected User
<b>Application Support (%)</b>	Indicates the percentage of Applications that should be assigned to the User from the entire set of Applications involved in the Request
<b>Covered Applications</b>	Indicates the number of Applications assigned to the User

Table 182. User details. (continued)

User	
Attribute	Description
Application Coverage(%)	Indicates the percentage of Applications actually assigned to the User from the entire set of Applications that should be assigned to the User

The other operations for User analysis are:

- Entitlements assigned to the selected User
- Applications assigned to the selected User

### Applications assigned to a selected User

Select the User to be examined in the left frame and click on the **Applications** tab.

All Candidate Roles aggregated to the selected User are listed in the central frame.

Selecting a Role, the Applications involved with this Role are shown in the **Applications** frame on the right.

For every row of Candidate Roles, the data set is shown in the table below:

Table 183. 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"> <li>•  Scheduled to be exported</li> <li>•  Exportation in progress</li> <li>•  Successfully exported</li> <li>•  Error</li> </ul>
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	“Spread” on page 376 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 183. Candidate Role attributes (continued)

Attribute	Description
<b>Entitlement Type</b>	Entitlement types include the following ones: <ul style="list-style-type: none"> <li> <b>Permission</b></li> <li> <b>IT role</b></li> <li> <b>Business role</b></li> <li> <b>External role</b></li> </ul>
<b>Attribute 0... Attribute 9</b>  (for Users)	Attributes that are configured in the User Attributes section.
<b>Attribute 0... Attribute 9</b>  (for Entitlements)	Attributes that are configured in the Entitlements Attributes section.

For each row of Applications, the following data set is displayed:

Table 184. Application attributes.

Attribute	Description
<b>In/Out</b>	The Application status can be one of the following: <ul style="list-style-type: none"> <li> <b>In Role:</b> Application aggregated to the Role/User</li> <li> <b>Out of Role:</b> Application not aggregated to the Role/User</li> </ul>
<b>Name</b>	Indicates the name of the Application

## Role analysis shortcut

Select a Role to be examined from the central **Role Search** frame, then click **Actions > Show Role**.

## View Entitlement details

In the **Entitlement Details** (opened by default), are automatically shown the data summarized in the table below:

Table 185. Entitlement details.

Attribute	Description
<b>Application</b>	Indicates the name of the Application
<b>Entitlement Name</b>	Indicates the name of the Entitlement
<b>Users</b>	Indicates the number of Users assigned the selected Entitlement
<b>User Support (%)</b>	Indicates the percentage of Users that should be assigned the Entitlement from among the entire set of Users involved in the Request

Table 185. Entitlement details. (continued)

Attribute	Description
<b>Covered Users</b>	Indicates the number of Users covered by the Entitlement
<b>User Coverage (%)</b>	Indicates the percentage of Users actually possessing the Entitlement from among the entire set of Users that should have the Entitlement
<b>Org Units</b>	Indicates the number of OUs involved in the selected Entitlements
<b>Org Unit Support (%)</b>	Indicates the percentage of OUs that should be assigned the Entitlement from among the entire set of OUs involved in the Request
<b>Covered Org Units</b>	Indicates the number of OUs covered by the Entitlement
<b>Org Unit Coverage(%)</b>	Indicates the percentage of OUs actually assigned with the Entitlement from among the entire set of OUs that should be assigned with the Entitlement
<b>OU Spread</b>	"Spread" on page 376 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 very scattered/localized Entitlement distribution in the OU hierarchy.
<b>Minimum Farness</b>	"Farness" on page 377 is a numeric index used that identifies the path and calculates the minimum distance between an OU and the centroid of distribution, rather than between an OU and a particular attribute such as an Entitlement.
<b>Average Farness</b>	Indicates the average distance of all OUs from the centroid of distribution.
<b>Average Coverage (%)</b>	Indicates the average percentage of OUs covered by (assigned with) the Entitlement
<b>Maximum Coverage (%)</b>	Indicates the maximum percentage of OUs covered by (assigned with) the Entitlement
<b>Attribute 0... Attribute 9</b> (for Entitlements)	Attributes configured in the section Entitlement attributes.

## View User details

In the **User Details** (opened by default), are automatically shown the data summarized in the table below:

Table 186. User details.

User	
Attribute	Description
<b>Last Name</b>	Indicates the User's surname.
<b>Name</b>	Indicates the User's name.
<b>User ID</b>	Indicates the User's User ID.

Table 186. User details. (continued)

<b>User</b>	
<b>Attribute</b>	<b>Description</b>
<b>Organization Unit</b>	Indicates the OU in which the User is registered
<b>Entitlements</b>	
<b>Entitlements</b>	Indicates the number of Entitlements assigned to the selected User
<b>Entitlement Support (%)</b>	Indicates the percentage of Entitlements that should be assigned to the User, from among the entire set of Entitlements involved in the Request
<b>Covered Entitlements</b>	Indicates the number of Entitlements assigned to the User
<b>Entitlement Coverage (%)</b>	Indicates the percentage of Entitlements actually assigned to the User, from among the entire set of Entitlements that should be assigned to the User
<b>Applications</b>	
<b>Applications</b>	Indicates the number of Applications involving the selected User
<b>Application Support (%)</b>	Indicates the percentage of Applications that should be assigned to the User, from among the entire set of Applications involved in the Request
<b>Covered Applications</b>	Indicates the number of Applications assigned to the User
<b>Application Coverage(%)</b>	Indicates the percentage of Applications actually assigned to the User, from among the entire set of Applications that should be assigned to the User

---

## Configure

Use the following functions for configuring the listed elements:

- Risk data sets
- Risk criteria






### Data snapshot

Use this tool to upload a data snapshot that you can utilize to run analyses other than role mining.

To view the details of a data snapshot on the right pane, select one of the items listed under **Data Snapshot**.

The following details are listed:

Table 187. Data snapshot details

Detail	Description
Type	The data source. It can be: <ul style="list-style-type: none"> <li>• IAG-DB</li> <li>• File Import</li> </ul>
Status	One of the following upload states: <ul style="list-style-type: none"> <li>•  : In progress</li> <li>•  : Deleting data not allowed (Disabled)</li> <li>•  : Data uploaded successfully (Completed)</li> <li>•  : Error</li> <li>•  : Warning (Old data snapshot)</li> </ul>
Start Date	Upload start date (mm/dd/yy; hh/mm/ss)
End Date	Upload end date (mm/dd/yy; hh/mm/ss)
Uploading Time	Time needed to upload files
Upload	
Item	Description
Organization Units rows	Number of OUs rows uploaded or discarded
Users rows	Number of users rows uploaded or discarded
Applications rows	Number of applications rows uploaded or discarded
Entitlements rows	Number of entitlements rows uploaded or discarded
Assignments rows	Number of assignments rows uploaded or discarded

Click History to view the data snapshot history.

Click Data to view the data uploaded.

To start a new data snapshot operation, click **Actions** > **Add**. The Import Type window displays the options for choosing the data source:

- File Import
- IAG-DB

**Note:** You can run only one snapshot per day. If you need to add another snapshot on the same day, you must first remove the former one. To do so, select the snapshot and click **Actions** > **remove**.

### Add data: File Import

When you choose **File Import** as the data source for the data snapshot or bulk data load operation, a window is displayed. You are required to provide data files for the following items:

- Organization Units



- Users
- Applications
- Entitlements
- Assignments

Optionally, for a bulk data load you can also provide a data file for entitlement hierarchies.

You are required to provide the following information For each type of data file:


*Table 188. File import details*


Attributes	Description
File location	Enter the name of the folder where the file is located. A <b>Browse</b> button is available.
File separator	The character used to separate fields in the file. For example, a semicolon (;).
File Name	The name of the file

Click **Load Data** to confirm the operation.

Click **Undo All** button if you need to clear all fields.

Click **Cancel** to cancel the data snapshot or bulk data load operation.

When the operation completes with success, the status changes to  **Completed**.

If errors occur, the status is  **Error**.


If errors are returned, click **Back** to return to the file specification window and repeat the operation. The **Request History** phase is not available until the Upload phase is terminated.


**Note:** If errors occurred during the Data Validation process, the error type is shown in the same frame.


**Attention:** If the file format for the upload operations does not comply with the required format, a diagnostic window is displayed. Every incorrect value is traced.

### Add data: IAG-DB Import

When you choose **IAG-DB** as the data source for the data snapshot or bulk data load operation, the data is loaded from the AG Core data base.

While the operation is in progress, the status is shown as  **In progress**. When

the operation completes successfully, the status changes to  **Completed**. If



errors occur, the status is  **Error**.

### History

The **History** tab contains the list of requests made on a selected risk criteria with different data sets in different data snapshots.

You can use filters to search for a request.

Table 189. History filters

Attribute	Description
Dataset	The name of the data set created from a snapshot. Click  to search for a data set.
Relevance Criteria	Click  to search for a criterion.
Status	The status of the data snapshot can be: <ul style="list-style-type: none"> <li>• In progress</li> <li>• Complete</li> <li>• Error</li> <li>• Deleting</li> <li>• Warning</li> </ul>

## Data

Select this tab to view the data included in the data snapshot or bulk data load.

The data is displayed in the following tabs:

- Organization Units (OU search - OU Structure)
- Users
- Applications
- Entitlements
- Entitlement Hierarchy
- Assignments

### Organization unit (OU search - OU structure)

In the **OU** tab, select one of the listed items and click **Actions > View Tree** to open the **OU Structure** tab and view the exact position of the OU in the hierarchy.

### Users

Select this tab to search and view users.

You can use the following filters to search for users:

- Master UID
- Surname
- Name
- Organization Unit

Select a user and click **Actions > View Tree** to get the exact position of the User OU.

### Applications

Select this tab to search and view applications.

### Entitlements

Select this tab to search and view entitlements.

You can use the following filters to search for entitlements:

Table 190. Filters for entitlements

Filter	Description
Name	Entitlement name
Entitlement Type	The entitlement type can be one of the following: <ul style="list-style-type: none"> <li>• Permission</li> <li>• IT Role</li> <li>• Business Role</li> <li>• External Role</li> </ul>
Application	Entitlement application

### Entitlement hierarchy

Select this tab to search and view entitlement hierarchies.

You can use the following filters to search for hierarchies:

Table 191. Filters for Entitlement hierarchies

Filter	Description
Parent Entitlement Name	The name of the parent of the selected entitlement
Parent Entitlement Type	The entitlement type can be one of the following: <ul style="list-style-type: none"> <li>• Permission</li> <li>• IT Role</li> <li>• Business Role</li> <li>• External Role</li> </ul>
Parent Application	The name of the application associated with the parent entitlement.  If the parent entitlement type is Business Role, it is associated with a default virtual application.
Child Entitlement Name	The name of the child of the selected entitlement
Child Entitlement Type	The entitlement type can be one of the following: <ul style="list-style-type: none"> <li>• Permission</li> <li>• IT Role</li> <li>• Business Role</li> <li>• External Role</li> </ul>
Child Application	The name of the application associated with the child entitlement.  If the child entitlement type is Business Role, it is associated with to a default virtual application.

Click **Hierarchical View** to display the Entitlement Hierarchy Search window and to set the filter data.

Select the entitlements to be examined from the list produced and click **View Tree** in the Entitlement Hierarchy Search window to view hierarchy details.

## Assignments

Select this tab to view the assignments associated with users and entitlements. You can use the following filters to search for assignments:

*Table 192. filters for assignments*

Filter	Description
Entitlement Name	The name of the entitlement
Entitlement Type	The entitlement type can be one of the following: <ul style="list-style-type: none"> <li>• Permission</li> <li>• IT Role</li> <li>• Business Role</li> <li>• External Role</li> </ul>
Application	The name of the application associated with the entitlement. If the entitlement type is Business Role, it is associated with a default virtual application.
Person Code	The User ID of the user
Person Surname	The surname of the user
Person Name	The name of the user
Organization Unit	The OU name
Redundant/Inherited	The parent of the entitlement. This filter is available only for the following operations: <ul style="list-style-type: none"> <li>• Redundant</li> <li>• Inherited</li> </ul>

## Access data sets

This section explains the operations needed to create a data set from the snapshot uploaded.

The **Datasets** tab, displays the data sets listed in the system. In this pane, you can find the following buttons:

- **Filter/Hide Filter:** allows you to show/hide the filters option.
- **Search:** allows you to get results according to the filters setting.
- **Add:** allows you to perform empty data sets. The empty data set is displayed in the **Datasets** pane (left).
- **Remove:** allows you to delete data sets.

In this tab, the **Automatic** button enables you to create automatically a combination of data sets.

This mechanism can be useful, for example, if the administrator of a big company wants to know how many U.S.A. and Italian users there are in eleven selected OUs of the company.

In this way, the administrator has the possibility to choose two sets of objects, for example:

- 11 first level OUs (named A, B, C, D, ..., M)
- 2 attributes (named 1, 2)

and get the automatic combination of 22 data sets, as graphically shown below:

## Datasets


A1	B1	C1	D1	E1	F1	G1	H1	I1	L1	M1
A2	B2	C2	D2	E2	F2	G2	H2	I2	L2	M2

Figure 115. Data set combinations.

The filters available (clicking **Filter/Hide Filter**) are **Name** and **Dataset Type**.

The data sets details/attributes and W/B list details are described in the table below:

Table 193. Data sets details/attributes.

Attribute	Description
<b>Name</b>	Data set name.
<b>Created by</b>	Data set author.
<b>Creation Date</b>	Date (dd/mm/yyyy) and Hour (hh/mm/ss) of data set creation.
<b>Dataset Type</b>	Label name.
<b>Description</b>	Brief description of data set contents.
<b>White and Black Lists Details</b>	
<b>Attribute</b>	<b>Description</b>
<b>Organization Unit</b>	OUs involved (White list)/ not involved (Black list) in the data set.
<b>Users Attributes</b>	Users attributes involved (White list)/ not involved (Black list) in the data set.
<b>Applications</b>	Applications involved (White list)/ not involved (Black list) in the data set.
<b>Entitlements Attributes</b>	Entitlements attributes involved (White list)/ not involved (Black list) in the data set.
	<b>Note:</b> Removing a data set also removes the aggregated requests.

From the tabs on the right pane, you can view the subset of detailed data:

- **Details.** From this tab, you can view the detailed data of the selected data set.
- **History**

- **Data Filters**

## Relevance criteria

The Relevance Criteria tab is described.

The buttons available in this section are:

- **Filter/Hide Filter:** allows you to show/hide the filters option.
- **Search:** allows you to get results according to the filter settings.
- **Add:** allows you to add an object to the W/B lists (available only in the right pane).
- **Remove:** allows you to remove objects from the W/B lists (available only in the center pane).

The only available filter in the **Relevance Criteria** tab is the **Name** filter. For a complete introduction to this section, see *The Access approach*.

Selecting an item from the **Relevance Criteria** tab on the left, the **Details** tab opens on the right.

*Table 194. Relevance Criteria details.*

Properties	Description		
<b>Name</b>	Risk criteria name		
<b>Created by</b>	Risk criteria creator		
<b>Creation Date</b>	Creation date (dd/mm/yyyy). Creation hour (hh/mm/ss)		
<b>Description</b>	Brief description of risk criteria		
Relevance attributes			
Name	Description	ON	OFF
<b>User Relevance</b>	Number of assigned permission	Considered in the risk analysis	Unconsidered in the risk analysis
	Number of SOD violations		
<b>Entitlement Relevance</b>	Number of assigned business activity		
	Number of SOD constraints		
<b>Assignments Relevance</b>	Similarity divergence		
	Last certification age		







## History

The **History** tab on the right contains the list of requests performed on the selected risk criteria with different data sets in different data snapshots.

**Note:** The contents in this section are the same as those of of the risk analysis section. To start a new request, go to the risk analysis section.

In these frames, the following filters can be used for a request search (click **Filter/Hide Filter**):

Table 195. History filters

Attributes	Description
Status	<ul style="list-style-type: none"> <li> : Deleting data not allowed (Disabled)</li> <li> : Data uploaded successfully (Completed)</li> <li> : Error</li> <li> : Warning (Old data snapshot)</li> </ul>
Data Snapshot	Snapshot upload date. Click  <b>Data Snapshot</b> to quickly search for the data snapshot.
Dataset	Risk criteria name. Click  <b>Dataset button</b> to quickly search for the risk criteria.

Click **Details** in the upper section of the pane, to view the results of your request in the Map window.

See Map. For the functionality of the map, see Map management.

## Monitor

The functions that are available for monitoring some elements are contained in the following list.

- Access Distribution
- Coverage Factors
- Access Trend
- “Access summary” on page 432
- Report
- “Scheduled tasks” on page 435

### Access distribution

The access distribution and its related filters are described.

The risk distribution is used to consult the following analysis items:

- **Average Score**
- **Score**
- **Assignments**
- **Users**
- **Entitlements**

The filters available for this section are described in the table below:

Table 196. Access distribution filters.

Filter	Description
Dataset Name	Name of the data set analyzed.
Type	Dataset label name.

Table 196. Access distribution filters. (continued)

Filter	Description
Order By	<p>These filters can be activated by selecting the corresponding check boxes under the filters text boxes:</p> <ul style="list-style-type: none"> <li>• <b>Average Score</b></li> <li>• <b>Score</b></li> <li>• <b>Assignments</b></li> <li>• <b>Users</b></li> <li>• <b>Entitlements</b></li> </ul>

The Dashboard Tree pane on the left (**Relevance Criteria** tab) lists the relevance criteria involved in the analysis, and the related snapshot.

By clicking the **DataSnapshot** tab, the same information is available, starting from the snapshot. The dashboard results reference information contained in the Dataset that is created according to the snapshot considered.

If there are no items selected in the Dashboard pane on the left, the filter section is disabled.

Clicking a single column, opens and displays the Risk Map (see also Map Management) for the selected OU.

## Coverage factors

This section provides you with the graphical visualization of the analysis results.

Risk coverage is used to consult the following analysis items:

- **Assignments**
- **Users**
- **Entitlements**

In this section, searching is limited to the data set search and the only filter available is the Dataset Type filter. The dashboard tree pane on the left lists the snapshots involved in the analysis and the related data sets (second level of the hierarchy). By selecting the **Datasets** tab, the information is available starting from the data set view.

Clicking one of the red points, displays the related Risk Map (see also Map management) .

## Access summary

The Analysis tab and its functions are described.

The **Analysis** tab, displays the access summary operation already performed. In this pane, you can find the following buttons:

- **Filter/Hide Filter:** allows you to show/hide the filters option.
- **Search:** allows you to get results according to the filter settings.
- **Add:** allows you to perform a new request.
- **Remove:** allows you to delete a request.



The following tables describe the filters for the access summary request and its related attributes:

Table 197. Analysis filters












Filter	Description
Data Snapshot	Click  <b>Search entity</b> to search requests from the data snapshot upload date. Click  <b>Clear</b> to clear the fields.
Dataset	Click  <b>Search entity</b> to search requests from the data set. Click  <b>Clear</b> to clear the fields.
Relevance Criteria	Click  <b>Search entity</b> to search requests from the relevance criteria applied. Click  <b>Clear</b> to clear the fields.
Status	Status of the request: <ul style="list-style-type: none"> <li> : Complete</li> <li> : In progress</li> <li> : Error</li> <li> : Warning</li> <li> : Deleting</li> </ul>

Table 198. Analysis attributes.






Attribute	Description
Code	Progressive code number automatically attached to the request.
Data Snapshot	Analyzed data snapshot.
Dataset	Analyzed data set.
Relevance Criteria	Applied relevance criteria.
Status	Status of the request: <ul style="list-style-type: none"> <li> : Complete</li> <li> : In progress</li> <li> : Error</li> <li> : Warning</li> <li> : Deleting</li> </ul>
Average Score	Score percentage.
Score	Quantity for evaluating access analysis.
Assignments	Number of involved assignments.
Users	Number of involved users.

Table 198. Analysis attributes. (continued)

Attribute	Description
Entitlements	Number of involved entitlements.

When you select a request and click  **Details**, the Map window displays.

For information about the map features, see Map.

From this entry point, you can select several Map analysis operations.

## Access trend

In this section, you can view the results from the snapshot comparison and use them for monitoring the score trend.

Access trend is used to consult the following analysis items:

- **Average Score**
- **Score**
- **Assignments**
- **Users**
- **Entitlements**

This web interface is the desktop page of the module and allows the administrator to continuously monitor the access trend development before starting any new analysis.

The filters available for this section are described in the table below:

Table 199. Access distribution filters.

Attribute	Description
Dataset Type	Dataset label name.
View Graph	These filters are activated by selecting the corresponding check boxes in the Trend Analysis pane on the right: <ul style="list-style-type: none"> <li>• <b>Average Score</b></li> <li>• <b>Score</b></li> <li>• <b>Assignments</b></li> <li>• <b>Users</b></li> <li>• <b>Entitlements</b></li> </ul>

The **Dashboard tree** pane on the left lists the snapshots involved in the analysis and the related data sets (second level of the hierarchy). By selecting the **Relevance Criteria** tab, the information are available starting from the **Relevance Criteria view**. Clicking one of the red points, shows the related Map (see also Map management).

## Report

Scheduling and downloading are the main functions in Reports.

- Request schedules reports.
- Download downloads reports.

For unauthorized users, this menu is not available.

## Scheduled tasks

In this section, are displayed all scheduled tasks still running or just started.

In the **Actions** menu, the **Remove** item allows you to remove the scheduled tasks from the list.

These tasks are scheduled using the **Task Planner** module.

## Tools

Several functions speed up and facilitate the tasks of the following modules:

- Bulk Data Load
- Reset Flags

## Bulk data load

Use this tool to upload a data snapshot that you can utilize for the Role Mining process.

To view the details of a bulk data load on the right pane, select one of the items listed under **Bulk data Load**.

The following details are listed:

*Table 200. Bulk data load details*






Detail	Description
Upload Date	The date and time that the upload of data was started.
Type	The data source. It can be: <ul style="list-style-type: none"> <li>• IAG-DB</li> <li>• File Import</li> </ul>
Status	One of the following upload states: <ul style="list-style-type: none"> <li>•  : In progress</li> <li>•  : Deleting data not allowed (Disabled)</li> <li>•  : Data uploaded successfully (Completed)</li> <li>•  : Error</li> <li>•  : Warning (Old data snapshot)</li> </ul>
Start Date	Upload start date (mm/dd/yy; hh/mm/ss)
End Date	Upload end date (mm/dd/yy; hh/mm/ss)
Upload	
Item	Description
Org Units rows	Number of OUs rows uploaded or discarded
Users rows	Number of users rows uploaded or discarded

Table 200. Bulk data load details (continued)

Detail	Description
Applications rows	Number of applications rows uploaded or discarded
Entitlements rows	Number of entitlements rows uploaded or discarded
Entitlements Hierarchy rows	Number of entitlement hierarchies rows uploaded or discarded
Assignments rows	Number of assignments rows uploaded or discarded

Click **Data** to view the data uploaded.

To start a new bulk data load operation, click **Actions > Add**. The Import Type window displays the options for choosing the data source:

- File Import
- IAG-DB

**Note:** There is only one bulk data load at a time. Every time you add one, the previous one is automatically deleted. Only one data load is displayed at anytime.

### Add data: File Import

When you choose **File Import** as the data source for the data snapshot or bulk data load operation, a window is displayed. You are required to provide data files for the following items:

- Organization Units
- Users
- Applications
- Entitlements
- Assignments

Optionally, for a bulk data load you can also provide a data file for entitlement hierarchies.

You are required to provide the following information For each type of data file:


Table 201. File import details


Attributes	Description
File location	Enter the name of the folder where the file is located. A <b>Browse</b> button is available.
File separator	The character used to separate fields in the file. For example, a semicolon (;).
File Name	The name of the file

Click **Load Data** to confirm the operation.

Click **Undo All** button if you need to clear all fields.

Click **Cancel** to cancel the data snapshot or bulk data load operation.

When the operation completes with success, the status changes to  **Completed**.

If errors occur, the status is  **Error**.




If errors are returned, click **Back** to return to the file specification window and repeat the operation. The **Request History** phase is not available until the Upload phase is terminated.

**Note:** If errors occurred during the Data Validation process, the error type is shown in the same frame.

**Attention:** If the file format for the upload operations does not comply with the required format, a diagnostic window is displayed. Every incorrect value is traced.

### Add data: IAG-DB Import

When you choose **IAG-DB** as the data source for the data snapshot or bulk data load operation, the data is loaded from the AG Core data base.

While the operation is in progress, the status is shown as  **In progress**. When the operation completes successfully, the status changes to  **Completed**. If errors occur, the status is  **Error**.

## Reset flags

This section allows you to reset the flags for the exportation of the roles into the reports.

In the **Reset** tab (right), you can view the flag details:

Table 202. Reset details.

Detail	Description
<b>Flag</b>	Name of the flag.
<b>Last Reset Date</b>	Last date in which the flags have been reset (dd/mm/yyyy; hh:mm:ss)
<b>Last Reset User</b>	Last user who reset the flags.
<b>Flags to Reset</b>	Number of flags to reset.
<b>Reset Flags</b>	Number of flags already reset.
<b>Misalignments</b>	Number of unsuccessful reset operations.
<b>Status</b>	Status of the reset operation: <ul style="list-style-type: none"><li>• In Progress</li><li>• Complete</li><li>• Error</li></ul>

To reset flags, after selecting a flag in the **Flags** tab (left), click **Reset** in the **Reset** tab.

---

## Settings

The following functions are available for setting values of some elements of the module:

- Attributes
- Data File Templates

### Attributes

Select this tab to map parameters for data snapshots used for analysis in Access Optimizer.

Map the parameters before you run the data snapshot. The mapping has no effect on an existing snapshot.

The **Parameter** tab lists the attributes that you can configure. Typically they are User attributes and Entitlement attributes.

Select a parameter to display a list of attributes on the right pane. The list contains ten editable fields where you can enter the name of an attribute.

Enter the names that you want to be displayed in the data snapshot.

For User attributes, you can enter names that replace the names of attributes of the User ERC table. The replacement is visible only in Access Optimizer.

Select the **Used** check box next to an attribute to make it available in the analysis.

Click **Save** to save your mapping.

### Mining Attributes

Select this tab to map parameters for bulk data loads used for role mining.

Map the parameters before you run the data snapshot. The mapping has no effect on an existing snapshot.

The **Parameter** tab lists the attributes that you can configure. Typically they are User attributes and Entitlement attributes.

Select a parameter to display a list of attributes on the right pane. The list contains ten editable fields where you can enter the name of an attribute.

Enter the names that you want to be displayed in the data snapshot.

For User attributes, you can enter names that replace the names of attributes of the User ERC table. The replacement is visible only in Access Optimizer.

Select the **Used** check box next to an attribute to make it available in the analysis.

Click **Save** to save your mapping.

### Data file template

Use the data file templates to setup your import files before you run a data snapshot. You do not need to do this task if you plan to import the data from the IAG data base.

The data file templates are fixed structures that you must use to build your import files. The structure is common to all data types. It comprises the following column details for the file records:

*Table 203. Column details*

Detail	Description
Position	Position of the column in record
Name	Column name
Length	Column width in number of characters
Mandatory	Column is mandatory (Yes/No)
Key	Column is a key field. If true, it must be populated and duplicates yield errors.
Foreign Key	Secondary key
Description	Column description

Select a data type in the left pane to view the record structure in the right pane.

By default records are separated by a semicolon (;). You can use other separation characters, such as the vertical bar (|), or more than one character, such as |#|. To upload an empty value, in a not mandatory position, use two consecutive separators, for example:

;;

See the following import file examples for each data type:

- Organization Units
- Users
- Applications
- Entitlements
- Assignments

### Organization units

The organizational units upload is described.

This is the sample text file for the organizational units upload:

```
11;Finance;
111;Temporary Assistance (Finance);11
12;Marketing;
121;Temporary Assistance (Marketing);12
.....
.....
```

There are four OUs in this sample file.

The OU code (11 in the sample) is in position 1, has a maximum length of 256 characters (like all other data in this set), is a mandatory element, and is a data key that must be interpreted as an OU ID.

The OU name is in position 2. It is neither a mandatory element nor a key.

The parent OU code is in position 3. It is the parent of the OU in position 2. It is not mandatory but is a foreign key.

Therefore, the template item row is as follows:

**OU Code;OU Name;Parent OU Code**

For the Description field of position 3, you must follow the formatting rule described below:

- Organization Unit Parent ID. This field must be null for direct children of the root.

## Users

The users upload is described.

This is the sample text file for the users upload:

```
EXMPL001;Sebrle;Vaclav;11;;20002406 - Member of K Analysis Team;49000;305 - Finance Division;10003200 - K Management Unit;10003206 - K Analysis Team;Bratislava - Apolo;;;N-Z;20;3
EXMPL002;Neumannova;Katerina;11;;20002406 - Member of K Analysis Team;49000;305 - Finance Division;10003200 - K Management Unit;10003206 - K Analysis Team;Bratislava - Apolo;;;A-M;12;0
EXMPL003;Sorokina;Elena;11;;20007693 - Revenue Assurance Specialist;49000;305 - Finance Division;10003202 - Revenue Assurance & Billing Unit;10005801 - Revenue Assurance Team;Bratislava - Apolo cebtrum;;;A-M;32;7
```

There are three users in this sample file.

The code (EXMPL001 in the sample) is in position 1, has a maximum length of 256 characters (like all other data in this set), is a mandatory element, and is a data key that must be interpreted as a User ID.

The user surname is in position 2. It is a mandatory element but is not a key.

The user Name is in position 3. It is a mandatory element but is not a key.

The OU code is in position 4. It is mandatory and a foreign key.

User attributes are in positions 5-14.

Therefore, the item row is as follows:

**User Code; User Surname; User Name; OU Code; Attribute 0; Attribute 1;...; Attribute 9; Number of Assigned Permission; Number of SOD Violations**

## Applications

The applications upload is described.

This is the sample text file for the applications upload:



```
Active Directory
SAP
RACF
SAPIST
IRS
.....
.....
```

This sample file has five applications.

The application name is in position 1. It is a mandatory element and a data key.

Therefore, the item row is as follows:

### Application Code

### Entitlements

The entitlements upload is described.

This is the sample text file for the entitlements upload:

```
Supervisor;1;Active Directory;;;;;;;;;;a;23
Operator1;1;SAP;;;;;;;;;;a;54
Operator2;2;SAP;;;;;;;;;;a;10
SAP1;1;SAP;;;;;;;;;;a;6
CCA2;2;Oracle;;;;;;;;;;a;13
.....
.....
```

This sample file has five entitlements.

The entitlement name, with a maximum length of 256 characters, is a mandatory element in position 1.

The entitlement type, with a maximum length of 15 characters, is a mandatory element in position 2.

The application name in position 3 has a maximum length of 256 characters, is a mandatory element and is a foreign key.

The data described in the first 3 positions makes a unique set of data keys.

Entitlement attributes are in positions 4 to 13.

Therefore, the item row is as follows:

**Entitlement Name; Entitlement Type; Application Name; Attribute 0; Attribute 1;...; Attribute 9; Number of Assigned Business Activity; Number of SOD Constraints**

The mandatory formatting rules described below apply to the Description field of positions 2 and 3:

- Types: 1) Profile 2) IT role 3) Job role.
- This field must be null for job roles. It will be replaced by the technical application JOB\_ROLE\_APPLICATION.

**Assignments**

The assignments upload is described.

This is the sample text file for the assignments upload:

```
Operator_Query;1;CLF;EXMPL001;28/06/2012
FRAUD;1;CLF;EXMPL001; 29/06/2012
INFOLINE_SUPER;2;SAPIST;EXMPL001; 28/07/2012
READ;1;IRS;EXMPL001; 29/07/2012
H_READ;3;;EXMPL001; 30/07/2012
.....
.....
```

This sample file has five assignments: three profiles (Type=1), one IT role (Type=2) and one job role (Type=3).

In this scheme, all elements are data key, foreign key and mandatories.

Position 1 contains the entitlement name, with a maximum length of 256 characters.

Position 2 contains the entitlement type, with a maximum length of 15 characters.

Position 3 contains the application name, with a maximum length of 256 characters.

Position 4 contains the user code, with a maximum length of 256 characters.

Therefore, the item row is as follows:

**Entitlement Name; Entitlement Type; Application Name; Person Code; Last Certification Age**

In the Description field of position 2 and 3, you can find the formatting rules described below that you must follow:

- Types: 1) Profile 2) IT role 3) Job role
- Job roles must have this field null. It will be replaced by the technical application JOB\_ROLE\_APPLICATION.

## Mining Data file template

Use the mining data file templates to setup your import files before you run a bulk data load. You do not need to do this task if you plan to import the data from the IAG data base.

The data file templates are fixed structures that you must use to build your import files. The structure is common to all data types. It comprises the following column details for the file records:

Table 204. Column details

Detail	Description
Position	Position of the column in record
Name	Column name
Length	Column width in number of characters
Mandatory	Column is mandatory (Yes/No)
Key	Column is a key field. If true, it must be populated and duplicates yield errors.
Foreign Key	Secondary key
Description	Column description

Select a data type in the left pane to view the record structure in the right pane.

By default records are separated by a semicolon (;). You can use other separation characters, such as the vertical bar (|), or more than one character, such as |#|. To upload an empty value, in a not mandatory position, use two consecutive separators, for example:

;;

See the following import file examples for each data type:

- Organization Units
- Users
- Applications
- Entitlements
- “Entitlements hierarchy” on page 446
- Assignments

### Organization units

The organizational units upload is described.

This is the sample text file for the organizational units upload:

```
11;Finance;
111;Temporary Assistance (Finance);11
12;Marketing;
121;Temporary Assistance (Marketing);12
.....
.....
```

There are four OUs in this sample file.

The OU code (11 in the sample) is in position 1, has a maximum length of 256 characters (like all other data in this set), is a mandatory element, and is a data key that must be interpreted as an OU ID.

The OU name is in position 2. It is neither a mandatory element nor a key.

The parent OU code is in position 3. It is the parent of the OU in position 2. It is not mandatory but is a foreign key.

Therefore, the template item row is as follows:

**OU Code;OU Name;Parent OU Code**

For the Description field of position 3, you must follow the formatting rule described below:

- Organization Unit Parent ID. This field must be null for direct children of the root.

## Users

The users upload is described.

This is the sample text file for the users upload:

```
EXMPL001;Sebrle;Vaclav;11;;20002406 - Member of K Analysis Team;49000;305 - Finance Division;10003200 - K Management Unit;10003206 - K Analysis Team;Bratislava - Apolo;;;N-Z;20;3
EXMPL002;Neumannova;Katerina;11;;20002406 - Member of K Analysis Team;49000;305 - Finance Division;10003200 - K Management Unit;10003206 - K Analysis Team;Bratislava - Apolo;;;A-M;12;0
EXMPL003;Sorokina;Elena;11;;20007693 - Revenue Assurance Specialist;49000;305 - Finance Division;10003202 - Revenue Assurance & Billing Unit;10005801 - Revenue Assurance Team;Bratislava - Apolo cebtrum;;;A-M;32;7
```

There are three users in this sample file.

The code (EXMPL001 in the sample) is in position 1, has a maximum length of 256 characters (like all other data in this set), is a mandatory element, and is a data key that must be interpreted as a User ID.

The user surname is in position 2. It is a mandatory element but is not a key.

The user Name is in position 3. It is a mandatory element but is not a key.

The OU code is in position 4. It is mandatory and a foreign key.

User attributes are in positions 5-14.

Therefore, the item row is as follows:

**User Code; User Surname; User Name; OU Code; Attribute 0; Attribute 1;...; Attribute 9; Number of Assigned Permission; Number of SOD Violations**

## Applications

The applications upload is described.

This is the sample text file for the applications upload:

```
Active Directory
SAP
RACF
SAPIST
IRS
.....
.....
```

This sample file has five applications.

The application name is in position 1. It is a mandatory element and a data key.

Therefore, the item row is as follows:

### Application Code

### Entitlements

The entitlements upload is described.

This is the sample text file for the entitlements upload:

```
Supervisor;1;Active Directory;;;;;;;;;;a;23
Operator1;1;SAP;;;;;;;;;;a;54
Operator2;2;SAP;;;;;;;;;;a;10
SAP1;1;SAP;;;;;;;;;;a;6
CCA2;2;Oracle;;;;;;;;;;a;13
.....
.....
```

This sample file has five entitlements.

The entitlement name, with a maximum length of 256 characters, is a mandatory element in position 1.

The entitlement type, with a maximum length of 15 characters, is a mandatory element in position 2.

The application name in position 3 has a maximum length of 256 characters, is a mandatory element and is a foreign key.

The data described in the first 3 positions makes a unique set of data keys.

Entitlement attributes are in positions 4 to 13.

Therefore, the item row is as follows:

**Entitlement Name; Entitlement Type; Application Name; Attribute 0; Attribute 1;...; Attribute 9; Number of Assigned Business Activity; Number of SOD Constraints**

The mandatory formatting rules described below apply to the Description field of positions 2 and 3:

- Types: 1) Profile 2) IT role 3) Job role.
- This field must be null for job roles. It will be replaced by the technical application JOB\_ROLE\_APPLICATION.

### Entitlements hierarchy

The entitlement hierarchy upload is described.

This is the sample text file for the entitlement hierarchy upload:

```
I_EXT_CARE_ACADEMY_DELIVERY_R;2;YOYODYNE;I_EXT_PAMS_C;2;YOYODYNE
I_EXT_VERTU_PROJECT_C;2;YOYODYNE;I_EXT_VERTU_LOGISTICS_C;2;YOYODYNE
I_EXT_VERTU_PROJECT_C;2;YOYODYNE;I_EXT_VERTU_MANUFACTURING_C;2;YOYODYNE
I_EXT_YOYODYNE_HR;2;YOYODYNE;I_EXT_YOYODYNE_HR_ADDITIONALS;2;YOYODYNE
I_EXT_AMS_R;2;YOYODYNE;I_AMS_R;2;YOYODYNE
.....
.....
```

This sample file has five hierarchies.

In this scheme, all elements make up a unique set of data keys, foreign keys and mandatory elements.

The parent entitlement name in position 1 has a maximum length of 256 characters, is a mandatory element and is both a data and foreign key.

The parent entitlement type in position 2 has a maximum length of 15 characters, is a mandatory element and is both a data and foreign key.

The parent entitlement application name in position 3 has a maximum length of 256 characters, is a mandatory element and is both a data and foreign key.

The child entitlement name in position 4 has a maximum length of 256 characters, is a mandatory element and is both a data and foreign key.

The child entitlement type in position 5 has a maximum length of 15 characters, is a mandatory element and is both a data and foreign key.

The child entitlement application name in position 6 has a maximum length of 256 characters, is a mandatory element and is both a data and foreign key.

Therefore, the item row is as follows:

**Parent Entitlement Name; Parent Entitlement Type; Parent Entitlement Application Name; Child Entitlement Name; Child Entitlement Type; Child Entitlement Application Name**

The mandatory formatting rules described below apply to the Description field of positions 2, 3, 5 and 6:

- Types: 1) Profile 2) IT role 3) Job role.
- This field must be null for job roles. It will be replaced by the technical application JOB\_ROLE\_APPLICATION.
- The child entitlement type cannot be bigger than the one of the parent.
- This field must be null for job roles. It will be replaced by the technical application JOB\_ROLE\_APPLICATION.

**Assignments**

The assignments upload is described.

This is the sample text file for the assignments upload:

```
Operator_Query;1;CLF;EXMPL001;28/06/2012
FRAUD;1;CLF;EXMPL001; 29/06/2012
INFOLINE_SUPER;2;SAPIST;EXMPL001; 28/07/2012
READ;1;IRS;EXMPL001; 29/07/2012
H_READ;3;;EXMPL001; 30/07/2012
.....
.....
```

This sample file has five assignments: three profiles (Type=1), one IT role (Type=2) and one job role (Type=3).

In this scheme, all elements are data key, foreign key and mandatories.

Position 1 contains the entitlement name, with a maximum length of 256 characters.

Position 2 contains the entitlement type, with a maximum length of 15 characters.

Position 3 contains the application name, with a maximum length of 256 characters.

Position 4 contains the user code, with a maximum length of 256 characters.

Therefore, the item row is as follows:

**Entitlement Name; Entitlement Type; Application Name; Person Code; Last Certification Age**

In the Description field of position 2 and 3, you can find the formatting rules described below that you must follow:

- Types: 1) Profile 2) IT role 3) Job role

- Job roles must have this field null. It will be replaced by the technical application JOB\_ROLE\_APPLICATION.



---

## Chapter 18. Introduction to Access Risk Controls for SAP

Access Risk Controls for SAP (ARCS) engine extends the capabilities of ARC to the authorization framework of SAP systems, enabling the implementation of a SoD analysis based on the SAP system transactions.

The activity-based SoD model defines SoD conflicts in terms of high-level business-oriented activities. This approach allows business experts to define and maintain SoD policy separately from the low-level entitlements, which are administered by IT specialists.

Starting from the activity-based SoD model of an organization, ARCS supports native inspection of SAP roles involved in the activities modeled and low-level SAP authorization objects.

The ARCS module enables you, using the functions implemented by the RBAC engine of the ISIG platform, to assign cluster roles to users of a SAP system; the cluster roles are defined as SAP roles aggregates.

A generic SAP role is composed by a specific set of transactions (T) and authorizations objects (AO).

The transaction object is a specific type of AO, which determines the elementary operation performed by the user on the system.

The real access privileges which a user has on a SAP system do not depend exclusively on the enabled transactions, but derive from the specific combination of AOs associated to the transaction.

The transaction represents the main object that determines what a user is enabled to do but this alone is not sufficient; it is necessary to analyze the combined presence of multiple AOs which determine what and how to operate using the transaction.

The ARCS module can perform a SoD transaction-oriented analysis considering possible AO combinations that can significantly modify the behavior of the transaction.

---

### ARCS Data Model

The basic entities of the ARCS Data Model are in compliance with the main entities described in "IBM Security Identity Governance and Intelligence extended data model" on page 21.

The main differences regard the structure of the SAP Roles and Risk Entitlements.

From a Business Model point of view, a valid approach is to associate Risk Entitlements to the Business Activities hierarchy, that in ARCS is recognized as Business Activity Mapping.

For the purpose of modeling then, the:

- Business Activity Tree of ARCS is an exact clone of Business Activity Tree of ARC.
- The associations of Activities and Risks in ARCS are exact replicas of the ones defined in ARC.

To make and keep this correspondence over time, see “Activity Tree: aligning ARC to ARCS” on page 452.

For a coherent model, when Business Activity Mapping is defined on ARCS, we need to match it in ARC.

To obtain such alignment, see “Business Activity Mapping: ARCS to ARC” on page 451.

## SAP roles and risk entitlements

Considering all the processing steps the ARC module provides the following indications.

A SAP role can be identified by:

1. A generic transaction Tk
2. A transaction set (T1, T2,... Tn)
3. A generic authorization object AOj
4. An authorization object set (AO1, AO2, ..., AOn)
5. The aggregation between one or several transactions with one or several authorization objects.

Usually, when a SAP role is aggregated to a generic transaction Tk, the SAP system automatically detects the authorization objects set which is needed to run the transaction Tk.

The most common case is the one described in bullet 5, where a SAP role is identified from the aggregation between TRs and AOs.

A risk entitlement can be aggregated to each SAP role.

A risk entitlement identifies a composition of a transaction and authorization objects that are a potential risk for the SAP system.

An example follows to better clarify this concept.

Consider the four different and structured SAP roles:

- SR1 (T1, O1, O2, O3)
- SR2 (T2, O4, O5)
- SR3 (T3, O1)
- SR4 (T3, O5)

Based on the TRs (T1, T2 and T3) and the AOs (AO1, AO2, AO3, AO4 and AO5), five risk entitlements are identified:

- RISK1 (T1, O1)
- RISK2 (T1, O4)
- RISK3 (T2, O5)
- RISK4 (T2, O3, O5)

- RISK5 (T3, O2, O5)

These five combinations of TRs and AOs can be a potential risk for the SAP system.

They are, therefore, aggregated in the following way:

- SR1 (T1, O1, O2, O3) -->RISK1 (T1, O1)
- SR2 (T2, O4, O5) -----> RISK3 (T2, O5)
- SR3 (T3, O1) -----> RISK5 (T3, O2, O5)
- SR4 (T3, O5) -----> RISK5 (T3, O2, O5)

If you consider two combinations of risk entitlements in SoD conflict:

- (RISK1, RISK2)
- (RISK1, RISK5)

you will easily recognize that a user U1, with assigned SR1 and SR2, is not enabled to perform potentially risky SAP operations, because the combination (RISK1, RISK3) is not in SoD conflict.

Consider now a cluster role composed by a set of SAP roles; consequently, also the cluster role is aggregated to a different risk entitlement set.

Consider two cluster roles:

- CR1 (SR1, SR2), that are automatically characterized by RISK1 and RISK3.
- CR2 (SR1, SR3), that are automatically characterized by RISK1 and RISK5.

Now consider again the same user U1 and assign to him CR2, in addition to SR1 and SR2.

The risky profile of U1 will evolve as shown below:

U1 ---> SR1, SR2 and CR2 ---> RISK1, RISK3, RISK5 ---> **SoD conflict** ---> **(RISK1, RISK5)**

## Business Activity Mapping: ARCS to ARC

When a Business Activity Mapping is defined on ARCS, we need to align it into ARC.

To build a new Business Activity Mapping, you need to associate a Business Activity with a SAP Risk Entitlement, built on a set of Authorization Objects (AOs).

The SAP Risk Entitlement is associated with a SAP Role, through the AOs objects that characterize the SAP Role.


The SAP Role is related to a SAP Application.

To align the Business Activity Mapping in ARC, you need to define a new Permission (in AG Core) with the same name of the aforementioned SAP Role.

The Permission must be associated to an Application named with the same name of the SAP Application.

According to this scheme, there is a scheduled Task, named **AccessRiskControls4SAPSync** (Task Planner module) that automatically aligns the Business Activity Mapping built in ARCS to ARC.

If you want to test this aligning procedure, run the steps listed below:

1. Access the Task Planner module and select the **Manage > Task** tab
2. In the list of Tasks, verify if the Task **AccessRiskControls4SAPSync** is active (  icon), otherwise select it and start it (**Actions > Start** )
3. In the **Manage > Task > Scheduling** tab, click **Edit**, define the scheduling settings, and click **Save**.
4. In the Access Risk Controls module, associate a SAP Risk Entitlement to an Activity (go to **Manage > Business Activities > Risk Entitlement** and select **Actions > Add**).
5. In the Access Governance Core module, add a Permission (go to **Manage > Roles** and select **Actions > Add > Edit**) with the same name of the SAP Role related to the SAP Risk Entitlement (step 4).
6. The Permission must be added to an Application (**Manage > Applications > Permissions**) and its name must be the name of the SAP Application related to the SAP Role (step 5).
7. After the completion of the **AccessRiskControls4SAPSync** task, verify in the ARC module that the Business Activity Mapping is aligned (**Manage > Business Activity Mapping**).

## Activity Tree: aligning ARC to ARCS

The Activity Tree of ARCS is a direct clone of the Activity Tree of ARC.

The ARC Activity Tree can vary any time.


Every Activity of ARC can be associated to a set of Risks (Business Model - RBAC Model).

After the installation of the product and during the first period of administration and configuration of the operative environment, the structure of the ARC Activity Tree can vary widely and the same for the set of Risks joined to Activities.

Any time that you add/remove an Activity into the ARC Activity Tree or that you associate a Risk to an Activity, there is a scheduled task, named **AccessRiskControls4SAPSync** (Chapter 20, "Introduction to Task Planner," on page 545 module) that automatically aligns the ARCS Activity Tree and/or the relations Activity-Risk.

The scheduling period is decided by the administrator (generally, it's reasonable to schedule this task at least one time per day).

To test the alignment procedure, run the following steps:

1. Access the Task Planner module and select **Manage > Task** .
2. In the list of Tasks, verify if the Task **AccessRiskControls4SAPSync** is active (  icon), otherwise select it and start it (**Actions > Start**).
3. Go to **Manage > Task > Scheduling**, click **Edit** to define the scheduling settings, and click **Save**.

4. In the Access Risk Controls module, add/remove an Activity ( **Manage > Business Activities > Actions > Add/Remove**).

After running of **AccessRiskControls4SAPSync** task, verify the alignment of the ARCS Activity Tree (**Manage > Business Activities**).

---

## Introduction to the ARCS-SAP adapter agent

The ARCS-SAP adapter agent is a specialized module of the IBM Security Identity Governance platform, integrated with the Access Risk Compliance Control for SAP (ARCS) module.

The ARCS-SAP adapter agent must be installed on the SAP side and is interrogated by the ARCS module to download specific data sets from the SAP server.

The scope of this documentation is to provide:

- An outline of the installation procedure for the ARCS-SAP adapter agent.
- A brief description of the agent functions.

The installation of the ARCS-SAP adapter agent does not require special prerequisites. The agent was developed and tested on the following SAP versions:

- R/3 4.6c
- R/3 4.7
- ERP 6.0

## Distribution

The distribution structure is made for managing two distinct sets of Change Requests: Workbench Requests and Customizing Requests

### Workbench Requests

In this area, you can make structural updates of the environment (for example, to drop or to update a table of the DB).

The distribution for Workbench is differentiated based on the type of SAP system coding.

If the SAP system is Unicode-based, you have to use the package `Unicode.zip`.

If it is a non-Unicode system, you have to use the package `Non_Unicode.zip`.

Each package is an SAP Change Request.

Each package contains exactly two files, named:

- `Kxxxxxx.xxx`
- `Rxxxxxx.xxx`

### Customizing Requests

In this area, you can make customizations actions (for example, to add an authorization object or to update the configuration related to a process).

For the SAP system, the package `Role.zip` must be used.

Here you can find the definition of the role Z\_ARCS\_REMOTE.

Each package contains exactly two files, named:

- Kxxxxxx.xxx
- Rxxxxxx.xxx

## Installation procedure

Before starting with the installation procedure, import the SAP libraries sapjco3.jar and libsapjco3.so.

For addressing this prerequisite, see the section related to the SAP libraries import.

To install the ARCS SAP adapter agent, you must perform the following steps:

1. Import the two preselected Change Requests into the SAP system (Workbench Requests (Unicode or Non-Unicode) and Customizing Requests).
2. Extract the two preselected packages: for each package, two files named Kxxxxxx.xxx and Rxxxxxx.xxx are extracted.
3. Copy the file Kxxxxxx.xxx into the directory <DIR\_TRANS>/cofiles.
4. The owner of the files must be <SID> adm (or equivalent role in Microsoft environment) and the permissions must be set to 755.
5. Copy the file Rxxxxxx.xxx into the directory <DIR\_TRANS>/data.
6. The owner of the files must be <SID> adm (or equivalent role in Microsoft environment) and the permissions must be set to 755.
7. Import the change requests into the target system:
  - In the STMS transaction, select the import buffer of the target system.
  - Append the two CR <SID>Kxxxxxx to the import buffer.
  - Import the two CR <SID>Kxxxxxx into the target system.
8. In the SU01 transaction, create a user of type "Communication" and then assign it to the SAP role Z\_ARCS\_REMOTE.

Generally, the suffix <DIR\_TRANS> coincides with the path /usr/sap/trans.

However, this indication might vary from system to system.

## ARCS-SAP adapter agent functions

The agent functions are:

- z\_start\_synch
- z\_get\_job\_status
- z\_get\_synch\_data
- z\_get\_single\_role
- z\_get\_tcode

### **z\_start\_sync**

This feature creates a SAP job that makes mass extractions of SAP authorization data and populates the relative data and log tables.

Synchronization can be done in the following modes:

- Delta mode: if the parameter SYNCH\_DELTA\_DATE is set
- Full mode: if the parameter SYNCH\_DELTA\_DATE is not set

The job is called dynamically.

For a Delta mode extraction the job is called Z\_CCS\_SYNCHDATA\_DELTA.

In case of a Full mode extraction the job is called Z\_CCS\_SYNCHDATA\_FULL.

The two tables below show all the parameter features, grouped according to Input (Import) or Output (Export) parameters:

*Table 205. z\_start\_sync - INPUT parameters.*

Field	Type	Dimension	Values	Description
SYNCH_DATA	Numeric	1	0	Extraction of all data types
			1	Extraction of roles and other data  Extracted roles are all those associated to authorization objects (OA) (table agr_1251) to obtain the object detail which is then used to create the range.  For the extraction of other data, a range containing the transactions (table tstc) is first created. OAs are associated to every transaction (table usobt_c). Therefore, for each OA, reference is made to the tactz table (range created in the Role extraction phase) to obtain the ACTVT value.
			3	Account details extraction  First, all accounts are extracted from the table usr04. With the <code>USR_USER_PROFS_PROFILES_GET</code> function, all profiles associated to the account are extracted.  Finally, using <code>BAPI_USER_GET_DETAIL</code> all account details, such as name and surname, are read.
			4	Massive profile extraction  Access to the table usr10 with the filter set to type "G"
			5	Extraction of all the roles  Access to the table agr_define
SYNCH_DELTA_DATE	Dats	8	ggmmaaaa	To be set for Delta mode  If not set, full synchronization will be assumed.

*Table 206. z\_start\_sync - OUTPUT parameters.*

Field	Type	Dimension	Values	Description
SYNCH_DATE	DATS	8	ggmmaaaa	Synchronization data

### **z\_get\_job\_status**

This function returns the status and log of the SAP job launched with the `z_start_sync` command.

The function reads the job name from the job summary table (TBTCO), and if multiple jobs are present, selects the last in order of date/time.

Output (Export) parameters are described in the following table:

Table 207. *z\_get\_job\_status* - *OUTPUT* parameters.

Field	Type	Dimension	Values	Description
JOB_STATUS	CHAR	1	R, A, F, C	Indicates the status of the job: <ul style="list-style-type: none"> <li>• R: Ready</li> <li>• A: Active</li> <li>• F: Finished</li> <li>• C: Cancelled</li> </ul>
START_TIMESTAMP	CHAR	14	ggmmaaaaooommss	Job start date/time
END_TIMESTAMP	CHAR	14	ggmmaaaaooommss	Job end date/time
RUNTIME	CHAR	6	ooommss	Job execution time
SYNCHTYPE	CHAR	5	DELTA, FULL	Synchronization type

### **z\_get\_sync\_data**

This command allows the ARCS module to receive packaged authorization data from the tables in the queue.

The packet size can be configured by setting the Input (Import) parameters which will define the package number and size as well as the type of data to be extracted.

This data is taken from the custom tables based on the value of SYNCH\_DATA.

This type of transmission helps avoiding possible timeout issues related to SAP processes and ensures data consistency if the system should fail during the transmission between SAP and ARCS.

Table 208. *z\_get\_sync\_data* - *INPUT* parameters.

Field	Type	Dimension	Values	Description
PACKET_NUM	CHAR	16		Identifies which packet must be sent
PACKET_SIZE	CHAR	8		Identifies packet dimension (Num. of table records)
SYNCH_DATA	NUMERIC	1	1, 2, 3, 4, 5	Identifies type of data to be extracted: <ul style="list-style-type: none"> <li>• 1: Roles</li> <li>• 2: Other data</li> <li>• 3: Accounts</li> <li>• 4: Profiles and profile types</li> <li>• 5: Collective roles</li> </ul>



Table 209. z\_get\_sync\_data - OUTPUT parameters.

Field	Type	Dimension	Values	Description
ROLE_DATA	CHAR	TBD		Package with the required data describing the structure of a single SAP role
OTHER_DATA	CHAR	TBD		Package with required data

The following tables describe the structure (data track) of the packages:

- ROLE\_DATA
- OTHER\_DATA

Table 210. ROLE\_DATA.

Field	Elementary Data	Type	Dimension	Description
AGR_NAME	AGR_NAME	CHAR	30	Role
TEXT	AGR_TITLE	CHAR	80	Role description
OBJECT	XUOBJECT	CHAR	10	Authorization object (OA)
ATEXT	XUTEXT	CHAR	60	OA description
TIMESTAMP	ZTIMESTAMP	CHAR	14	Timestamp from the last OA modification
FIELD	XUFIELD	CHAR	10	"FIELD" field name
VON	XUVAL	CHAR	40	"From" value
BIS	XUVAL	CHAR	40	"To" value

Table 211. OTHER\_DATA.

Field	Elementary Data	Type	Dimension	Description
ID_DATA	ZTRAK	CHAR	1	Identifies two types of data, characterized by the same structure (record track), distinguished by the letters A or B
NAME	TCODE	CHAR	20	Cod. transaction
TEXT	TTEXT_STCT	CHAR	36	Transaction description
OBJECT	XUOBJECT	CHAR	10	OA
ACTVT	ACTIV_AUTH	CHAR	2	ACTVT value: <ul style="list-style-type: none"> <li>• A: transaction scope</li> <li>• B: explosion diagram for the asterisks</li> </ul>

## **z\_get\_single\_role**

This function returns the authorization information to ARCS for an individual role, provided as an Input (Import) parameter.

*Table 212. z\_get\_single\_role - INPUT.parameters.*

Field	Type	Dimension	Values	Description
ROLE_NAME	CHAR	30		Unique SAP role identifier

*Table 213. z\_get\_single\_role - OUTPUT.parameters.*

Field	Type	Dimension	Values	Description
ROLE_DATA	CHAR	TBD		Package with the required data describing the structure of a single SAP role

## **z\_get\_tcode**

This function returns to ARCS the existing transaction codes associated to the Input (Import) data values.

*Table 214. z\_get\_tcode - INPUT parameters.*

Field	Type	Dimension	Values	Description
TCODE_FROM	CHAR	20		Initial code of the transaction to be searched for
TCODE_TO	CHAR	20		Final code of the transaction to be searched for

*Table 215. z\_get\_tcode - OUTPUT parameters.*

Field	Type	Dimension	Values	Description
TCODE_DATA	CHAR	TBD		Data structure of the transactions found

The following table describes the structure (data track) of the package TCODE\_DATA:

*Table 216. Structure of TCODE\_DATA.*

Field	Elementary Data	Type	Dimension	Description
TCODE	TCODE	CHAR	20	Transaction code
TTEXT	TTEXT_STCT	CHAR	36	Transaction description



## **ARCS-SAP adapter Agent:User Role**

For integrating two systems, IGI and SAP, a custom role that is named Z\_ARCS\_REMOTE is needed.

This role manages the authorization for:

- RFC calls
- Creating of jobs

For examining the structure of the role, proceed as follows:

1. Log in to SAP console.
2. In **SAP Easy Access** pane window page, specify the name of transaction: PCFG
3. Click green icon on the left (or click **Enter** by keyboard).
4. In the filter **Role**, set the name of the role: Z\_ARCS\_REMOTE.
5. Click  **Display** button.
6. Select the tab **Authorizations**.
7. Click  **Display Authorizations Data** button.
8. Now you can view the hierarchical structure of the role Z\_ARCS\_REMOTE
9. Clicking the nodes of the hierarchy you can browse into all components of the role.

The Z\_ARCS\_REMOTE is structured into two main segments:

- Segment AAAB (Cross-application Authorization Objects).
- Segment BC\_A (Basis: Administration).

---

## Manage

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

- Business Activities
- Business Activity Mapping
- Risk Definitions
- Domains

### Business activities

This section comprises all functions for the management of the business activity and for modeling a business activity tree structure.

In the left pane **Business Activity** are present two tabs.

In the **Tree View** tab, you can:

- Browse in the business activity tree for selecting the desired activity.
- Add or remove activities (**Actions** menu)

In the **Search** tab are available the filters to search for an activity (click **Filter/Hide Filter**) and the **Actions>View** button for toggling to the **Tree View** tab.

The table below lists the available filters:

Table 217. Business activity filters.

Filter	Description
Name	Name of the business activity.

Table 217. Business activity filters. (continued)

Filter	Description
<b>Identifier</b>	The univocal identifier of the business activity.
<b>Description</b>	Brief description of the business activity.


The contents of the right pane changes depending on the tab clicked in the upper side of the pane. When the Business Activity web interface has just been accessed, the **Details** tab is active by default. Under this tab are available two different panes:

- **Activity details**
- **Activity property**

After an activity is selected in the left pane, the **Activity details** pane shows the related data contained in the AGCore database. The **Activity details** pane displays data, regarding the selected activity, contained in the external repositories.

The tables below lists the activity details:

Table 218. Activity details.

Detail	Description
<b>Parent Activity</b>	Name of the parent activity (automatically set after the activity selection in the left frame).
<b>Name</b>	Name used within the organization to identify the activity.
<b>ID Code</b>	The univocal identifier of the activity.
<b>Description</b>	Brief description of the activity.
<b>Owner</b>	User who is responsible for the considered activity. Use the  <b>User</b> button on the right side of the attribute box to insert a user.

An activity can be aggregated to a set of properties that characterize it.

The Activity property pane displays properties that can add specific information to the selected activity.

For example, a property can have, as value, an external link to the set of implementing regulations and standards compliance that must be implemented by that activity. Another example consist of considering the values of properties into the structure of a rule.

A property is identified by a pair of attributes <Name,Value>.

Properties can be easily added/removed/saved through **Add** or **Remove** or **Save** buttons under the **Actions** menu in the upper right side of the pane.



**Note:**

It is possible to have multi-values properties. It is also possible to specify a property **PROP\_1** and associate to it a value *VALUE\_1*.

Then add a new line, in the **Activity Property** pane, and specify the same property name (**PROP\_1**) associated to a different value (*VALUE\_2*).

In the list below are described the main operation groups related to the business activities:

- Details
- “Risk entitlements”
- “Risk memberships” on page 462
- “Applicable domains” on page 462

### **Risk entitlements**

In this section, you can link risk entitlements to activities.

Selecting an activity from the left pane, the **Risk Entitlements** tab (right) is enabled and shows a list of the risk entitlements associated to the selected activity.

From the **Risk Entitlements** tab, you can **Add** or **Remove** a risk entitlement (**Actions** menu).

For adding a risk entitlement, by clicking **Actions > Add**, the window Add Risk Entitlement opens. In this window, the following filters can be used for the risk entitlement search (click **Filter/Hide Filter**):

Table 219. Permission filters.



<b>Filter</b>	<b>Description</b>
<b>SAP system</b>	Name of the SAP system for filtering risk entitlements. Use the  <b>Set SAP system</b> button on the right side of the attribute box to set the SAP system.
<b>Type</b>	Type of filtered risk entitlements. Use the  <b>Set Risk Entitlement Type</b> button on the right side of the attribute box to set a permission type.
<b>Name</b>	Risk entitlement name.

Table 219. Permission filters. (continued)

Filter	Description
<b>Status</b>	<p>This filter can have one of the following four values:</p> <ul style="list-style-type: none"> <li>• <b>TBD</b>: when a risk entitlement is not associated to any activity but is not in the status Ignored or Missing Activity.</li> <li>• <b>Linked</b>: a risk entitlement is associated to an activity.</li> <li>• <b>Ignored</b>: when a risk entitlement is not associated to any activity.</li> <li>• <b>Missing Activities</b>: when the operator does not know to which activities to associate the risk entitlement.</li> </ul>

## Risk memberships

This section allows you to display all risks aggregated to a selected activity.

The **Risk Membership** tab contains the list of risks associated with the activity selected in the left frame.

Selecting a risk from the list and clicking **Actions>Risk**, the Activities risk window opens displaying the list of all activities associated with the risk selected.

If the **Hier** column is flagged with the  icon, the Risk selected is associated with all activities included in the selected activity.

After selecting an activity, by clicking **Actions>View**, the Tree View window opens and displays the exact position of the activity in the hierarchy.

## Applicable domains

This section allows you to display all domains aggregated to a selected activity.

The **Applicable Domains** tab contains the list of domains that are already aggregated to the activity selected in the left frame. In the **Applicable Domains** tab, the filters that can be used to perform a domain search are **Name** and **Description**.

## Activities and permissions



From this tab, you can associate the permissions to one or more activities.

The relationship between activities and permissions is "many to many".

An activity can be described using a set of aggregated permissions that are necessary for its implementation; in addition, a single permission can be aggregated to more than one activity.

In the **Permission** tab (left), you can search for a specific permission according to the filters summarized below (clicking **Filter/Hide Filter**):

Table 220. Permission filters.

Filter	Description
<b>Application</b>	Name of the application in which the illegal permission are filtered. Use the  Set Application button on the right side of the attribute box to insert an application.
<b>Type</b>	Type of filtered permission. Use the  Set Permission Type button on the right side of the attribute box to insert a permission type.
<b>Name</b>	Permission name.
<b>Status</b>	This filter can have four values: <ul style="list-style-type: none"> <li>• <b>TBD</b>: when a permission is not associated to any activity but is not in the status Ignored or Missing Activity.</li> <li>• <b>Linked</b>: a permission is associated to an activity.</li> <li>• <b>Ignored</b>: when a permission is not associated to any activity.</li> <li>• <b>Missing Activities</b>: when the operator does not know to which activities to associate the permission</li> </ul>

The results are displayed in the same pane according to the attributes summarized below:

Table 221. Permission attributes.

Attribute	Description
<b>Status</b>	Status of the permission.
<b>Name</b>	Name of the permission.
<b>Type</b>	Type of application.
<b>Application</b>	Name of the application.

From the **Permission** tab, by clicking a permission, the **Details** tab (right) is enabled.

In the upper section of this pane information is displayed about the selected permission and two check boxes that allow to switch the status of the selected permission: from TBD to Ignore or Missing activity.

Table 222. Permission details.

Detail	Description
<b>Name</b>	Name of the permission.
<b>Application</b>	Name of the application.
<b>Description</b>	Brief description of the permission.

To add an activity, click **Add** and, from the Add window, choose the desired activity from the **Tree view** tab or clicking the **Search** tab entering the filters for the search operation (clicking **Filter/Hide Filter**).


Table 223. Activity filters.

Filter	Description
<b>Name</b>	Activity name.
<b>Identifier</b>	Unambiguous identifier of activity.
<b>Description</b>	Brief description of the activity.

To remove an activity, in the **Details** tab from the list of the associated activities, select the desired activity, then click **Remove**.

When the Permission-Activity association is removed, the status of the permission returns in TBD status.

After the desired operation has been performed, click **Save** in the bottom right part of the pane.

	<b>Note:</b> When a permission is in Linked status, it is not possible to switch it to any other status. To switch the status of the Linked permission is necessary to remove the associated activity.
---	--

## Risk Definitions

This page lists the risks defined in the system and their associated activities.

The Risk tab on the left displays the list of risks defined in the system.

Use the Filter button to find a specific risk definition or to narrow down the search to specific definitions. The following filters are available:

Table 224. Available filters to find a Risk definition.


Filter	Description
Name	Risk name
Description	Description of the risk
Status	Risk status. It can be: <b>Assigned Risk</b> The risk is already assigned to the mitigation <b>Not Assigned Risk</b> The risk is not yet assigned to the mitigation
Type	The risk type. It can be: <b>Risk</b> A possible threat or potential damage <b>SoD</b> A segregation of duties conflict

The list of risk definitions is imported from Access Risk Control.

As you select a risk definition from the list in the Risk tab, its details are displayed on the right. The details are:



Table 225. Details of a Risk definition.

Detail	Description
<b>Name</b>	Risk name
<b>Description</b>	Description of the risk nature
<b>Type</b>	Type of risk ( <b>SoD</b> or <b>Risk</b> )
<b>Scope Type</b>	Type of visibility scope: <ul style="list-style-type: none"> <li>• <b>Model:</b> Risk is assigned as a user role</li> <li>• <b>Scope:</b> Risk is assigned directly to a user (owner)</li> <li>• <b>Both:</b> Risk can be assigned using a model or a scope</li> </ul>
<b>Level</b>	Level of risk (measured from 0 to 9)
<b>Impact</b>	Description of the risk impact
<b>Likelihood</b>	Value between 0 and 1
<b>Tolerance</b>	Description of the risk tolerance
<b>Trend</b>	Description of the risk trend
<b>Risk acceptance rational</b>	Description of the manageable risk acceptance. Risk acceptance is a value < tolerance
<b>Owner</b>	Name of the person responsible for an activity in a company. Use the  <b>User</b> button on the right side of the attribute box to insert a user (owner)
<b>Creation Date</b>	Date of the risk creation (dd/mm/yyyy; hh/mm/ss)

Click the **Activity** tab in the right-hand page to display the list of activities associated with the selected risk. Select an activity and click **Actions > View** to view the exact position of the selected activity in the tree structure of business activities. You can run this task also by:

1. Selecting a risk definition from the list in the left page.
2. Clicking **Actions > Risk** to display a panel with the associated activities.
3. Selecting an activity and clicking **Actions > View**.
4. Scrolling the tree structure until you find the highlighted activity.

## Domains

In this section, you can define an unlimited number of domains.

The **Domain** tab contains the list of domains registered in the system. Select a domain to view its details in the **Details** tab.

In the **Domain** tab, a domain can be added (**Add** button) or removed (**Remove** button).

The filters available for a domain search are name and description (click **Filter/Hide Filter**).

The domain details are described in the table below:

Table 226. Domain details.

Detail	Description
Type	Type of domain.
Name	Name of the mitigation action.
Description	Brief description of the mitigation.
Extended Description	Extended description.
Note	This attribute can be utilized to indicate a specific message.

In the list below are shown the main operation groups related to the domains:

- Details
- Permissions
- Applications
- Mitigation Controls
- Activities

## Permissions



In this section are available the procedures to aggregate permissions to domains.

In the **Permissions** tab are listed all the permissions already aggregated to the domain selected in the **Domain** tab. In the same pane it is possible to add and remove a permission by clicking **Add** or **Remove**.

Clicking **Add**, opens the Add window that shows the list of all permissions listed in the system.

In the **Permissions** tab and in the Add window, the following filters can be used for the permissions search (click **Filter/Hide Filter**):

Table 227. Permissions filters.

Filter	Description
Application	Application of the permission. Use the  <b>Set Application</b> button on the right side of the attribute box to insert an application.
Name	Name of the permission.
Type	Type of permission. Use the  <b>Set Permission Type</b> button on the right side of the attribute box to insert a type.

## Applications

In the **Applications** tab are listed all applications already aggregated to the domain selected in the **Domain** tab.

In the same tab you can add and remove an application by clicking **Add** or **Remove**.

Clicking **Add** opens the Add window that contains the list of all applications listed in the system.

In the **Applications** tab and in the Add window, the **Name** (name of the application) filter can be used for applications search (click **Filter/Hide Filter**).

## Mitigation controls

In the **Applicable Domains** pane are listed all the mitigations already aggregated to the domain selected in the **Domain** tab.

In the same pane you can remove a mitigation by clicking **Remove**. The **Add** pane contains the list of all the mitigations listed in the system. From this pane, you can add a mitigation to a domain by clicking **Add**.

The filters available for a mitigation search are **Name** and **Description** (click **Filter/Hide Filter**).

## Activities

This paragraph allows to view the activities aggregated to a domain.

In the **Activities** tab are listed all the activities already aggregated to the domain selected in the **Domain** tab, on the left. In this tab, the following filters can be used for the permissions search (click **Filter/Hide Filter**):

Table 228. Activities filters.

Filter	Description
Name	Name of the activity.
Identifier	Univocal identifier of the business activity.
Description	Description of the activities.

---

## Configure

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

- Configuration Set
- SAP System
- Rules


## Configurations

This section describes the basic operations that you can use to manage your configurations.

The **Configuration** tab displays all the configurations listed by the system.

To find a particular configuration, use the **Name** and **Description** filters (after clicking **Filter**).

Select a configuration from the list to display its details. Click the **Actions** button to:

- Set the configuration as  working, by clicking **Current**.
- Change the configuration name or description, by clicking **Edit**.
- Add or remove a configuration, by clicking **Add** or **Remove**.

## SAP System

This section describes the basic operations that you can use to manage your SAP systems.

The **SAP system** tab displays a list of the SAP systems available to Access Risk controls for SAP.

You can enter a SAP system name and description as filters to find a particular system or group of systems (after clicking **Filter**).

As you select a SAP system, the SAP system details are displayed on the right.

After you select a SAP system, click **Actions** to:

- Make the SAP system the one in use, by clicking **Switch**.
- Add a SAP system.
- Remove the SAP system.

Under **SAP system details** you can view and edit the SAP system:

- Name
- Description
- IAM Target
- Realm

You can also set the connection parameters of the SAP System and verify the connection. You can set the following connection parameters:

- User ID
- SAP Client
- Password
- Packet size
- System number
- Version
- Language
- Host Name

## Rules

Rules are used to define event management based on event type or for the automation particular policies.

The seven Rule Class concepts are summarized below:

- **Live events:** Rules triggered by Event Queues (for more information about Events, see Events in Integration Interface. These types of events are processed in real time. Their purpose is to control the input/output data flow.
- **Deferred events:** Rules triggered by the Event Queue IN. These types of events are processed by scheduling (see Task Planner). Their purpose is to aggregate events.
- **Authorization Digest:** Rules triggered by changes in the User data set. These types of events are processed in real time. Their purpose is to validate enforcements.
- **Account:** Rules for the creation of a user account.
- **Attestation:** Rules automatically applied in campaigns of attestation.

- **Hierarchy:** Rules for the automatic building of hierarchies based on user attributes.

You can select the class of Rules in the filter section (click **Filter** button).

The filtering approach requires the selection of a **Rule Class** and, according to the class, you can select from **Queues** or **Rule Sequence (Flow)** combo boxes.

The **Actions** menu of the tab **Rules** in the left frame lists the following actions:

**Import**

For importing the XML representation of a Rule or of a Rule Sequence (Rule Flow).

**Export** For exporting a Rule or a Rule Sequence (Rule Flow).

**Add** Adds a Group of Rules (function maintained for legacy reason).

**Remove**

Removes a Rule or a Group of rules (for Groups, function maintained for legacy reason).

**Enable/Disable**

Enable or disable a Rule execution into a sequence.

**Move Up/Down**

Move the Rule up/down in the Rule sequence.

In the right frame you can find two main accordion panes:

**Rules Package**

In this accordion pane are available all functions for manage a Rule selected in the left frame.

**Package Imports**

In this accordion pane are present all functions for managing packages of rules.

**Rules Package**

In this accordion pane are available all functions for managing Rules through the Rules editor.

According to the selection on the left tab **Rules**, a set of rule are listed in this pane.

The **Actions** menu hosts the following actions:

**Verify** For checking the formal structure of the code involved in a rule (needs the selection of one of the rule listed).



**Modify**

For modifying the rule, opening the Rules editor pop-up window.

**Delete** For deleting selected rule.

**Create** For creating a new rule.

**Add**

This function add a rule selected by the list to a  **Group** (legacy versions) or  **Rule Sequence** selected in the **Rules** tab, on the left.

## Rules Editor

The Rules Editor speeds up the writing of code contained in a Rule.

The figure below shows the Rules Editor panel:

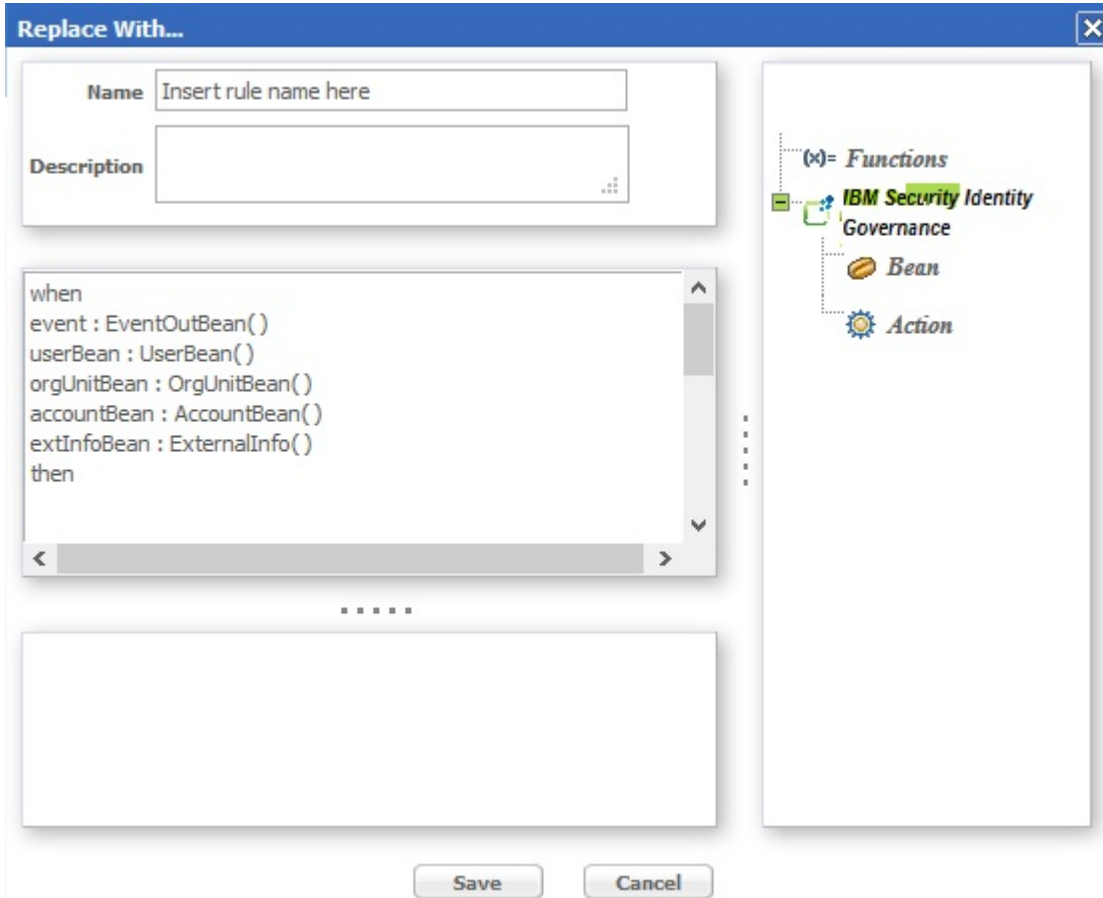


Figure 116. The Rules Editor panel.

The table below shows the symbols of several buttons and icons present in the Rules editor:

Table 229. Symbols of the Rules editor.












Icon	Description
	Import a Java class
	Java class
	New variable
	New function
	Bean
	Action
	Associated rule: rule that is associated to a rules group

Table 229. Symbols of the Rules editor. (continued)

Icon	Description
	Split: used to construct flow processes in situations that require a branch point.
	Constraints
	Rules group
	Flow process

All the Rules must have the following structure:

- **Condition Area** (between “when” and “then”)
- **Action Area** (immediately after “then”).

The word **when** identifies the beginning of the conditions area.

Any number of conditions can be inserted and the actions will be executed only if all the conditions are verified (logic AND between each condition)

The word **then** identifies the beginning of the actions area.

Actions are written in normal Java code; all classes making up the libraries delivered with the product are available for writing actions.

A complete list and descriptions are available in the **Replace with...**

The conditions are written according to Drools syntax.

Every condition verifies, within the Working Memory, whether or not there are one or more objects identified by the Beans. If such objects are actually found, the actions described above will be executed on them.

The **Replace with...** window contains the code obtained from the Editor.

From the frame on the right side of the window, predefined code blocks can be selected and placed directly into the **Replace with...**

The objects are grouped in a hierarchy and managed through a tree structure.

The **Object** frame contains the nodes corresponding to the higher level object categories. The two initial main categories are:

- Functions
- Ideas

Based on the selection, the objects can be **Functions**, **Bean** or **Action** and their methods are visible below the selected object (fourth level of the tree):

Now, select a leaf object (a method) and insert it into the **Replace With...** frame (left) using the **Actions>Add** button.

This operation can be performed to modify or create a Rule.

**Note:** The name of a Bean can be written without its system path ONLY if it has been imported into the Package that contains the Rule.

## Functions

The Functions category contains functions for fundamental Rule-writing constructs; the same frame lists the following four elements:

- if
- ifelse
- ifelseif
- for

Select one of the functions and click **Add** to insert the related parametric code into the **Replace with...** frame, at the end of the already-listed code. The parameters to edit are easily recognized because they are between two '\$' symbols.

For example, in the IF ELSE construct, you have to edit the parameters CONDITION1, ACTION1 and ACTION2.

Proceed in one of two ways to edit the parameters:

- Directly write the code instead of the corresponding symbolic string (e.g., CONDITION1 included between two '\$' characters);
- Use the editor again.

In this last case, click **Field > Bean > AccountBean** and select one of the objects listed, then click **Add**:

Selecting \$ACTION2\$ places the selected code block in the position that was covered by \$ACTION2\$. If none of the parameters in the window are selected, click **Ok** to place the code block at the end of the already-present code. To eliminate a potentially wrong insertion, cancel the corresponding code directly in the **Replace With...** frame.

## Bean and Action Elements

The IBM Security Identity Governance folder contains the following two folders:

- Bean
- Action

These folders contain ALL the Beans and Actions imported into the Rules Package; in particular, the Bean folder contains the Beans imported into the Package that are part of the libraries delivered with the product. Client users of the AG Core can create additional personalized Beans.

This paragraph analyzes how to use a Bean in the Bean folder. By selecting Bean, the content of the Bean folder is presented in the form of a tree, where every Bean is a node and its child nodes represent its methods.

After selecting the Bean, click Add to insert it into the **Replace With...** frame.

Be sure to insert a semicolon (;) at the end of each line and put the code in order.

Be sure to assign the String parameter a string that makes sense.



The Action folders contain ALL Actions imported into the Package of the selected Rule; in particular, the Action folder contains all Actions imported into the Package that are part of the libraries delivered with the product.

The procedure for inserting Actions (even custom Actions) is exactly the same as that for inserting Beans.

## Package Import

From the tabs bar, select **Configure > Rules** then click on the **Package Import** accordion pane on the right.

Configuring a Package consists of declaring certain objects available to all Rules in the Package.

Such a declaration consists of specifying an appropriate Java code in the allotted text box.

To make configuration of the Packages easier, insert blocks of predefined code (on the right side of the frame there is a small vertical toolbar with buttons).

The following actions are available for each Package:

- Import specific classes
- Insert variables
- Insert functions

The Rules programmer can write the Rule's code to directly call the objects that are set up for the Package containing the Rule.

Importing a class into a Package adds a class to a Rule without having to specify the entire path.


For example, after importing the class `UserBean()` into the Package, it is possible to directly write `UserBean()` instead of `com.engiweb.profilemanager.common.bean.UserBean()`.

## Package Editor

An administrator familiar with programming languages can insert any object in the Package by writing the code directly in the text box.

A Package Editor is also available to assist administrators to accomplish this task.


The Editor uses the following buttons, located on the right-hand side of the text box:

-  New Import
-  New Variable
-  New Function

Variables usually support objects that are already instanced with global visibility to all the Rules of the Package; if, for example, there is an object that contains all the parameters required to connect to the DB, the object can be assigned to an "sql" variable (always visible to the Package's Rules) and can be used in the Rule code, as shown in figure above.

Lastly, it is possible to create Functions that always have global visibility to all the rules of a package. For example, if several rules request an operation for the arithmetic average of two numbers, this can be created directly in the Package instead of in each single rule.

### Import a Class


To import a class, click on  **New Import** button in the vertical toolbar on the right-hand side of the Package Imports pane.

The Classes window opens (figure below) with a list of available classes

Choose a class, then click **Ok**.

The Java code corresponding to the selected class is written in the text area on the right-hand side of the Replace With... window.

### Enter a New Variable

To insert a new variable, click on  **New Variable** in the vertical toolbar on the right-hand side of the Package Imports accordion pane.

The text box displays the code corresponding to the declaration of a new variable.

The code is parametric and thus must be edited in the allotted spaces, defined by the characters <>.

Insert the object (specify entire system path) in the space <your class here>.

Insert a variable name in the space <variable name>; this name can then be used in every Rule of the Package.

### Enter a New Function

To insert a new function click on  **New Function** in the vertical toolbar on the right-hand side of the Package Imports accordion pane.

The text box displays the code corresponding to the declaration of a new variable.

The code is parametric and thus must be edited in the allotted spaces, defined by the characters <>.

Edit the parameters as follows:

- Replace <return Type> with the type of objects that result from processing the function (e.g. an integer, a string, a class, etc.).
- Replace <args here> with the list of parameters given to the function at input.
- {} needs to contain the body of the function, i.e., all the code that implements the function.

### How to Schedule a Rules Flow

It is possible to link a Rules Flow to a scheduled Job. The IBM Security Identity Governance Task Planner is the module dedicated to scheduling several types of

Jobs that optimize different tasks in the IBM Security Identity Governance Platform. The Flows that can be scheduled belong to the Rule Classes Advanced or/and Deferred Events.



After creating a Flow Process, open the upper toolbar and click on the button related to the IBM Security Identity Governance Task Planner.

In the Task Planner module, from the tabs bar, select **Manage > Job** Classes to access the Job Classes GUI.

From the list of Job Classes, choose the AdvancedRuleFlow or DeferredEventsRuleFlow (depending on what is needed) then select the Jobs tab and choose a relevant Job from the list produced.

Click on the **>Job** button in the Jobs frame, then populate the fields with the values of the chosen Job Class.

## Monitor

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

- User Violations
- SAP Role Violations
- SAP Authorization Violations
- Role Warnings
- Reports

### User Violations

This section enables you to view:

- Information on risky or conflicting activities related to a selected user
- Domains and activities that are associated with a user
- SAP Roles and Authorizations associated with a user

The User Violations tab displays conflicting users listed by the system for SoD and FSoD violations.

A user is qualified as conflicting as a consequence of having two or more SAP authorizations that are in conflict.

You can use the following filters to find a conflicting user (after clicking **Filter**):

*Table 230. Filters to find conflicting users*

Filter	Description
Organization Unit	OU to which the user belongs. Use the <b>OU Search</b> button on the right to get a list of OUs.
Hierarchy	When this check box is selected, the operation is executed starting from the selected OU root and down through the entire subtree originating from the root.
Search Identity	The user's name, last name, or ID.

Table 230. Filters to find conflicting users (continued)

Filter	Description
DN	The distinguished name of the user.
Search Type	Can be: <b>All</b> The search is made on all users <b>Conflicting</b> The search is made on conflicting users only.
Conflict level	Can be: <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> </ul> This filter becomes unavailable if you set <b>Search Type</b> to <b>All</b> .

After you select a user with violations, you can use the following tabs on the right-hand panel to view related information:

#### Risk Info

Displays risk information details for each domain.

#### Assignment details

The **Domain** accordion pane lists the domains associated with the user.

The **Activity search** accordion pane lists the activities associated with the user. Click **Actions > View** to find the position of the activity in the OU tree view.

In either accordion pane, you can use the following filters to search information (after clicking **Filter**):

Table 231. Filters helpful for searching a domain or an activity for conflicting users.

Filter	Description
Name	Name of the domain/activity
Description	Description of the domain/activity

#### SAP Roles

Shows all the SAP roles and authorizations associated in hierarchy with:

- SAP Roles (SoD process)
- User directly (Full SoD process)

#### SAP Authorizations

Lists all the SAP Authorizations associated with the user in a flat mode.

## SAP Role Violations

This section enables you to view and analyze conflicting SAP roles.

A conflicting SAP role allows users to run conflicting activities.

The **Roles** tab displays a list of SAP roles. You can use the following filters to find a specific SAP role (after clicking **Filter**):

Table 232. Filters you can use to find SAP roles.

Filter	Description
Role Type	One of the following types of entitlement: <ul style="list-style-type: none"> <li>• SAP Role</li> <li>• Collective Role</li> </ul>
Name	The role name
Search type	Can be: <p><b>All</b>      The search is made on all roles</p> <p><b>Conflicting</b> The search is made on conflicting roles only</p>
Conflict level	Can be: <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> </ul> <p>This filter becomes unavailable if you set <b>Search type</b> to <b>All</b>.</p>

You can use the **Actions** button to:

- Refresh a selected role
- Download a new role
- Download a selected role
- Remove a selected role

After you select a SAP role, you can use the following tabs on the right-hand panel to view related information:

**SAP Role details**

Shows the following details of the selected role:

- Name
- Description
- Role type
- Created by
- Creation date
- Modified by
- Last modification date and time

**Warning**

Lists any warnings released for the selected role. You can use a search filter to find specific warnings, based on the warning code or severity.

**Conflict Info**

Provides a tree view of conflict information details for all domains.

**Activity**

Displays a list of the activities associated with selected role. Click **Actions** > **View** to find the exact position of the activity in the OU tree structure.

### Transaction

Lists the transactions related to the selected SAP role. You can use a search filter to find specific transactions, based on the transaction group, name, and description.

### Authorization Object

Lists the authorization objects related to the selected SAP role. You can use a search filter to find specific authorization objects, based on any of their attributes.

### SAP Authorization

Lists the SAP authorizations related to the selected SAP role. You can use a search filter to find a specific SAP authorization objects, based on its name and on whether there is or not a segregation of duties.

## SAP authorization violations

This section enables you to view and analyze conflicting SAP authorizations.

A conflicting SAP authorization allows for the execution of conflicting activities.

The **SAP Authorizations** tab displays a list of SAP authorization names, their conflict level, and their application (their set of permissions). You can use the following filters to find specific authorizations (after clicking **Filter**):

Table 233. Filters you can use to find SAP authorizations.

Filter	Description
Name	The SAP authorization name
Search type	Can be: <b>All</b> The search is made on all SAP authorizations <b>Conflicting</b> The search is made on conflicting SAP authorizations only
Conflict level	Can be: • Low • Medium • High  This filter becomes unavailable if you set <b>Search type</b> to <b>All</b> .

After you select a SAP authorization, you can use the following tabs on the right-hand panel to view related information:

### SAP Authorization details

Shows the following details of the selected role:

- Name
- Description
- Created by
- Creation date
- Modified by
- Last modification date and time

### Conflict Info

Provides a tree view of conflict information details for all domains.

### Activity

Displays a list of the activities associated with the selected authorization. Click **Actions > View** to find the exact position of the activity in the OU tree structure.

## Role warnings

This section enables you to view and analyze role-related warnings.

The **Warnings View** tab displays a list of roles on which warnings were raised, the role description, the warning code, the severity of the warning, and a description of it. You can use the following filters to find specific warnings (after clicking **Filter**):

Table 234. Filters you can use to find role warnings.

Filter	Description
Role Name	The name of the role on which the warning was raised
Severity	The level of severity of the warning. It can be: <ul style="list-style-type: none"><li>• Low</li><li>• Medium</li><li>• High</li></ul>
Code	The code that identifies the warning.

After you select a role, you can click the **Actions** menu and select:

#### Statistics

To view a graphical display of the number of occurrences of the warning code.

#### Details

To view the details of the role.

## Report

You can request and download reports.

The main functions in this section allow you to:

- Request (configuration of the assigned reports)
- Download

You can start the following reports for a SAP System:

#### SAP and Collective Role Risks

List of SoD Risks for SAP and Collective roles

#### SAP Authorizations Risks

List of SoD Risks for SAP Authorizations

#### User Risks

List of FSoD-SoD Risks for Users

#### User with FSoD Risks

List of FSoD Risks for Users

**SAP Authorization Definition**

List of SAP Authorizations

**SAP Authorization and Business Activity Catalog**

List of SAP Authorizations linked to Business Activities

**SAP Role Catalog**

List of SAP Roles

**SAP Role and AuthObj Catalog**

List of AuthObj for each SAP Role

**SAP Role and Business Activity Catalog**

List of SAP Roles linked to Business Activities

**SAP Role and Transaction Catalog**

List of Transactions for each SAP Role

You can download the reports in PDF or XLSX format.

---

## Tools

Several functions speed up and facilitate the tasks of the following modules:

- Data Refresh
- Bulk Data Load
- Configuration Set Comparison

### Data refresh

You can view a list of the currently scheduled Operations and the scheduled operations history.

The main functions in the section allow you to:

- Start one of the scheduled jobs listed in the **Scheduled Operations** tab
- Monitor or remove the status listing of a scheduled job in the **Scheduled History** tab

In the **Scheduled Operations** tab, you find a list of the following scheduled jobs:

- Load Data from SAP
- SAP Role Analysis
- User Analysis
- Collective Role Analysis
- Warning Analysis
- SoD Analysis

After any update related to SAP/Collective Roles or Users, the first operation that you have always to run is the SoD Analysis.

After the SoD Analysis, you can choose the operation that you need.

A best practice is to run this sequence:

1. SoD Analysis
2. SAP Role Analysis (if you need)
3. Collective Role Analysis (if you need)
4. User Analysis (if you need)



Click **Actions > Start** to start the job immediately if it is not in the **Waiting** or **Executing** state.

In the **Scheduled History** tab, you find a list of the scheduled job instances. When you select a job that analyses roles or users, the list of related roles is displayed below. Click **Actions > Remove** to remove a selected job status from the list.

## Bulk Data Load

You can run several types of bulk data-loading in the AG Core database.



The **Action** tab (left) shows the supported operations.

After you select an operation in **File Batch**, click one of the following options:

- **Download** to get a template (XLS file), related to the currently selected operation.
- **Browse** to search in the file system for an XLS file for the selected loading operation.

When the operation is completed, an information record is appended in the lower-right pane to the list of the previously completed operations.

In the same pane, you can click:

- **Input File**  to get the file used in the operation.
- **Log File**  to get the operation report.

The following procedures are available:

- Add Risk Entitlement to Activity
- Insert Risk Entitlement
- Remove Risk Entitlement
- Remove Risk Entitlement from Activity

A generic record track distinguishes between **Mandatory** and **Optional** fields.

If a Mandatory field is empty or populated with unexpected values, the row is skipped unless specified otherwise in the documentation.

According to the data load behavior, populating an Optional field with unexpected/wrong values could cause a row to be skipped.

Here the procedure for running a bulk data load.

### Add Risk Entitlement to Activity Record Track

This batch procedure can be used to aggregate Risk Entitlement to an Activity. It verifies that **Mandatory** fields are populated.

The XLS source file is organized into **2 sheets**.

*Table 235. Add Risk Entitlement to Activity Track (sheet 1).*

Information	Description	Validation
SAP_SYSTEM	SAP application name	Mandatory
RISK_ENTITLEMENT	Risk Entitlement name	Mandatory

Table 235. Add Risk Entitlement to Activity Track (sheet 1). (continued)

Information	Description	Validation
TRANSACTION	Transaction name.	Mandatory
ACTIVITY_REF	Reference to Activity on sheet 2 of the file XLS.	Mandatory

Table 236. Add Risk Entitlement to Activity Track (sheet 2).

Information	Description	Validation
ACTIVITY_REF	Reference to Activity.	Mandatory
CODE	Activity code.	Mandatory
ACTIVITY	Activity name.	Mandatory
ENVIRONMENT	Environment name.	Optional

The SAP\_SYSTEM field contains the name of the SAP application, already registered in the system. If there is no such SAP application, the row is skipped.

The RISK\_ENTITLEMENT field contains the name of a Risk Entitlement, already registered in the system. If not, the row is skipped.

The ACTIVITY\_REF column on sheet 1 refers to the same column on sheet 2.

Values possibly contained in this column on sheet 1 must also be present in the same column on sheet 2. Conversely, the ACTIVITY\_REF column on sheet 2 can contain values that are not present or referenced in sheet 1.

The ENVIRONMENT field is optional. If this field is populated, existence of an environment with the specified name is verified. Otherwise the row is skipped. If left blank, the default Environment is used.

### Insert Risk Entitlement Record Track

This batch procedure can be used to insert Risk Entitlement (with the joined Transaction) in the system.

Table 237. Insert Risk Entitlement Track.

Information	Description	Validation
SAP_SYSTEM	SAP application name	Mandatory
RISK_ENTITLEMENT	Risk Entitlement name	Mandatory
RISK_ENTITLEMENT_DESCRIPTION	Risk Entitlement description about Risk Entitlement.	Optional
TRANSACTION	Transaction name (into SAP Authorization Model, Transaction is a specific type of Authorization Object).	Mandatory
TRANSACTION_DESCRIPTION	Brief description about Transaction.	Optional

Table 237. Insert Risk Entitlement Track. (continued)

Information	Description	Validation
AUTH_OBJ	Authorization Object (AO) name linked to the Transaction. AO can be characterized: <ul style="list-style-type: none"> <li>• by a condition (AO_CONDITION)</li> <li>• by several fields (AO_FIELD)</li> <li>• for every field a condition (AO_FIELD_CONDITION) might be specified.</li> </ul>	Optional
AO_CONDITION	Two values are allowed (with other values, the row is skipped): AND/OR.	Mandatory ONLY if AUTH_OBJ field is not empty
AO_FIELD	AO field name	Optional
AO_FIELD_CONDITION	Four values are allowed (with other values, the row is skipped): <ul style="list-style-type: none"> <li>• ANY_FROM</li> <li>• NONE_FROM</li> <li>• ANY_BUT</li> <li>• ALL_INT0</li> </ul>	Mandatory ONLY if AO_FIELD field is not empty
AO_FIELD_VALUE	The value related to AO_FIELD	Mandatory ONLY if AO_FIELD field is not empty

It verifies that **Mandatory** fields are populated.

It provides the insertion of the new Risk Entitlement with its Transaction and the Authorization Objects possibly involved in the Transaction.

The SAP\_SYSTEM field contains the name of the SAP application, already registered in the system. If there is no such SAP application, the row is skipped.

The RISK\_ENTITLEMENT field contains the name of a Risk Entitlement, already registered in the system. If not, the row is skipped.

The TRANSACTION field contains the name of a Transaction, already registered in the system. If not, the row is skipped.

If the Transaction indicated is not registered in the system, it is added.

If the AUTH\_OBJ is indicated and is not registered in the system, it is added.

If AUTH\_OBJ is present, AO\_CONDITION become a mandatory field.

### Remove Risk Entitlement Record Track

This batch procedure can be used to remove Risk Entitlements. In absence of any mandatory information, the row is skipped.

Table 238. Remove Risk Entitlement Track.

Information	Description	Validation
SAP_SYSTEM	SAP application name	Mandatory
NAME	Risk Entitlement name	Mandatory
DESCRIPTION	A brief description about Risk Entitlement.	Optional

## Remove Risk Entitlement from Activity Record Track

This batch procedure can be used to remove Risk Entitlement from an Activity.

The structure of the record track is as outlined in Add Risk Entitlement to Activity.

## Configuration Set Comparison

In this section, you can compare two different configurations, and check whether or not the changes made in a specific configuration alter the model compared to the operating configuration.



The **Compare Configuration** tab displays all the configurations listed by the system. To compare another configuration with the operating configuration (which is already selected), select that configuration in the **Compare Configuration** pane.

You can run the following operations related to mitigation controls:

- “Configurations”
- “Comparison Dashboard”
- “Comparison Details” on page 485

### Configurations

Select an additional configuration in the **Compare Configuration** pane and click the **Configurations** tab on the right to view information about the User and the Entitlement analyses of the configurations:

- The  icon shows that the analysis completed successfully.
- The  icon shows that the analysis failed.

The bordered green configuration is the operating configuration information.

### Comparison Dashboard

Select an additional configuration in the **Compare Configuration** pane and click the **Comparison Dashboard** tab on the right: Four dashboards for the two configurations are displayed:

- **Conflicting Collective Roles**
- **Conflicting SAP Roles**
- **Conflicting SAP Authorizations**
- **Conflicting Users**

These dashboards show the structure of the compared configurations.

## Comparison Details

Select an additional configuration in the **Compare Configuration** pane and click the **Comparison Details** tab on the right: With this operation you can compare detailed reports of paired configurations.

In this situation, additional information is provided about changes in the number and types of conflicts on a single ARCS model entity present in both configurations. The **Comparison Details** tab enables you to access the following two tabs:

- **Users**
- **Entitlements**

In the **Users** tab, you can define filters to list sets of conflicting users registered on the system. You can use the following attributes:

*Table 239. Filters available to search for conflicting users in a configuration set comparison.*

Filter	Description	
<b>Organization Unit</b>	OU to which the user belongs	
<b>Hierarchy</b>	Select this check box to set the operation to start executing from the root of the selected OU and down through the hierarchy originating from that root	
<b>Search Identity</b>	Enter the user's name and surname, or the User ID	
<b>DN</b>	The user's Distinguished Name.	
<b>Conflicting state</b>	<b>All</b>	All possible conflicting states
	<b>Unaltered</b>	The user remains with the same number of risks in both configurations
	<b>Altered</b>	Every user with a modified number of risks ( <b>Enhanced, Worsened</b> )
	<b>Enhanced</b>	In the operating configuration the user has a lower number of risks than the compared configuration
	<b>Worsened</b>	In the operating configuration the user has a higher number of risks than the compared configuration

The risk level distribution provides a view of the qualitative mix of risk levels among the total number of risks. For example: a user has 11 total risks. Of these, 4 have a low risk level and 7 have a high risk level. Therefore, the user is characterized by the low/high qualitative mix of risk levels.

In the **Entitlement** tab, you can define filters to list sets of conflicting entitlements registered on the system. You can use the following attributes:

Table 240. Filters available to search for conflicting entitlements in a configuration set comparison.

Filter	Description	
<b>Type</b>	Choose one of the following types of entitlement: <ul style="list-style-type: none"> <li>• SAP Authorization</li> <li>• SAP Role</li> <li>• Collective Role</li> </ul>	
<b>Application</b>	The name of the application on which the conflicting entitlements are filtered	
<b>Name</b>	Name of the entitlement	
<b>Conflicting state</b>	<b>All</b>	All possible conflicting states
	<b>Unaltered</b>	The entitlement remains in a conflicting state with the same mix of conflict level values (High, Medium, Low) in both configurations
	<b>Altered</b>	Every user with a modified number of risks ( <b>Enhanced, Worsened</b> )
	<b>Enhanced</b>	In the operating configuration the entitlement has a lower number of risks than the compared configuration
	<b>Worsened</b>	In the operating configuration the entitlement has a higher number of risks than the compared configuration

The concept of risk level distribution, described in the **Users** tab, applies also here.

---

## Chapter 19. Introduction to Report Designer

Report Designer (RD) module provides a modeler capable of outlining every type of report.

Using this module, the administrator can visually describe the report creation process from beginning to end.

Using the Access Governance Core authorization system, authorized users can access and run a set of reports from within each IBM Security Identity Governance and Intelligence module.

In case of unauthorized users, the **Report** tab, if present, is not active.

The Report Designer module is used to:

- Create queries and scopes.
- Assign one or more scopes to a query.
- Define a new report and associating a query to it.
- Aggregate the same query to one or more reports.
- Define the report-entitlement assignment (the report is available to the user that holds the entitlement).
- Localize the report.
- Assign a report status.

---

### Report modeling for the Identity Governance and Intelligence platform

Report Designer (RD) is the Identity Governance and Intelligence module dedicated to the design and definition of reports.

This module is used to:

- Create queries and scopes.
- Assign one or more scopes to a query.
- Define a new report, adding a query to it.
- Add the same query to one or more reports.
- Define the report-entitlement assignment (the report will be available if you have the entitlement).
- Localize the report.
- Assign a report status.

This section outlines the main concepts about creating a report with the RD module.

**Note:** An administrator experienced in the SQL language must manage this section.

## Create a query

In the RD, the administrator can create free handwritten SQL queries in a dedicated text area. Click the **Query management** tab, and specify the following information about the query in the **Query details** section:

**Name** Name of the query. The following text is an example: Remediations to risks Batch QUERY

### Description

Description of the query. The following text is an example: Batch query to assign remediation to risks

### SQL query

Query text. The following text is an example:

```
select distinct rem.name as BATCH_REMEDIATION,
               rem.code as BATCH_CODE,
               rem.description as BATCH_DESCRIPTION,
               rem.desc1 as BATCH_EXT_DESCR,
               r.name as BATCH_RISK_NAME,
               e.name as BATCH_ENVIRONMENT
from #PMSHEMA#.environment e,
     #PMSHEMA#.risk
     #PMSHEMA#.risk_remediation rr,
     #PMSHEMA#.remediation rem
where e.id = r.environment
and r.id = rr.risk
and rr.remediation = rem.id
and lower(e.name) = lower ('#env_name#')
```

Additional support is also provided for writing more efficient and flexible queries, based on three main concepts:

- “Schema” on page 489
- Scopes
- Filters

The following figure shows the text area used to specify a query:

The next table summarizes the set of product queries available in the RD module:

Table 241. Product queries

Query name	Query description
Access Certification Campaign Status	Access certification completion status
Access Certification Status query	User certification completion details by OU
Access Rights not assigned to any user query	Entitlement published but not assigned
Access Rights not assigned to any OU query	Entitlement not assigned to any OUs
Access Rights Visibility by OUs query	Role visible to users because of belonging OU
Account Status query	User ID and account status on common target pool
Activities hierarchy Batch query	Batch insert activities hierarchy
Applications Batch query	Batch query to find application
Application Entitlements dictionary query	Entitlement by application
Delegation assignments details query	User assigned roles by delegation



Table 241. Product queries (continued)

Query name	Query description
Entitlements Batch query	Batch query to find entitlements
Entitlements to Users Batch query	Not applicable
Events-IN from HR system query	User Event-IN
Events-OUT to Targets query	User Event-OUT
IBM Security Identity Governance Audit query	Not applicable
IBM Security Identity Governance Report Structure query	Report columns, sequence and localization information
IBM Security Identity Governance Report Visibility query	Reports assignment on entitlements
Mitigations assigned to Risk query	Batch remediation to risks
Organizational Units Batch query	Not applicable
OU visibility: campaign status query	Roles visibility certification completion status by OU
Profile to domain Batch query	Batch query to add profile to domain
Profile to Activity Batch sheet 1 query	Batch add profile to activity sheet 1- Role realm
Profile to Activity Batch sheet 2 query	Batch add profile to activity sheet 2- Role realm
Remediation to Risks Batch query	Batch query to assign remediation to risks
Resources Batch query	Not applicable
Role hierarchical structure query	Role tree structure
Risk Structure query	Risk definitions
Risk Structure Batch query	Batch risk definition
Role Risk Overview query	Operates on the role realm
Role Structure Changes query	Query to detect role changes in applications
Technical error event log from last targets import query	Query to detect target application import events
Technical mapping query	Entitlement mapping on business activity
User Assignments query	User with assigned roles
User Assignments Changes query	Query to detect the user access entitlement assignments changes
Users Batch query	Not applicable
Users by Application query	User list with scope on OU and application
User Risks and Assigned Mitigations query	Not applicable
User Risk Count query	Not applicable

## Schema

A schema is a set of tables related to a specific subsystem of a generic database. A set of schemas characterizes Identity Governance and Intelligence and the entire list of available schemas is determined at installation time. Every schema is associated to a database administrator name that is specified during the installation process.

In the **System Entities** tab, the RD administrator can register all the schemas used for building queries and reports.

Every schema is inventoried using a name-value pair. Generally, the name is built using a generic string of characters that clearly identifies the database subset. The value must match the database administrator name. When defining a query in the report designer module, specify at least one schema.

The next table describes two different ways of specifying a schema:

*Table 242. Schema specification*

Procedure 1	Procedure 2
from #PMSHEMA#.application a, #PMSHEMA#.entitlement e1, #PMSHEMA#.entitlement e2, #PMSHEMA#.task_profile tp, #PMSHEMA#.task tk, #SCHEMA#.environment env	from REALM_DEMO.application a, REALM_DEMO.entitlement e1, REALM_DEMO.entitlement e2, REALM_DEMO.task_profile tp, REALM_DEMO.task tk, Report.environment env

In **Procedure 1**, the system keys **#PMSHEMA#** and **#SCHEMA#** enable the administrator to have a multi-schema query without having to actually specify the name of the schema in the query.

This is very useful for managing the database schema of different organizations.

Suppose the following:

```
PMSHEMA = Org_01
SCHEMA = Org_01_ENV
```

where Org\_01 and Org\_01\_ENV are two schemas for Organization01.

But what if Organization02 requires the same query?

This requires changing the settings in the System Entities tab, as follows:

```
PMSHEMA = Org_02
SCHEMA = Org_02_ENV
```

Therefore, the Report Designer administrator only writes the query once and can use it for different organizations.

The Identity Governance and Intelligence data model uses the realm concept to represent a generic organization.

Identity Governance and Intelligence allows for multi-realm management whereby the administrator can create individual models to manage several organizations while keeping the different realm-related contexts separate. A realm is essentially a model that describes an organization in terms of a set of objects and the relationships between them. A realm is implemented using a database.

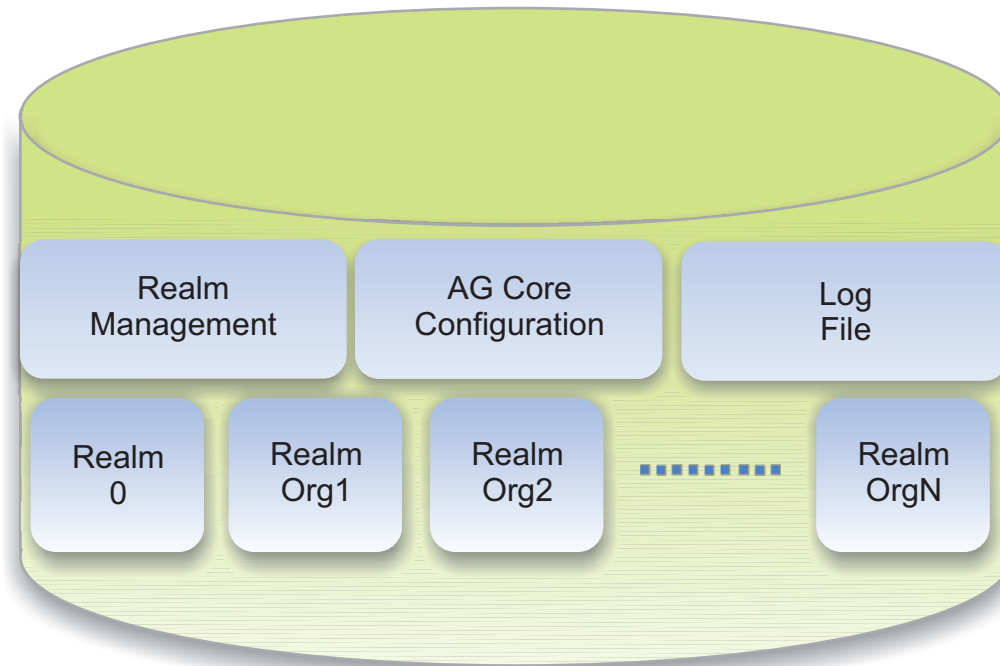


Figure 117. Realms.

In the Identity Governance and Intelligence data model, the schema value, defined in the **System Entities** tab, usually matches a realm name.

**Procedure 1** could be a management model called "Multi Schema/Multi Realm Parametric Queries".

The general structure of this procedure is:

```
#Name of Schema#.Name of Table
```

In **Procedure 2** the **REALM\_DEMO** and **Report** keys are the names of two different schemas that match two different realms. The **Procedure 2** query only works for these two schemas.

The general structure of this procedure is:

```
Name of Schema.Name of Table
from swim.request r,
swim.applications app,
swim.roles ro,
report.tmp_application tmpa
```

### Scope

When writing a query, the administrator can define one or more temporary tables (tmp.) to which the administrator can add one or more scopes.

The scope is a selective breakdown of database data. The scope functions as a filter and a collector between the temporary tables and the database entities (OUs, Applications, Entitlements, Users).

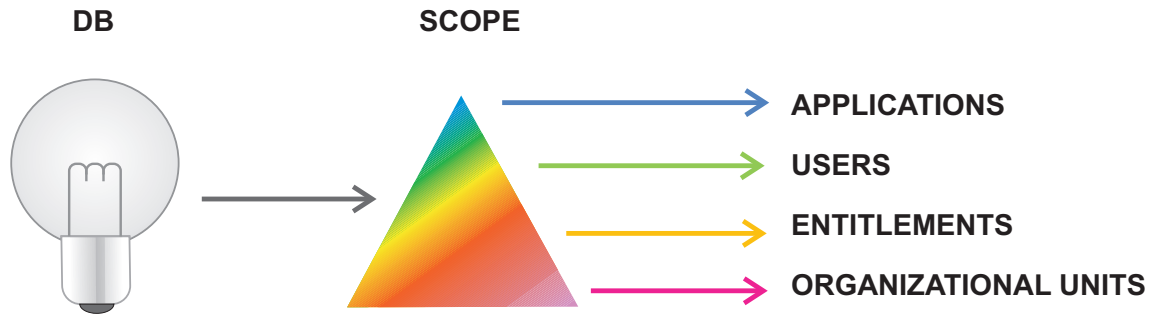


Figure 118. Scopes.

For example, a user needs a query to select data for all transactions <\$100,000 made in the month of March in a national real estate franchise.

When dealing with such a large volume of data, how is it possible to isolate the owners of the corresponding agencies? This requires a user scope that can extract all the data-of-interest related to a given user.

What if a user needs to classify local transaction density? In this case, how can the user associate transactions to the territories where they took place? Invoking the Organization Unit scope, it will extract all OU-related data.

Additionally, different users (who have different roles and access rights for data within the Identity Governance and Intelligence database) can call the same report. If two different users, who have the same role but different visibility rights to an organization data set, execute the same report (but with different specialized visibility tags), they will both get different results.

The administrator in charge of designing reports can use the scope concept in situations that require a parametric configuration, relating to the visibility of a particular entity of the Identity Governance and Intelligence data model, based on the rights of the users executing the report.

The Report Designer module offers the following product scopes:

Table 243. Product scopes

Scope name	Scope description	Entity name
AG-Core Entitlement	Entitlement scope	Entitlement
AG-Core Org. Unit-Hierarchy	Organization unit scope-including hierarchy	Org_unit
AG-Core Application	Application scope	Application
AG-Core User	User scope	User
AG-Core Org. Unit	OU certification status	Org_unit
AG-Core Business Activity	Business activity scope	Task
AG-Core Account	Account configuration scope	PwdCfg
AG-Core Working Environment	Procedure that works only on production environment.	System
AG-Core Role Structure Procedure	Allows the visibility of roles hierarchical structure	System
AC Org. Unit Scope	Organization unit scope	System

Table 243. Product scopes (continued)

Scope name	Scope description	Entity name
AC User	User roles certification status	System
AC OUUser Procedure	Users (of specific OUS) certification status	System
ARC Role Procedure	Procedure to calculate risks on roles	System
ARC User Procedure	Procedure to calculate risks per users	System

In the highlighted portion of the query below, **#PMSHEMA#** refers to the main Identity Governance and Intelligence database tables and **#SCHEMA#** refers to the Report Designer database. In the example below, an application entity of the Identity Governance and Intelligence model serves to manage the concept of application visibility.

The Report Designer administrator needs to link a temporary table to the application scope:

```

select distinct e.name as ROLE_NAME,
e.description as ROLE_DESC,
a.name as APPLICATION_NAME,
a.description as APPLICATION_DESC
from #PMSHEMA#.entitlement e,
#PMSHEMA#.application a,
#SCHEMA#.tmp_application tmp
where a.id = tmp.id
and eap.entitlement = e.id
and eap.application = a.id
.....

```

After writing the query and defining the relationship between the database and the temporary tables, the next logic step is to associate the scope to the query in the Scope management tab.

The administrator might also write a query and define the temporary tables without associating a scope. In this case, the temporary tables do not contain any data and the scope is not visible in the report wizard.

The administrator can configure a joined scope (which is, consequently, visible in the Report Wizard) in the Report tab. It must be taken into account that the scopes, present in the module, are product scopes, and have their entity visibility configured by default, but is possible to configure their Entity Visibility according to your needs.

## Filters and custom filters

As the following sample code shows, the where condition of a generic query can specify one or more filters in order to produce well-tailored data:

```
select...  
...where  
    t.state = '#event_state#'  
    and t.operation = '#event_operation#'  
    and t.target = '#target_name#'  
    and t.process_id = ...
```

In the wizard, the **Filters** tab shows the set of filters specified in the where condition. As the figure below shows, the user might associate a label to an **X value** to create a custom filter:

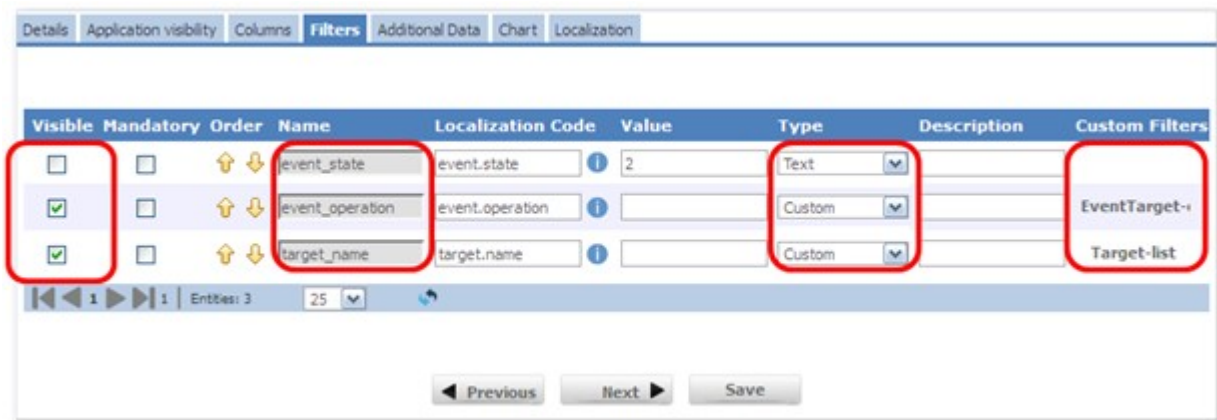


Figure 119. Filters tab in Filter configuration.

For example, in the third row of the figure above, the aggregated label **Target-list** customizes the target\_name data model element. In the final report, the data related to target\_name will display under the Target\_list heading and will be more meaningful for the user requesting the report.

This feature is particularly useful when the original name of the data model element is not very easy to understand.

For example, if the data model element is a numeric value that indicates a specific system (for example, "1" = "Create User", "2" = "Modify User", "3" = "Remove User"), it is easier to associate a meaningful label that, in the report, represents the literal status value:


"1": User is present  
"2": User has been amended  
"3": User is not present

In the wizard, you can configure the filters using the Filters tab.

---

## Report classification: product reports and new reports

The RD module provides a large set of product reports.

Product reports are marked with the  product icon.

The RD Administrator can assign these reports as they are, or modify their settings as needed. The list of product reports is continuously updated as the RD module evolves.

### Note:

Modification of any product report is strictly forbidden.

Be careful with the batch-type reports. Their behavior is closely linked to the AG Core database. Any change might affect the report execution.

The RD Administrator can also create customized reports.

Report configuration is extremely flexible; a dedicated set of tabs (such as Details or Localization) offers several options to determine which set of data the report will display.

### The Report wizard: how to design a report

Designing a report is very easy. A specific wizard organizes all the required steps. The following figure shows the conceptual scheme of the wizard:

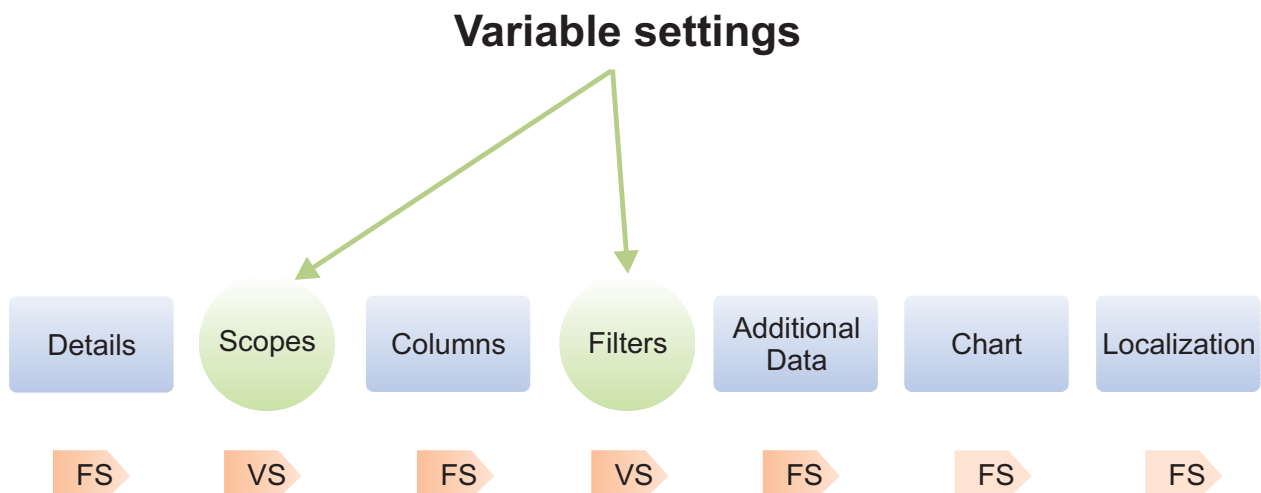


Figure 120. Wizard Steps.

The wizard is composed by five fixed settings and two variable settings.

The **Fixed Settings (FS)** tabs are available and visible in all report configurations, while the **Variable Settings (VS)** tabs are associated only to specific reports:

- Details
- Scopes
- Columns

- Filters
- Additional Data
- Chart
- Localization Tab

Using the wizard specific tabs, the RD Administrator can configure the scopes and filters present in a query.

The RD Administrator can also write a simple query without defining any additional settings; in that case the report configuration will not display such settings.

Below are shown all steps of a generic report wizard, along with all characteristics of the main configuration frame.

### **Details tab**

The **Details** tab is present in all report configuration wizards and consists of:

- A box with the associated query information.
- A text area for selecting a report name, writing a brief report description.
- An **Add** button for adding a new report category.
- A text area for selecting an inventoried report category.
- A text area for configuring the report status (New, Assigned, Locked).

The following figure describes the layout of the **Details** tab:



**Details** Organization Unit visibility Columns Filters Additional Data Chart Localization

**SQL Query**

**Name** Access Certification Campaigns Status QUERY

**Description** Access Certification Completion Status

**Name** Access Certification Campaigns Status

**Description** This report details on the completion level of running Access Certification campaigns.

**Report Category** Recertification

**Status** Assigned

◀ Previous Next ▶

Figure 121. The Details tab of the Report Configuration wizard.

### Scope configuration: Visibility tabs

After the **Details** tab, the wizard displays a subset of tabs based on the number of scopes linked to the report aggregated query.

The following figure shows some possible scope subset tabs:

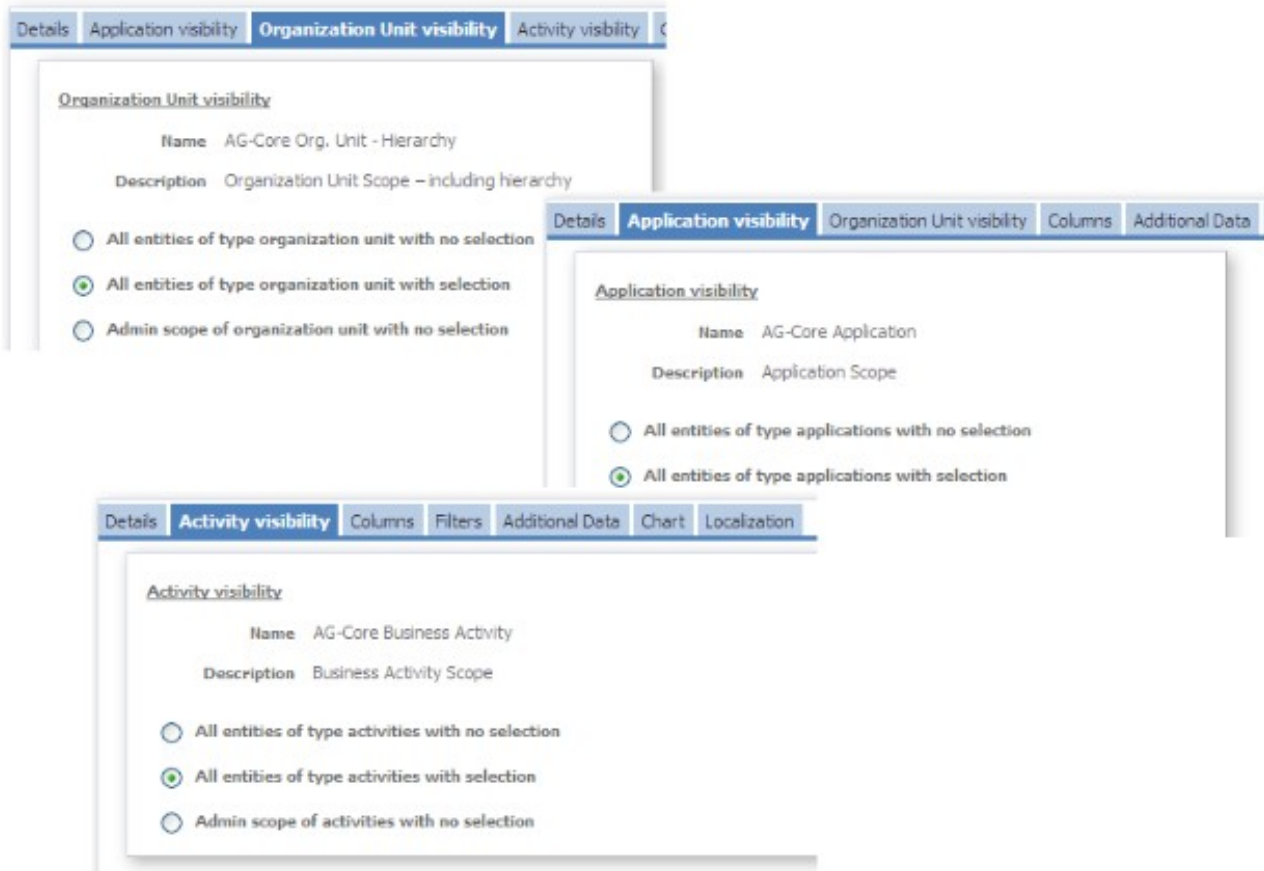


Figure 122. Scope subsets: some combinations.

The model has a **Scope** tab for any available, distinct *Scope Entity*. The table below shows the complete list of entities:

Table 244. Available entities.

Scope	Description
Activity	This entity is related to the business activity concept of the IBM Security Identity Governance data model.
Application	This entity is related to the application concept of the IBM Security Identity Governance data model.
Entitlement	This entity is related to the entitlement concept of the IBM Security Identity Governance data model.
Organization unit	This entity is related to the organization unit concept of the IBM Security Identity Governance data model.
Password configuration	This entity is related to the environment configuration defined in the Access Governance core module.
User	This entity is related to the user concept of the IBM Security Identity Governance data model.

To set the entity visibility for each *Scope Entity*, the RD administrator can click the related radio-button from a fixed list, as the next figure shows:

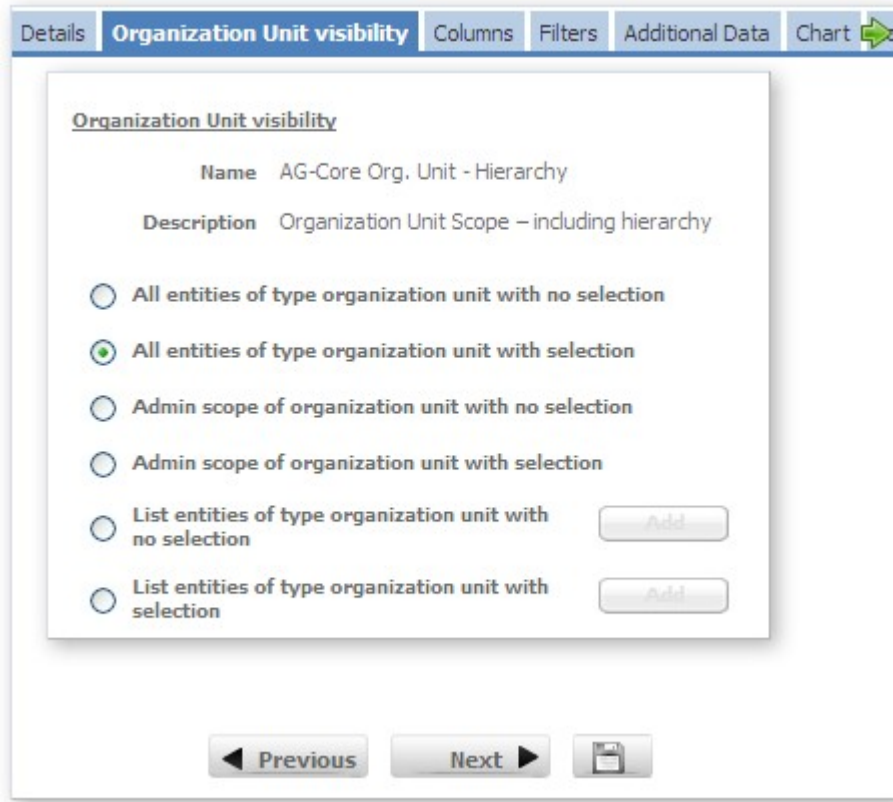


Figure 123. Entity visibility configuration.

The table below shows the visibility options for all available *Scope Entities*:

Table 245. Visibility options for each entity.

Visibility	Description
All entities of type entity with no selection	The authorized user can view all entities but cannot select any of them.
All entities of type entity with selection	The authorized user can select the desired entities.
Admin scope of entity with no selection	Authorized users cannot select from entities within their visibility (Applications, Entitlements, Organization Unit, and so on).
Admin scope of entity with selection	Authorized users can select from entities within their visibility (Applications, Entitlements, Organization Unit, and so on).
List entities of type entities with no selection	The authorized user cannot select any entity from the limited list (defined by the administrator).
List entities of type entities with selection	The authorized user can select any entity from the limited list (defined by the administrator).


## Columns tab

From this tab, the RD administrator can choose which columns to display in the report.

The following table shows eight parameters that characterize each item:


Table 246. Report columns configuration.


Column	Description
Visible	If this check box is selected, the report will show the column.
Order	With the up arrow/down arrow is possible to choose the column position.
Name	Column name
Localization Code	The localization code is defined in this field.
Type	The data type is set in this field.
Column Width	The column width is defined in this field.
Order By	Column sorting order

The RD Administrator can click the  **Localization Help** button, near the Localization Code text area, to verify that a localization code exists and is correct. From the Localization Help window, the RD Administrator can only search for the localization code and its aggregated localized messages but cannot perform any operation.

The RD Module displays these codes according to the chosen default language.

The Localization Help window opens and, if the localization code is registered, the **Localization Code** and **Code Type** fields are automatically populated with the specified value. If the localization code is not registered, the search operation does not show any results. In this case, see Edit Labels.



To order the columns in ascending or descending order, click  **Order By**.

The **Column to order** pane (right) lists columns available for insertion in the frame, **Column to use for order condition** (left). Select the column to order and click the **Add** button . The Order condition window opens. Click the Ascending or Descending radio buttons to choose the sorting order.

The Column to use for order condition frame on the left is now automatically populated with the selected column.

Click **Ok**. The columns are now displayed with the  **Order by** icon.

The **Order By** heading indicates the sorting order of the columns in a given report.

If the  icon (**Descending order**) is present, the number in parenthesis next to the icon indicates the column element that will be listed first. If the  icon

(**Ascending order**) is present, the number in parenthesis next to the icon indicates the column element that will be listed last.

**Note:** The module will save any changes made in this window, allowing the administrator to verify the label localization.

## Filters tab

After writing the query, the RD administrator can set and customize the **Filters**. To display the filters, select the related check box in the **Visible** column, as the following figure shows:

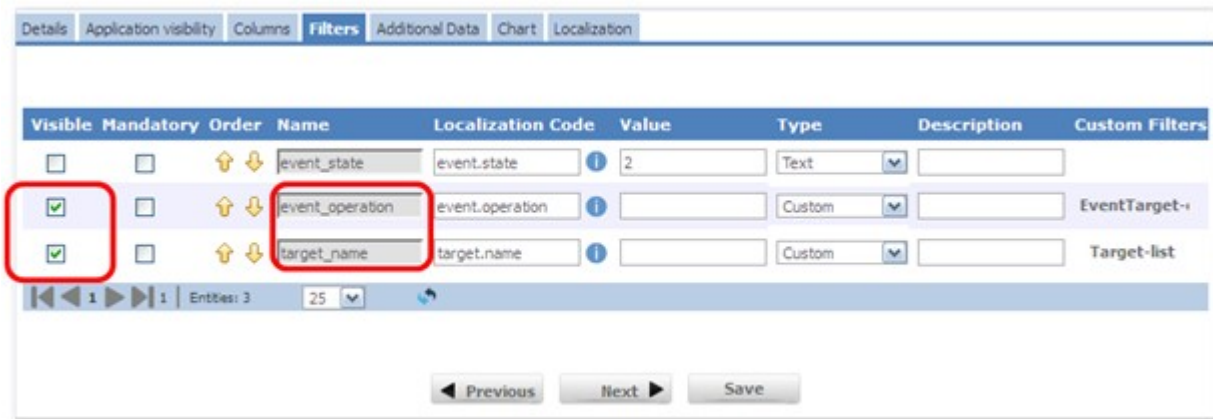


Figure 124. Filters tab.

An authorized user can now configure these filters (event\_operation and target\_name) when executing the report from a generic IBM Security Identity Governance application.

The RD module provides a set of custom filters. The administrator can assign these custom filters directly as they are, or modify their settings as needed. The table below lists all custom filters delivered with the product:

Table 247. Product custom filters.

Filter name	Custom filter description
Target-list	List of targets
EventIN-operation	EventIN codes
EventTarget-operation	EventTarget codes
SoD Type	Names of SoD types

The RD Administrator can modify the current localization code in the **Localization Code** field. If the localization is unsuccessful, it is displayed in red in the **Report Filters Localization** section of the Localization tab. The administrator can add a filter value in the **Fixed Value** text field.

This option is a suggested filter structure for the authorized user executing the report from a generic IBM Security Identity Governance application. The user can also modify this value as needed.

For example, might be configured the filter **user\_code** with a fixed value of 03\* and type Text. The report available will have a preset filter value of 03\*, meaning that the report will contain all users whose user code begins with 03.

However, the user can change this preset value in the **Type** area, as the table below outlines:

*Table 248. Filter type.*

Item	Description
<b>Custom</b>	Relabeled filter
<b>Date (DD/MM/YYYY)</b>	Only date format allowed for this filter type
<b>Extended Date</b>	Both hh:mm:ss and DD/MM/YYYY formats allowed for this filter type (Inserting hour before date automatically populates the current hh:mm:ss, which you can modify)
<b>Number</b>	Only number format allowed for this filter type
<b>Text</b>	Only text format allowed for this filter type

### **Additional data tab**

The RD Administrator can configure additional information in the following three panes:

- the **Send Email** pane
- the **Additional Information** pane
- the **Report Output Format** pane

The following figure shows these panes:

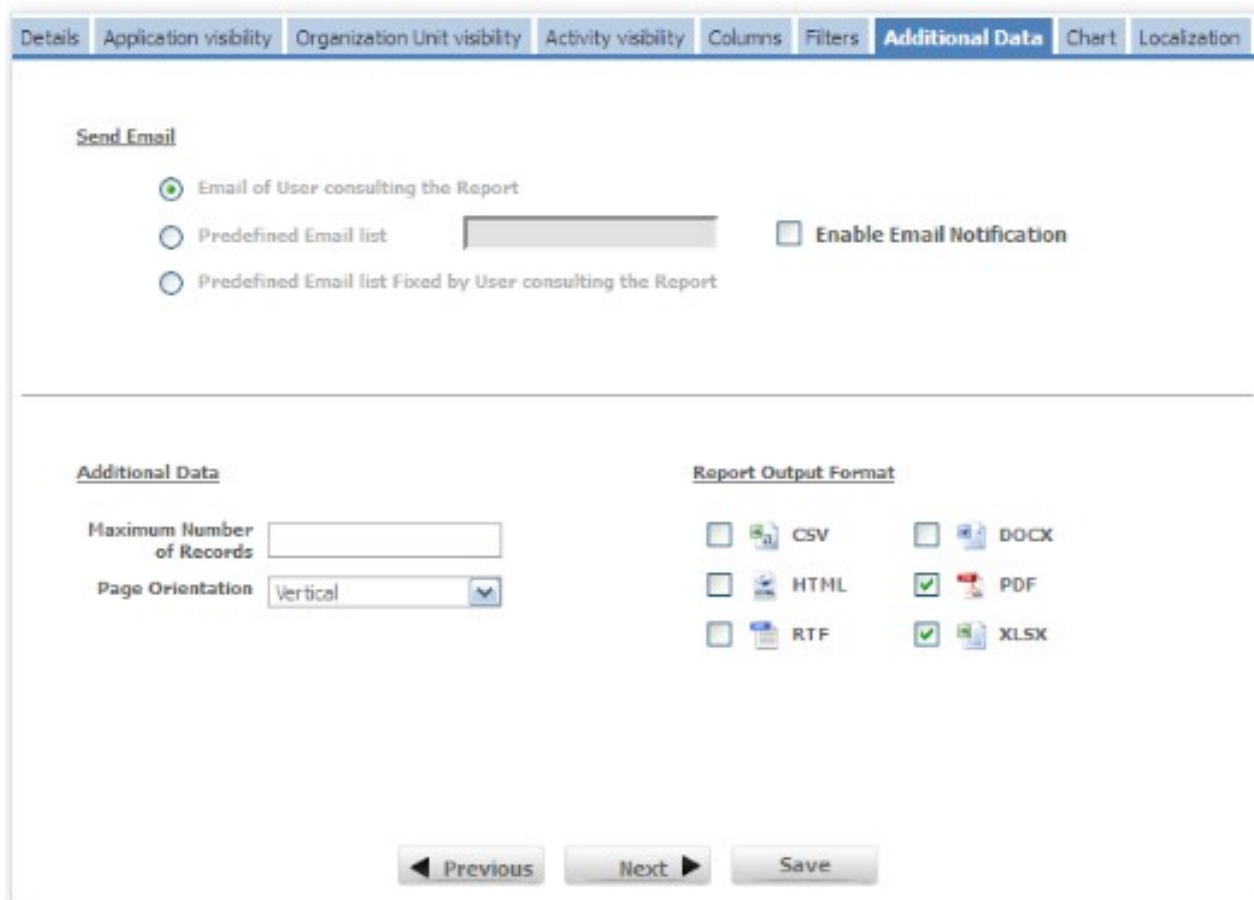


Figure 125. Additional data tab.

In the **Send Email** pane, the RD Administrator can choose to select the **Enable Email Notification** check box to enable the email notification. The following table lists the available email options:

Table 249. Send email pane details.

Available options	Description
<b>Email of User Consulting the Report</b>	A default setting to send an email notification to the user executing the report.
<b>Predefined Email List</b>	List of email addresses to send notifications to: Separate multiple addresses by a semi colon.
<b>Predefined Email List Fixed by User consulting the Report</b>	This option allows the user executing the report to define the list of email addresses to send notifications to.

The table below lists the options available in the **Additional Data** pane:

Table 250. Additional data pane details.

Available options	Description
<b>Maximum Number of Records</b>	Allows a maximum limit to be set on the amount of data drawn by the report.

Table 250. Additional data pane details. (continued)

Available options	Description
<b>Page Orientation</b>	Allows to choose the orientation of the page for the report output: <ul style="list-style-type: none"><li data-bbox="933 321 1045 348">• <b>Vertical</b></li><li data-bbox="933 359 1081 386">• <b>Horizontal</b></li></ul>



The RD Administrator can choose one or more of the following output formats in the **Report Output Format** pane:

- **CSV**
- **HTML**
- **RTF**
- **DOCX**
- **PDF**
- **XLSX**

**Note:** To proceed with the report configuration, the RD Administrator must choose at least one report output format.

### **Chart tab**

Under this tab, the RD Administrator can configure the following summary chart types:

-  Bar Chart
-  3D Pie Chart

as shown below:



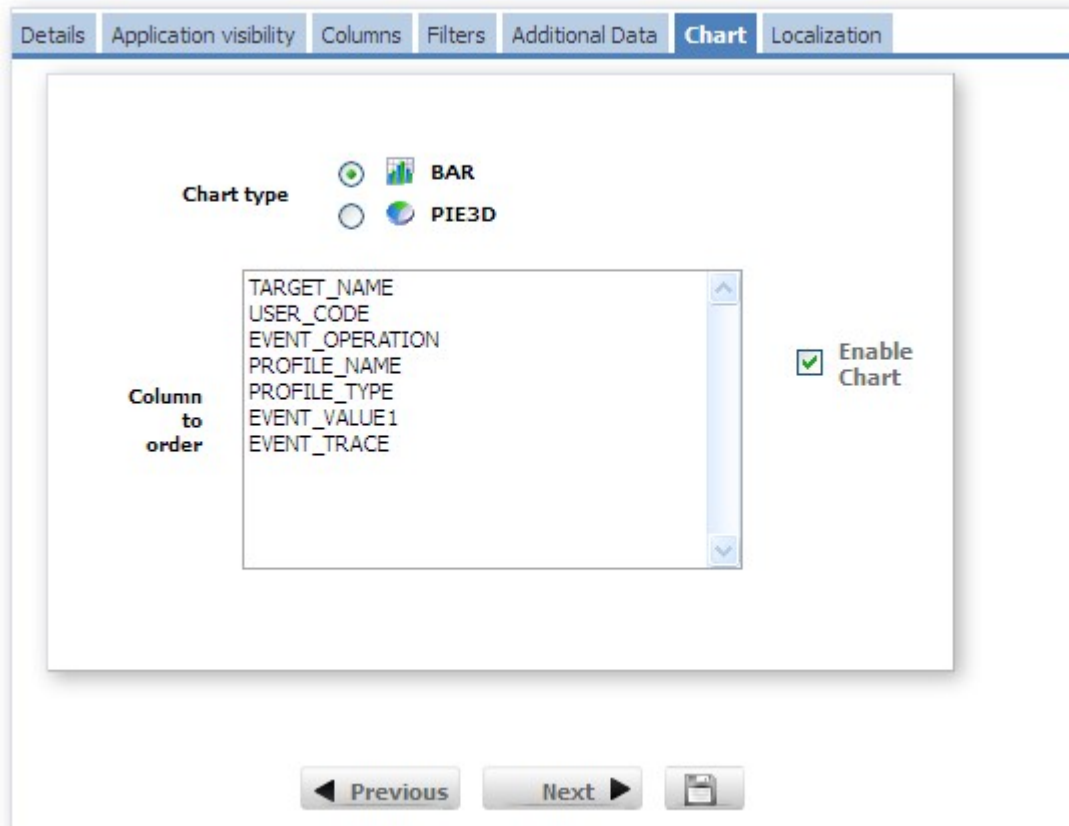


Figure 126. Chart tab.

To enable the chart, the RD Administrator can select the **Enable Chart** check box. The columns available in the **Column to order** box, depend on which columns the RD Administrator selects in the Columns tab.

To make a given column visible in the report, the RD Administrator must select that column in the **Column to order** box. The RD Administrator cannot choose more than one column.

The figure below shows a sample bar chart in the *Report5.20-Status/Report Visibility*:

## 5.20 - Status/Report Visibility - chart

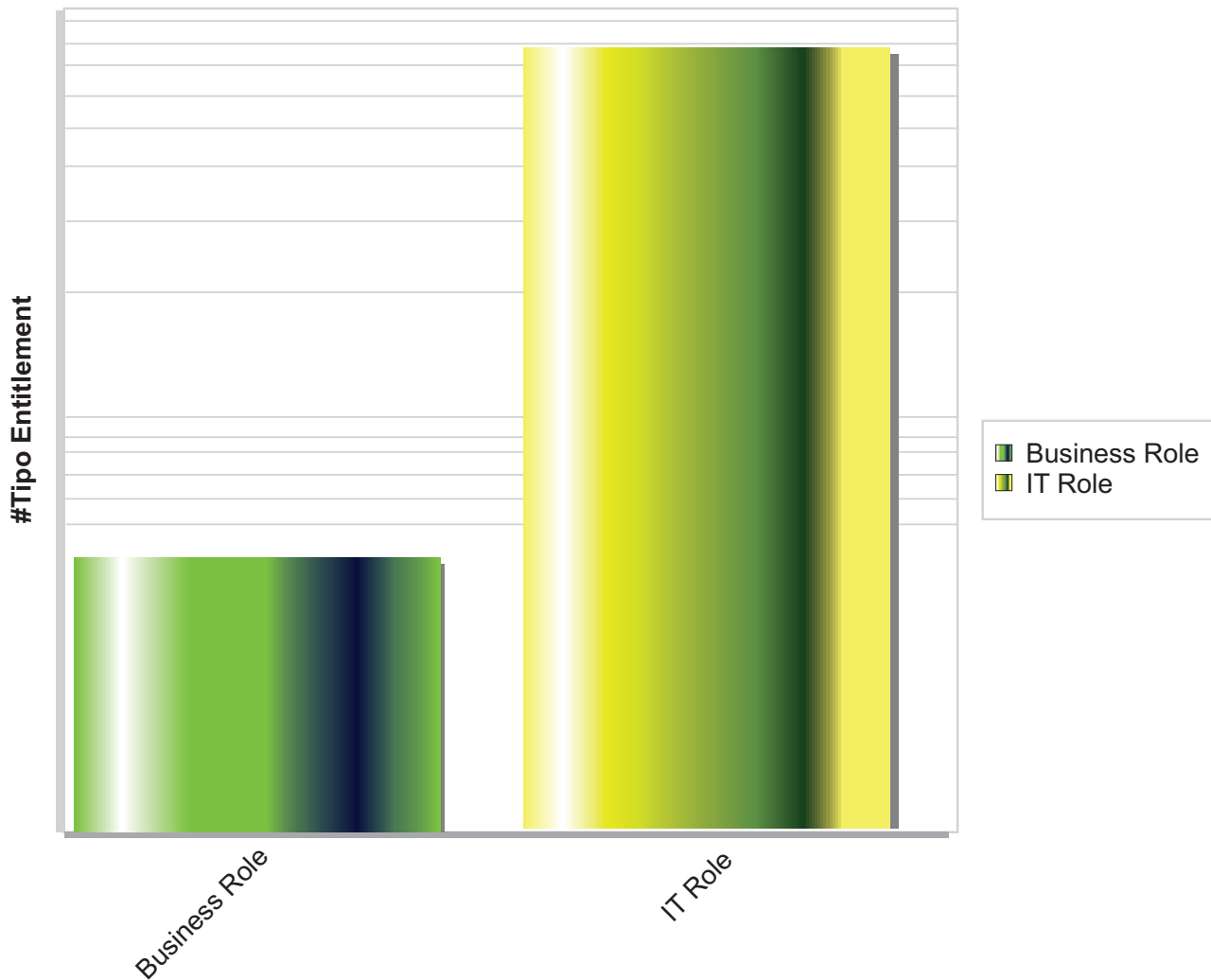


Figure 127. Bar chart.

This example illustrates a chart that summarizes the type (horizontal axis) and quantity (vertical axis) of the entitlements involved in the report. The chart above shows that the report involves Business Role and IT Role entitlements. Four are Business Role entitlements and seventy-seven are IT Role entitlements.

The report output format in the example is an XLSX file. The RD Administrator can configure a report output format under the Additional Data tab.

### Localization tab

The figure below shows how to use the **Localization** tab to edit and localize the following:

- Report labels
- Column labels
- Filter labels

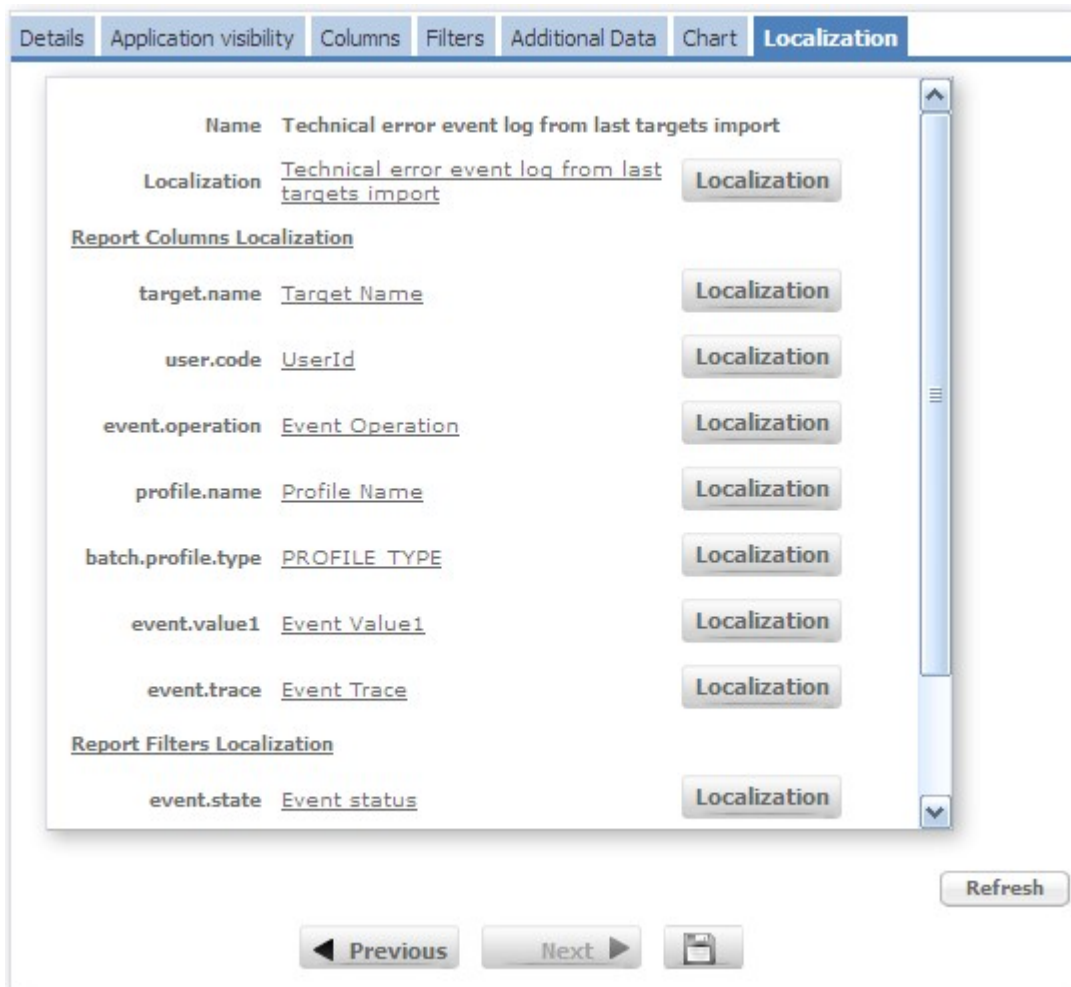


Figure 128. Localization tab.

To edit and localize labels, click **Localization**.

The localization process is based on two main elements:

- The localization code
- The localization message

For each configured language, the RD Administrator must associate each localization code to a specific localization message (**Languages** button in **Edit Labels** section). If the localization message is not configured, the module automatically populates the corresponding language field with the localization code.

Insert the appropriate localization message in the field and click **Ok** to update and automatically save it. Or, if needed, keep the default localization code.

**Note:** You should first set your preferred language in the **Languages** window of the **Edit Labels** tab.

If the localization message is not localized in any languages, the localization code will be displayed in red.

In this case, the field in the Localization windows displays the localization code. If the codes are not correct, write the appropriate localization message. Otherwise, keep the localization code and click **Ok** to complete the configuration. The color of the localization code changes to black.

Scroll down the list to verify that all values are localized. If, after saving the transaction, some values are not localized, a Warning window provides suggestions.

**Note:** The field values are automatically refreshed but the **Refresh** button is still active.

---

## Report status and report category

An appropriate status value must characterize a report.

There are three possible values for the status:

- **New:** Report is not yet executed by an IBM Security Identity Governance module (ARC, AGC, ARCS)
- **Assigned:** Report is assigned like an entitlement (of type profile) to an application role (IT Role, BRole)
- **Locked:** Report is locked and cannot be executed by any IBM Security Identity Governance module (this status is reversible).

After the creation, the default status for a report is **New**, but it can change to **Assigned** or **Locked**.

The RD administrator can also decide to catalog the reports into categories:

- **Audit**
- **Changes Detection**
- **Export**
- **Orphaned**
- **Recertification**
- **Status**
- **Sync**
- **Tech Info**
- **Violations**

Categories group together a set of reports that have the same characteristics, for example the user category groups together all user reports, while the audit category groups together all audit reports.

The RD administrator customizes the categories as needed.

---

## Available reports

Report Designer includes a set of categorized reports.

## Analysis reports

Table 251. Analysis reports available

Name	Description
Export Tech Transformation <i>(if External SoD is set, this report is not relevant)</i>	Produces a downloadable xlsx file containing the complete Business Activity Mapping data associated to an Environment. Use this report to migrate a configuration from one deployment to another or to create a backup of your system.
Role Usage Status Summary	Role usage details for identifying candidate Roles for deletion.
Access Rights not assigned to any OU	Access Entitlements (Business Roles, IT-Roles, Permissions) that are not assigned to any OU as standard privileges belonging to the specific OU (visibility).
Access Rights not assigned to any user	Entitlements (Roles and Permissions) that are not assigned to any user.

## ARCS reports

Table 252. ARCS reports available

Name	Description
ARCS - User with FSOD Risks	Full SOD (FSOD) Risks by users. For each of the selected user, the report shows the FSOD Risks that are assigned and the Activities that cause the Risks. Other details include the SAP System, Risk type and severity, Domain of reference. You can select by Risk type and user attribute (code, name and surname).
ARCS - SAP and Collective Role Risk overview	Risks joined to SAP and Collective Role. For each of the selected SAP and Collective Role, the Report shows the Risks that are assigned and the Activities that cause the Risks. Other details include the SAP System, SAP Role type and severity, Domain of reference. You can select Risks based on involved activities.
ARCS - User Risks	Risks joined to Users. For each of the selected user, the Report shows the Risks that are assigned and the Activities that cause the Risks. Other details include the SAP System, Risk type and severity, Domain of reference. You can select by Risk type and user attribute (code, name and surname).
ARCS - SAP authorization Risk overview	Risks joined to SAP authorization. For each of the selected SAP authorization, the Report shows the Risks that are assigned and the Activities that cause the Risks. Other details include the SAP System, Risk type and severity, Domain of reference. You can select Risks based on involved activities.
SAP Authorization and Business Activity Catalog	Technical Transformation, that is the associated SAP Authorization for each Business Activity.
SAP Role and AuthObj Catalog	SAP Role Catalog filtered by SAP System. It also shows SAP Role links to Authorization Objects.

Table 252. ARCS reports available (continued)

Name	Description
SAP Role and Transaction Catalog	SAP Role Catalog filtered by SAP System. It also shows SAP Role links to Transactions.
SAP Role Catalog	SAP Role Catalog filtered by SAP System. It also shows SAP Role incompatibility by level (Low/Medium/High).
SAP Authorization Definition	SAP Authorization definition, showing how an SAP Authorization is joined to Transactions, Authorization Objects, and Fields. It also shows the logical conditions among objects.
SAP Role and Business Activity Catalog	SAP Roles by Business Activity.

## Audit reports

Table 253. Audit reports available

Name	Description
Workflow history	Requests and steps from the audit trail.
Audit Trail - User authorizations history	Sequence of add, remove and reviews user requests, by user
IDEAS Audit	Collection of data for audit and compliance purposes. You can configure the amount of information displayed by selecting users reported (Visibility).

## Campaigns reports

Table 254. Campaigns reports available

Name	Description
Certification - Fulfilment status summary	Status summary with details for the fulfilment status (applicable for Applications not subject to write back sync).
Certification - Status summary by OU	Report of Organization Unit Entitlements Certification. Each Reviewer in a Certification of this type reviews an Organization Unit, and is expected to review all access privileges. This report aggregates all entitlements that can be granted to users belonging to these OUs.
Certification - Status summary by Reviewer	Report of User Entitlement Certification. Reviewer in a certification of this type review the access privileges of the users in his scope.
Certification - OU visibility - Status summary	Completion status of an OU visibility Certification Campaign.
Access Certification Campaigns Status	Completion status of Access Certification Campaigns. For each Organization Unit the Report shows the number of Users that require a Review and the actual Certification statistics. Only Organization Units where an Access Certification action is required, are included in this Report.

## Export reports

Export reports use an associated query that produce files that can be used with the Bulk Load tool.

Table 255. Export reports available

Name	Description
External Role Bulk	External Roles using the Export External Role Hierarchy query.
Export Tech Transformation	Business activity mapping data for an environment.
Remediations to risks Bulk <i>(if External SoD is set, this report is not relevant)</i>	Remediation details and the associated remediated risks.
Entitlements Bulk	List of the Entitlements.
Applications Bulk	List of all the Applications.
Organizational Units Bulk	Hierarchy of Organizational Units (OU).
Resources Bulk	List of Resources.
Entitlements to Users Bulk	List of users and their assigned Entitlements (Business Roles, IT-Roles, Permissions).
Users Bulk	List of the users
Activities hierarchy Bulk <i>(if External SoD is set, this report is not relevant)</i>	Business activities and their hierarchical structure.
Profile to domain Bulk <i>(if External SoD is set, this report is not relevant)</i>	Exports Permissions to Domain IDEAS configurations for editing and re-import.
Risk Structure Bulk <i>(if External SoD is set, this report is not relevant)</i>	Details on the Risk structure. You can select Risks based on the Environment.

## Optimizer reports

Table 256. Optimizer reports available

Name	Description
User KRI summary	Extracts User Score indicators and computes the average overall Score index. This Report does not including the Similarity Divergence KRI.
Candidate Role - User List	Candidate Role users assigned. Use it to support shrinking of the number of user assignments in systems other than IGL.
Candidate Role - Entitlement List	Candidate Role entitlement list. Use it to support the manual constructions of roles in systems other than IGI
Candidate Role - Role Metrics	Candidate Roles core metrics dump.

## Policies reports

Table 257. Policies reports available

Name	Description
IDEAS Report List	All reports available.
IDEAS Report Visibility	Administrative Roles (Entitlements) that include each report. Users who have an Admin Role for the report can configure and run the report.
IDEAS Report Structure	Reports structures, including columns and localization details.
Mitigations assigned to Risks <i>(if External SoD is set, this report is not relevant)</i>	For each Risk, the report shows the Mitigations assigned and Mitigation details.
Access Rights Visibility by OUs	Entitlements (Business Roles, IT-Roles, Permissions) that are directly assigned to each OU. Report visibility can be set based on Application.
Technical Transformation <i>(if External SoD is set, this report is not relevant)</i>	Business Activity Mapping relations, with entitlements (Roles/Permissions ) for each Business Activity.
Risk Structure <i>(if External SoD is set, this report is not relevant)</i>	Shows detailed information on Risks. You can select Risks based on Activities and other parameters such as Risk Type and Environment. Details provided for each Risk include: name, description, type, severity and referred activities.

## Status reports

Table 258. Status reports available

Name	Description
Users by Application	For each of the selected Applications, the Report shows the users (and the belonging Organization Unit) that have assigned entitlements from that Application.
User Assignments	Access rights by user. Users are selected depending on visibility settings. For each selected user, the report shows Entitlements (Permissions, IT-roles, Business Roles) assigned to the user.
Delegation assignments	Delegation assignments with information on delegated and represented users. Details include OU, email and delegated Entitlements, including validity start and end dates for the Entitlements).
Account Status	Account details and status are provided together with possible locking codes.
Account matching status	For every Account configuration, the number of matched, unmatched, and orphans accounts.
Accounts created in last X days	List of all accounts created in the last X days.
Account expiring in next X days AM	List of all accounts created that are going to expire in the next X days.
Activities created in last X days	List of all activities (Access Risk Controls module) created in the last X days.



Table 258. Status reports available (continued)

Name	Description
Permission created in last X days	List of all permission created in the last X days.
Technical transformation status	List of Business Activity Mapping relations defined in the system.
User Permission's indirect assignments	Permission assigned through the assignment of a Business Role or an IT Role.
Role hierarchical structure	Role Structure. Only structured Entitlements (such as Business Roles and IT Roles) are considered.
Application Entitlements dictionary	Entitlements (Business Roles, IT-Roles, Permissions), by Applications, with details for each entitlement.

## Sync reports

Table 259. Sync reports available

Name	Description
Reconciliation - Sync Status by Target	Accounts and Permissions reconciliation status where conditions are applicable to the use IGI as Master repository or as a slave.
Reconciliation - Sync Status	Accounts and Permissions reconciliation status where IGI is the master source of data
Reconciliation - Sync Status [Coarse Grain]	Accounts and Permissions reconciliation status where IGI is the master source of data. No changes propagated from target system back to IGI. This version compares at permission level, ignoring rights name and values
Reconciliation - Target event queue extraction	Events arrived from the target system queue during the last synchronization.
Import from Target - error event log	Shows details of all Events generated during the last import from target system applications.
Events-OUT - Targets Queue extract	Events in the outbound queue applicable only in case of automatic provisioning towards target system applications.
Events-IN - HR Queue extract	Events in the inbound queue, received from HR system used as authoritative source.
User Assignments Changes	Lists all users changed their Permissions (Business Roles, IT-Roles, Permissions) assignments in the last 7 days. Users can be selected by Organization Units and Application. For applications, only Users that have assigned Entitlements from the specified Application are included.
Role Structure Changes	Roles that had changes in their entitlements in the last 7 days.

## Violations reports

Table 260. Violations reports available

Name	Description
User Violations and Mitigations <i>(if External SoD is set, this report is not relevant)</i>	Allows Compliance Managers, or other authorized Reviewers, to certify Risks and related Mitigation Controls. Each Reviewer in a Certification of this type is focused on the set of users defined by his visibility settings, and is expected to review all Risks connected to access-privileges for each of these users. Furthermore, Mitigation Controls possibly linked to those Risks are reviewed.
Application - Licence status summary	Active accounts versus licence counts per Application.
User Violations Count <i>(if External SoD is set, this report is not relevant)</i>	Provides a number of statistics on users that have associated Risks. Visibility can be set at the Application, Organization Unit, and Activity levels.
Role Violations Overview <i>(if External SoD is set, this report is not relevant)</i>	Provides details on Risks associated to Entitlements. For each selected Entitlement, the report shows the Risks that are assigned and the Activities that cause the Risks. Other details include the belonging Application, Entitlement type, Risk type and severity, Domain of reference. You can select Risks based on involved activities.

## Available dashboard items

Create and customize dashboard items in Report Designer. A set of configured dashboard items is provided.

Dashboard items are listed in the Report Designer in **Manage > Dashboard**. They are listed in the following table by name and the Administrative Role that they are assigned to in the product as shipped.

Table 261. Dashboard items available

Name	Intended Administrative Role
<b>Access certification status</b>	Available to any user who is assigned as a supervisor or reviewer in one or more access campaigns.  Not listed in Report Designer. See the description in User Manager.
<b>Access request history</b>	Employee
<b>Account matching status</b>	Application Manager
<b>Accounts created in last x days</b>	Application Manager
<b>Accounts expiring in next x days with application scope</b>	Application Manager
<b>Accounts expiring in next x days with OU scope</b>	User Manager
<b>Activities created in the last x days</b>	Application Manager

Table 261. Dashboard items available (continued)

Name	Intended Administrative Role
Approval tasks	Available to any user who has an Admin Role with access to the Daily Work workflow.  Not listed in Report Designer. See the description in User Manager.
Business activity mapping status	Application Manager
Approval tasks	User Manager
Days until the next password expiration	Employee
Delegation assignments	User Manager
Locked accounts	User Manager
My entitlements	Employee
My requests	Employee
Partial requests	Employee
Pending requests	User Manager
Permissions created in the last x days	Application Manager
Policy violation requests	Employee
Recent requests	Employee
Rejected requests	Employee
Unmatched accounts	Application Manager
User violations	User Manager
User violations without mitigation	User Manager

---

## Building a new report: A brief roadmap

A roadmap is provided to configure a new report.

The RD administrator can use the following logical roadmap (not mandatory) to define the reports:

1. Create a query (found in the dedicated **Query Management** section).
2. Import the **Query Columns**.
3. If the query contains definitions for temporary tables, use the scope list from the scope management section to associate the scope to the query.
4. From **Manage > Report**, choose the query to associate to the report.
5. Follow the steps in the wizard to configure the report.

---

## Manage

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

### Query



In this section, the administrator can choose to create and customize queries or configure the report using an already existing query.

The **Query** pane (left), contains the list of inventoried queries, filters for the query search and controls to perform the import/export operations.

The **Name** and **Description** filters are available for the query search.


The **Query** pane, lists the results, according to the following attributes:

Table 262. Query Attributes.

Name	Description
<b>Name</b>	Query name. An icon is present near the item name, depending on the type of item: <ul style="list-style-type: none"> <li>•  for a product item.</li> <li>•  for a custom item.</li> </ul>
<b>Description</b>	Brief query description (maximum 256 characters)

The tabs on the right contains the following main sections:

- Query Management tab
- Scope Management tab
- Joined Report tab

	<b>Note:</b> In this section, switching from one tab to another does not discard intermediate changes. However, the <b>Save</b> button (top right corner of the host pane) is still active.
--	---

The main operations available in this section are listed below.

## Query search


Proceed as follows:


1. In the **Query** pane, click **Filter/Hide Filter**.
2. Set the data filter (**Name** and **Description**) and click **Search**. The results are displayed in the same pane.
3. To import a query:
  - In the left pane, click **Import**.
  - In the Import Query/Report window that displays, click **Browse** to search for a file to upload (available formats are .zip, .gzip, .tar and .gz).
  - After the file selection, click **Ok** to confirm the operation.
  - An Import Query window opens, showing the process status.
  - After the process is finished, click **Ok** in the window showing the operation outcome.
  - At the end of the operation, a window displays, asking if the administrator wants to import another file. In the same window, click **Ok** to import a new file.
4. To export a query:
  - In the left pane, select the **Query** to be exported.
  - In the left pane, click **Export**.

- A system-based window displays, prompting you to either open or save the file in XML format.
- Click **Ok** in the window showing the operation outcome.

The XML file name contains:

- The name of the query.
- The date the query was created.
- The time the query was generated.

	<p><b>Note:</b> If an imported query has the same name as an existing query, a Warning displays a diagnostic message regarding the effects of the operation.</p>
---	--

	<p><b>Note:</b> Attempting to import a file that is not in XML format generates a Warning which displays a diagnostic message regarding the effects of the operation.</p>
---	---

## Create a query

Proceed as follows:

1. In the **Query** pane (left), click **Add**.
2. In the **Query Details** pane (right), specify the query details and write the query according to your needs.
3. At the bottom right corner, click **Save**.
4. Click **Ok** in the window showing the operation outcome.

The query will be saved as custom query.

For help about the query processing, click **Help** at the bottom right corner in the same pane.

## Modify a query

This operation is available only for the custom query.

Proceed as follows:

1. In the **Query** pane (left), select the query to be modified.
2. In the **Query Details** pane of the **Query Management** tab (right), modify the SQL query and any query data.
3. At the bottom right corner, click **Save**.
4. Click **Ok** in the window showing the operation outcome.

## Remove a query

This operation is available only for the custom query.

Proceed as follows:

1. In the **Query** frame (left) select the query to be removed.
2. Click **Remove**.

3. Click **Ok** to confirm the operation.
4. Click **Ok** in the window showing the operation outcome.

**Note:** Removing a query eliminates its links with the scope and the report.

### Query management tab

In the **Query Details** pane, the SQL query text area allows you to create a custom query.

If you need assistance writing the query, click **Help**, in the bottom right corner of the same pane. The Available query Keys window displays. After selecting the query key, click **Ok** to automatically insert the key into the **SQL Query** text area.

The RD administrator can add, modify or remove the report columns.

There are two ways to add and populate the columns:

- Individually, using the Add function.
- Automatically, using the Import query columns function.

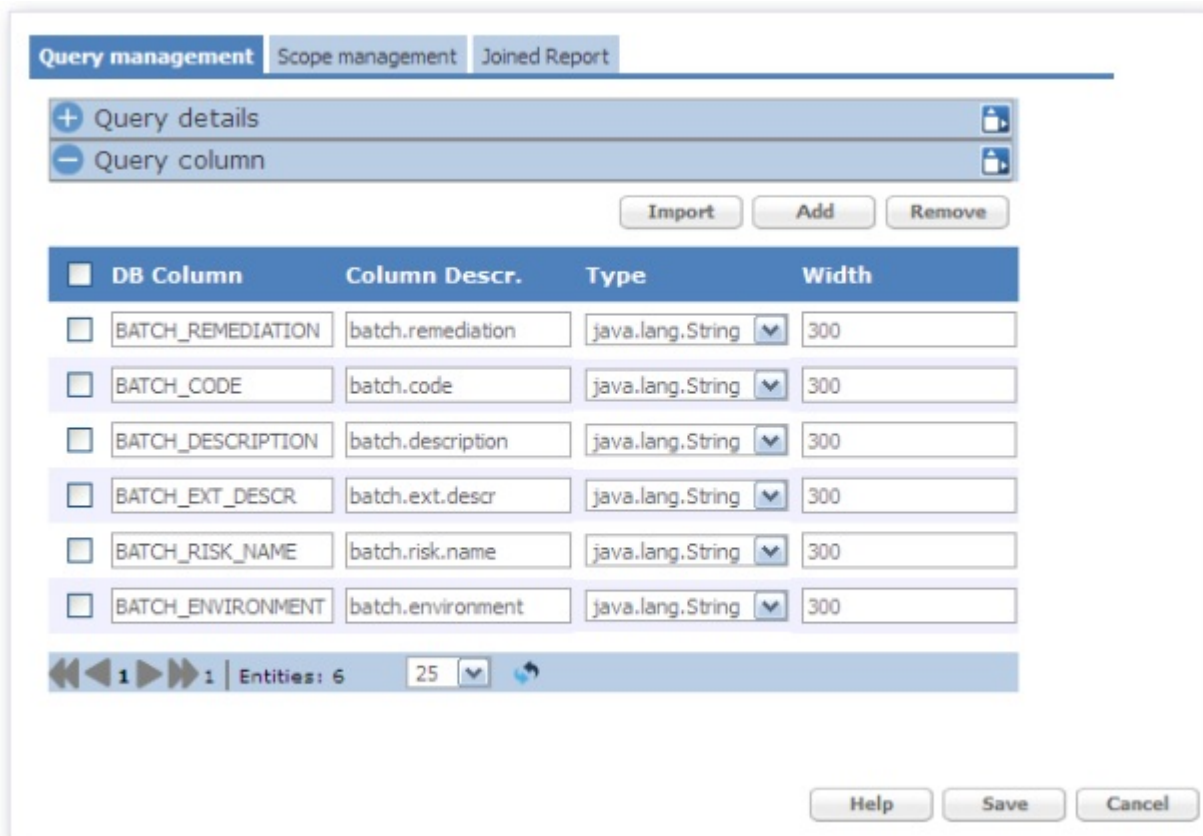


Figure 129. The Query Management window.

### Add and fill query columns individually

This operation is available only for a custom query.

Proceed as follows:

1. In the Query column pane, click **Add**.

2. Fill the column fields with the values defined in the query.
3. At the bottom right corner of the same pane, click **Save**.

If necessary, repeat the steps 2 and 3.

### **Add and fill query columns automatically**

This operation is available only for the custom query.

Proceed as follows:

1. In the Query column pane, click **Import query columns**, this automatically adds the columns and populates them with the values defined in the query.
2. At the bottom right corner of the same pane, click **Save**.

### **Remove query columns**

This operation is available only for the custom query.

Proceed as follows:

1. In the Query column pane, click **Remove**.
2. At the bottom right corner of the same pane, click **Save**.


#### **Note:**


Removing columns in this frame also eliminates them from the **Report Wizard section > Columns** tab.

### **Scope management tab**

In this section, scopes can be associated to queries.

The **Query** tab, displays the queries listed in the system. The **Scope management** tab displays the list of scopes already associated to the selected query.

Clicking **Add**, the Scope List window opens, displaying the list of scopes that the RD Administrator can associate to the queries selected in the Query pane on the left. The Scope list windows provides **Name** and **Description** filters for a scope search (clicking **Filter/Hide Filter**). From this window, you can add a new scope by clicking **New**, and edit a  custom scope by clicking **Edit**.

**Note:** The  product scopes cannot be edited.

To view the scope details, click **Details**. You cannot perform changes in this window. To remove a scope, click **Remove**.

#### **Note:**

- Removing a scope results in the loss of its visibility configuration; the tmp. table is still part of the query but contains no data.
- After removing a scope from the selected query, all aggregations with any other query will be lost.

### **Joined Report tab**

This section displays the reports associated to a selected query.

In the **Query** tab, when selecting a query, the list of associated reports is displayed in the right frame.

## Report

In this section, you can find the procedures for customizing a report based on the values defined in the relevant query.

In this section, you can:

- Create a report
- Copy a report
- Attempt a query execution



The report filters are listed in the table below:

*Table 263. Report filters.*

Filter	Description
<b>Name</b>	Report name.
<b>Description</b>	Brief report description.
<b>Status</b>	Report status: <ul style="list-style-type: none"> <li>• <b>Assigned</b></li> <li>• <b>Locked</b></li> <li>• <b>New</b></li> </ul>
<b>Report Category</b>	Inventoried reports category.

The same pane lists the results, according to the following attributes:

*Table 264. Report attributes.*

Attribute	Description
<b>Name</b>	Report name. An icon is present near the item name, depending on the type of item: <ul style="list-style-type: none"> <li>•  for a product item.</li> <li>•  for a custom item.</li> </ul>
<b>Status</b>	Report status: <ul style="list-style-type: none"> <li>• <b>Assigned</b></li> <li>• <b>Locked</b></li> <li>• <b>New</b></li> </ul>
<b>Report Category</b>	Inventoried reports category. Click <b>Add</b> to inventory a new category.

The main sections described in this paragraph are listed below:

- Report Inventory
- Create a New Report
- Configure a Product Report
- Copy a Report
- Simulate a Report



## Report Inventory

The RD module has a list of **Product Reports** that the RD Administrator can assign directly to the users. The administrator can also use the procedure in this section to create a new report.

### Report search

Proceed as follows:

1. In the **Reports** tab, click **Filter/Hide Filter**.
2. Set the data filter and click **Search**. The results are displayed in the same pane.
3. To import a report:
  - In the left pane, click **Import**.
  - In the Import Report/Query window that displays, click **Browse** to search for a file to upload (available formats are .zip, .gzip, .tar and .gz).
  - After the file selection, click **Ok** to confirm the operation.
  - An Import Report window opens, showing the process status.
  - After the process is finished, click **Ok** in the window displaying the operation outcome.
  - At the end of the operation, a window displays, asking if the administrator wants to import another file. In the same window, click **Ok** to import a new file.
4. To export a report:
  - In the left pane, select the **Report** to be exported.
  - In the left pane, click **Export**.
  - A system-based window displays, prompting you to either open or save the file in XML format.
  - Click **Ok** in the window displaying the operation outcome.

The XML file name contains the report name, date, and hour.

### Create a report

To create a report, proceed as follows:

1. From the **Reports** tab, click **Add** .
2. The **Details** tab opens. This is the starting point of the Report Configuration Wizard.

### Configure a product report

Proceed as follows:

1. Perform a report search.
2. In the **Reports** tab, select the desired report.
3. In the right pane the wizard opens by default. Follow the steps to configure the **Product Report**.

### Copy a report

Proceed as follows:

1. Perform a report search.
2. In the **Reports** tab, select the desired report.

3. Click **Copy**.
4. The **Details** tab opens by default. Insert the required information and follow the wizard to configure the report.

**Note:** This operation is recommended for changing configuration settings while still maintaining the joined report query values.

## Report simulation

Proceed as follows:

1. Perform a report search.
2. In the **Reports** tab, select the desired report.
3. Click **Test**.
4. The Report Simulation window opens.
5. Clicking **Ok**, the Report Simulation Wizard begins.
6. Choose the **Report format** (PDF, XLSX, CSV), then click **Next**, followed by **Execute**.
7. A system-based window displays prompting you to save the file in the chosen format.
8. Click **Ok** in the window showing the operation outcome.

The file name contains the report name, date, and hour.

## Remove a report

Proceed as follows:

1. Perform a report search.
2. In the **Reports** tab, select the desired report.
3. Click **Remove**.
4. To confirm the operation, click **Ok** in the window that displays.
5. Click **Ok** in the window showing the operation outcome.

## Dashboard

Configure dashboard items to be used on Dashboard home pages in Service Center.

Dashboard items are special types of reports. They are associated with a query, which produces the data to display. Dashboard items must be assigned to an Entitlement in order to be visible.

Users who have the Admin Role have the Entitlements assigned to the Admin Role. The corresponding dashboard items are included in the Dashboard home page Service Center. Users who are assigned to multiple Admin Roles see a **Dashboard** home page in Service Center. It consists of all the dashboard items from all of their Admin Roles.

You work with dashboard items in **Report Designer > Manage > Dashboard**.



- A list of dashboard items is shown in the left pane, **Dashboards**.
- Attributes are organized in tabs in the right pane. The tabs that are shown depend on the dashboard item you select.

The following controls are in the left pane:

- A list of dashboard items
- **Actions** - Click to select **Copy**, **Test**, or **Remove**
- **Filter** - Filters are used to search the list.

In the list, you can see information in fields for each dashboard item, as listed in the following table.

Table 265. Dashboard item fields

Field	Description
<b>Name</b>	Dashboard item name. An icon shows the type of item: <ul style="list-style-type: none"> <li>•  Product item, which can be copied but not deleted. Only some attributes can be edited for a product item.</li> <li>•  Custom item.</li> </ul>
<b>Code</b>	Not used for dashboard items
<b>Status</b>	<ul style="list-style-type: none"> <li>• <b>New</b> - Not yet assigned to an entitlement</li> <li>• <b>Assigned</b> - The dashboard item is assigned to an Entitlement.</li> <li>• <b>Locked</b> - The dashboard item is locked and cannot be edited.</li> </ul>
<b>Category</b>	Existing product report category or administrator-defined category.

## Dashboards for personas

See the following sections to see how the Dashboard home page can be configured for personas.

- Application Manager
- User Manager
- Employee

## Tasks for working with dashboard items

You can perform the following tasks for dashboard items.

- Search, by using filters
- Edit
- Test
- Copy
- Remove
- Assign to an Entitlement

### Note:

- You cannot create dashboard items. Copy a product dashboard item and edit it.
- You cannot remove product dashboard items. You can delete copies that you made.

## Searching for a dashboard item

1. In the left pane, click **Filter**.
2. Enter the search criteria in the fields: **Name**, **Code**, **Status** , or **Category** .
3. Click **Search**. The list is updated to show only dashboard items that meet the search criteria.

Click the **Dashboard** tab above the left pane to show the full list again.

Table 266. Dashboard item filters

Filter	Description
<b>Name</b>	Dashboard item name
<b>Code</b>	User-assigned code. Product dashboard items do not have a code and cannot be assigned a code.
<b>Status</b>	Dashboard item status values <ul style="list-style-type: none"><li>• <b>New</b></li><li>• <b>Assigned</b></li><li>• <b>Locked</b></li></ul>
<b>Category</b>	User-assigned category

The attributes for filters appear in the **Details** tab for a dashboard item.

See “Available dashboard items” on page 514 for the full list of available dashboard items.

## Editing a dashboard item

You can edit some information in a provided dashboard item. You can edit all information in a dashboard item that you copied.

1. In the left pane, select a dashboard item.
2. The **Details** tab opens in the right pane. You can move among the tabs in the following ways:
  - Click the tabs at the top of the right pane.
  - Use the wizard. Click **Next** and **Previous** to move through the tabs.
3. Click **Save** to save your changes.

## Testing a dashboard item

You can test a dashboard item to display the effects of your changes.

1. In the left pane, select a dashboard item.
2. Click **Test** in the left pane. A sample of the dashboard item is shown.
3. Click **OK** when you are done.

## Copying a dashboard item

You cannot create new dashboard items directly. Copy a an existing product dashboard item and edit it.

1. In the left pane, select a dashboard item.
2. Select **Actions > Copy**.
3. Enter a name for the copy.

4. Click **Save**.

## Removing a dashboard item

You cannot remove product dashboard items. You can remove any copies that you made.

1. In the left pane, select a dashboard item.
2. Select **Actions > Remove**. This menu item is not active for product dashboard items.
3. Click **OK** to confirm.

## Assigning a dashboard item to an entitlement

1. In **Report Designer**, click **Configure > Assignment**.
2. In the **Report/Dashboard > Entitlement** tab, click a dashboard item. The current assignments are shown in the right pane. You can also click the **Entitlement > Report/Dashboard** tab to see the list of entitlements and the reports assigned to them.
3. In the right pane, use the **Actions** menu to add or remove entitlements.

## Details tab

Configure basic information about the dashboard item.

Table 267. Details tab fields

Field	Description
<b>Query name</b>	Read-only field. Click <b>Show Query</b> to go to the <b>Query</b> tab and view the query.
<b>Description</b>	Description of the dashboard item.
<b>Name</b>	Name of the dashboard item.
<b>Status</b>	<ul style="list-style-type: none"> <li>• <b>New</b> - Not yet assigned to an entitlement</li> <li>• <b>Assigned</b> - Automatically set if the dashboard item is assigned to an entitlement.</li> <li>• <b>Locked</b> - The dashboard item cannot be assigned.</li> </ul>
<b>Chart layout</b>	Choose one of the following chart types: Single value, Table, Pie, Line, Bar, Area, Scatter. Depending on the query, not all choices can be available.
<b>Show legend</b>	Check to show a legend for the chart.

## Organization Unit visibility tab

Configure the scope of data that is available in the dashboard item. This tab is available only if the query scope is set for Organization Unit scope.

The following table lists the fields in the **Organization Unit visibility** tab.

Table 268. Organization Unit visibility tab fields

Field	Description
Name	Read only. The name of the Organization Unit scope.
Description	Read only. The description of the scope.
All entities of type Organization Unit with no selection	Choose to use all data from all entities of the Organization Unit.
Admin scope of Organization Unit with no selection	Choose to constrain the data for the dashboard item to the administrative scope of the Organization Unit. <b>Note:</b> An Admin Role that includes a dashboard item of this scope must have a scope of <b>Org Unit</b> . Set the Admin Role scope in <b>Access Governance Core &gt; Configure &gt; Admin Roles</b> in the <b>Scope</b> tab.

## Application visibility tab

Configure the scope of data available in the dashboard item. This tab is available only if the query scope is set for Application scope.

Table 269. Application visibility tab fields

Field	Description
Name	Read only: the name of the Application scope.
Description	Read only: the description of the scope.
All entities of type Application with no selection	Choose to use all data from all entities of type Application.
Admin scope of Application with no selection	Choose to constrain the data for the dashboard item to the administrative scope of the Application. <b>Note:</b> An Admin Role that includes a dashboard item of this scope must also have a scope of <b>Application</b> . Set the Admin Role scope in <b>Access Governance Core &gt; Configure &gt; Admin Roles</b> in the <b>Scope</b> tab.


## Layout tab

Configure how columns are available and labeled in the dashboard item. A list of the columns that are defined by the query is shown. Configure information for each column.

Table 270. Layout tab fields

Field	Description
Selected columns	Select to show the column. Clear to hide the column.
Name	Read only: the name of the column. It is read from the query.

Table 270. Layout tab fields (continued)

Field	Description
Localization Code	The name of the localization code that corresponds to the column name. Click the information icon to the right to display the current list of localizations for the code. 

## Filters tab

Determine how filters are available in the dashboard item. A list of columns that are candidates for filters is shown.

Table 271. Filter tab fields

Field	Description
Visible	Check to allow the user to filter data by this column on the dashboard. The user sees <b>Filters</b> in the <b>Settings</b> menu for the dashboard item as it appears in the Service Center. Clear to disable filtering for this column
Mandatory	Read only. If checked, a filter must be set for this column.
Order	Select a filter column, then click the arrows to position it in the list. The order determines the axis assignment for the columns.
Name	Read only: the column to filter.
Localization Code	The name of the localization code that corresponds to the column name.
Value	Enter a value to constrain the query. For example, if the query object is <b>Accounts expiring in the next x days</b> , then specify the number of days to use to constrain the query for the dashboard item.
Type	Select the data type to display.
Description	Enter a description for the filter.
Custom Filters	If you set <b>Type</b> to <b>Custom</b> , you can choose a custom filter from the list.

## Localization

Configure localized strings for labels in the dashboard item. When you click **Localization** for a field, a dialog prompts you for the localized string to use for each language.

Table 272. Localization tab fields

Field	Description
Localization	The name of the dashboard item.

Table 272. Localization tab fields (continued)

Field	Description
Columns localization	A line appears for each column. The localization code and text is shown.
Filters localization	A line appears for each filter. The localization code and text is shown.

## Configure

Use the following functions for configuring the listed elements:

- Report Assignment
- Menu

### Report assignment

From this section, you can move to the Report/Dashboard-Entitlement and Entitlement-Report/Dashboard tabs.

#### Report/Dashboard-Entitlement

The **Report/Dashboard > Entitlement** tab (left), contains the list of inventoried reports and filters for the Report search.

The table below summarizes the filters (clicking the **Filter/Hide Filter** button) available for the Report search:

Table 273. Report filters.

Filter	Description
Name	Name of the report.
Code	
Status	Available report status: <ul style="list-style-type: none"> <li>• Assigned</li> <li>• Locked</li> <li>• New</li> </ul>
Category	Category of the report.
Display Type	Display types of the report: <ul style="list-style-type: none"> <li>• Report</li> <li>• Dashboard</li> </ul>

The same frame lists the results according to the following attributes:

Table 274. Report attributes.



Name	Description
Name	Name of the report. An icon is present near the item name, depending on the type of item: <ul style="list-style-type: none"> <li>•  for a product item.</li> <li>•  for a custom item.</li> </ul>



Table 274. Report attributes. (continued)

Name	Description
Status	Available report status: <ul style="list-style-type: none"> <li>• <b>Assigned</b></li> <li>• <b>Locked</b></li> <li>• <b>New</b></li> </ul>
Report Category	Category of the report

After creating a report, the administrator can assign it to a user.

The administrator can also assign reports to an application role (IT Role, Business Role) as permission-type entitlements. When a report is selected, the entitlements already assigned to that report are displayed in the **Assignment** tab.

If you click **Add** in the **Assignment** tab, the **Entitlements** panel is displayed and enables you to search (clicking **Filter**) and associate new entitlements with the report. The following table lists and describes the assignable entitlement filters.

Table 275. Assignable entitlement filters.

Filter	Description
<b>Application</b>	Application name: Entitlements filtered mainly according to the specified application.
<b>Name</b>	Name of assignable entitlement: matches with the application entitlements inventoried in the AG Core Module.
<b>ID Code</b>	
<b>Type</b>	Entitlement type: <ul style="list-style-type: none"> <li>• <b>IT Role</b></li> <li>• <b>Business Role</b></li> </ul>

## Entitlement->Report/Dashboard

The **Entitlement > Report/Dashboard** tab (left) contains the list of entitlements and filters for the entitlement search.

The table below summarizes the available filters for the entitlements search:

Table 276. Entitlement filters.

Filter	Description
<b>Application</b>	Application name: Entitlements filtered mainly according to the specified application.
<b>Name</b>	Name of assignable entitlement: matches with the application entitlements inventoried in the AG Core Module.
<b>ID Code</b>	
<b>Type</b>	Entitlement type: <ul style="list-style-type: none"> <li>• <b>IT Role</b></li> <li>• <b>Business Role</b></li> </ul>

In the same tab are listed the results, according to the **Name** (Entitlement name) and **Application** (Application name) attributes. After selecting an entitlement from the list, the **Assignment** tab displays the reports that are already assigned to that entitlement.

If you click **Actions > Add** in the **Assignment** tab, the **Reports/Dashboard** panel is displayed and enables you to search (clicking **Filter**) and associate new reports to the entitlements. The following table lists and describes the assignable report filters:

*Table 277. Assignable Reports filters.*

Filter	Description
<b>Name</b>	Name of the report.
<b>Code</b>	
Status	Available report status: <ul style="list-style-type: none"> <li>• <b>Assigned</b></li> <li>• <b>Locked</b></li> <li>• <b>New</b></li> </ul>
Category	Category of the report.
<b>Display Type</b>	Display types of the report: <ul style="list-style-type: none"> <li>• <b>Report</b></li> <li>• <b>Dashboard</b></li> </ul>

## Report-Entitlement tab

The **Report > Entitlement** tab (left), contains the list of inventoried reports and filters for the report search.



The table below summarizes the filters available for the Report search:

*Table 278. Report filters*

Filter	Description
Name	Name of the report.
Description	Brief description of the report.
Status	Available report status: <ul style="list-style-type: none"> <li>• Assigned</li> <li>• Locked</li> <li>• New</li> </ul>
Report Category	Category of the report.

The same frame lists the results according to the following attributes:

Table 279. Report attributes.

Name	Description
Name	Name of the report. An icon is present near the item name, depending on the type of item: <ul style="list-style-type: none"> <li> for a product item.</li> <li> for a custom item.</li> </ul>
Status	Available report status: <ul style="list-style-type: none"> <li>Assigned</li> <li>Locked</li> <li>New</li> </ul>
Report Category	Category of the report

After creating a report, the administrator can assign it to a user.

The administrator can also assign reports to an application role (IT Role, Business Role) as permission-type entitlements. After selecting a report from the list, the **Assignment** pane automatically displays the entitlements already assigned to that report.

Clicking **Add**, the **Entitlements** panel that displays, showing the list of the available entitlements and allowing the RD administrator to perform a search and aggregate new entitlements to the report. Each search produces a list of results. The following table describes the assignable entitlement filters:

Table 280. Assignable Entitlement filters.

Filter	Description
Application	Application name: Entitlements filtered mainly according to the specified application.
Name	Name of the assignable entitlement: Matches with the application entitlements inventoried in the AG Core Module.
Type	Entitlement type: <ul style="list-style-type: none"> <li>IT Role</li> <li>Business Role</li> </ul>

## Report search

Proceed as follows:

1. In the **Report > Entitlement** tab, click **Filter/Hide Filter**.
2. Set the Report filters and click **Search**.
3. The results are displayed in the same pane.

## Assigned entitlements search

Proceed as follows:

1. Perform a **Report Search**.

2. Choose the desired report from the list of results.
3. The **Assignment** tab lists all entitlements associated to the selected report.

### Assign entitlement to a report

Proceed as follows:

1. Perform a **Report Search**.
2. Choose the desired report from the list of results.
3. Click **Add**, in the **Entitlements** window that opens, set the filters and click **Search**.
4. Select the desired entitlement from the results list and click **Ok**.

The **Assignment** tab displays the assigned entitlement.

### Remove assigned entitlements

Proceed as follows:

1. Perform an **Assigned Entitlements Search**, then select the entitlement to remove (use the [Ctrl] or [Shift] keys for multiple selections).
2. Click **Remove**.
3. Click **Ok** to confirm.
4. Click **Ok** in the window displaying the operation outcome.

**Note:** After removing an entitlement, all users having that entitlement will no longer be able to use the report associated to that entitlement.

### Entitlement-Report tab

The **Entitlement > Report** tab (left) contains a list of entitlements and filters for the entitlement search.

The table below summarizes the available filters for the Entitlements search:

*Table 281. Entitlement filters.*

Filter	Description
Application	Application name: Entitlements filtered mainly according to the specified application.
Name	Name of the assignable entitlement: matches with the application entitlements inventoried in the AG Core Module.
Type	Entitlement type: <ul style="list-style-type: none"> <li>• IT Role</li> <li>• Business Role</li> </ul>

The same frame lists the results, according to the **Name** (Entitlement name) and **Application** (Application name) attributes.

After selecting an entitlement from the list, the **Assignment** tab displays the reports that are already assigned to that entitlement.

Clicking **Add**, the **Reports** window that opens, displaying the list of available reports and allowing the RD Administrator to perform a search and associate a

new report to the entitlements. Each search produces a list of results. The following table describes the assignable reports filters:

*Table 282. Assignable reports filters.*

Filter	Description
Name	Name of the report.
Description	Brief description of the report.
Status	Available report status: <ul style="list-style-type: none"><li>• Assigned</li><li>• Locked</li><li>• New</li></ul>
Report Category	Category of the report.

### Entitlement search

Proceed as follows:

1. In the **Entitlement > Report** tab (left), click **Filter/Hide Filter**.
2. Set the Entitlement filters and then click **Search**.
3. The results are displayed in the same frame.

### Assigned report search

Proceed as follows:

1. Perform an **Entitlement search**.
2. Choose the desired entitlement from the list of results.
3. The **Assignment** tab lists all reports associated to the selected entitlement.

### Assign report to an entitlement

Proceed as follows:

1. Perform a **Report Search**.
2. Choose the desired Report from the list of results.
3. Click **Add**, in the **Reports** window that opens, set the filters and click **Search**.
4. Select the desired report from the results list and click **Ok**.

The **Assignment** tab displays the assigned report.

### Remove assigned report


Proceed as follows:

1. Perform an **Assigned Report search**, then select the report to remove (use the [Ctrl] or [Shift] keys for multiple selections).
2. Click **Remove**.
3. Click **Ok** to confirm.
4. Click **Ok** in the window displaying the operation outcome.

## Menu

In this section, the RD administrator can categorize reports into folders.

The administrator can only add to a folder reports with a specific status (see Assigned Status).

The **Reports** tab lists the available reports. If the reports have the icon  , it means that the report has already been added to a folder.

In the **Folder Menu** tab, the RD administrator can modify the folder hierarchy and the report position.

The administrator must create and add the first folder to the root folder. The administrator can then create and add new folders below the first.

The RD administrator can:

- Only add a report to a folder, not to its sub-folders.
- Only add a report to a single folder.
- Always place a report as a hierarchy leaf.




You can use the following filters to search specific reports:

*Table 283. Report filters.*

Filter	Description
Name	Name of the report
Description	Brief description of the report
Status	Available report status: <ul style="list-style-type: none"> <li>• Assigned</li> <li>• Locked</li> <li>• New</li> </ul>

The report search produces results based on the following attributes:

*Table 284. Report attribute.*

Attribute	Description
Name	Name of the report. An icon is present near the item name, depending on the type of item: <ul style="list-style-type: none"> <li>•  for a product item.</li> <li>•  for a custom item.</li> </ul>
Status	Available report status: <ul style="list-style-type: none"> <li>• Assigned</li> <li>• Locked</li> <li>• New</li> </ul>
Menu	 Report is associated to a folder.

The RD administrator needs to locate newly created folders to find easier a desired report.

From the **Folder Menu** tab, the administrator can locate a folder using the **Localize** button.

The administrator needs to categorize all reports of an entitlement.

After creating a folder, it will have the following label: [dir.34908187xxxxxxxxExx]; where:

**dir** Is the directory.

**code number**

Is the number of directory.

The administrator could locate the folder with the name "Entitlement Reports." This feature is particularly useful when the data model elements do not have names easy to understand.

**Note:** The RD Administrator can select localization languages from the **Languages** button in the Edit Labels section.

When the administrator creates folders containing reports, the user requesting the reports will see the following:

*Figure 130. Categorizing of reports into folders.*

In the figure above:

- The blue rectangle contains reports that the user has requested, but because the reports are not in any folder yet, searching for a specific report is difficult.
- The red rectangle contains reports that the user has requested. In this case, though, the reports are in the **Risks** folder, which makes searching for a specific report much easier.

For example, to find reports regarding the User Risk Count, you can simply open the **Risks** folder and find easily the report "User Risk Count".

## Report search

Proceed as follows:

1. In the **Reports** tab, click **Filter/Hide Filter**.
2. Set the Report filters and then click **Search**.
3. The results are displayed in the same pane.

## Add directory (Create folder)

Proceed as follows:

1. From the **Folder Menu** tab, select the **Root** folder.
2. Click **Add dir**.

The new folder is automatically created and is associated to the Root folder.

After creating the first folder, the administrator can associate it to another folder, performing the same **Add dir** operation.

## Locate folder

Proceed as follows:

1. Add a directory. Then, from the **Folder Menu** tab, select the desired folder.
2. In the same pane, click **Localize**.
3. In the window Localization that is displayed, enter the desired localization text.
4. Click **Ok** in the window showing the operation outcome.

## Remove folder

Proceed as follows:

1. From the **Folder Menu** tab, select the desired folder.
2. In the same pane, click **Remove**.
3. In the Warning window that is displayed, click **Ok** to confirm the operation and close the window.

### Note:

The RD administrator can only remove folders that do not contain nested directories.

If the administrator wants to remove a folder with nested directories, the nested directories must be deleted first.

## Add report to a folder

Proceed as follows:

1. Perform a **Report Search**.
2. From the **Reports** tab, select the desired reports.
3. In the **Folder Menu** tab, select the target folder, then, in the **Reports** tab, click **Add**.

This automatically associates the report to the target folder.

## Remove report from a folder

Proceed as follows:

1. From the **Folder Menu** tab, click on the desired folder to display the reports added to the folder.
2. Choose the report to remove, and click **Remove**.
3. Click **Ok** in the Warning window to confirm the operation.

This automatically removes the report from the folder.

---

## Settings

The following functions are available for setting values of some elements of the module:

- Edit Labels
- System Entities
- Scopes
- “Custom filters” on page 541



**Note:**

Only an experienced administrator can perform the operations available in this section of the RD module.

Inappropriate changes to any configuration in this section can degrade the performance of the report designer module.

## Edit labels tab

In this section, the RD administrator can associate a specific localization code to the messages available for all languages.

In the **Localization codes** tab, the localization codes registered by the system are listed.

The RD administrator can use the following filters to search for the localization codes:

*Table 285. Localization Code filters.*

Filter	Description
Code	Name of the localization code.
Message	Text contained in the "message" section.
Language	Localization code language.
No Localization	When selecting this check box, you can search for localization codes which is not localized.

In the right pane, there are some tabs that correspond to the languages available. When a localization code on the right is selected, the first tab that opens, represents the default language sets.

By default, the language tabs always display the **Code** and **Localized message** fields.

In the right pane, clicking **Languages** opens a window and allows the administrator to modify the default language used to load the label groups associated with the different application objects.

The Languages in use (Browser) text box displays the language that is currently set for the browser. The Default Language text box displays the language that is currently set.


To modify the language, proceed as follows:

1. Click **Change** near the Default Language text box.
2. Select one of the languages from the **Default Language** window that displays.
3. Click **Ok** to confirm the selected default language.

To add languages in the list of available languages (from right to left), proceed as follows:

1. Select the desired language from the available languages list box on the right.
2. Click **Add to Table on Left** to move the selected language into the languages in use list box on the left.

To remove a language from the list of languages in use (from left to right), proceed as follows:

1. Select the desired language from the languages in use list box on the left.
2. Click  **Remove Languages** to move the selected language into the available languages list on the right.

Every operation described in this section is automatically saved.

**Note:**

Languages found in the Languages in Use list box match with those available in the Localization phase.

The settings described in this section are not related to the language settings of the browser.

The browser language settings affect the labels on the tab bar only.

To edit a localized message, proceed as follows:

1. In the **Localization codes** tab, select the desired code.
2. The tab on the right displays the **Code Name** and **Localized Message** in the default language chosen in the Language in Use window.
3. In the same pane, modify the localized message.
4. Click **Save**.

## System entities

In this section, the RD administrator can manage the system entity keys used to write the query.

The RD administrator can use the following filters to search for entity keys (clicking **Filter/Hide Filter**):

*Table 286. Entity Key Filters.*

Filter	Description
Name	Name of the entity key.
Reference Entity	This field is fixed and cannot be modified. System is the only reference entity.

The table below describes the four message localization attributes in the **Entity Key Details** tab:

*Table 287. Entity Key Details.*

Attribute	Description
Reference Entity	System is the only reference entity.
Name	Name of the entity key.
Value	Name of one of the available realms to be deployed.
Description	Brief description of the entity key.

## Edit entity keys

Proceed as follows:

1. In the **Entity Keys list** tab, select the desired key. The **Entity Key details** tab displays details of the selected entity key.
2. In the same tab, modify the entity key details.
3. Click **Save**.

## Add an entity key

Proceed as follows:

1. In the **Entity Keys list** tab, click **Add**.
2. In the **Entity Key details** tab, insert the **Localized Message** details.
3. Click **Save**.

## Remove an entity key

Proceed as follows:

1. In the **Entity Key list** tab, select the entity key to remove.
2. In the same pane, click **Remove**.
3. Click **Ok** to confirm the operation.

## Scope

In this section, the RD administrator can create scopes.

The **Scope List** tab, contains scopes that the RD administrator can associate to queries.

The administrator can also perform scope searches using the filters **Name** and **Description** (click **Filter/Hide Filter** ).

The same frame lists the results according to the following attributes:

*Table 288. Scope search attributes.*



Attribute	Description
Name	Scope name. An icon is present near the item name, depending on the type of item: <ul style="list-style-type: none"><li>•  for a product item.</li><li>•  for a custom item.</li></ul>
Description	Brief scope description (maximum 256 characters).

Table 288. Scope search attributes. (continued)

Attribute	Description
Entity	Scope entity: <ul style="list-style-type: none"> <li>• <b>Application</b></li> <li>• <b>Entitlement</b></li> <li>• <b>Org_Unit</b></li> <li>• <b>PwdCfg</b></li> <li>• <b>Resource</b></li> <li>• <b>System</b></li> <li>• <b>Task</b></li> <li>• <b>User</b></li> </ul>

In the **Scope Details** tab, the RD Administrator can create the desired scope according to the following attributes:

Table 289. Scope Details

Detail	Description
<b>Name</b>	Scope name.
<b>Description</b>	Brief scope description (maximum 256 characters).
<b>SQL Query</b>	Query text.
<b>Reference Entity</b>	Scope entity: <ul style="list-style-type: none"> <li>• <b>Application</b></li> <li>• <b>Entitlement</b></li> <li>• <b>Org_Unit</b></li> <li>• <b>PwdCfg</b></li> <li>• <b>Resource</b></li> <li>• <b>System</b></li> <li>• <b>Task</b></li> <li>• <b>User</b></li> </ul>

## Scope search

Proceed as follows:

1. In the **Scope List** tab, click **Filter/Hide Filter**.
2. Set the filter data (**Name**, **Description**), then click **Search**. The results are displayed in the same pane.

## Create scope

Proceed as follows:

1. Perform the scope search.
2. In the **Scope List** tab, click **Actions > Add**.
3. In the **Scope Details** tab, set the scope attributes.
4. Click **Save** to save the scope and add it in the **Scope List** tab.

For help about the query processing, click **Help** in the **Scope Details** tab.

## Modify scope

Proceed as follows:

1. Perform the scope search and select the scope to modify.
2. In the **Scope Details** tab, modify the scope.
3. Click **Save**.

## Remove scope

Proceed as follows:

1. Perform the scope search.
2. In the **Scope List** tab, select the desired scope and click **Remove**.
3. A Warning window displays a message about the effects of the operation.
4. Click **Ok** to confirm the operation.

### Note:

Removing a scope results in the loss of its visibility configuration. The tmp table is still part of the query but contains no data.

After removing a scope from the selected query, all aggregations with any other query are lost.

## Custom filters



In this section, the RD administrator can customize filters.

The **Custom Filters** tab, contains the list of available custom filters that the RD administrator can associate to the report.

The administrator can also perform a custom filter search using the **Name** (filter name) and the **Description** (brief filter description) filters by clicking **Filter/Hide Filter**.

The same pane lists the results according to the following attributes:

Table 290. Custom Filter Attributes.

Name	Description
Name	Scope name. An icon is present near the item name, depending on the type of item: <ul style="list-style-type: none"><li>•  for a product item.</li><li>•  for a custom item.</li></ul>
Description	Brief scope description (maximum 256 characters).

In the **Filter details** tab, the RD Administrator can create the desired filters according to the following attributes:

Table 291. Filter details.

Name	Description
Name	Scope name.
Description	Brief scope description (maximum 256 characters).
SQL Query	Query text.

## Create custom filters

Proceed as follows:

1. In the **Custom Filters** tab, click **Add**.
2. In the **Filter details** tab, set the filter detail attributes.
3. Click **Save** to save the filters in the **Custom Filters** tab.

For help about query processing, click Help in the same pane.

## Modify custom filters

Proceed as follows:

1. In the **Custom Filters** tab, select the custom filter to modify.
2. In the **Filter details** tab, modify the filter detail attributes.
3. Click **Save**.

## Remove custom filters

Proceed as follows:

1. In the **Custom Filters** tab, select the custom filter to remove.
2. Click **Remove**.
3. Click **Ok** to confirm the operation.

**Note:** The RD administrator cannot remove the product  custom filters.

---

## Monitor

The functions that are available for monitoring some elements are contained in the following list.

### Report queue

After the report is run, the RD administrator can check the report status and the report download.

The table below lists the different report execution statuses:

Table 292. Report execution statuses.

Execution status	Description
Pending	Report execution is pending.
Running	Report is in execution.
Download	Report is ready to be downloaded.

Table 292. Report execution statuses. (continued)

Execution status	Description
Error	Error during the report execution.

The **Report Property** pane (bottom) displays properties of the report, as described in the table below:

Table 293. Report properties.

Properties	Description
Name	Name of the key: <ul style="list-style-type: none"> <li>• Report name</li> <li>• Application</li> <li>• Language</li> <li>• File format</li> <li>• User ID</li> </ul>
Description	Description of the key.
Value	Value of the key.

**Note:** A Report with Download status is available for download until it is deleted.

The following figure shows a sample report in **XLSX** format (User imported report) :

ID	IDEAS ID	Deleted	User ID	First Name	Surname	Employment type	User Status	User type	Position
51164	83491	0	s25140	Sandra	Strecher	I	A	primary	staff@34:34000:50037950
51165	83492	0	s25488	Oi Yan	Fung	I	A	primary	staff@34:34000:50037837

Figure 131. Report sample: User removal.





---

## Chapter 20. Introduction to Task Planner

Task Planner (TP) module is a scheduler that helps you manage asynchronous processes that can be performed at a future time.

An example of these types of processes is the production of a set of reports.

These processes usually involve massive interrogations of one or more databases and might require a relatively long time. They are therefore preferably run at night when the system is not used for ordinary operations.

The IBM Security Identity Governance and Intelligence Task Planner is based on the job concept. A job describes an executable function, such as a massive database update, and is distinguished by the following triad:

- Name
- Java class
- Set of parameters

A single-job-based approach does not usually allow for execution of complex functions. In some cases, it might be convenient to have a load-balancing mechanism to allocate parts of the processing operation to other machines.

The IBM Security Identity Governance and Intelligence Task Planner effectively provides for the following requirements:

- Simple single-job writing capabilities.
- Ability to describe even the most complex relations between different jobs.
- Transparency and flexibility in time-limited job scheduling.
- Load-balancing in the system running a job set.

---

### Architecture and components

This section describes the main task planner components.

The IBM Security Identity Governance task planner consists of four components:

- Hibernate framework
- Scheduler engine
- EJB layer
- Application

#### Hibernate framework

Hibernate is an ORM (Object Relational Mapping) framework that manages information persistence in the database. ORM is a group of management methods and techniques that integrate an object-oriented paradigm into the relational paradigm of a relational database management system (RDBMS). The objective of ORM is to program the relational database interaction using a purely object-oriented paradigm, concealing a relational paradigm translation from the developer. For more information on Hibernate, see: <http://www.hibernate.org>

## Scheduler engine

The scheduler engine is the core component of the system; it hosts the task planner basic framework, based on the Quartz library. This layer mainly provides all the internal services used by the EJB layer. Quartz is a full-featured, Open Source Job scheduling system that can be integrated with or used with any J2EE or J2SE application. From the smallest stand alone application to the largest system.

Quartz can be used to create simple or complex schedules, executing up to tens of thousands of jobs. The Quartz Scheduler includes many enterprise-class features, such as JTA transactions and clustering. For more information on Quartz, see: <http://quartz-scheduler.org/>

IBM Security Identity Governance Task Planner is perfectly compliant with Quartz Jobs. Default jobs (bundled with the IBM Security Identity Governance platform) as well as custom jobs can therefore be used with the Quartz interface.

## EJB layer

The EJB layer hosts the task planner module basic components: job classes, jobs and tasks.

## Application

This layer is mainly composed of a:

- Front end Administration Module (entirely documented in this manual).
- Back end IBM Security Identity Governance jobs set, which provides the task planner common functions based on the EJB layer.

Use the product jobs for managing the IBM Security Identity Governance platform common activities.

You can define third-party jobs.

---

## Guide to task modeling

The IBM Security Identity Governance task planner distinguishes among three main concepts: job class, job and task.

The job class is a single unit of code (generally a Java class method) that must be run. Every operation executed by the scheduler must implement the job interface and the associated execute method, according to the Quartz library guidelines.

Each individual job can be defined by a set of job class parameters needed to perform that job. Therefore, every job is characterized by a set of job class attributes.

A task can be composed of a single job or a set of jobs.

### The task structure

The task is the main unit managed by the IBM Security Identity Governance task planner.

A task can be built on:

- A single job (a tree with a single node).
- A list of jobs (a tree with a single level of nodes).
- A tree-hierarchy of jobs.

Running a task composed of a single job means running that job.

If a task is composed of a list of jobs, the task starts running when the first job in the list begins, and ends when the last job in the list terminates.

If a task is composed of a tree of jobs, it proceeds by running any job in the hierarchy according to the predefined order.

Generally, the execution of a child node begins when the execution of the parent node ends. After the jobs are added to a task, their execution type needs to be defined, for example the job behavior.

You can choose between the following:

- Start if parent OK: Job starts if parent completed successfully.
- Start if parent KO: Job starts if parent failed.

## Task status

Three different status characterize a task:

- **Start** (Active)
- **Inconsistent**
- **Stop** (Inactive)

### Start (Active) status

If the task is running (for example, the task is active), the associated jobs are enqueued and will be run according to the task time planning attributes. The set of jobs associated with a task can be structured as follows:

- A single job.
- A list of jobs.
- A hierarchy of jobs.


The time planning attributes are applied to the first job of the task.

If the first job is structured as a job list, the time planning attributes are associated with the first job of the list. The other jobs are subsequently scheduled as indicated in the list.


For example, Job K begins running only after Job K-1 has finished.

If the task is structured as a composite set of Jobs, executing any level of nodes depends on the execution type of the parent job.

### Inconsistent status

A task is characterized as  inconsistent when a misalignment between the task planner module and the scheduler engine occurs. This misalignment might be

caused by unpredictable external problems. A task can be restored to its original condition using the synchronization process, which synchronizes all tasks aggregated to a scheduler.

It primarily reactivates tasks that were  active before the misalignment, where no action is taken for the tasks that were  inactive.

### Stop (Inactive) status

After entering the stop state, a scheduler will try to stop all currently running jobs. Any job queued after that time will be discarded. Other jobs cannot be queued until the scheduler reenters the Start state.

---

## How to implement a new job

This section provides the basic elements needed to understand how to implement and deploy a new job.

Any job to be used in the IBM Security Identity Governance task planner must be structured according to the Quartz guidelines (<http://quartz-scheduler.org/>).

### General job structure

The following example shows the general structure of a job:

```
public class Test extends ACrossJob {  
  
    @Override  
  
    public List<WorkPropBean> getInitPropertyList() {  
  
        // TODO Auto-generated method stub  
  
        return null;  
  
    }  
  
    @Override  
  
    public boolean execute(Properties workProperties, StopProcess stopObject) throws  
        Exception {  
  
        // TODO Auto-generated method stub  
  
        return false;  
  
    }  
  
    @Override  
  
    public void interrupt() throws Exception {  
  
        // TODO Auto-generated method stub  
  
    }  
  
}
```

```
}
```

Parameters list of a job

Job parameters can be specified through the method `List<WorkPropBean> getInitPropertyList()`:

```
public List<WorkPropBean> getInitPropertyList() {  
  
    List<WorkPropBean> result = new ArrayList<WorkPropBean>();  
  
    WorkPropBean message = new WorkPropBean();  
    message.setType(WorkPropType.STRING.getValue());  
    message.setRequired(false);  
    message.setName("Message");  
    message.setValue("Hello World!");  
    message.setDescription("System out message");  
    result.add(message);  
  
    WorkPropBean exception = new WorkPropBean();  
    exception.setType(WorkPropType.INT.getValue());  
    exception.setRequired(false);  
    exception.setName("Exception");  
    exception.setValue("0");  
    exception.setDescription("set value 1 if you want an exception ");  
    result.add(exception);  
  
    WorkPropBean wait = new WorkPropBean();  
    wait.setType(WorkPropType.INT.getValue());  
    wait.setRequired(false);  
    wait.setName("Wait");  
    wait.setValue("0");  
    wait.setDescription("Time wait before continue");  
    result.add(wait);  
  
    return result;  
  
}
```

Parameters specified here are configured using the Task Planner web interface.

Three parameters are specified in this example: message, exception and wait.

Five elements of information must be specified for every parameter:

- Type (setType)
- Specifies if the parameter is mandatory (setRequired, where the value *false* means that it is not mandatory to set this parameter and a default value is provided)
- Name (setName)
- Value (setValue)
- Description (setDescription).

## Managing job execution

Job execution is managed using the method `public boolean execute (Properties inputParameters , StopProcess stopProcess )`:

```
public boolean execute(Properties inputParameters, StopProcess stopProcess)
throws Exception {
```

```
Integer wait = (Integer) inputParameters.get("Wait");
```

```
if (wait != null && wait > 0) {
```

```
try {
```

```
Thread.sleep(wait);
```

```
} catch (InterruptedException e) {
```

```
e.printStackTrace();
```

```
}
```

```
}
```

```
// you can use this mode to check if the process is stopped:
```

```
stopProcess.throwExceptionifStopped();
```

```
// or this other one:
```

```
if (!run) {
```

```
throw new Exception("Interrupted Process!!!");
```

```
}
```

```
Integer ex = (Integer) inputParameters.get("Exception");
```

```
if (ex == null || ex == 0) {
```

```
System.out.println("[SystemOUTJob] message: " + inputParameters.get("Message"));
```

```

} else {

throw new Exception("Test exception");

}

return false;

}

```

The parameters indicated in `getInitPropertyList ()` are provided with `inputParameters`.

The `stopProcess` parameter takes care of terminating execution.

If the return value is `true`, the job is automatically restarted after the current execution terminates. This behavior might be useful when you need to loop a job, but this requires a dedicated subset of code lines to manage the job behavior.

If the return value is `false`, the job is terminated.

## Job interruption

In order for the Task Planner to interrupt a job execution, the method `public void interrupt ()` must be used:

```

boolean run = true;

public void interrupt() throws Exception {

// You can use StopProcess Object in the execute method instead of this...

run = false;

}

```

A set of code lines can be specified in the body of the method to manage interruptions.

## How to deploy the new job

When the new job is ready, it takes the form of a JAR named `MyCustomJob.jar`.

To deploy this new job, perform the following steps using the Task Planner web interface:

1. Stop the Application Server
2. Save `MyCustomJob.jar` in the directory:
  - `/opt/IBM Security Identity Governance/jboss-6.1.0.Final/IBM Security Identity GovernancePlatformEnvCustom/lib`
3. Start the Application Server

## How to configure the new job

After the deployment, use the Task Planner web interface to:

- Add the new job class and define the job parameters.

- Build a task using the newly added job.
- Schedule the task.

## Manage

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

- Jobs
- Tasks

## Jobs

In this section, the administrator can add jobs and configure job class attributes.



The **Jobs** tab displays the jobs listed in the system. You can search for specific jobs using the filters described below (click **Filter/Hide Filter** and click **Search**):

*Table 294. Job filters.*

Filter	Description
Name	Name of the job.
Job classes	Name of the job class.
Context	Task group.

The job pane lists the results according to the following attributes:

*Table 295. Job attributes.*

Attribute	Description
Used	Job status:  : Job assigned to one or more tasks  : Job not assigned to any task
Name	Name of the job.
Job classes	Name of the job class.

In the **Actions** menu, all available buttons for managing jobs are listed below:

- **Add**: Allows you to add a job.
- **Remove**: Allows you to delete a job.

The contents of the right pane changes depending on the tab selected in the upper side of the pane. The **Details** tab is active by default:

*Table 296. Job details.*



Detail	Description
Name	Name of the job.
Job class	Name of the job class .
Context	Task group.
Description	Brief job description (maximum 256 characters).



**Note:** For a **Used Job** (✔) the Remove button is disabled. To remove it, the job must first be removed from all tasks. A Used Job cannot be modified unless it is first removed from all tasks.

In the **Details** tab, click the **Edit** tab (bottom of the pane) to edit a job and configure the following job class parameters:

Table 297. Job Class parameters.

Parameter	Description
Mandatory	This field is distinguished by:  : a parameter value is mandatory.  : a parameter value is not mandatory.
Name	Name of the job class attribute.
Type	Type of the job class attribute.
Value	Value of the job class attribute.
Mode	Status of the value: <ul style="list-style-type: none"> <li>Modifiable : Value modifiable in tab <b>Manage &gt; Task &gt; Jobs</b>.</li> <li>Not Modifiable : Value not modifiable.</li> </ul>
Description	Brief name/value description (maximum 256 characters).

The list below shows the main job-related operations:

- Tasks
- History

## Tasks

From the **Jobs** web interface, select a (✔) Used Job and click on the **Task** tab to view the task associated to the job. The following filters are used to perform a task search (click **Filter/Hide Filter**):

Table 298. Task filters.

Filter	Description
Name	Name of the task.
Context	Task groups.
Scheduler	Scheduler that executes the task.

Select the desired task and, from the **Actions** menu, click **Task**. This enables the **Manage > Tasks** tab. The desired task can be quickly configured.

## History

From the **Jobs** web interface, select a (✔) Used Job and click on the **History** tab to view the scheduling results of a job assigned to a specific type of task. This is only


possible for the  Active Task , whose scheduling has already begun and ended. The following filters are used to perform a task search (click **Filter/Hide Filter**):

Table 299. History filters.

Filter	Description
Scheduler	Scheduler that executes the task.
Task	Scheduled task.
Start Date from	Start date of the task from a specific date.
Start Date to	Start date of the task to a specific date.
Results	Tasks results: <ul style="list-style-type: none"> <li>Completed: search only successfully completed tasks.</li> <li>Error: search only tasks that have generated errors.</li> </ul>

In the **Actions** menu, all available buttons for managing the jobs history are listed below:

- **Task**: allows you to go to the **Manage > Tasks** tab quickly.
- **Remove**: allows you to remove one or more history results.
- **Clear All**: allows you to clear all history results.

From the **Actions** menu, clicking **Task** enables the **Manage > Tasks** tab.

## Tasks

In the task planner module, the administrator can create and configure tasks, define job class parameters, and configure scheduling.




Here the administrator can manage tasks that are listed in the system. You can search specific jobs using the filters displayed below by clicking **Filter/Hide Filter** and by clicking **Search**:

Table 300. Task filters.



Filter	Description
<b>Name</b>	Name of the task.
<b>Context</b>	Task groups.
<b>Scheduler</b>	Scheduler that executes the task.

The **Task** search tab lists results according to the following attributes:

Table 301. Task attributes.

Attribute	Description
Active	Task status displayed by one of the following icons:  : <b>Active Task</b>  : <b>Inactive Task</b>  : <b>Inconsistent Task</b>
Name	Name of the task.
Context	Task group.
Scheduler	Scheduler that executes the task.

In the **Actions** menu, all available buttons for managing the tasks are listed:

- **Monitor:** for monitoring the selected task scheduling ( **Active Tasks** only).
- **Start/Stop:** starts or stops a task.
- **Add:** adds tasks.
- **Remove:** deletes tasks ( **Inactive Task** only).


**Note:** When you add a task, you must fill the **Name** and **Scheduler** fields.


In the **Details** tab, click the **Edit** tab to edit the following task details:

Table 302. Task details.

Detail	Description
<b>Name</b>	Name of the task.
<b>Scheduler</b>	Scheduler that executes the task.
<b>Context</b>	Task groups.
<b>Enable History</b>	If this check box is selected, the scheduling history is available.
<b>Description</b>	Brief task description.

**Note:**

For an  **Active Task**, the **Remove** button is disabled. To remove it, the task must first be stopped.

An  **Active Task** cannot be modified unless it is first stopped.

The list below describes the main task related operations:

- **Jobs**
- **Scheduling**
- **History**

## Jobs

In the **Task** web interface, select a task in the left pane and click the **Jobs** tab on the right to view the task structure and the job components.

Here you can modify a task already built.


In the **Actions** menu, all available buttons for managing jobs are listed below:

- **Move Up**: allows you to move up a job.
- **Move Down**: allows you to move down a job.
- **Add**: allows you to add or associate a new job.
- **Remove**: allows you to remove a job.

After the selection of a task in the left pane, click **Add** to choose the first job to be associated to the selected task.

To produce a list of several jobs (a set of nodes positioned on the first level of the hierarchy), repeat the previous operation for several times.

To produce a tree of jobs, select any job in the hierarchy already present and, in the same tab, click **Add** to add the new chosen job as a child node of the previously selected parent node.

All operations described above are available for the  **Inactive Tasks** only.

After building the task, you can define the **Job Class** attribute values for any job of the task.



Select a job from the tree-structure. Then, in the pane on the right, click the **Edit** tab to enter the available attributes described in the following table:

Table 303. Job attributes.

Attribute	Description
<b>Name</b>	Name of the task.
<b>Job Class</b>	Name of the job class.
<b>Identifier</b>	Job identifier.
<b>Execution Type</b>	<p>In this field, select the job behavior:</p> <ul style="list-style-type: none"><li>• <b>Start if parent OK</b>: Job starts if parent completed successfully.</li><li>• <b>Start if parent KO</b>: Job starts if parent failed.</li></ul> <p>These selections are also available for all child nodes.</p>

For any job class, you can edit a set of parameters according as described in the next table:

Table 304. Job Class parameters.

Parameter	Description
<b>Mandatory</b>	This field is distinguished by:  : A parameter value is mandatory.  : A parameter value is not mandatory.
<b>Name</b>	Name of the job class attribute
<b>Type</b>	Type of job class attribute
<b>Value</b>	Value of job class attribute
<b>Description</b>	Brief name/value description (maximum 256 characters)

**Note:** During the configuration of the platform, the parameter `cacheTimeMinute` of the job **SystemRuleEngine**, is generally set to 0 (zero) as default value. When the platform it's ready to be set in production, it's better to change the value of `cacheTimeMinute` for getting a more efficient behavior of the rule engine. Proceed as follows:

1. Select the tab **Manage > Tasks**.
2. In the **Task** tab, select the Rule Engine item.
3. In the central frame select the **Jobs** tab and left double-click on **SystemRuleEngine** job.
4. In the rightmost frame, click the **Edit** tab.
5. Set the `cacheTimeMinute` to a value > 0 (a value of 600 minutes is recommended).

## Scheduling

In the **Task** web interface, select a task in the left pane and click the **Scheduling** tab on the right to view the task scheduling. Two options are available:

- **Simple Execution.**


Table 305. Simple execution attributes.

Attribute	Description
<b>Scheduling</b>	<b>Recurring:</b> If this check box is selected, the task is run recursively.
	<b># iterations:</b> If the check box <b>Recurring</b> is selected, this text area is disabled. If the check box <b>Recurring</b> is not selected, you can define the number of the execution repetitions.
	<b>Frequency:</b> Frequency of the task execution.
<b>First Start</b>	<b>Date:</b> Task execution date ( <i>dd /mm/yyyy</i> ).
	<b>Hours and Minutes:</b> Duration ( <i>hh:mm</i> ) of the task execution.

- **Advanced Execution.**

Table 306. Advanced execution attributes.

Attribute	Description	
<b>Scheduling</b>	<b>Recurring:</b> If this check box is selected, the task is run recursively.	
	<b># iterations:</b> If the check box <b>Recurring</b> is selected, this text area is disabled. If the check box <b>Recurring</b> is not selected, you can define the number of the execution repetitions.	
	<b>At the hour:</b> To set the hour of the task execution.	
	<b>At the minute:</b> To set the minute of the task execution.	
<b>Calendar scheme</b>	<b>Week Days</b>	If this radio button is selected, the task starts on selected week days (select the <b>Weekdays</b> check boxes).  The task start time is defined by <b>First Starts</b> (last row of the table).
	<b>Days of Month</b>	If this radio button is selected, the task starts: <ul style="list-style-type: none"> <li>• On specific days.</li> <li>• Never (<b>Clear All</b> button).</li> <li>• Every day (<b>Select All</b>).</li> <li>• On selected week days (select the <b>Weekdays</b> check boxes).</li> <li>• On the last day of the month.</li> </ul>
<b>First Starts</b>	<b>Date:</b> Date of the future task execution ( <i>mm/ dd / yyyy</i> ).	
	<b>Hours and Minutes:</b> Duration of the future task execution specified in hours and minutes ( <b>hh:mm</b> ).	

**Note:** When you try to modify the scheduling of an  **Active Task**, a warning message is displayed informing you that: The Scheduling of an active Task cannot be modified

## History

In the **Task** web interface, select a task in the left pane and click the **History** tab on the right to view the task scheduling results.


This is only possible for the  **Active Task** whose scheduling has terminated. The following filters are used to perform a task search (click **Filter/Hide Filter**):

Table 307. History filters.


Filter	Description
<b>Job</b>	Name of the job. Click  <b>Search Jobs</b> to choose a specific job.
<b>Start Date from</b>	Start date of the task from a specific date.
<b>Start Date to</b>	Start date of the task to a specific date.

Table 307. History filters. (continued)

Filter	Description
Results	Tasks results: <ul style="list-style-type: none"> <li>Completed: search successfully completed tasks only.</li> <li>Error: search tasks that have generated errors only.</li> </ul>

The following table summarizes the attributes of the task results:

Table 308. Task attributes.

Attribute	Description
Name	Name of the task.
Scheduler	Scheduler type.
Start Date	Scheduling start date.
Elapsed Time	Time of scheduling (starting from Start Date).
Message	This field is only populated when an error message displays.
Instance	Name of the host performing the job available when an error occurs.

In the **Actions** menu, all available buttons for managing the jobs history are listed:

- **Job:** to go to the **Manage > Jobs** tab quickly.
- **Clear All:** to clear all history results.
- **Remove:** to remove one or more history results.

In the **History** tab, click the **Jobs** button to enable the **Manage > Jobs** tab.

---

## Monitor

This section displays all task histories.

The **History** search tab displays all tasks listed in the system. You can search for a specific task using the filters displayed below by clicking **Filter /Hide Filter**:



Table 309. History filters.

Name	Description
Scheduler	Search by scheduler name.
Task	Search by task name.
Job	Search by job name.
Start date from	Start date of the task from a specific date.
Start date to	Start date of the task to a specific date.
Results	Tasks results: <ul style="list-style-type: none"> <li>Completed: search successfully completed tasks only.</li> <li>Error: search tasks that have generated errors only.</li> </ul>

In the **Actions** menu, all available buttons for managing jobs are listed below:

- **Job<**: allows you to go to **Manage>Jobs** tab quickly.
- **Task<**: allows you to go to **Manage>Tasks** tab quickly.
- **Clear All**: allows you to clear all history results.
- **Remove**: allows you to remove one or more history results.

In the same tab, selecting a  **Task**:

- Enables the **>Task** button in the **Actions** menu. Click it to enable the **Manage > Tasks** tab.
- Opens the task tree-structure, displaying the associated  /  jobs. Selecting a specific job enables the **>Job** button, in the **Actions** menu, which enables the **Manage > Jobs** tab.

---

## Settings

The following functions are available for setting values of some elements of the module:

- Scheduler
- Context

### Scheduler

In this section, the administrator can view the scheduler details and perform a scheduler synchronization.

The **Scheduler** search tab displays all schedulers listed in the system.



You can use the **Name** filter to perform a scheduler search by clicking **Filter/Hide Filter**.


In the **Actions** menu, all available buttons for managing jobs are described below:

- **Task**: allows you to go to the **Manage > Task** tab quickly.
- **Synchr.**: allows you to synchronize all tasks to the selected scheduler.

In the same tab, selecting a scheduler:

- Enables the **Task** button in the **Actions** menu. Click it to enable the **Manage > Tasks** tab and view the task associated to the selected scheduler.
- Enables the **Synchr.** button in the **Actions** menu. Click it for synchronizing all tasks associated to the selected scheduler.

The **Synchr.** button primarily reactivates tasks that were  active before the misalignment. No action is taken for tasks that were  inactive.

Synchronization reactivates  inconsistent tasks. Only active tasks can become inconsistent.

The **Details** tab shows information (**Name** and **Description**) about the selected scheduler. The five available schedulers are described in the table below:



Table 310. Scheduler Set.

Name	Description
System	This scheduler contains all system tasks critical to core system operations. This scheduler should be stopped only if strictly necessary.
Reports	This scheduler is intended to run the report task only. This task might be critical, affecting overall system performance. Reports can be launched without the possibility for checking the amount of data to be involved.
Connectors	This scheduler is intended to run connector tasks only. Connector tasks poll the connector worktable to find work items to be executed. Single connectors are scheduled in the connector configuration.
Singleton	This scheduler is intended to use one thread only. Use this scheduler for tasks to be run sequentially only.
Custom tables	This scheduler runs custom tasks that are developed to address very specific customer needs. Custom tasks are not controlled tasks and can therefore impact system performance.

The **Details** tab also displays the scheduler attributes. Information fields for each attribute are described in the table below:



Table 311. Scheduler attributes.

Name	Description
Name	Name of the scheduler attribute
Value	Attribute value
Description	Brief attribute description

The **History** tab displays the history of the selected scheduler.

The following filters are used to perform a task search by clicking **Filter/Hide Filter**:

Table 312. History filters.

Filter	Description
Task	Name of the task. Click  Search Tasks to choose a specific task.
Job	Name of the job. Click  Search Jobs to choose a specific job.
Start date from	Start date of the task from a specific date.
Start date to	Start date of the task to a specific date.
Results	Task results: <ul style="list-style-type: none"> <li>• Completed: search successfully completed tasks only.</li> <li>• Error: search tasks that have generated errors only.</li> </ul>

In the **Actions** menu, all available buttons for managing the history results are described below:

- **>Job**: allows you to go to the **Manage > Jobs** tab quickly.
- **>Task**: allows you to go to the **Manage > Tasks** tab quickly.
- **Remove**: allows you to remove one or more history results.
- **Clear All**: allows you to clear all history results.

From the **Actions** menu:

- By selecting a task, the **>Task** button is enabled. Click it to enable the **Manage > Tasks** tab and view the task associated to the selected scheduler.
- By selecting a job, the **>Job** button is enabled. Click it to enable the **Manage > Jobs** tab and view the job associated to the selected task.

## Context

In this section, the administrator can group tasks.

This feature is useful when data model elements do not have names easy to understand.

The **Context search** tab displays all contexts that are listed in the system. You can search specific context using the name filter by clicking **Filter/Hide Filter**.

In the **Actions** menu, all available buttons for managing context are described below:

- **Task**: allows you to go to the **Manage > Tasks** tab quickly and view the task associated to the selected context.
- **Add**: allows you to add a context.
- **Remove**: allows you to remove a context. All tasks associated to a removed context are available in the system again but are no longer grouped under that context.

If you click **Edit** (pane on the right), you can modify the **Name** and the **Description** of a context.

---

## Chapter 21. Request

The Reports frame on the left contains the assigned reports.

The Report Designer (RD) administrator can classify the available reports into a hierarchy of folders, labeled with specific names. Every folder can contain a specific set of reports (leaves of the hierarchy) or other folders.

For each folder, it is possible to repeat recursively this structure..

When the authorized user plans a report, they can configure some settings, organized into a Wizard composed of several steps. The available settings are provided according to the design outlined by the Administrator of the RD Module.

After the Report is configured, as the last step of the Wizard, click the **Execute** button. A complete overview of the configuration actions is shown below.

### How to configure a report

The configuration of a report is managed through an interactive utility that guides users through a multi-step process.

In every step it is possible to configure a specific Tab, dedicated to a limited subset of information.

The Administrator can easily go back and forward through the sequence of steps of the wizard.

The sequence of steps of the configuration is shown in the table below:

*Table 313. Configuration steps.*

Step (tab)	Description	Always/Optional
<b>Details</b>	Shows the description of the Report (read only).	Always present
<b>Users</b>	Lets you choose which Users will be considered in the Report generation.	Optional
<b>Application</b>	Lets you choose which Application will be considered in the Report generation.	Optional
<b>Entitlements</b>	Lets you choose which Entitlements will be considered in the Report generation.	Optional
<b>Organization Units</b>	Lets you choose which Organization Units will be considered in the Report generation.	Optional
<b>Activities</b>	Lets you choose which Activities will be considered in the Report generation.	Optional

Table 313. Configuration steps. (continued)

Step (tab)	Description	Always/Optional
<b>Configurations</b>	Lets you choose which type of Account Configurations will be considered in the Report generation.	Optional
<b>Filters</b>	Lets you specify which type of Filters will be used for the Report generation.	Always present
<b>Processing Policy</b>	Lets you specify the scheduling parameters for the Report run.	Always present

## Details tab

The **Details** tab is the first tab present in all reports.

The tab includes the following data:

- **Name:** the name of the report
- **Code:** univocal identifier of the report
- **Description:** brief read-only description of the report
- **Report Category:** indication of the report classification group

## Visibility – Users tab

In this tab you can select the users that will be involved in the report.

The complete list of available users can be found in the Assignable pane (**Actions** > **Add** button).

From the list displayed in the Assignable pane, select the user (using the [Ctrl] or [Shift] keys for multiple selection) to aggregate to the report.

After the selection, click the **Ok** button and the selected items will be automatically added into the Assigned tab.

If you need to remove one or more users from the set shown in this last tab, you can be select them and click the **Actions** > **Remove** button.

When the configuration activity in this tab is finished, click the **Next** button.

## Visibility – Applications tab

In this tab you can select the applications that will be involved in the report.

The complete list of available applications can be found in the Assignable pane (**Actions** > **Add** button).

From the list displayed in the Assignable pane, select the application (using the [Ctrl] or [Shift] keys for multiple selection) to aggregate to the Report.

After the selection, click the **Ok** button and the selected items will be automatically added into the Assigned tab.

If you need to remove one or more applications from the set shown in this last tab, select them and click the button.

When the configuration activity in this tab is finished, click the **Next** button.

### **Visibility – Entitlements tab**

In this tab you can select the entitlements that will be involved in the report.

The complete list of available entitlements can be found in the Assignable pane (**Actions > Add** button).

From the list displayed in the Assignable pane, select the Entitlement (using the [Ctrl] or [Shift] keys for multiple selection) to aggregate to the Report.

After the selection, click the **Ok** button and the selected items will be automatically added into the Assigned tab.

If you need to remove one or more entitlements from the set shown in this last tab, select them and click the **Actions > Remove** button.

When the configuration activity in this Tab is finished, click on **Next** button.

### **Visibility – Organization Units tab**

In this tab you can select the organization units that will be involved in the report.

The complete list of available organization units can be found in the Assignable pane (**Actions > Add** button).

From the list displayed in the Assignable pane, select the OU (using the [Ctrl] or [Shift] keys for multiple selection) to aggregate to the Report.

After the selection, click the **Ok** button and the selected items will be automatically added into the Assigned tab.

If you need to remove one or more organization units from the set shown in this last tab, select them and click the **Actions > Remove** button.

When the configuration activity in this Tab is finished, click the **Next** button.

### **Visibility – Activities tab**

In this tab you can select the activities that will be involved in the report.

The complete list of available activities can be found in the Assignable pane (**Actions > Add** button).

From the list displayed in the Assignable pane, select the activity (using the [Ctrl] or [Shift] keys for multiple selection) to aggregate to the report.

After the selection, click the **Ok** button and the selected items will be automatically added into the Assigned tab.

If you need to remove one or more activities from the set shown in this last tab, select them and click the button.

When the configuration activity in this tab is finished, click the **Next** button.

## Visibility – Configurations tab

In this tab you can select the configurations that will be involved in the report.

The complete list of available configurations can be found in the Assignable pane (**Actions > Add** button).

From the list displayed in the Assignable pane, select the configuration (using the [Ctrl] or [Shift] keys for multiple selection) to aggregate to the report.

After the selection, click the **Ok** button and the selected items will be automatically added into the Assigned tab.

If you need to remove one or more configurations from the set shown in this last tab, select them and click the **Actions > Remove** button.

When the configuration activity in this Tab is finished, click the **Next** button.

## Filters tab

In this tab you can:

- Set the filters for the report
- Choose the output format that will be generated by selecting the related radio button.

Under the **Filters** tab you can find a **Filter** box in which to configure additional filters that can refine the result of the report.

The following output formats for the report are available:

- XLSX
- RTF
- PDF
- HTML
- DOCX
- CSV

Typically, for every report, only a subset of these six formats can be chosen.

The first format type of the list is selected by default.

## Schedule Tab

The **Schedule** tab provides the configuration of scheduling rules for the production of the report.

The available options are:

- **Frequency:** From this combobox you can set the Connector frequency start from once to 12 Hours.
- **Immediately:** Selecting this radio button the Connector starts immediately.
- **Date:** You can set the date (dd/mm/yyyy) and the hour (hh:mm) of the Connector start.

To complete the configuration of the report, click the **Execute** button. A diagnostic message will advise you that a report has been scheduled and will be processed. A complete list of scheduled reports is shown in the section Download.





---

## Chapter 22. Download

You can follow the status of a report and download it.

The following table shows a list of the possible report execution statuses:

*Table 314. Report execution Status.*

Execution Status	Description
Pending	The Report is waiting to run.
Running	The Report is running.
Download	The Report is ready to be downloaded by the user.
Error	An error occurred during the report execution.

**Note:** When the report is in Download status, you can download it as often as you want until it is deleted by the administrator.



---

## Chapter 23. IBM Security Identity Governance and Intelligence documentation

After you log in, you can access the following interfaces:

**IBM Security Identity Governance and Intelligence Chapter 1, “Administration Console,” on page 3**

Central Administration is the administration dashboard that provides control over the various management features of the IBM Security Identity Governance and Intelligence platform.

**IBM Security Identity Governance and Intelligence Service Center**

The Service Center contains the applications that are available to the user.

For complete documentation, see the IBM Security Identity Governance and Intelligence Knowledge Center at [http://www.ibm.com/support/knowledgecenter/SSGHJR\\_5.2.1](http://www.ibm.com/support/knowledgecenter/SSGHJR_5.2.1).



---

## **Part 2. Appendixes**



---

## **Appendix. Accessibility features for IBM Security Identity Governance and Intelligence**

Accessibility features assist users who have a disability, such as restricted mobility or limited vision, to use information technology content successfully.

### **Accessibility features**

IBM Security Identity Governance and Intelligence Version 5.2.1 is not tested for accessibility.

The online product documentation in IBM Knowledge Center is enabled for accessibility. The accessibility features of IBM Knowledge Center are described at [http://www.ibm.com/support/knowledgecenter/doc/kc\\_help.html#accessibility](http://www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility).

### **Related accessibility information**

In addition to standard IBM help desk and support websites, IBM has established a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:

TTY service  
800-IBM-3383 (800-426-3383)  
(within North America)

### **IBM and accessibility**

For more information about the commitment that IBM has to accessibility, see ([www.ibm.com/able](http://www.ibm.com/able)).





---

# Index

## A

- accessibility features for this product 575
- account
  - defaults, adding to target 92
  - defaults, changing 94
  - defaults, removing from target 95
- account defaults 82, 92
  - add 83
  - change 84
  - remove 85
- accounts
  - adding default values 92
- adapter profile 80
- attribute map 81

## C

- connection status of target 96

## D

- Dashboard
  - configuring dashboard items for 522
- dashboard item
  - configuring in Report Designer 522
- Dashboard item
  - list of 514
- Dashboards
  - dashboard items for 514
- default values, accounts 92

## H

- Hide Filter 152

## P

- passwords
  - changing account passwords 71
  - configure password service 72, 75
  - Configure Password Service
    - AGC 73
  - forcing a change 72
  - Process Designer 75

## R

- reconciliation
  - changing a schedule 101
  - creating a schedule 100
  - deleting a schedule 102
  - deleting reconciliation schedule 102
  - managing schedules 97
  - overview 97
  - process 98
  - reconciling accounts immediately 99
  - viewing requests 103

- removing account defaults 95

- Report Designer
  - Dashboard 522
  - Dashboard items 514
  - Dashboard tab 522

## T

- target
  - creating 88
- target account defaults 82, 92
- target definition file 80
- target type 83, 84, 85
- target type account defaults 82
- target types 79
  - import 80
  - import attribute map 81
- targets
  - changing 90
  - deleting 91
  - reconciling accounts 99, 100, 101, 102
  - status 88
  - testing connection 96
  - viewing connection status 96
  - viewing reconciliation requests 103

## U

- user virtual attributes
  - adding custom attributes 107
- UserErc
  - adding columns 107







Printed in USA